HP SiteScope

for the Windows, Solaris and Linux operating systems

Software Version: 10.10

Deployment Guide

Document Number: T8362-90003
Document Release Date: July 2009
Software Release Date: July 2009

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notices

Trademark Notices

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

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

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

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

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

Unix® is a registered trademark of The Open Group.

Documentation Updates

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

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

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

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

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

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

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

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

Support

Visit the HP Software Support web site at:

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

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

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

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

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

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

To find more information about access levels, go to:

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

Table of Contents

PART II: BEFORE INSTALLING SITESCOPE

PART III: INSTALLING SITESCOPE

PART IV: RUNNING SITESCOPE SECURELY

PART V: GETTING STARTED AND ACCESSING SITESCOPE

PART VI: APPENDIXES

Welcome to This Guide

Welcome to the HP SiteScope Deployment Guide. This guide introduces you to SiteScope, provides information on getting started, describes server installation, and details the upgrade process.

This chapter includes:

How This Guide Is Organized

This guide contains the following parts:

Part I Introduction to SiteScope

Introduces SiteScope and provides a getting started roadmap. In addition, it provides information on deployment planning, agentless monitoring, and SiteScope licensing.

Part II Before Installing SiteScope

Provides an overview of the installation, and describes the system requirements and recommended server configurations. It also describes how to upgrade existing SiteScope installations.

Part III Installing SiteScope

Describes how to install and uninstall SiteScope on Windows, Linux, and Solaris platforms. It also describes how to configure SiteScope using the Configuration Tool, and size your operating system and SiteScope and to achieve optimum performance when monitoring many instances.

Part IV Running SiteScope Securely

Describes how to configure options to harden the SiteScope platform, set user permissions and credentials required to access the monitor, and configure SiteScope to use Secure Sockets Layer (SSL).

Part V Getting Started and Accessing SiteScope

Describes how to start and stop the SiteScope service, and log in to SiteScope for the first time. It also describes the recommended administration steps you should perform following SiteScope installation.

Part VI Appendixes

Describes how to configure IIS and integrate SiteScope with SiteMinder policy-based authentication.

Who Should Read This Guide

This guide is for the following users of SiteScope:

- SiteScope administrators
- HP Business Availability Center administrators

Readers of this guide should be knowledgeable about enterprise system administration and HP Business Availability Center data collectors.

HP SiteScope Documentation

HP SiteScope documentation provides complete information on deploying, administering, and using SiteScope.

SiteScope includes the following documentation:

Release Notes (including What's New). Provides a list of new features, version limitations, and last-minute updates. In SiteScope, select **Help** > **What's New**.

Online Help. You access SiteScope Help by selecting **Help** > **SiteScope Help** in SiteScope. Context-sensitive help is available from specific SiteScope pages by clicking **Help** > **Help on this page** and from specific windows by clicking the **Help** button.

SiteScope Help includes the following online guides:

- Documentation Updates. Lists details of updates to the SiteScope Help.
- Glossary. Defines key terms used in SiteScope.
- Using SiteScope. Describes how to administer and work with SiteScope application.

Books Online/Printer-Friendly Documentation. All SiteScope documentation is available in PDF or other printer-friendly format. To access PDF files, in SiteScope select **Help** > **SiteScope Help** and select the PDFs tab.

The following Books Online guides are only available in PDF format and can also be accessed from the Main Topics tab in SiteScope Help:

- **HP SiteScope Deployment Guide.** Introduces you to SiteScope, provides information on getting started, describes server installation, and details the upgrade process and working with integrations.
- **HP SiteScope Failover Guide.** Explains how to install and work with SiteScope Failover, a special version of SiteScope that enables you to implement failover capability for infrastructure monitoring.

The **SiteScope Monitor Metrics and Measurements** document is available in Word format from the Main Topics tab in SiteScope Help. This document is a collection of information for all SiteScope monitors and their respective counters or metrics. The document lists all metrics that can be configured per monitor as well as versions of applications or operating systems that are supported. Newer versions of this document may be available from your HP Software Support representative.

Books Online can be viewed and printed using Adobe Reader 4.0 or later. Reader can be downloaded from the Adobe Web site (www.adobe.com).

Additional Online Resources

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

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

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract.

To find more information about access levels, go to:

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

To register for an HP Passport user ID, go to:

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

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

Part I

Introduction to SiteScope

1

Introduction to SiteScope

HP SiteScope is an agentless monitoring solution designed to ensure the availability and performance of distributed IT infrastructures—for example, servers, operating systems, network devices, network services, applications, and application components. This Web-based infrastructure monitoring solution is lightweight, highly customizable, and does not require that data collection agents be installed on your production systems. SiteScope also acts as a monitoring foundation for other HP offerings such as Business Availability Center, HP Software-as-a-Service, and HP LoadRunner. With SiteScope, you gain the real-time information you need to verify infrastructure operations, stay apprised of problems, and solve bottlenecks before they become critical.

SiteScope provides different tools, such as templates, the Publish Template Changes wizard, and automatic template deployment that enable you to develop a standardized set of monitor types and configurations into a single structure. SiteScope templates can be speedily deployed across the enterprise and quickly updated to make sure that the monitoring infrastructure is compliant with the standards set in the template. SiteScope also includes 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.

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 HP 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.

SiteScope was pioneered as the industry's first agentless monitoring solution. SiteScope users have benefited from its industry proven, agentless monitoring architecture. Unlike agent-based monitoring approaches SiteScope reduces total cost of ownership by:

- Gathering detailed performance data for infrastructure components.
- Eliminating the need for extra memory or CPU power on production systems to run a monitoring agent.
- Reducing the time and cost of maintenance by consolidating all monitoring components to a central server.
- Removing any requirement to take a production system offline in order to update its monitoring agent.
- Eliminating time needed to tune monitoring agents to coexist with other agents.
- Reducing installation time by eliminating the need to physically visit production servers or wait for software distribution operations.
- Reducing the possibility of an unstable agent causing system downtime on a production server.

  By starting with SiteScope and adding other HP solutions such as Business Availability Center and Service Level Management, you can create a solid infrastructure monitoring that enables you to manage your IT infrastructure and service levels from a business point of view.

2

Getting Started Roadmap

This chapter provides a basic step-by-step roadmap for getting up and running with SiteScope.

1 Register your copy of SiteScope.

Register your copy of SiteScope to gain access to technical support and information on all HP products. You are also eligible for updates and upgrades. You can register your copy of SiteScope on the HP Software Support Web site (http://www.hp.com/go/hpsoftwaresupport).

2 Read about where to get help.

Learn about the various sources of assistance, including HP Services and HP Software Support, as well as the SiteScope Help. For details, see "HP SiteScope Documentation" on page 11.

3 Plan your SiteScope deployment.

Create a complete deployment plan prior to installing SiteScope software. Use "Deployment Methodology and Planning" on page 19 to assist you. For in-depth deployment planning best practices, consult your HP representative.

4 Install SiteScope.

See "Installation Overview" on page 54 for a basic understanding of the steps involved in deploying the SiteScope application. For information on deploying SiteScope securely, see "Hardening the SiteScope Platform" on page 153.

5 Log in to SiteScope and initiate system administration.

Log into the SiteScope Web interface using a Web browser. Use the checklist in "Post-Installation Administration" on page 183 to guide you through basic platform and monitor administration tasks to prepare SiteScope for operational deployment.

6 Roll out SiteScope to business and systems users.

Once the SiteScope system is up and running with defined users and incoming monitor data, begin the process of educating business and systems users on how to access and use SiteScope monitors, reporting and alerting functionality.

For complete details on using and administering SiteScope, see the SiteScope Help.

3

Deployment Methodology and Planning

Deploying SiteScope is a process that requires resource planning, system architecture design, and a well-planned deployment strategy. This chapter outlines the methodology and considerations you need to take for successful deployment and use of SiteScope.

Note: Use the information below to assist you in your preparations before beginning the installation. For in-depth deployment planning best practices, consult your HP Professional Services representative.

This chapter includes:

An Enterprise System Monitoring Methodology

Having a consistent methodology is essential for effective system monitoring. However, it is not always obvious how to approach, develop, and deploy an enterprise monitoring solution. The solution needs to consider the role of the IT infrastructure and how it contributes to the success of the organization. System monitoring is a tool you use to ensure the availability and function of services used by the organization to meet its key objectives. You can use the following as a guide to plan your system monitoring.

- **What to monitor**

  Effective enterprise system management uses a multi-tiered monitoring approach. SiteScope gives you the tools to implement this. At one level, you want to monitor individual hardware elements in the infrastructure to see that they are running and available. You want to add to this monitoring of key services and processes on these systems. This includes low level operating system processes as well as processes indicating the health and performance of key applications. On top of this, you want to create transactional monitoring of business processes to see that key applications and services are available and function as expected.

- **What threshold level represents an event**

  The availability and performance of information systems is critical to enterprise business success. The thresholds that you set for monitors is determined by the nature of the system or business process you are monitoring.

- **How often the system should be checked**

  How often you have a system checked can be as important as the event threshold you set. The availability of mission critical information systems should be checked regularly during the periods that there are to be accessible. In many cases, systems need to be available 24 hours a day, 7 days a week. You control how often SiteScope checks a system with the Frequency setting for each monitor. Too much time between checks may delay detection of problems. Too frequent checking may load an already busy system unnecessarily.

➤ **What action to take when an event is detected**

As a monitoring application, SiteScope provides you with the tools to detect problems. You use SiteScope alerts to send timely notification when an event threshold has been triggered. An email notification is a commonly used alert action. SiteScope includes other alert types that can integrate with other systems.

You can develop an alert escalation scheme by defining multiple alert definitions with different alert trigger criteria. You use the **When** settings for alerts to customize the relation between detected events and alert actions.

Another event action may be to disable monitoring and alerting for systems that are dependent on a system that has become unavailable. SiteScope group and monitor dependency options can be used to avoid cascading series of alerts.

➤ **What automated response can be performed**

When problems are detected, an automated response to resolve the problem is ideal. While this is not possible for all systems, the SiteScope Script Alert type does provide a flexible and powerful tool for automating corrective actions for a variety of situations. You should consider what problems that may arise in your environment could be addressed with an automated response.

Business System Infrastructure Assessment

1 Gather technical and business requirements before making architectural and deployment decisions. Actions for this stage include:

- ➤ Develop a list of all business applications to be monitored. This should consider end-to-end services such as order processing, account access functions, data queries, updates and reporting.
- ➤ Develop a list of servers that support the business applications. This must include servers supporting front-end Web interfaces, back-end databases, and applications servers.
- ➤ Develop a list of network devices supporting the business applications. This includes network appliances and authentication services.
- ➤ Identify heartbeat elements to be monitored. Heartbeat elements are services that act as foundational indicators of the availability of a particular business system or resource.
- ➤ Outline templates of monitors that represents the resources to be monitored for each system.

2 Identify stakeholders and key deliverables for the business system monitoring activity. Deliverables include:

- ➤ what reports should be generated
- ➤ what alert actions should be taken when events are detected
- ➤ to whom should alerts be sent
- ➤ what users require access to view and manage SiteScope
- ➤ what SiteScope elements need to be accessible to which stakeholders
- ➤ what are the thresholds for any Service Level Agreements (if applicable)

3 Understand the constraints within which the system monitoring function must operate. This includes restrictions on the protocols that can be used, user authentication requirements, access to systems with business sensitive data, and network traffic restrictions.

SiteScope Server Sizing

The foundation of successful monitoring deployment is proper sizing of the server where SiteScope is to run. Server sizing is determined by a number of factors including:

- the number of monitor instances to be run on the SiteScope installation
- the average run frequency for the monitors
- the types of protocols and applications to be monitored
- how much monitor data need to be retained on the server for reporting

Knowing the number of servers in the environment, their respective operating systems, and the application to be monitored is the starting point for estimating the number of monitors that may be needed.

See "Sizing SiteScope on Windows Platforms" on page 132 or "Sizing SiteScope on Solaris and Linux Platforms" on page 136 for a table of server sizing recommendations based on estimations of the number of monitors to be run.

Network Location and Environment

The majority of SiteScope monitoring is performed by emulating Web or network clients that make requests of servers and applications in the network environment. For this reason, SiteScope must be able to access servers, systems, and applications throughout the network. This helps determine where SiteScope should be installed.

The methods used by SiteScope for monitoring systems, servers, and applications can be divided into two categories:

- Standards-based network protocols. This includes HTTP, HTTPS, SMTP, FTP, and SNMP.
- Platform-specific network services and commands. This includes NetBIOS, telnet, rlogin, and Secure Shell (SSH).

Infrastructure monitoring relies on platform-specific services. As an agentless solution, monitoring requires that SiteScope log in and authenticate frequently to many servers in the infrastructure. For performance and security reasons, it is best to deploy SiteScope within the same domain and as close to the system elements to monitored as possible. It is also best to have SiteScope in the same subnet as the applicable network authentication service (for example Active Directory, NIS, or LDAP). The SiteScope interface can be accessed and managed remotely as needed using HTTP or HTTPS.

Note: Try to avoid deploying SiteScope in a location where a significant amount of the monitoring activity requires communication across a Wide Area Network (WAN).

For security reasons, it is recommended not to use SiteScope to monitor servers through a firewall because of the different protocols and ports required for server availability monitoring. SiteScope licensing is not server-based and supports having separate SiteScope installations for both sides of a firewall. Two or more separate SiteScope installations can be accessed simultaneously from a single workstation using HTTP or HTTPS.

Considerations for Windows Environments

SiteScope must be installed using an account with administrator privileges. It is also recommended that the SiteScope service be run with a user account that has administrator privileges. A local system account can be used, but this affects the configuration of connection profiles to remote Windows servers.

The following are some additional considerations for using SiteScope in a Microsoft Windows network environment:

- **Remote Registry Service.** SiteScope uses the Windows performance registry on remote machines to monitor server resources and availability. To enable this monitoring capability, the Remote Registry Service for the remote machines must be activated.
- **Windows 2000 Service Pack 2.** There is a known issue with Windows 2000 Service Pack 2. The Remote Registry Service has a memory leak. This often causes SiteScope monitors for a remote Windows 2000 server with Service Pack 2 to work intermittently. The memory leak is fixed in Windows 2000 Service Pack 3. To avoid this problem, it is recommended that you install Service Pack 3 on all Windows 2000 servers that you plan to monitor with SiteScope.

Considerations for UNIX Environments

SiteScope does not need to be installed or run by the root user unless the SiteScope Web server is run on a privileged port.

The following is additional information relating to the setup of agentless monitoring of remote UNIX servers with SiteScope:

- **Remote Login Account Shells.** SiteScope as an application can run successfully under most popular UNIX shells. When SiteScope communicates with a remote UNIX server it prefers communicating with either Bourne shell (sh) or tsch shell. The relevant login account on each remote UNIX server should, therefore, have its shell set to use one of these shells.

Note: Set shell profile only for the login accounts used by SiteScope to communicate with the remote machine. Other applications and accounts on the remote machine can use their currently defined shells.

- **Account Permissions.** It may be necessary to resolve command permissions settings for monitoring remote UNIX servers. Most of the commands that SiteScope runs to get server information from a remote UNIX server are located in the **/usr/bin** directories on the remote server. Some commands, however, such as the command to get memory information, are located in **/usr/sbin**. The difference between these two locations is that **/usr/sbin** commands are usually reserved for root user or other highly privileged users.

Note: Although SiteScope does require highly privileged account permissions, for security reasons, it is recommended not to run SiteScope using the root account or to configure it to use root login accounts on remote servers.

If you have problems with permissions, you need to either have SiteScope log in as a different user that has permissions to run the command, or have the permissions changed for the user account that SiteScope is using.

4

Understanding Agentless Monitoring

This chapter introduces SiteScope's agentless monitoring concept. Agentless monitoring means that monitoring can be accomplished without the deployment of agent software onto the servers to be monitored. This makes deployment and maintenance of SiteScope relatively simple compared to other performance or operational monitoring solutions.

This chapter includes:

About SiteScope Monitoring Capabilities

SiteScope is a versatile operational monitoring solution that provides many different monitor types for monitoring systems and services at various levels. Many of the monitor types can be further customized for special environments.

Enterprises and organizations often need to deploy and maintain multiple solutions to monitor operations and availability at these different levels. Operational monitoring can be divided into several levels or layers as described in the following table:

Monitor Type	Description
Server Health	Monitors server machine resources such as CPU utilization, memory, storage space, as well as the status of key processes and services.
Web Process and Content	Monitors availability of key URLs, the function of key Web-based processes, and monitors key text content.
Application performance	Monitors performance statistics for mission critical applications such as Web servers, databases, and other application servers.
Network	Monitors connectivity and availability of services.

Understanding the Agentless Monitoring Environment

The majority of SiteScope monitoring is performed by emulating Web or network clients that make requests of servers and applications in the network environment. For this reason, SiteScope must be able to access servers, systems, and applications throughout the network.

This section contains the following topics:

➤ "SiteScope Monitoring Methods" on page 29

➤ "Firewalls and SiteScope Deployment" on page 32

SiteScope Monitoring Methods

The methods used by SiteScope for monitoring systems, servers, and applications can be divided into two categories:

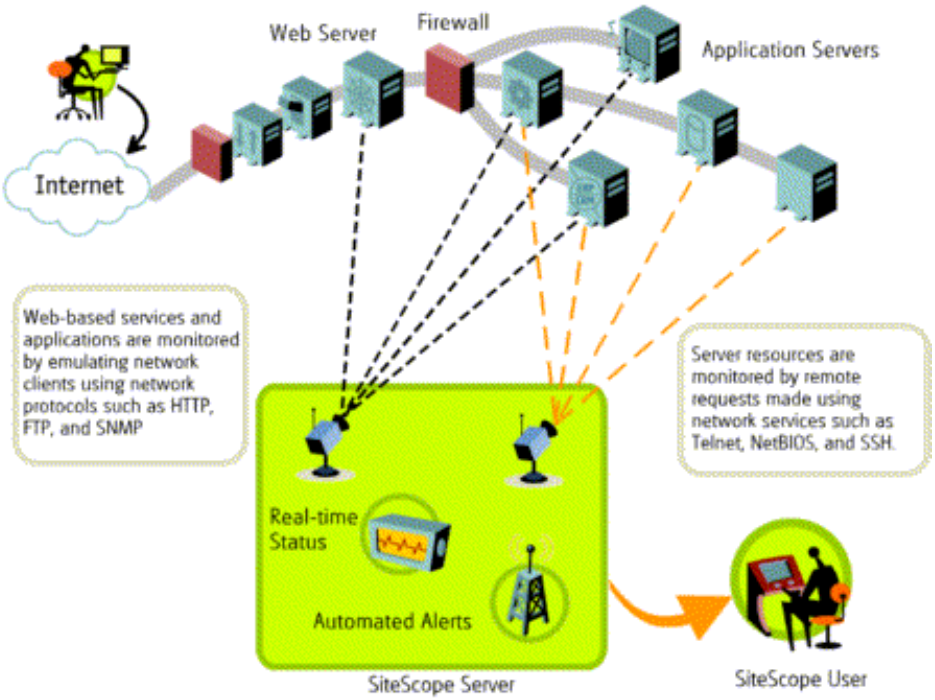
➤ **Standards-based network protocols.**

This category includes monitoring via HTTP, HTTPS, FTP, SMTP, SNMP, and UDP. These types of monitors are generally independent of the platform or operating system on which SiteScope is running. For example, SiteScope installed on Linux can monitor Web pages, file downloads, email transmission, and SNMP data on servers running Windows 2000, HP-UX, and Solaris UNIX.

➤ **Platform-specific network services and commands.**

This category includes monitor types that log in as a client to a remote machine and request information. For example, SiteScope can use Telnet or SSH to log into a remote server and request information regarding disk space, memory, or processes. On the Microsoft Windows platform, SiteScope also makes use of Windows performance counter libraries. Some limitations exist in monitoring across different operating systems for monitor types that rely on platform-specific services. For example, SiteScope for Windows includes the Microsoft Windows Performance Counter Monitor, which is not included in SiteScope for Solaris.

The following diagram shows a general overview of agentless monitoring with SiteScope. SiteScope monitors make requests of services on remote machines to gather data on performance and availability.



SiteScope Server monitors (for example, CPU, Disk Space, Memory, Service) can be used to monitor server resources on the following platforms:

- Windows NT/2000/2003 (x86 and Alpha, see note below)
- Sun Solaris (Sparc and x86)
- Linux
- AIX
- HP/UX
- Digital Unix

- SGI IRIX
- SCO
- FreeBSD

Note: An SSH connection is required to monitor server resources (for example, CPU utilization, memory) on Windows machines from a SiteScope running on UNIX. A Secure Shell client must be installed on each Windows machine that you want to monitor in this way. For more information on enabling this capability, see "SiteScope Monitoring Using Secure Shell (SSH)" in the SiteScope Help.

SiteScope includes an adapter configuration template that allows you to extend SiteScope capabilities to monitor other versions of the UNIX operating system. For more information, see "UNIX Operating System Adapters" in the SiteScope Help.

You need to enable login accounts on each server for which you want SiteScope to access system data remotely. The login account on the monitored servers must be configured to match the account under which SiteScope is installed and running. For example, if SiteScope is running under an account with the username **sitescope**, remote login accounts on servers that are to be monitored by this SiteScope installation need to have user login accounts configured for the **sitescope** user.

Firewalls and SiteScope Deployment

For security reasons, it is recommended not to use SiteScope to monitor servers through a firewall because of the different protocols and ports required for server monitoring. SiteScope licensing supports separate SiteScope installations for both sides of a firewall. Two or more SiteScope installations can be accessed from a single workstation using HTTP or HTTPS.

The following table lists the ports commonly used by SiteScope for monitoring and alerting in a typical monitoring environment:

SiteScope Function	Default Port Used
SiteScope Web server	Port 8080
FTP Monitor	Port 21
Mail Monitor	Port 25 (SMTP), 110 (POP3), 143 (IMAP)
News Monitor	Port 119
Ping Monitor	ICMP packets
SNMP Monitor	Port 161 (UDP)
URL Monitor	Port 80,443
Remote Windows Monitoring	Port 139
Email Alert	Port 25
Post Alert	Port 80,443
SNMP Trap Alert	Port 162 (UDP)
Remote UNIX ssh	Port 22
Remote UNIX Telnet	Port 23
Remote UNIX rlogin	Port 513

5

SiteScope Licenses

SiteScope licensing controls the number of monitors that can be run and, in some cases, the types of monitors that can be used. Unlike software that is sold based on the number of sites, seats, or users, SiteScope licensing is based on the monitoring requirements. This provides an efficient and flexible way to scale SiteScope to your environment.

This chapter includes:

Introducing SiteScope Licensing

Purchasing a SiteScope license and registering your copy of SiteScope gives you important rights and privileges. Registered users can access technical support and information on all HP products and are eligible for free updates and upgrades. You are also given access to the HP Software Support Web site. You can use this access to search for technical information in the HP Software Self-solve knowledge base as well as downloading updates to the SiteScope documentation.

Understanding SiteScope License Types

To use SiteScope, you must have a valid license. An evaluation license is available with each new installation or download of SiteScope. You can install SiteScope using a permanent license or the evaluation license.

Note: SiteScope requires a new general license number when upgrading from SiteScope 7.x to a SiteScope 8.x, 9.x, or 10.x version.

Contact your HP sales representative if you need to upgrade your SiteScope licensing.

There are two categories of SiteScope license:

- **General.** A license type needed to enable the SiteScope application. For details, see "General License Types" on page 34.
- **Option.** A license that enables optional monitoring capabilities and features. For details, see "Option License Types" on page 35.

Within these two categories, there are a total of four license types. The following table describes the SiteScope license types.

General License Types

This table describes general license types:

License Type	Description
Evaluation License	The default license supplied with the SiteScope download, enabling standard use of the product during the free evaluation period.
Extension License	A temporary license issued by HP which extends an evaluation period for a determined length of time.

License Type	Description
Permanent License	A standard license enabling on-going use of the product based on the number of monitor points included as part of the license.
Failover License	A special license issued by HP enabling the SiteScope instance to act as a failover for another SiteScope installation.

Option License Types

This table describes optional license types:

License Type	Description
Enterprise Application Option License	A special license issued by HP enabling a set of optional SiteScope monitors.
Solution Template Option License	A special license issued by HP to enable use of solution templates. Generally, there is a separate license for each solution template.
Enterprise Management System (EMS) Option License	A standard license issued by HP to enable use of Enterprise Management System integration monitors.
Web Script Monitor Option License	A special license issued by HP to enable use of monitoring with the Web Script monitor.

Note: Extension licenses can be issued for either Evaluation or Option licenses.

Each individual installation of SiteScope requires a unique monitor license. At present, there is no license server functionality in SiteScope to share a single license across multiple SiteScope installations.

The table below summarizes the differences between the Evaluation and Permanent licenses versus the Option license.

Topic	Permanent and Evaluation Licenses	Option License
General description	Enable the standard functionality of the SiteScope product.	Each license enables specific optional monitor types.
Number of installations per license key	Each installation of SiteScope requires a distinct permanent or evaluation license key.	Each installation of SiteScope requires a distinct option license to enable the optional functionality for that SiteScope server.
Monitor points	The license key includes a preset number of monitor points. The monitor points determine how many monitor instances can be created and how many metrics can be measured on an individual SiteScope server.	The option license key enables optional monitor types for the SiteScope installation on which it is used. The option license key does not increase the total number of monitor points governed by the permanent license key.
Other issues		The monitor points used for creation of optional monitor types are deducted from total monitor points included in the permanent license key.
Entering license key	Permanent license keys can be entered from the start up screen when SiteScope is run for the first time after installation or using the General Preferences page at any time within an evaluation period.	Option license keys can be entered using entry fields on the start up screen when SiteScope is started for the first time after installation or using the General Preferences page.

It is not mandatory to enter a license key to use SiteScope within the free evaluation period.

Understanding Monitor Licensing

Licensing for SiteScope is based on a point system that offers flexibility in scaling and deployment. A permanent SiteScope license provides a number of points that you use to activate a combination of monitor types.

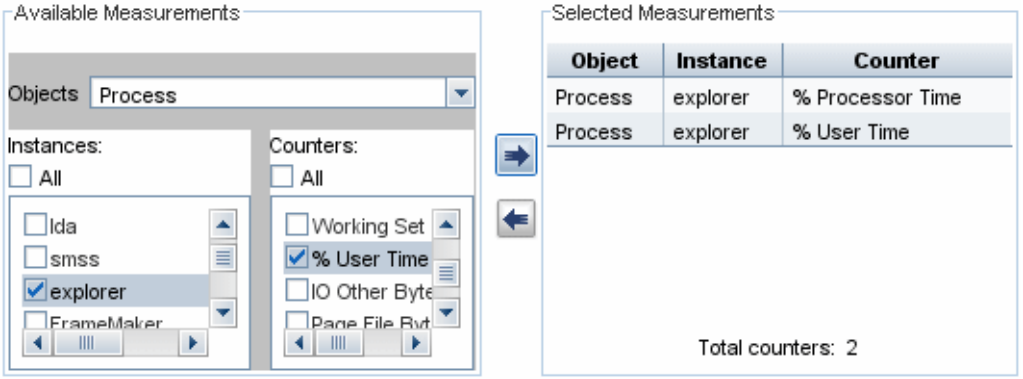
Note: SiteScope does not have user-based access licensing. There is no limit to the number of users that can access the SiteScope application server.

The number of SiteScope monitors that you can create is based on two factors:

- total number of monitor points you have purchased
- types of SiteScope monitors you want to use

The monitor types are divided into three categories based on how many points you need to activate them. For example, to set up one URL Monitor for a Web page, you need one monitor point per monitor instance. To set up an Apache Server Monitor, you need one monitor point for each server performance metric you want to monitor.

To set up a Microsoft Windows Resources Monitor or UNIX Resources Monitor, you need one monitor point per monitor instance. When you set up these monitors, you first select an object, then the relevant instances for the object, and then the relevant counters for each instance. In the following example for a Microsoft Windows Resources Monitor, the object selected is Process, the instance selected is explorer, and the counters selected are % Processor Time and % User Time. This costs one point for the explorer instance. If you selected another instance to monitor, it would cost two points, and so forth.



The following sections list the point usage for each instance of the various SiteScope monitor types:

- "System Monitors" on page 39
- "Application Monitors" on page 40
- "Web/URL Monitors" on page 41
- "Web Script Monitor" on page 41
- "Network Service Monitors" on page 42
- "Container Monitor Types" on page 42
- "Enterprise Application Monitors" on page 43
- "Solution Templates" on page 43

System Monitors

You use System monitors to verify the availability of infrastructure resources. The following monitor types are licensed at one point per monitor instance:

- Composite
- CPU
- Database
- DHCP
- Directory
- Disk Space
- File
- LDAP
- Log File
- Memory
- Microsoft Windows Dialup
- Microsoft Windows Event Log
- Microsoft Windows Resources
- News
- NonStop Event Log
- NonStop Resources (one point per object instance)
- Radius
- Script
- Service
- UNIX Resources (one point per object instance)

Application Monitors

You use Application monitors to check the availability and performance parameters of specific infrastructure applications. These monitor types allow you to monitor up to ten performance metrics per monitor instance and are licensed as one point per metric or measurement:

- Apache Web Server
- BroadVision Application Server
- CheckPoint FireWall-1
- Cisco Works
- Citrix MetaFrame
- ColdFusion Server
- DB2
- F5 Big-IP
- MAPI
- Microsoft Windows Performance Counter (Microsoft Windows platforms)
- Oracle 9i/10g Application Server
- Oracle JDBC
- Real Media Player and Server
- SunONE Server
- Sybase Database
- Tuxedo
- WebLogic Application Server
- WebSphere Application Server

Web/URL Monitors

You use URL monitor types to check the availability and content of Web pages. The following monitor types are licensed at one point per instance or per step, in the case of multiple step transactions:

- e-Business Transaction
- Link Check
- URL
- URL Content
- URL List (one point per URL)
- URL Sequence (one point per step)
- Web Server
- Web Service

Web Script Monitor

You use the Web Script monitor to monitor transactions between virtual end-users and target Web sites. The following monitor type is licensed at four points per transaction run by the monitor. A transaction can include as many URLs as needed. The monitor can include up to 12 measurements per transaction.

- Web Script Monitor

Network Service Monitors

You use Network Service monitors to verify the availability of a variety of services that may exist in the infrastructure. These monitor types are licensed as one point per instance:

- DNS
- Formula (Bandwidth) Composite
- FTP
- Mail
- Network Bandwidth (one point per interface)
- Ping
- Port
- SNMP
- SNMP by MIB
- SNMP Trap

Container Monitor Types

The sequence checking and compound monitoring functions provided by the Composite and e-Business Transaction monitors continue to be available. These monitor types are used to group member monitors, which are counted at the applicable monitor point rate. These monitors can be set up at no additional cost in monitor points beyond that of the member monitors which they contain.

Enterprise Application Monitors

These optional monitors are licensed per application type. You purchase an option license based on which of the following applications you want to be able to monitor:

- COM+
- SAP CCMS
- Siebel
- WebSphere MQ Status

Solution Templates

Solution templates are optimized monitor templates that include both optional and standard monitor types. Access to the template and the template-specific monitor types requires an option license. Purchase of the option license also includes access to Best Practices documentation for the specific solution.

License points usage is based on the solution template cost. The solution template cost is based on the number of points consumed by the monitors deployed by the template (each monitor has its own point consumption).

The table below displays the license points cost for solution templates that were configured on HP test environments. Note that license points consumption varies from one environment to another, depending on the size of the environment being monitored and the number of counters selected.

Solution Template	Typical License Point Usage
Active Directory with Global Catalog	34
Active Directory with no Global Catalog	33
AIX Host	13
ASP.NET	20
ASP.NET Applications	1

Solution Template	Typical License Point Usage
HP Quality Center Application Server for UNIX	11
HP Quality Center Application Server for Windows	11
HP Quality Center 10.0 License Status	12
HP Quality Center 9.2 License Status	6
HP QuickTest Professional License Server	3
HP Service Manager for UNIX	48
HP Service Manager for Windows	12
JBoss Application Server 4.x	3
Linux Host	13
Microsoft Exchange 2000	40
Microsoft Exchange 2003	49
Microsoft Exchange 2007	83
Microsoft Exchange 5.5	39
Microsoft IIS 6	98
Microsoft SQL Server 2005	18
Microsoft Windows Host	13
.NET CLR Data	1
Oracle Database 9i and 10g	202
SAP NetWeaver Application Server	13
SAP R/3 Application Server	13
Siebel Application Server 6.x-7.x for UNIX	93
Siebel Application Server 6.x-7.x for Windows	91
Siebel Application Server 8.x for UNIX	98
Siebel Application Server 8.x for Windows	101
Siebel Gateway Server for UNIX	6

Solution Template	Typical License Point Usage
Siebel Gateway Server for Windows	6
Siebel Web Server for UNIX	19
Siebel Web Server for Windows	19
Solaris Host	13
WebLogic 6.x, 7.x, 8.x Application Server	51
WebLogic 9.x-10.x Application Server	63
WebSphere 5.x Application Server	20
WebSphere 6.x Application Server	24

Estimating the Number of License Points

The number of license points that you purchase depends on how you plan to deploy SiteScope and what level of systems and services you want to monitor. The following are some guidelines for estimating the number of license points you need.

This section includes the following topics:

Server Health Monitoring

The number of points for Server Health Monitoring is based primarily on the number of server machines you want to monitor. Each server to be monitored requires one point for each of the following:

- CPU monitoring
- each hard disk or key disk partition
- memory
- each key server process or service
- each key file, log, or directory

Web Process and Content Monitoring

The number of points for Web Process and Content Monitoring is based on the number of Web-based processes and pages you want to monitor. Web-based processes include any sequence of Web pages. For example, logging into a secure server to verify account balances and then logging out. In many cases, the sequences of URLs includes the same path with different destination pages. In the case of online services, it may also be necessary to check back-end databases to confirm that data modified via the Web interface is being updated correctly. Other processes may include downloading files, and sending and receiving automated email messages.

- For monitoring each Web-based URL sequence, you need one sequence monitor instance for each Web-based process to be monitored, with one point for each URL or step in the sequence.
- For monitoring other Internet pages or processes, you need one point for each file download, email verification, or individual Web page content to be monitored.

Application Performance Monitoring

Monitoring application performance is an important tool in assuring the availability of network-based services and detecting performance problems. Because of the complexity of many applications and systems, it is also the most difficult in terms of estimating the number of monitor points needed. SiteScope's flexible licensing model makes it easy to modify your monitoring capacity to fit your needs.

The number of points for Application Performance Monitoring is based on:

- the number of applications deployed
- the types of applications
- the number of performance metrics that are to be monitored

The performance metrics for some applications, such as some Web servers, may be available with a single monitor instance and with a metric count of less than 10 metric points. For example, an Apache Web server presents its performance metrics on a single URL that includes the total number of accesses, the server uptime, and requests per second. Other applications and systems may involve multiple server addresses, modules, and metrics that require multiple monitor instances. Some applications may also be integrated with a database application to be monitored.

The following are guidelines for estimating points for application monitoring depending on how the data is accessed:

- one application monitor instance for each application, with one point for each performance metric to be monitored
- one monitor instance for each application status URL, with one point for each performance metric to be monitored

Network Monitoring

Network monitoring includes checking both connectivity and the availability of network services that allow users to access and use the network. This includes monitoring services like DNS, DHCP, LDAP, and RADIUS. Depending on your network hardware and configuration, you may also be able to access network performance statistics by querying network infrastructure via SNMP using the SiteScope SNMP monitor type.

The following are guidelines for estimating the number of points for network monitoring:

- one point for each key network destination
- one point for each key network service (for example, DNS or LDAP)
- one point for each metric to be monitored over SNMP

Purchasing Monitor Points

SiteScope Monitor points are sold in sets of 50, 100, 500, and 2000 point blocks to provide flexibility in deployment of monitors. For example, a block of 100 points enables you to set up various monitoring options:

- 10 application monitors to watch five performance metrics each (10 x 5 = 50 points)
- a combination of two URL sequence monitors that traverse 10 transaction steps each (2 x 10 = 20 points)
- 30 1-point network service or server monitors (30 x 1 = 30 points)

You could also use the same block of 100 points to set up:

- 10 application monitors watching one metric each (10 x 1 = 10 points)
- one URL Sequence monitor with five steps (5 points)
- 85 Network Service or Server monitors (85 points)

When you install SiteScope, it includes a free evaluation license. To use SiteScope beyond the evaluation period, you must request and activate a permanent license key for your copy of SiteScope. For more information on purchasing monitor points, please contact an HP sales representative.

Modifying SiteScope License Information

After you install SiteScope, you can modify or add to your licensing at any time. You can request a license from HP SiteScope sales staff by telephone or email. For information on how to contact a sales representative, visit the HP Web site at: http://www.hp.com/go/software.

When you receive your license key from HP, enter it into SiteScope using the browser interface.

To enter or modify license information in SiteScope:

1. From a Web browser, open the SiteScope instance you want to modify. The SiteScope service or process must be running.
2. In the left panel, click the **Preferences** context menu to open the preferences menu, and click **General Settings**. The General Settings properties are displayed in the content area on the right side of the screen.
3. Enter or modify the license key number in the **License number** box. If you have received an option license, click the **Add**  button and enter the license information in the Option Licenses dialog box. Enter multiple option licenses in the box by separating them with a comma (,).
4. Click **Save** to save the changes. The General Settings properties are displayed with the updated information. Any optional licensing enabled is displayed in the **Monitor licenses** box.

Part II

Before Installing SiteScope

6

Before You Install SiteScope

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 includes:

Installation Overview

The following is an overview of the steps involved in deploying the SiteScope application.

1 **Prepare a server where the SiteScope application is to be installed and run.**

Note: If upgrading from an earlier version of SiteScope, check the current configuration for end of life monitors and make a backup copy of key SiteScope data. For more information, see "Upgrading SiteScope" on page 63.

---

2 **Obtain the SiteScope installation executable.**

3 **Create a directory where the application is installed and set user permissions as necessary.**

Note: You must create a new directory for installation of SiteScope 10.10. Do not install version 10.10 into a directory used for a previous version of SiteScope.

---

4 **Run the SiteScope installation executable or installation script, directing the script to install the application into the location you have prepared.**

For more information, see "Installing SiteScope for Windows" on page 75 and "Installing SiteScope on Solaris or Linux" on page 103.

5 **Restart the server if necessary (Windows installations only).**

6 **Confirm that SiteScope is running by connecting to it using a compatible Web browser.**

For more information, see "Getting Started with SiteScope" on page 187.

7 **Perform post-installation steps to prepare SiteScope for production use.**

For more information, see "Post-Installation Administration" on page 183.

System Requirements

This section describes the minimum system requirements and recommendations for running SiteScope on the various supported operating systems.

Note:

- Before beginning the installation, review the information in the HP SiteScope Release Notes file for any last minute notes and limitations regarding the installation process.
- SiteScope can be installed as a 32-Bit application over 64-Bit environments of the supported Windows and UNIX operating systems.

This section includes the following topics:

System Requirements for Windows

Use these system requirements when installing SiteScope on Windows platforms:

Computer/Processor	800 MHZ or higher
Operating System	➤ Microsoft Windows 2000 Server/Advanced Server SP4 ➤ Microsoft Windows 2003 Standard/Enterprise SP1, SP2, ➤ Microsoft Windows Server 2003 Enterprise R2 SP1, SP2
Memory	1 GB minimum (2 GB or more is recommended)
Free Hard Disk Space	2 GB or more (10 GB or more is recommended)
Web Browser	Microsoft Internet Explorer 6.0 (SP1 or later) and 7.0; Firefox 2.0, 3.0
Java Plug-in (to view applets)	**Recommended**: 6u11 and later

System Requirements for Solaris

Use these system requirements when installing SiteScope on Solaris platforms:

Computer/Processor	Sun 400 MHz UltraSparc II Processor or higher
Operating System	Sun Solaris 9 or 10 (with latest recommended patch cluster)
Memory	1 GB minimum (2 GB or more is recommended)
Free Hard Disk Space	2 GB or more (10 GB or more is recommended)
Web Browser	Firefox 2.0, 3.0
Java Plug-in (to view applets)	**Recommended**: 6u11 and later

---

Note: To view SiteScope Management Reports on Solaris platforms, an X Window system must be running on the SiteScope server.

System Requirements for RedHat Linux

Use these system requirements when installing SiteScope on RedHat Linux platforms:

Computer/Processor	800 MHZ or higher
Operating System	RedHat ES/AS Linux 3, 4, 4.3, 5.2 **Note:** RedHat Linux 9 with Native POSIX Threading Library (NPTL) is not supported after this version of SiteScope.
Memory	1 GB minimum (2 GB or more is recommended)
Free Hard Disk Space	2 GB or more (10 GB or more is recommended)
Web Browser	Firefox 2.0, 3.0
Java Plug-in (to view applets)	**Recommended**: 6u11 and later

System Requirements for VMware

The following VMware environments are supported in SiteScope according to the configurations tested below:

Supported and Tested Environments	➤ VMware ESX 3.0 ➤ VMware VirtualCenter 3.0
Supported Environments Only	➤ VMware VirtualCenter 2.x ➤ VMware ESX 3.x ➤ VMware ESX 2.5 via VirtualCenter 2.x ➤ VMware ESX 3.x via VirtualCenter 3.x
VMware Configuration Tested	➤ 2 VMware Virtual Machines (VM) on one physical server ➤ Each VM with 2 CPUs at 2Ghz, 2 GB memory, and 10 GB disk space ➤ No other VMs resident on this physical server ➤ VMTools installed
SiteScope Configuration Tested	➤ 1 SiteScope on each VM (No other application resident on the VMs) ➤ Each VM with the same version of SiteScope ➤ 6500 total monitors with no more than 650 monitor runs per minute on each VM.

Use these minimum system requirements when installing SiteScope on VMware environments:

Computer/Processor	4 Intel Xeon physical processors, 2 GHz each
Operating System	Microsoft Windows 2003 Standard/Enterprise SP1
Memory (RAM)	4 GB
Free Hard Disk Space	20 GB (Hard Disk speed: 7200 rpm)
Network Card	1 physical gigabit Network Interface Card
Other Software	VMTools must be installed
Java Plug-in (to view applets)	**Recommended**: 6u11 and later

Note: Monitor capacity and velocity can be significantly impacted by numerous factors including, but not limited to the following: SiteScope server hardware, operating system, patches, third-party software, network configuration and architecture, location of the SiteScope server in relation to the servers being monitored, monitor types and distribution by type, monitor frequency, monitor execution time, Business Availability Center integration, and Database Logging. The published maximums should not be assumed to be possible in every environment.

Support for Monitoring 64-Bit Environments

SiteScope supports monitoring on the following 64-bit environments:

Operating System	➤ Windows 2003 Server 64-Bit ➤ Windows 2008 Server 64-Bit ➤ Solaris 64-Bit ➤ HP-UX 64-Bit ➤ Linux 64-Bit

Certified Configuration

The following configuration has been certified in a high load environment for an installation of SiteScope that was integrated with HP Business Availability Center.

Operating System	Microsoft Windows Server 2003, Enterprise Edition Version: 5.2.3790 Service Pack 2 Build 3790
System Model	ProLiant DL360 G4
System Type	X86-based PC
CPU	Intel Xeon, 3000 MHz (15 x 200)
Total Physical Memory	8,189.68 MB
Java Heap Memory	1024 MB
Total Number of Monitors	16000
Total Number of Remote Servers	1250
Monitor Runs per Minute	2000

Note:

- Negative Topaz ID errors in the log should be ignored.
- When working under high load, you should suspend all monitors before connecting to HP Business Availability Center for the first time.

SiteScope Capacity Limitations

When SiteScope is integrated with HP Business Availability Center, performing various very high load operations might cause problems in SiteScope. Use the following guidelines:

- Do not run the Publish Template Changes Wizard for over 3,000 monitors at once.
- Do not run the Monitor Deployment Wizard to create over 3,000 monitors at once.
- Do not copy/paste over 3,000 monitors in a single action.
- Do not perform a Global Search and Replace to modify Business Availability Center integration properties for over 2,500 monitors at one time.

SiteScope includes a tool that helps you predict system behavior and perform capacity planning for SiteScope. For details, see "SiteScope Capacity Calculator" on page 130.

7

Upgrading SiteScope

This chapter describes how to upgrade existing HP SiteScope installations to HP SiteScope 10.10 with the minimum possible interruption to your system and operations.

This chapter includes:

Before Performing the Upgrade

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 your monitoring environment.

Before upgrading SiteScope, you should consider the following:

- Before beginning the upgrade, review the information in the SiteScope Release Notes file for any last minute notes and limitations regarding the upgrade process. Failure to follow procedures listed in the Release Notes could result in unexpected data loss or failure of the upgrade process.
- You can upgrade SiteScope versions 9.0 and later directly to SiteScope 10.10. For versions of SiteScope earlier than 9.0, you must first upgrade to SiteScope 9.0.
- If your SiteScope configuration contains a group with more than 100 large subgroups, a memory overflow may occur during upgrade to SiteScope 10.10. Before you upgrade, you should split the problematic level of subgroups to contain less than 100 subgroups.
- The HTTP method for connecting to a UNIX remote server is no longer supported in SiteScope 10.10. If during an upgrade, SiteScope finds a UNIX remote server that uses the HTTP method, the upgrade process fails. To avoid this, change the method property in the version to be upgraded to one of the other valid options (ssh, telnet, or rlogin). For a list of affected UNIX remote servers, see the **<SiteScope root directory>\logs\upgrade.log** file.

Upgrading an Existing SiteScope Installation

It is recommended that you perform the following steps for upgrading:

1 **Run the End of Life Monitor Viewer to ensure that end of life monitors do not exist in the current deployment.**

You must perform this step before installing a new version of SiteScope. For more information, see "Using the End of Life Monitor Viewer" on page 66.

2 **Make a backup copy of key SiteScope data using the Configuration Tool.**

You must perform this step before installing a new version of SiteScope. For more information, see "Backing Up SiteScope Configuration Data" on page 69.

3 **Install newer versions of SiteScope in a clean directory structure.**

For information on naming the directory, see "Naming the SiteScope Directory" on page 70.

For information on installing SiteScope, see "Installing SiteScope for Windows" on page 75 and "Installing SiteScope on Solaris or Linux" on page 103.

4 **After installation, import monitor configuration data from earlier versions of SiteScope using the Configuration Tool.**

For more information, see "Importing Configuration Data" on page 70.

5 **After importing data from earlier versions of SiteScope, start SiteScope by by running the batch file/start command shell script**.

To avoid SiteScope restarting itself after an upgrade if it takes longer than 15 minutes for the monitors to run, start SiteScope by running the **go.bat** file from the **<SiteScope root directory>\bin** directory (on Windows platforms), or by running the start-monitor command shell script from <installpath>/**SiteScope/bin/** (on UNIX platforms).

Using the End of Life Monitor Viewer

The End of Life Monitor Viewer is an external tool that you can run on SiteScope configurations on any platform before an upgrade to check if the current configuration has any end of life monitors. Using the End of Life Monitor Viewer, you can prepare the SiteScope configuration for upgrade as follows:

- View details of end of life monitors (including template monitors). You can see monitor properties, monitor paths, and the recommended alternative monitor for the monitor type.
- Export this list of monitors with their properties to a .txt file.

Note: You cannot add, edit, or delete end of life monitors using the End Of Life Monitor Viewer.

Running the End of Life Monitor Viewer

Run the End of Life Monitor Viewer on the SiteScope configuration to ensure that end of life monitors do not exist in the current deployment.

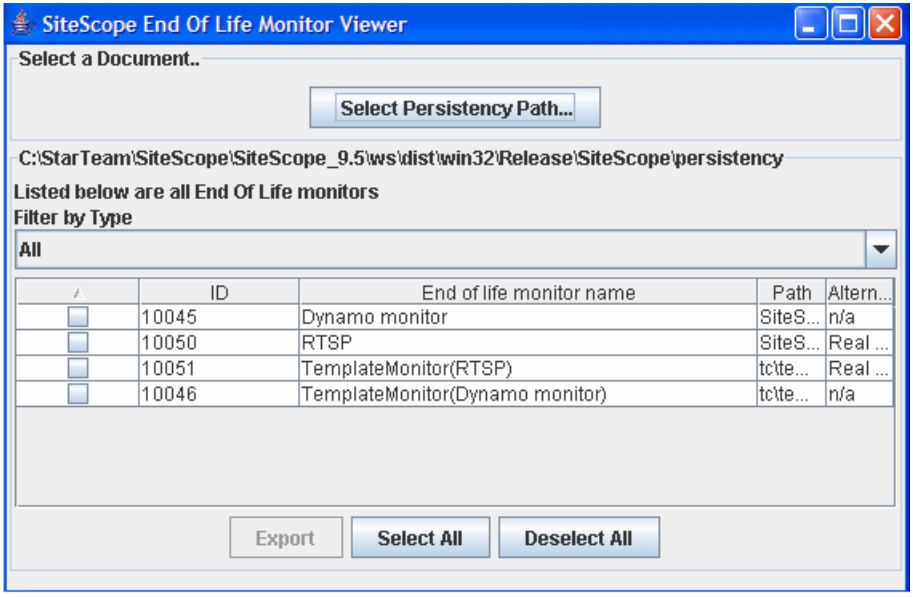
To run the End of Life Monitor Viewer:

1. Insert the installation media containing the SiteScope 10.10 software into the drive on the SiteScope machine you want to upgrade.
2. In the **\EndOfLifeMonitorViewer\<platform>** folder, extract the contents of the **upgrade.tools.zip** file to the <**SiteScope root directory**>.
3. From the <**SiteScope root directory**>**\upgrade** folder, run **EndOfLifeMonitorsViewer.bat** on Windows platforms, or **EndOfLifeMonitorsViewer.sh** file on UNIX platforms. The End of Life Monitor Viewer opens.
4. Click the **Select Persistency Path** button. The Open dialog box opens.
5. Enter the path to the persistency folder and click **Open**.

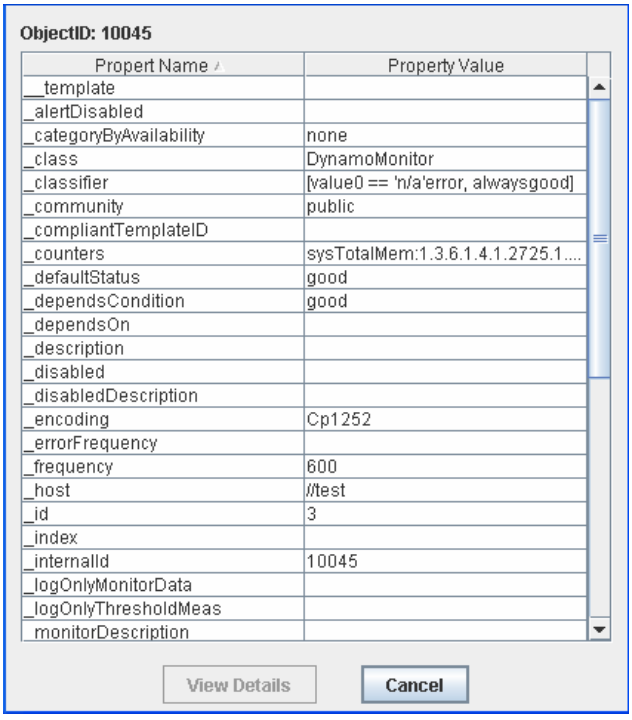
6 The End of Life Monitor Viewer checks the SiteScope configuration for end of life monitors, and displays the results.

If the configuration has end of life monitors, the following properties are displayed:

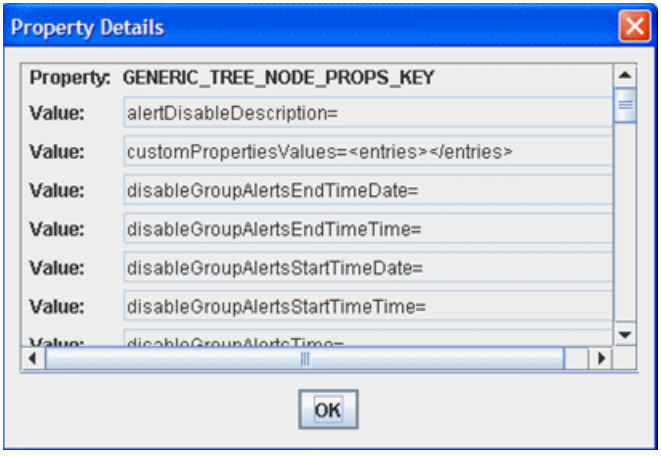
- Monitor ID
- End of life monitor name
- Full Path of the monitor
- Alternative monitor (if one exists)



Double-click a monitor row to display monitor details.



To view property details, select a property and click the **View Details** button.



7 To export information about the end of life monitors, select the monitors that you want to include in the .txt file and click **Export**. Enter the file name and location to which you want to save the file, and click **Save**. The selected monitors with their properties are saved in .txt format.

8 In the current SiteScope user interface, replace any end of life monitors with the recommended alternative monitors, and delete the end of life monitors.

For the lists of end of life and replacement monitors, see "List of Deprecated SiteScope Monitors" and "List of Deprecated Integration Monitors" in the SiteScope Help.

Backing Up SiteScope Configuration Data

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

Using the Configuration Tool, you can export SiteScope data such as templates, logs, monitor configuration files, and so forth from your current SiteScope for later import into SiteScope. The user data is exported to a ZIP file.

Note: You should make a backup of the **<SiteScope>\htdocs** directory and copy it to the SiteScope 10.10 directory after an upgrade so that you can see old reports, since this directory is not copied when you export SiteScope data.

For details on exporting SiteScope data using the Configuration Tool, see "Exporting User Data" on page 96 (for Windows) or "Exporting User Data" on page 124 (for Solaris or Linux).

Alternatively, you can have SiteScope export SiteScope data as part of the installation process. For details, see "Performing a Full Installation" on page 77 (for Windows) or "Performing a Full Installation" on page 106 (for Solaris or Linux).

Naming the SiteScope Directory

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:\10.10\SiteScope.

Importing Configuration Data

After upgrading SiteScope, monitor configuration data can be copied into SiteScope 10.10 from earlier versions of SiteScope using the Configuration Tool. For details, see "Importing User Data" on page 100 (for Windows) or "Importing User Data" on page 126 (for Solaris or Linux).

Troubleshooting and Limitations

This section describes troubleshooting and limitations for SiteScope upgrades.

This section includes:

Note: You can also check for other information relating to upgrading SiteScope in the HP Software Self-solve knowledge base (http://h20230.www2.hp.com/selfsolve/documents). To enter the knowledge base, you must log in with your HP Passport ID.

First SiteScope Restart After Upgrade Can Take a Long Time

Problem: The first SiteScope restart after an upgrade might take a long time (more than 15 minutes). If the monitors have not started to run after 15 minutes, SiteScope restarts itself.

Possible Solution:

- To avoid SiteScope restarting itself if it takes longer than 15 minutes for the monitors to run, start SiteScope by running the **go.bat** file from the **<SiteScope root directory>\bin** directory (on Windows platforms), or by running the start-monitor command shell script from <installpath>/**SiteScope/bin/** (on UNIX platforms).
- Disable any monitors that are targeting environments that are not running. This saves time waiting for the system to reply.

SiteScope Fails to Get the Customer ID

Problem: In versions of SiteScope earlier than 9.0, when SiteScope is connected to Business Availability Center, SiteScope stores the customer ID in a settings file under **<SiteScope root directory>\cache\persistent\TopazConfiguration**.

When loading SiteScope for the first time after upgrading to 9.x, SiteScope attempts to read the settings file and retrieve the HP Business Availability Center connection details. If this file is corrupt (this could be caused by in correctly performing the export configuration), SiteScope might not be able to get the customer ID and tries to retrieve it from HP Business Availability Center. If Business Availability Center is down during the restart, SiteScope is unable to retrieve the customer ID, and SiteScope restarts itself again.

Possible Solution: Make sure that any HP Business Availability Center that is connected to SiteScope is up and running before starting SiteScope after an upgrade.

Default Alert Action is Named According to Action Type

Problem: Alert actions were added to SiteScope 9.0. When upgrading to any version of SiteScope 9.0 or later, a default alert action is created that is named according to the action type (for example, Email, Pager, or SMS). This might be a problem if you want the default name to be concatenated with the alert holding the action.

Possible Solution: Before upgrading, open the **master.config** file located in **<SiteScope root directory>\groups** and change the **_AlertActionCompositeNameDelimiter** key to contain the delimiter you want to have in the concatenation.

Business Availability Center/ServiceCenter or Service Manager Integration

This note is relevant if you are upgrading SiteScope from a pre-10.00 version and are working with the Business Availability Center/ServiceCenter or Service Manager integration. When setting up the ServiceCenter monitor in SiteScope, a file called **peregrine.jar** is created and placed in the **WEB-INF\lib** directory on the SiteScope machine. This file must be backed up before upgrading SiteScope or it will be deleted during the upgrade. After the upgrade is complete, copy the backed up **peregrine.jar** file back to the **WEB-INF\lib** directory.

SiteScope Fails to Upgrade

If the upgrade process fails, check the **upgrade.log** file located in the **<SiteScope root directory>\logs** directory for reasons for the upgrade failure.

If the upgrade process fails when installing SiteScope on a Windows environment, SiteScope keeps trying to perform a restart.

Possible Solution: Perform the SiteScope installation again.

Part III

Installing SiteScope

8

Installing SiteScope for Windows

SiteScope for Windows is available as a single, self-extracting executable file that can be downloaded from the HP Web site and is also available on DVD. SiteScope is installed on a single server and run as a single application on the Windows platform.

This chapter includes:

Installation – Workflow

SiteScope version 10.10 installation follows a different procedure for first-time installation than for users with an earlier version of SiteScope already installed.

This section includes the following topics:

New Users

Users who do not have SiteScope installed must follow this procedure:

1 Install SiteScope 10.10.

For details, see "Performing a Full Installation" on page 77.

2 Connect to SiteScope.

For details, see "Connecting to SiteScope" on page 190.

Users with an Earlier SiteScope Version Installed

SiteScope version 10.10 does not automatically upgrade from a previous version of SiteScope. Users must follow this procedure:

1 Install SiteScope 10.10

You can install SiteScope version 10.10 on the same machine as your current SiteScope or on a different machine. If you install SiteScope on the same machine, you must install it in a different directory. For installation details, see "Performing a Full Installation" on page 77.

As part of the installation process, you can export data from your current SiteScope for later import into SiteScope version 10.10. Alternatively, you can export data from your current SiteScope independently using the Configuration Tool. For details, see "Exporting User Data" on page 96.

2 (Optional) Import SiteScope data from the previous version into SiteScope 10.10.

If you exported SiteScope data during the installation process, you can import the data using the Configuration Tool. For details, see "Importing User Data" on page 100.

3 Copy monitor configurations from the previous version into SiteScope 10.10.

If you have created or modified monitor configuration files in the previous SiteScope version, you may need to copy them to the 10.10 directory. You also need to check that your monitor configuration files point to the 10.10 directory. For details, see "Exporting User Data" on page 96.

Note: If you have third-party middleware and drivers, you must copy them manually.

---

4 Connect to SiteScope.

For details, see "Connecting to SiteScope" on page 190.

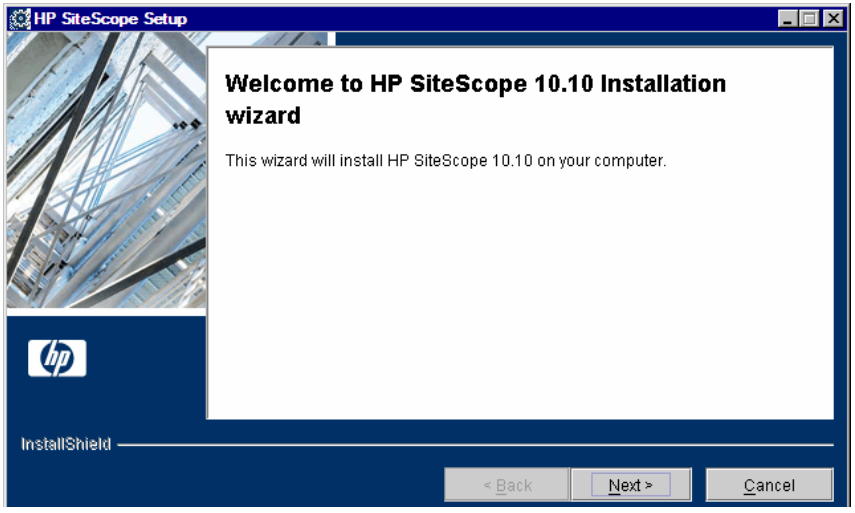
Performing a Full Installation

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

To install SiteScope:

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

2 Run the SiteScope **setup.exe** program. The InstallShield Wizard opens.

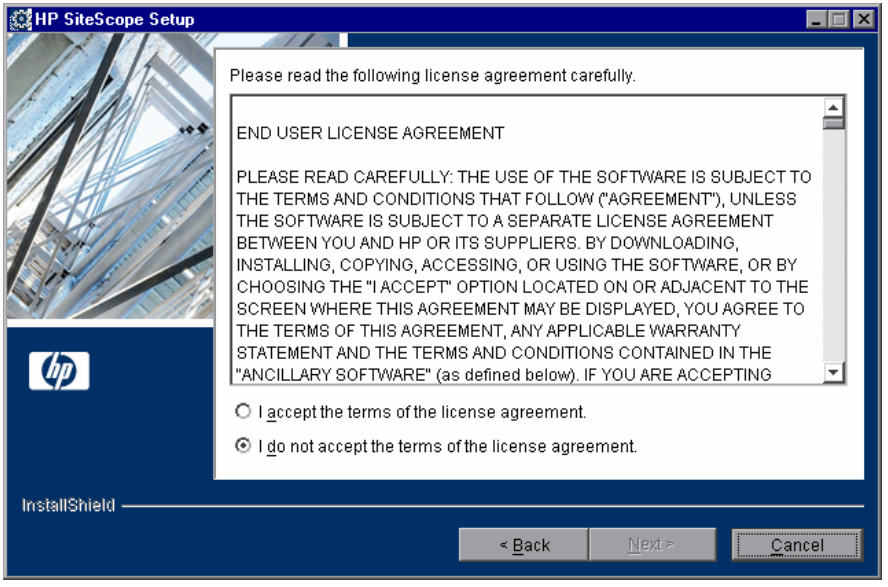


Click **Next** to begin the installation.

Note:

- If your server needs to be restarted because of other system work, the InstallShield Wizard tells you to restart your machine and then exits the installation.
- If your server has Microsoft Terminal Server service running, the service must be in **Install Mode** when you install SiteScope. If the service is not in the correct mode, the InstallShield Wizard gives you an error message and then exits the installation.

3 The license agreement screen opens.



Read the SiteScope License Agreement.

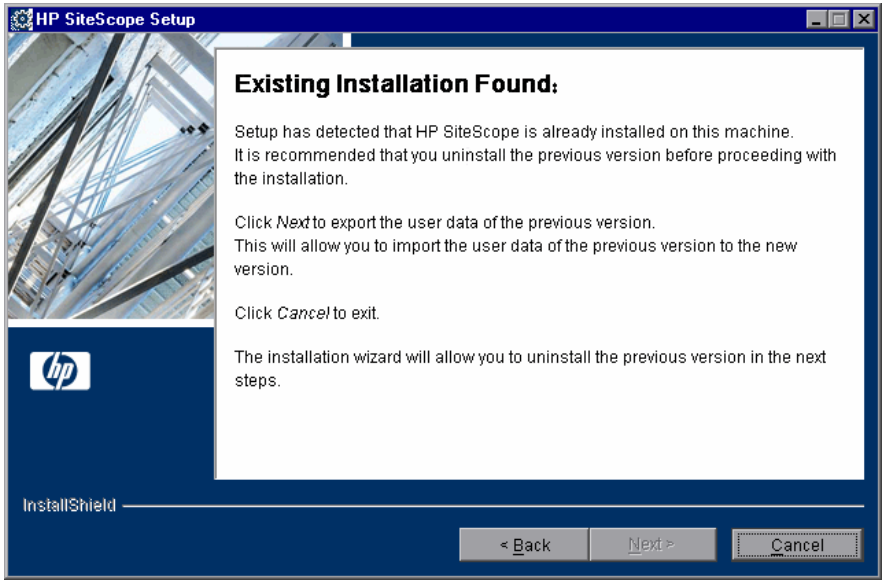
To install SiteScope, you must accept the terms of the license agreement by clicking **I accept** and then click **Next** to continue.

Note: If the installation process detects a previous version of SiteScope, you must uninstall the existing SiteScope version before you can install the latest version. For details on uninstalling SiteScope, see "Uninstalling SiteScope" on page 143.

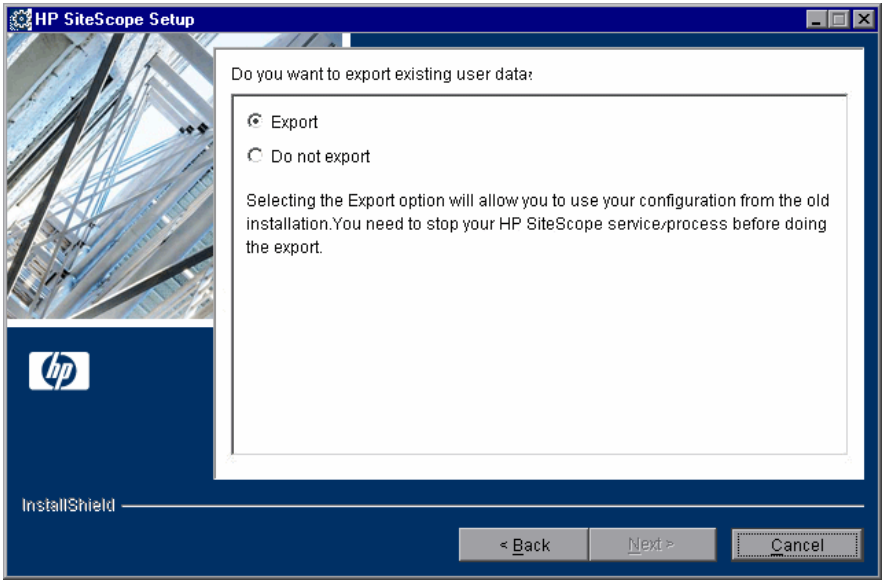
If you click **I do not accept**, the InstallShield Wizard closes.

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

4 If the installation process detects a previous version of SiteScope, the Existing Installation Found screen opens.



Click **Next** to continue. The Export Existing User Data screen opens, enabling you to export data from your current SiteScope for later import into the new SiteScope version.

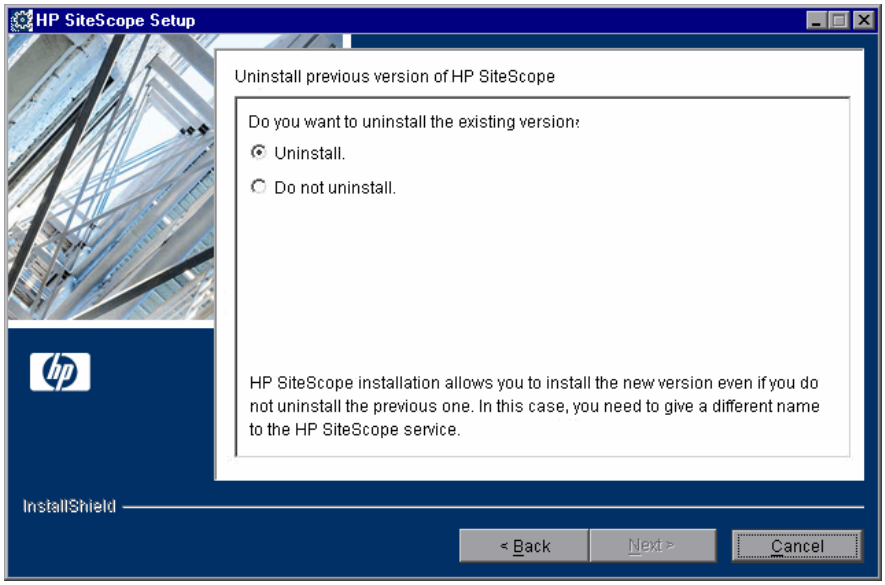


Select an option, and click **Next** to continue.

If you chose the export option, you must:

- Stop the SiteScope service or process before exporting the data.
- Enter the export user data settings as described in step 5 of “Exporting User Data” on page 96.
- Restart the SiteScope service or process after exporting the data.

You are then prompted to uninstall the existing SiteScope version.

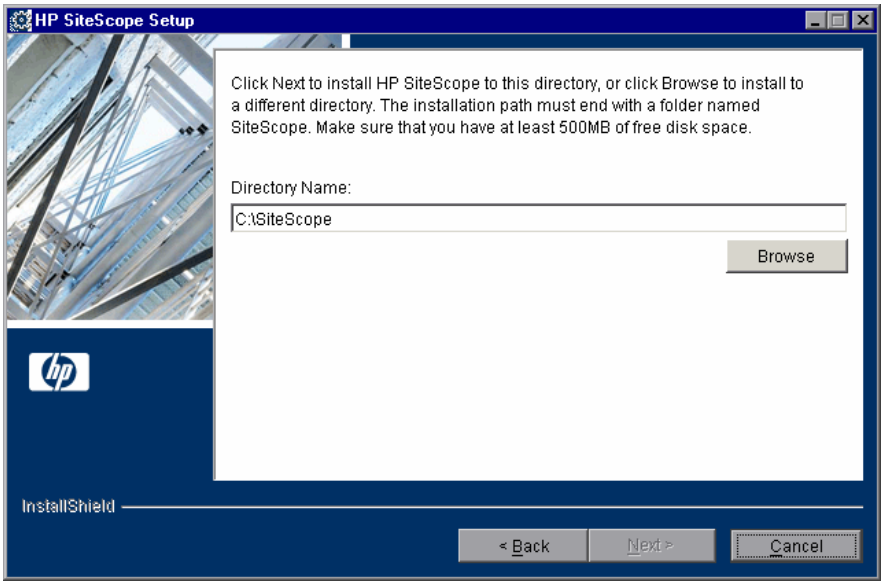


Select the uninstall option, and click **Next** to continue.

Note: If you uninstall the existing SiteScope, you must restart your machine before you can install the new version. After restarting the machine, you start the installation wizard from the beginning.

---

5 The installation directory screen opens.



Accept the default directory location, or click **Browse** to select another directory. If you select another directory, the installation path must end with a folder named **SiteScope** (the folder name is case sensitive).

After entering the new directory name, click **Next** to continue.

Note: An error message is displayed if the installation path does not end with a folder named **SiteScope**. If you did not use the correct case, that is to say, you typed sitescope, you must first change the destination folder to an invalid folder name to reset the InstallShield destination folder mechanism, and then enter the correct folder name.

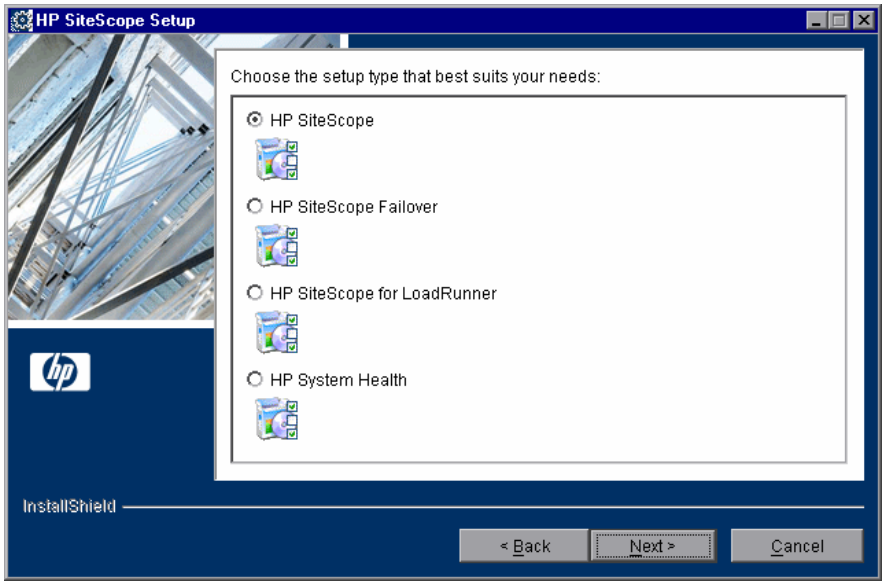
1. Type an invalid folder name. For example, SiteScope1.
2. Click **Next**, and then click **Back**.
3. Type a path that ends with the correct folder name.

For example, C:\Apps\SiteScope.

Do not leave any spaces in the installation path.

---

6 The SiteScope setup type screen opens.

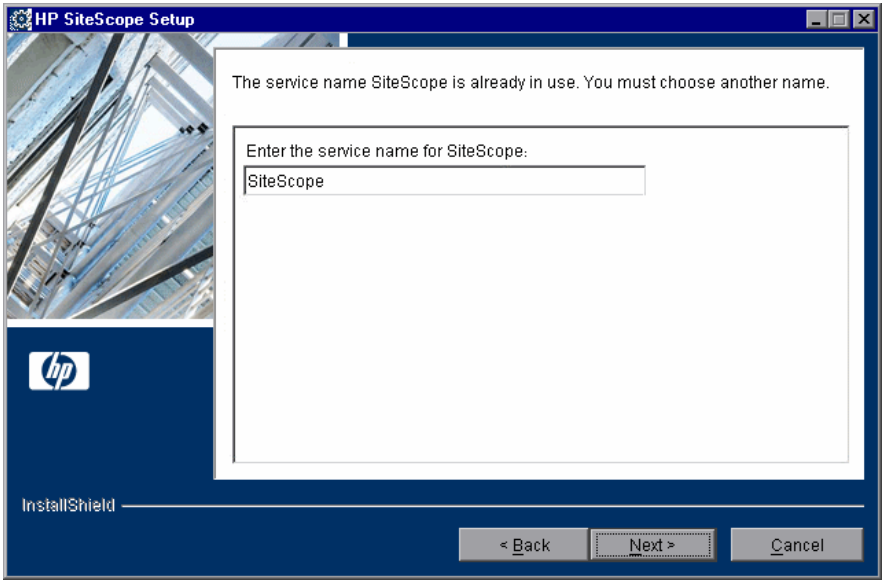


- **HP SiteScope.** This is the standard SiteScope installation.
- **HP Sitescope Failover.** This setup type provides a backup SiteScope server to enable monitoring availability after SiteScope server failure.
- **HP SiteScope for LoadRunner.** This setup type is used with an HP LoadRunner installation only. It enables LoadRunner users to define and use SiteScope monitors on a LoadRunner application. SiteScope provides additional monitoring that complements the native LoadRunner monitors. For details on working with LoadRunner, see the *HP LoadRunner Controller User's Guide* in the LoadRunner documentation.
- **HP System Health.** This setup type is used with an HP Business Availability Center installation only. It uses the SiteScope monitoring system to check configurations and ensure the system health of a Business Availability Center installation. For details, see "System Health" in *Platform Administration* in the HP Business Availability Center Documentation Library.

Select the type that is suitable for your site.

Click **Next** to continue.

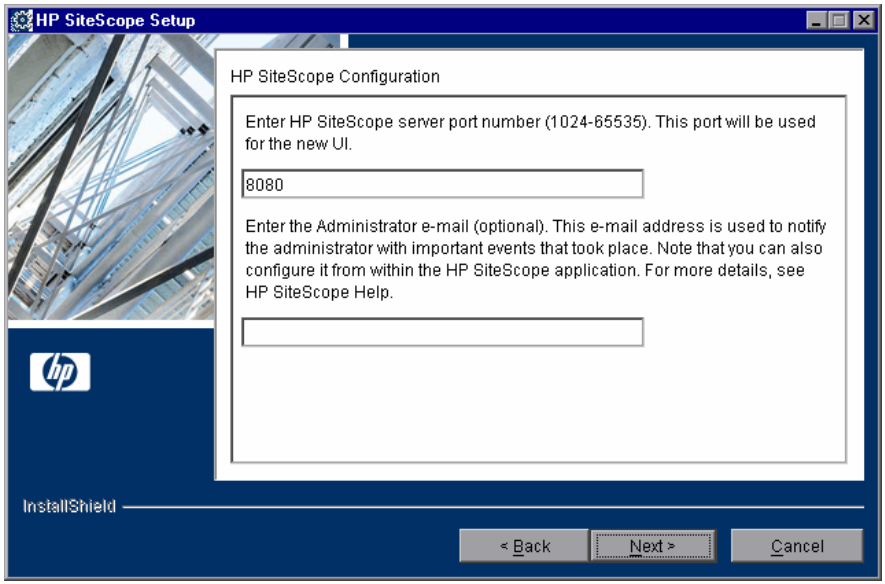
7 If you install SiteScope on a machine that has a previous version of SiteScope installed, the SiteScope service name screen opens.



Enter another name for the SiteScope service.

Click **Next** to continue.

8 The port and email definition screen opens.



Enter the port number you want or accept the default port 8080.

- You can change the port later when you run the Configuration Tool.
- If the port you entered is already in use, you are given an error message. In this case, enter a different port.

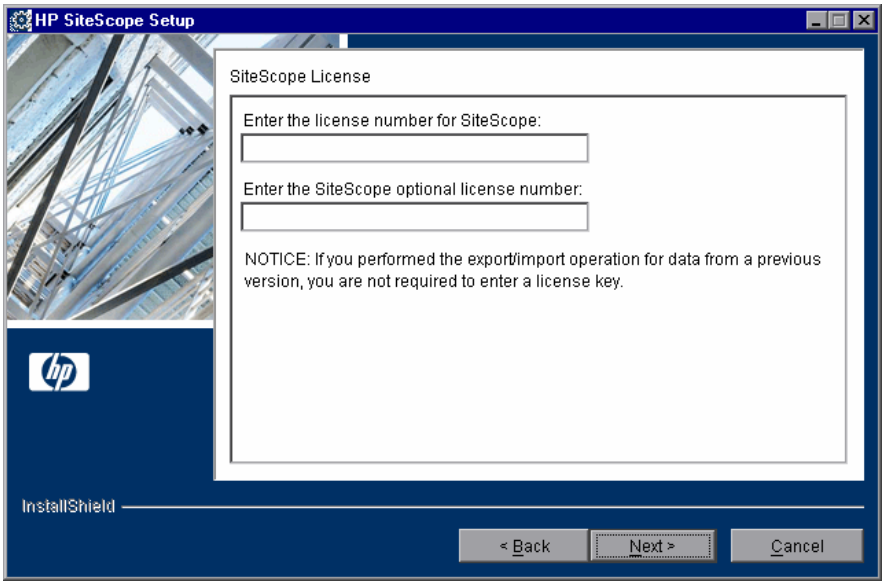
Enter the email address that SiteScope should use to send email alerts to the SiteScope administrator.

Note:

- You do not need to enter an email address at this point to install SiteScope. You can enter this information later using the Email Preferences settings in SiteScope.
- If the mail server uses NTLM authentication, this administrator email address must be a legal email address.

Click **Next** to continue.

9 The license screen opens.



Enter the license number for SiteScope.

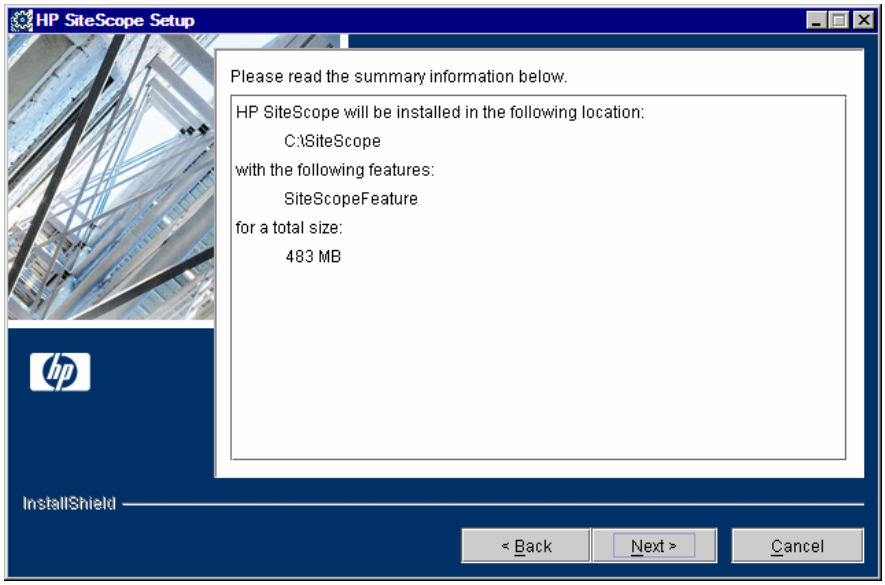
If you have an optional license, enter that number in the second text box.

Notes:

- It is not necessary to enter license information at this point to use SiteScope during the free evaluation period.
- The license screen is not displayed when you install **SiteScope Failover**. You enter the license number for SiteScope Failover in the General Preferences after installing SiteScope.

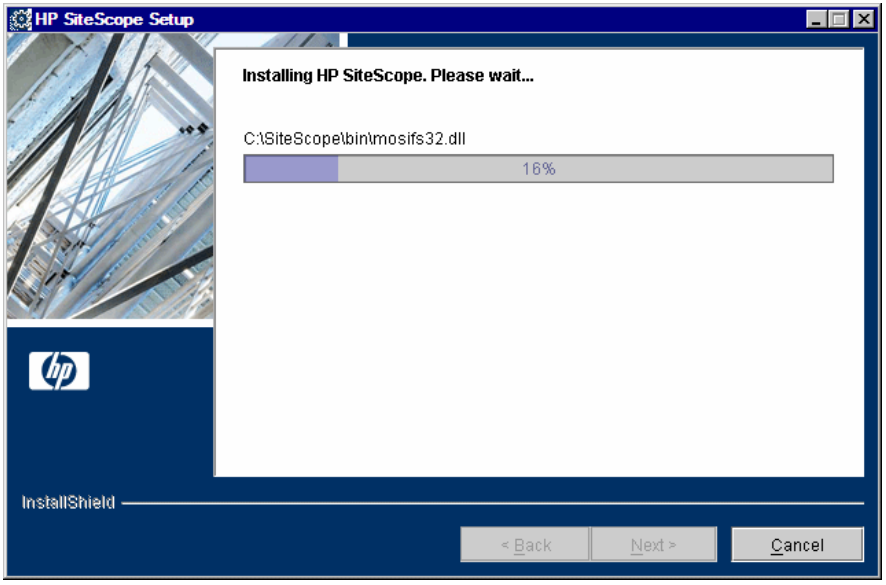
Click **Next** to continue.

10 A screen of summary information opens.

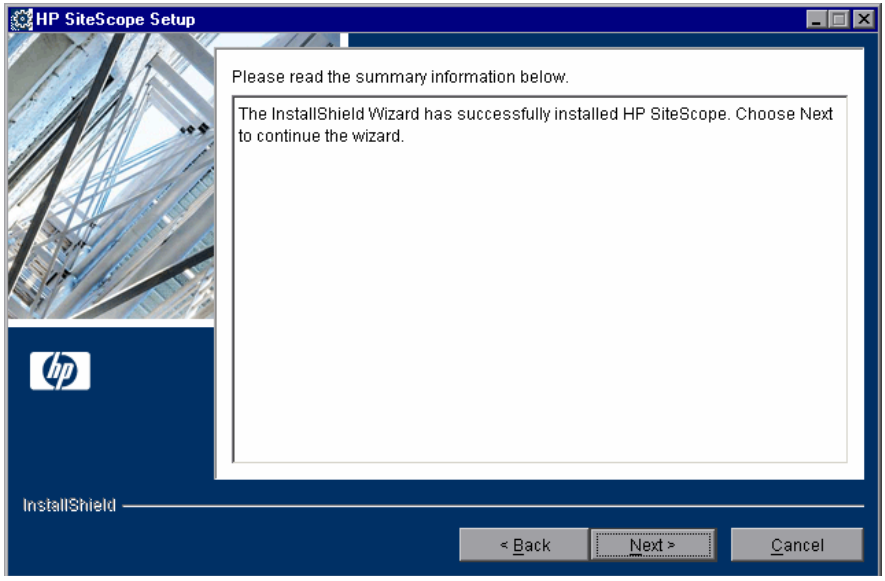


Check that the information is correct and click **Next** to continue, or **Back** to return to previous screens to change your selections.

11 The SiteScope installation process starts and an installation progress screen opens.



When the installation process is complete, a message about the successful installation opens.



Click **Next** to continue the wizard.

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.

For information on accessing the SiteScope interface, see “Connecting to SiteScope” on page 190.

Running the Configuration Tool

The Configuration Tool is a convenient utility for moving configuration data from one SiteScope installation to another. If you exported SiteScope data during the installation process, you can import the data using the Configuration Tool. If you have created or modified monitor configuration files in the previous SiteScope version, you may need to copy them to the 10.10 directory. You can also use the tool to change the port assigned to SiteScope, and to optimize SiteScope's performance by making sizing changes in the Windows Registry keys.

Note: Since the **\htdocs** directory is not copied when you export SiteScope data, you should make a backup of this directory and copy it to the SiteScope 10.10 directory after an upgrade, so that you can see old reports.

The Configuration Tool can be run as part of the installation process or independently. During the installation process, there is no sizing.

If the installation process detects a previous version of SiteScope, you are asked if you want to export user data. If you choose to export data, you can import that data later.

This section includes the following topics:

Changing SiteScope's Port Number

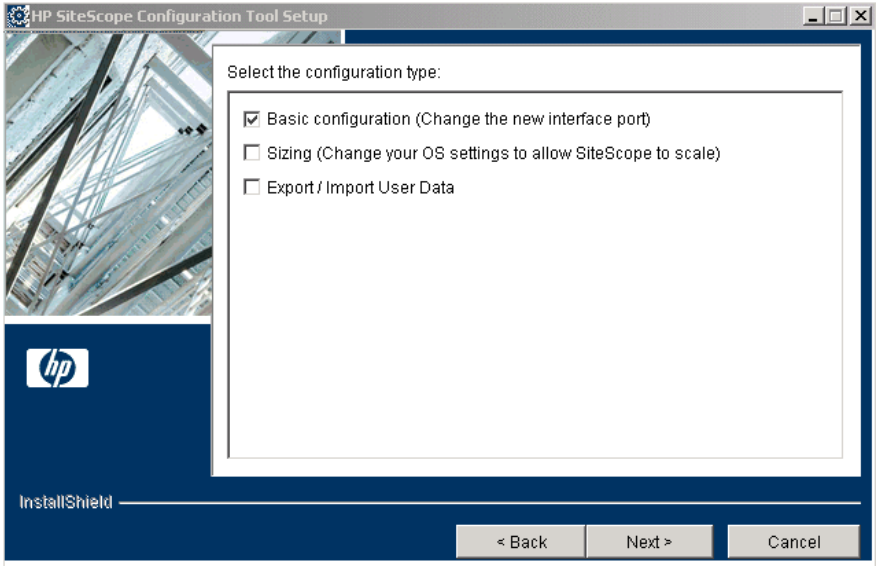
You can change SiteScope's port number if you cannot use the default port of 8080.

To change SiteScope's port number:

1 On the SiteScope server, select **Start** > **Programs** > **HP SiteScope** > **Configuration Tool**. The Configuration Tool opens.

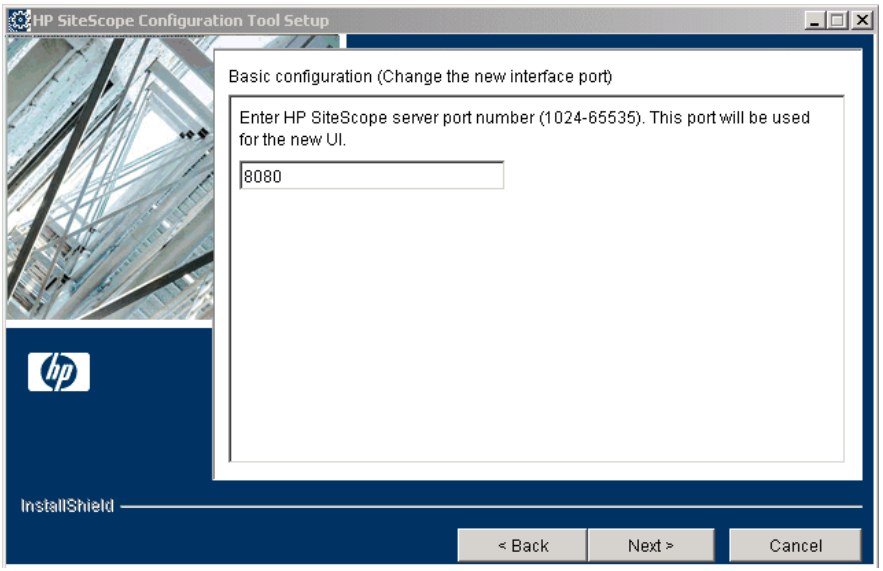
Click **Next** to start the wizard.

2 Select **Basic Configuration**.



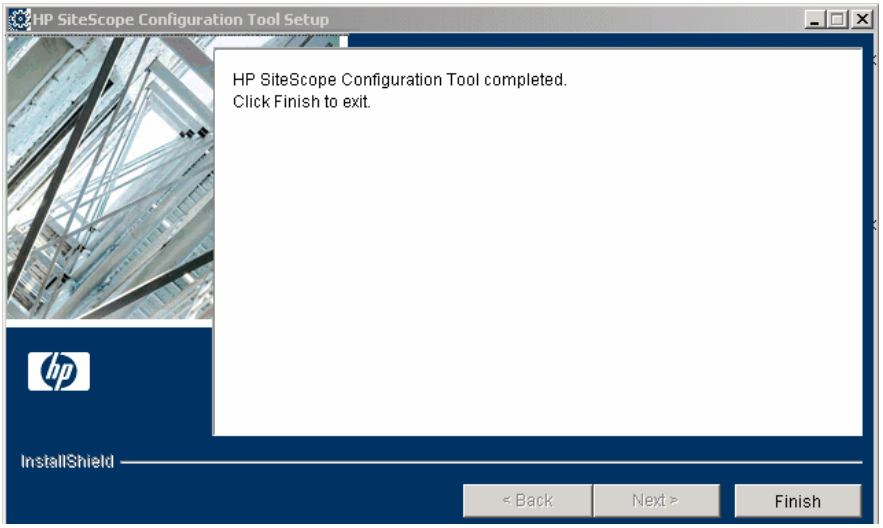
Click **Next**.

3 Enter the port number in the text box.



Click **Next**.

4 The final dialog box opens to show the status of the port change.



Click **Finish** to save your changes and exit.

Sizing SiteScope

You can optimize SiteScope's performance by making changes in the following Windows Registry keys:

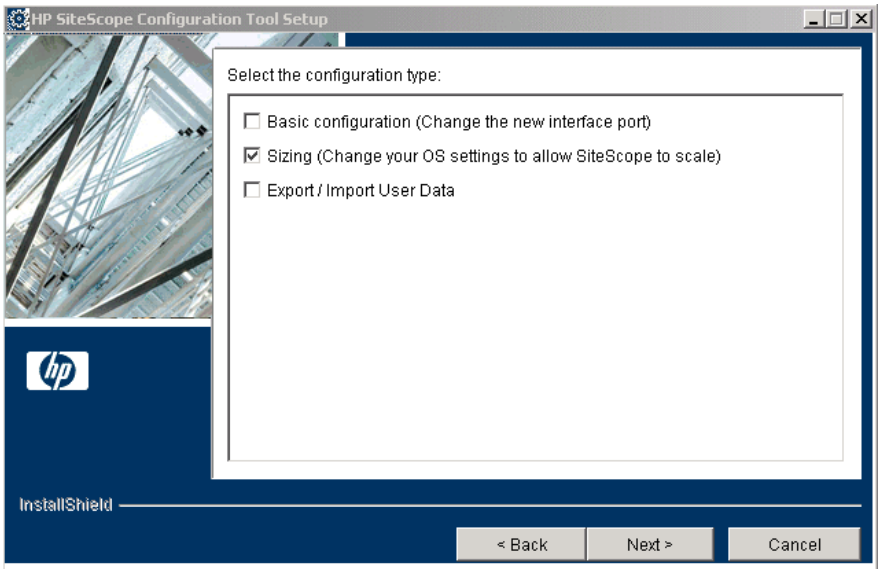
- **JVM heap size.** The value is changed from 512 MB to 1024 MB. For more details on JVM heap size, refer to http://java.sun.com/j2se/1.5.0/docs/guide/vm/gc-ergonomics.html.
- **Desktop heap size.** The value is changed from 512 MB to 2048 MB. For more details on Desktop heap size, refer to http://support.microsoft.com/kb/126962.
- **Popup errors.** These messages are turned off. For more details on popup errors, refer to http://support.microsoft.com/kb/128642.
- **Number of File Handles.** If Microsoft Windows 2000 SP4 is installed on the machine, changes the number of file handles from 10,000 to 18,000. For more details on changing file handles, refer to http://support.microsoft.com/kb/326591.

To perform optimization:

1 On the SiteScope server, select **Start** > **Programs** > **HP SiteScope** > **Configuration Tool**. The Configuration Tool opens.

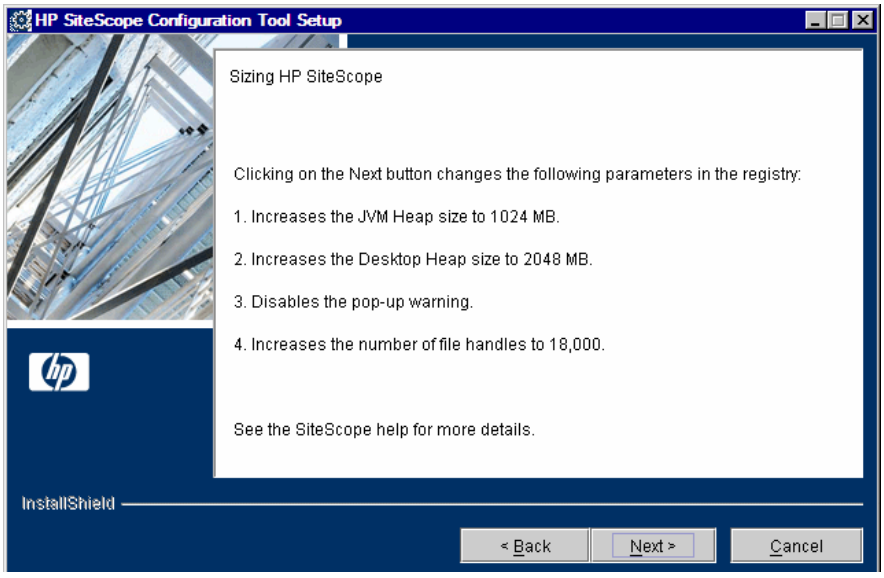
Click **Next** to start the wizard.

2 Select **Sizing**.



Click **Next**.

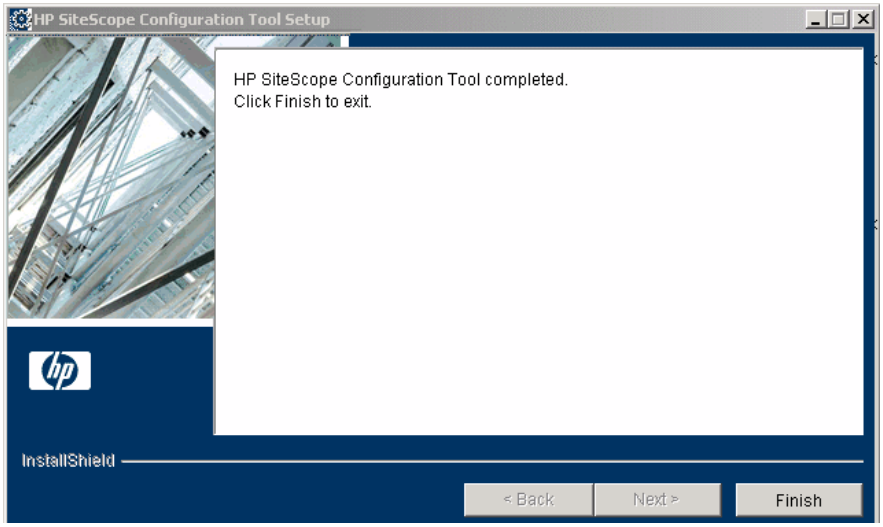
3 A screen listing the parameters in the Windows Registry opens.



Windows Registry keys are automatically changed to optimize your operating system's performance.

Click **Next**.

4 The final dialog box opens.



Click **Finish** to save your changes.

Exporting User Data

You can export SiteScope data such as templates, logs, monitor configuration files, and so forth from your current SiteScope for later import into SiteScope. Alternatively, you can export data from your current SiteScope independently using the Configuration Tool.

Note: Since the **\htdocs** directory is not copied when you export SiteScope data, you should make a backup of this directory and copy it to the SiteScope 10.10 directory after an upgrade, so that you can see old reports.

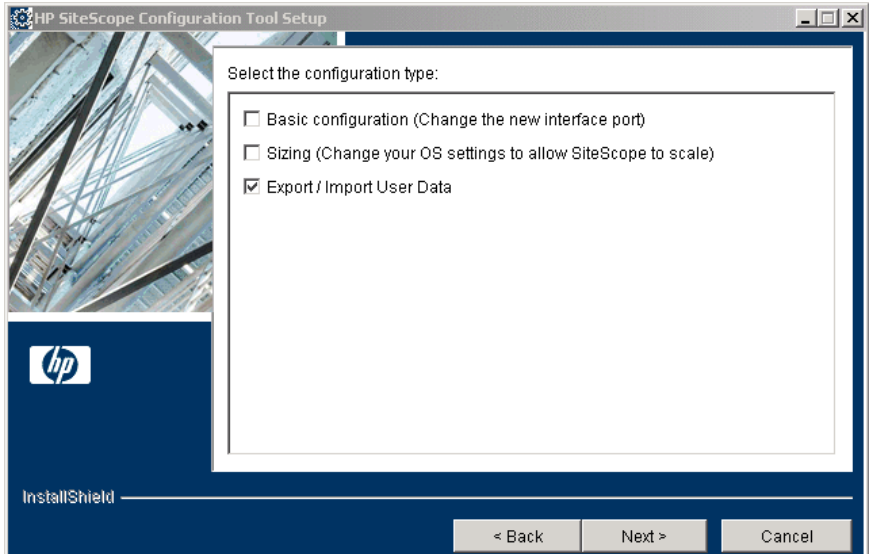
To export user data:

1 Stop the SiteScope service or process before exporting the data. For details, see "Starting and Stopping the SiteScope Service on Windows Platforms" on page 188.

2 On the SiteScope server, select **Start** > **Programs** > **HP SiteScope** > **Configuration Tool**. The Configuration Tool opens.

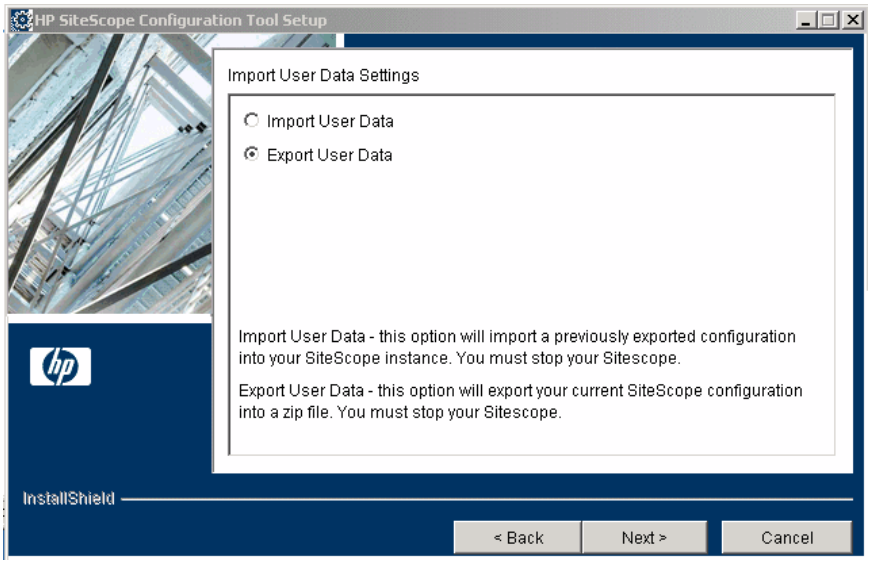
Click **Next** to start the wizard.

3 Select **Export/Import User Data**.



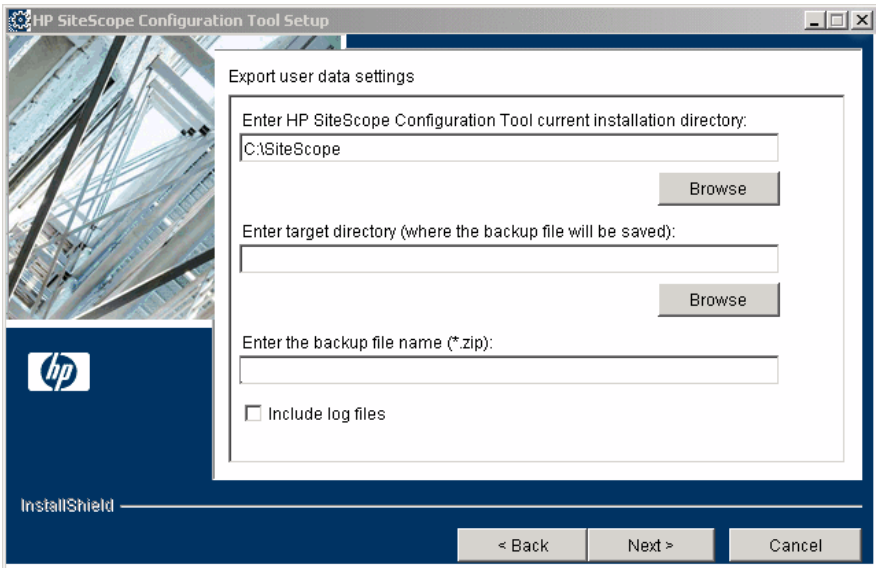
Click **Next**.

4 Select **Export User Data**.



Click **Next**.

5 The Export User Data Settings dialog box opens.



- In **Export user data settings**, accept the default directory given in the text box, or enter the full path of the SiteScope installation directory. For example, if you do not want to accept the directory path as listed and the installation directory path is D:\SS9_0\SiteScope, enter D:\SS9_0\SiteScope.
- In **Enter target directory**, enter the directory to which to export the user data file. The directory must already exist.
- In **Enter the backup file name**, enter a name for the exported user data file. The name must end in **.zip**.
- If you also want to export log files, select **Include log files**.

Click **Next** and then **Finish** to complete the export operation.

6 Restart the SiteScope service or process after exporting the data. For details, see “Starting and Stopping the SiteScope Service on Windows Platforms” on page 188.

Importing User Data

You can import SiteScope data such as templates, logs, monitor configuration files, and so forth.

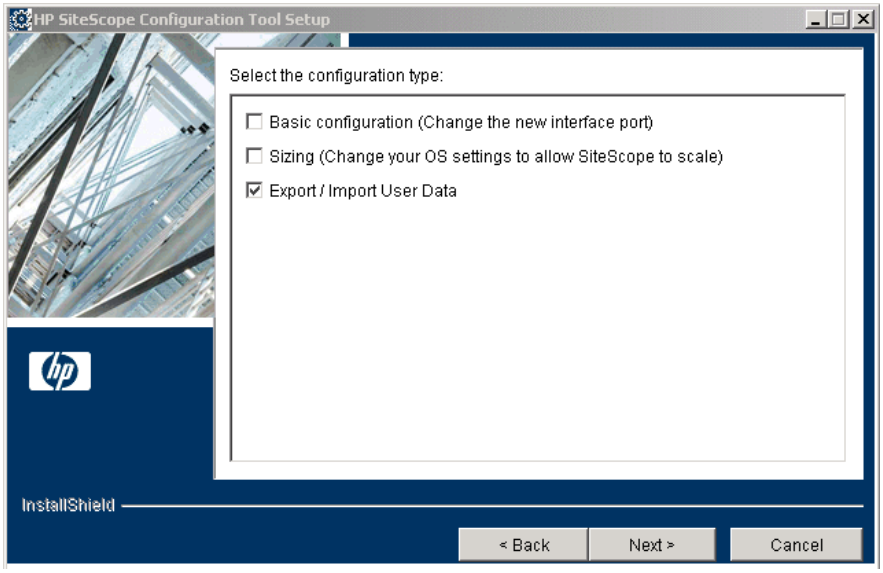
To import user data:

1 Stop the SiteScope service or process before importing the data. For details, see "Starting and Stopping the SiteScope Service on Windows Platforms" on page 188.

2 On the SiteScope server, select **Start** > **Programs** > **HP SiteScope** > **Configuration Tool**. The Configuration Tool opens.

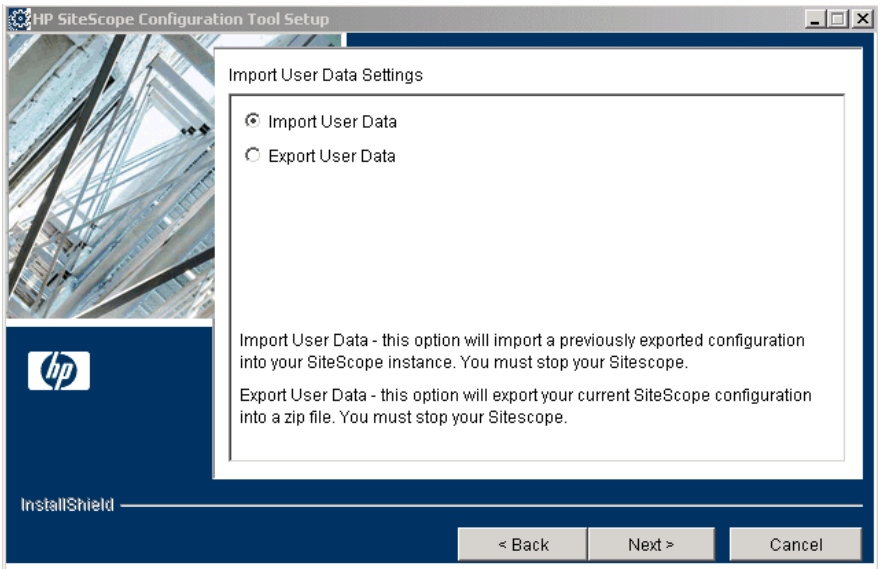
Click **Next** to start the wizard.

3 Select **Export/Import User Data**.



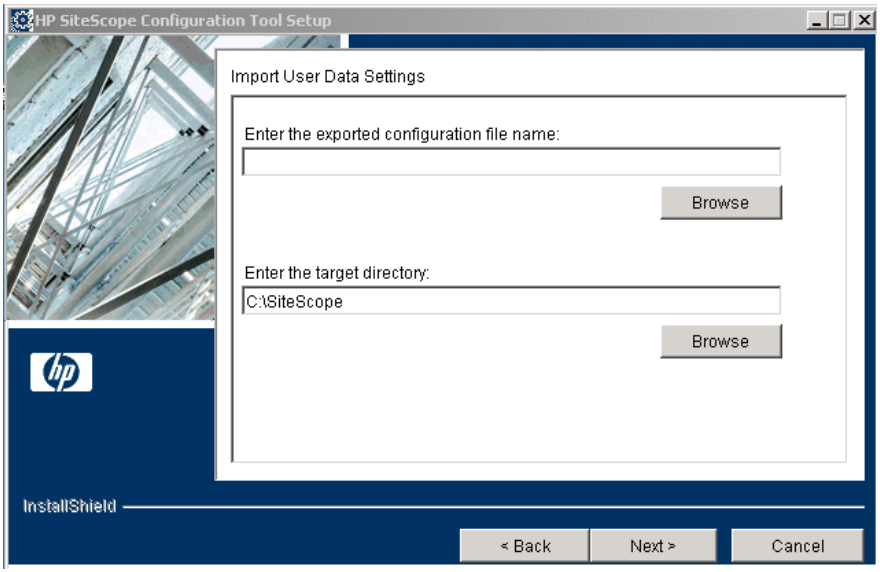
Click **Next**.

4 Select **Import User Data**.



Click **Next**.

5 The Import User Data Settings dialog box opens.



- In **Enter the exported configuration file name**, enter the name of the user data file to import.
- In **Enter the target directory**, enter the Sitescope installation directory to which to import the user data file.

Click **Next** and then **Finish** to complete the import operation.

6 Restart the SiteScope service or process after importing the data. For details, see "Starting and Stopping the SiteScope Service on Windows Platforms" on page 188.

Tip: After an upgrade, you can start SiteScope by running the **go.bat** file from the **<SiteScope root directory>\bin** directory. This avoids SiteScope restarting itself if it takes longer than 15 minutes for the monitors to run.

9

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 HP Web site. It is also available on DVD. SiteScope is installed on a single server and runs as a single application or process.

This chapter includes:

Installation – Workflow

SiteScope version 10.10 installation follows a different procedure for first-time installation than for users with an earlier version of SiteScope already installed.

This section includes the following topics:

New Users

Users who do not have SiteScope installed must follow this procedure:

1 Prepare for the SiteScope 10.10 installation.

For details see "Preparing for Installation" on page 105.

2 Install SiteScope 10.10.

For details, see "Performing a Full Installation" on page 106.

3 Connect to SiteScope.

For details, see "Connecting to SiteScope" on page 190.

Users with an Earlier SiteScope Version Installed

SiteScope version 10.10 does not automatically upgrade from a previous version of SiteScope. Users must follow this procedure:

1 Prepare for the SiteScope 10.10 installation.

For details, see "Preparing for Installation" on page 105.

2 Install SiteScope 10.10.

You can install SiteScope version 10.10 on the same machine as your current SiteScope or on a different machine. If you install SiteScope on the same machine, you can install in the same directory or in a different one. For details, see "Performing a Full Installation" on page 106.

As part of the installation process, you can export data from your current SiteScope for later import into SiteScope version 10.10. Alternatively, you can export data from your current SiteScope independently using the Configuration Tool. For details, see "Exporting User Data" on page 124.

3 (Optional) Import SiteScope data from the previous version into SiteScope 10.10.

If you exported SiteScope data during the installation process, you can import the data using the Configuration Tool. For details, see "Importing User Data" on page 126.

4 Copy monitor configurations from the previous version into SiteScope 10.10.

If you have created or modified monitor configuration files in the previous SiteScope version, you may need to copy them to the 10.10 directory. You also need to check that your monitor configuration files point to the 10.10 directory. For details, see "Exporting User Data" on page 124.

5 Connect to SiteScope.

For details, see "Connecting to SiteScope" on page 190.

Preparing for Installation

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

To prepare for installation of SiteScope on Solaris or Linux:

1 Create a user account that runs 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.

Note: Create a new directory for installation of SiteScope 10.10. Do not install version 10.10 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 is 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.

Performing a Full Installation

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 106.
- Console mode installation script using command line input. For details, see "Installing SiteScope Using Console Mode" on page 116.

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 116.

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

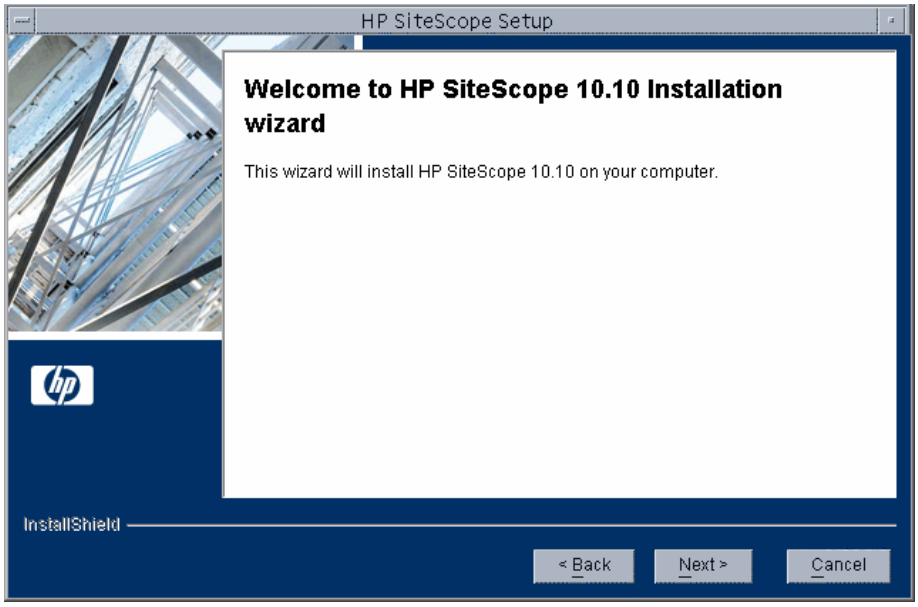
1 Download the SiteScope setup file on the machine where you want to install SiteScope.

Alternatively, copy the SiteScope setup file to a disk or network location where it is accessible to the user account that is to be used to install SiteScope.

2 Run the installation script with the following command:

```
SiteScopeSetup/inst
```

The installation executable initializes the InstallShield Wizard for HP SiteScope. The InstallShield Welcome window opens.



Click **Next** to continue.

3 The license agreement screen opens.

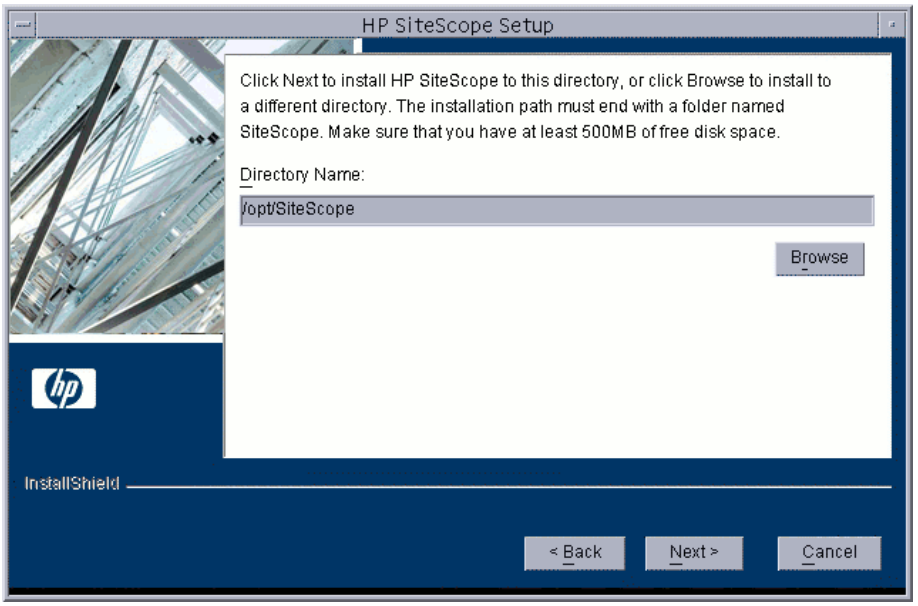
Read the SiteScope License Agreement.

To install SiteScope, you must accept the terms of the license agreement by clicking **I accept** and then click **Next** to continue.

If you click **I do not accept**, the InstallShield Wizard closes.

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

4 The installation directory screen opens.



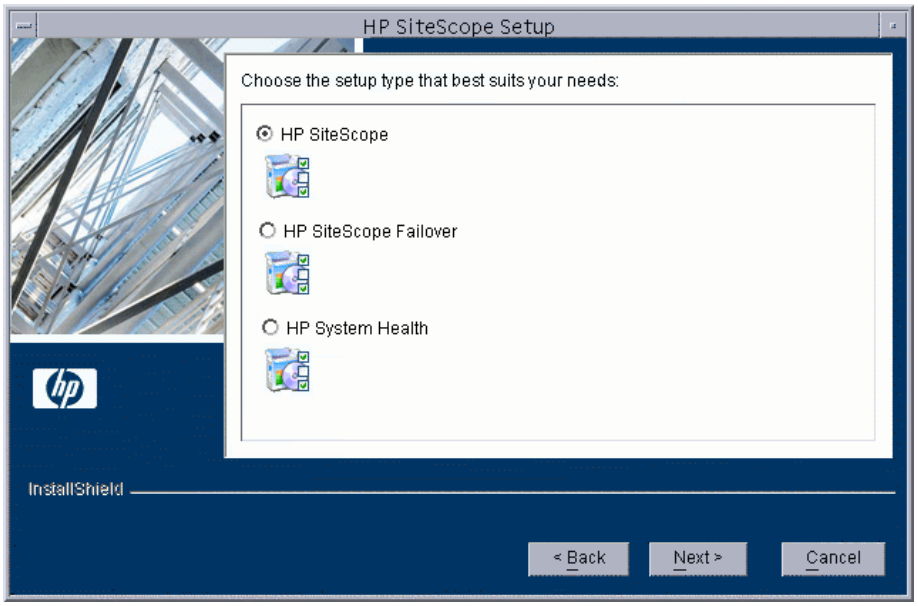
Accept the default directory location or click **Browse** to select another directory.

After entering the new directory name, click **Next** to continue.

Note: The installation path must end with a folder named **SiteScope**. There must not be any spaces in the installation path.

---

5 The SiteScope setup type screen opens.

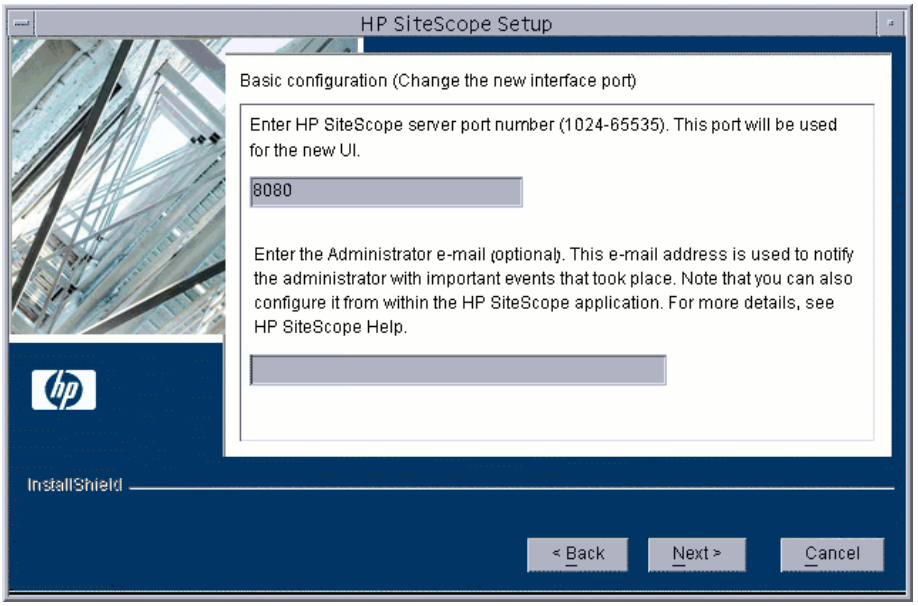


- **HP SiteScope.** This is the standard SiteScope installation.
- **HP Sitescope Failover.** This setup type provides a backup SiteScope server to enable monitoring availability after SiteScope server failure.
- **HP System Health.** This setup type is used with an HP Business Availability Center installation only. It uses the SiteScope monitoring system to check configurations and ensure the system health of a Business Availability Center installation. For details, see "System Health" in *Platform Administration* in the HP Business Availability Center Documentation Library.

  Select the type that is suitable for your site.

  Click **Next** to continue.

6 The port and email definition screen opens.



Enter the port number you want or accept the default port 8080.

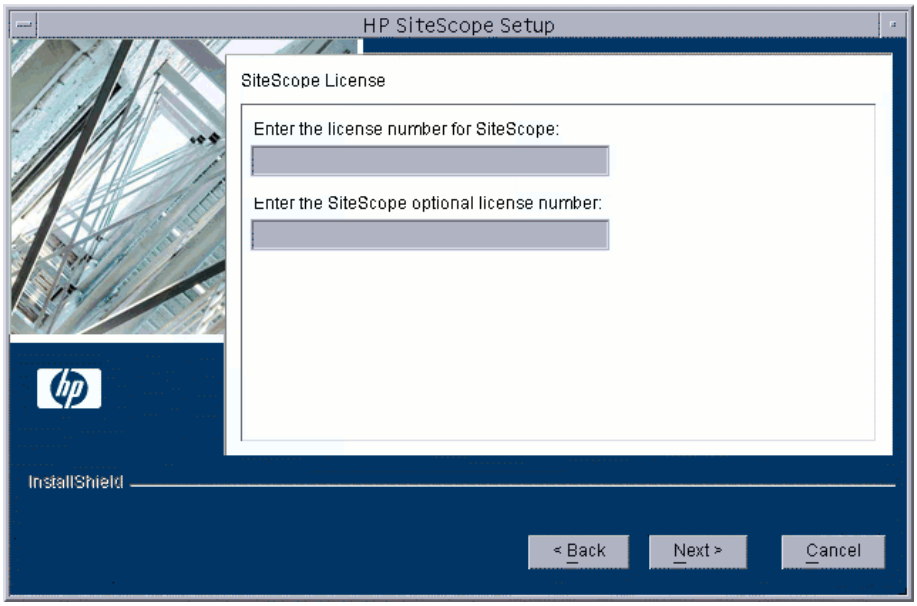
- You can change the port later when you run the Configuration Tool Utility.
- If the port you entered is already in use, you are given an error message. In this case, enter a different port.

Enter the email address that SiteScope should use to send email alerts to the SiteScope administrator.

Note: Entering an email 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.

Click **Next** to continue.

7 A screen for license numbers opens.



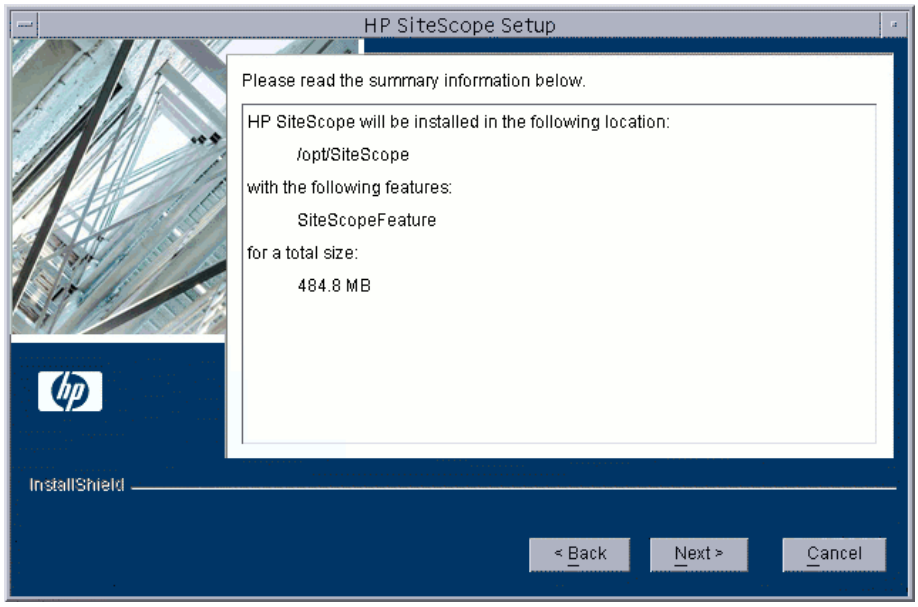
Enter the license number for SiteScope.

If you have an optional license, enter that number in the second text box.

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

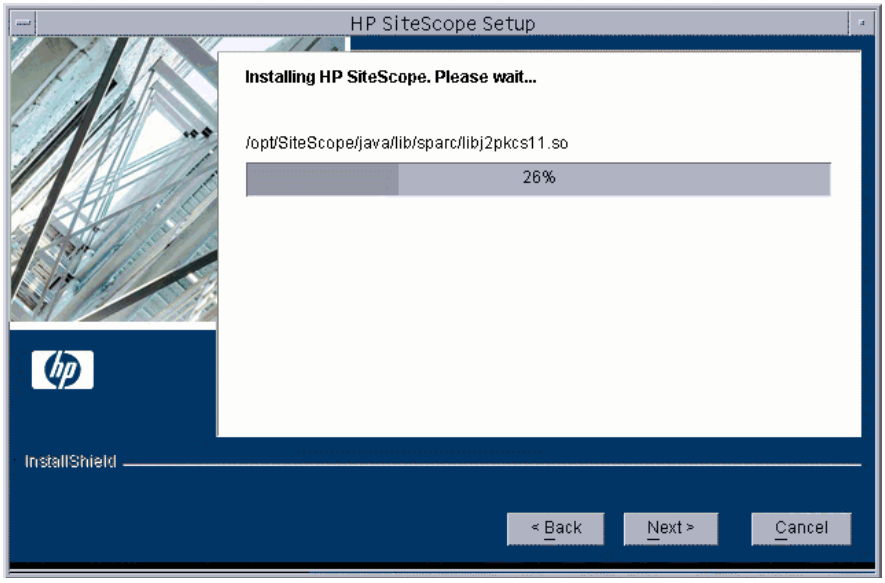
Click **Next** to continue.

8 A screen of summary information opens.

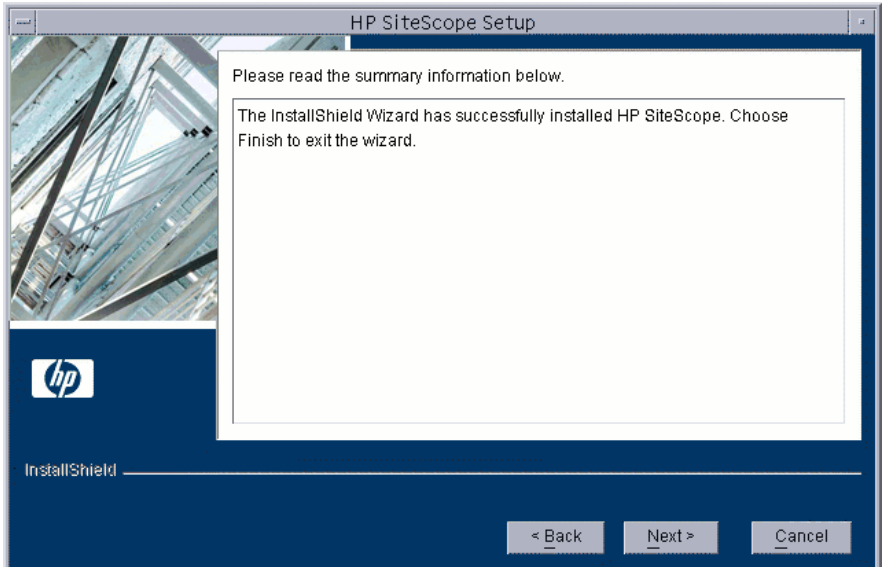


Check that the information is correct and click **Next** to continue, or **Back** to return to previous screens to change your selections.

9 The SiteScope installation process starts and an installation progress screen opens.



When the installation process is complete, a message about the successful installation opens. Click **Finish**.



10 Log out of the SiteScope server and log back in again.

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.

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

For information on accessing the SiteScope interface, see “Connecting to SiteScope” on page 190.

Installing SiteScope Using Console Mode

You can install SiteScope using a command line or console mode. 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:

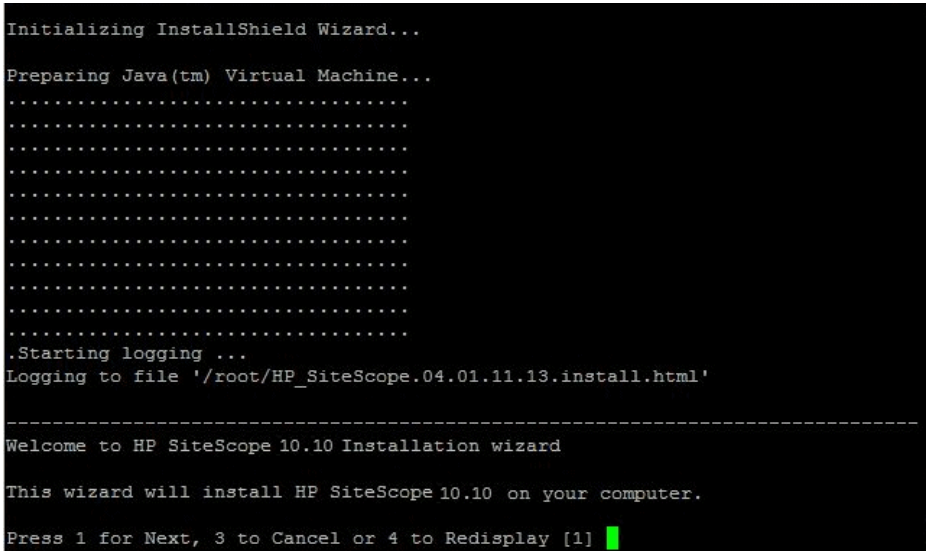
1. Download the SiteScope setup file to the machine where you want to install SiteScope.

   Alternatively, copy the SiteScope setup file to a disk or network location where it is accessible to the user account that is to be used to install SiteScope.

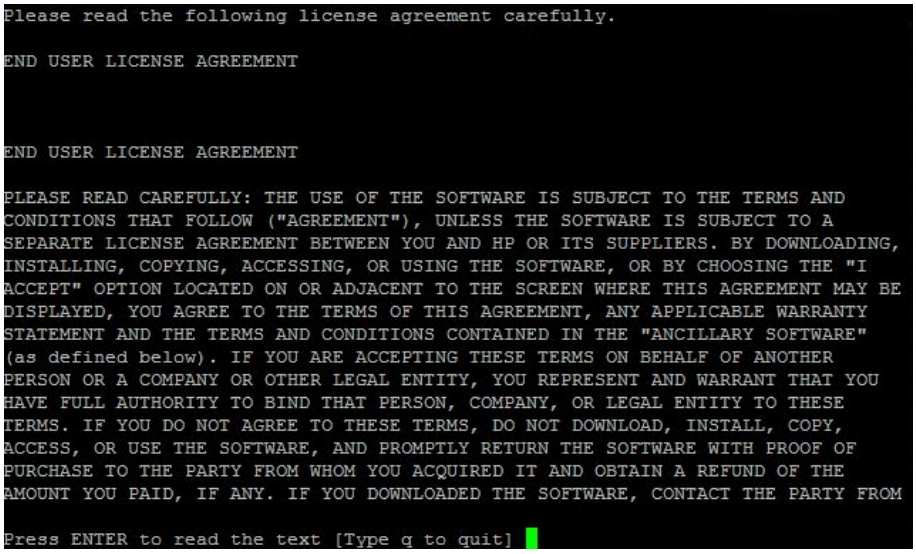
2. Run the following command:

```
/bin/sh SiteScopeInstall/SiteScopeSetup.bin – console
```

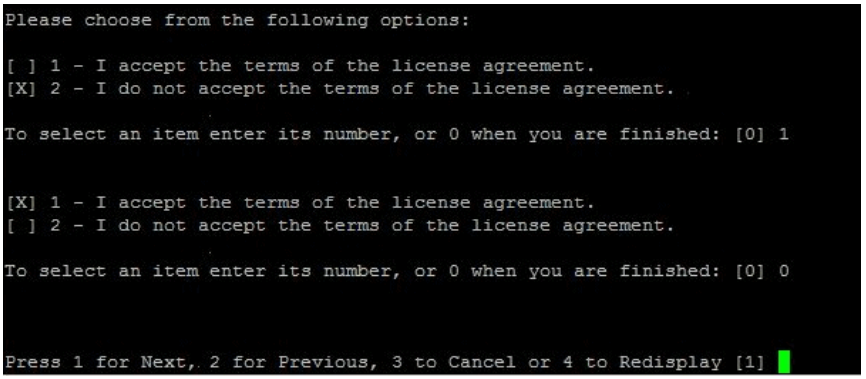
   The installation script initializes the Java Virtual Machine to begin the installation. A confirmation screen is displayed.



3 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.



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.

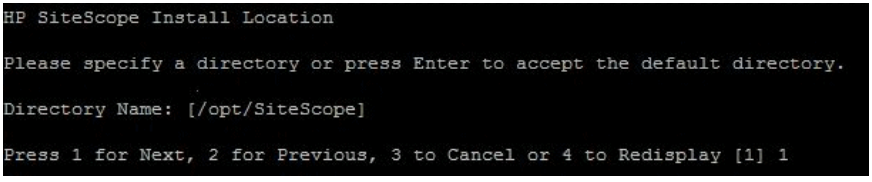


To install SiteScope, you must accept the terms of the license agreement. The default selection is to not accept the agreement. To accept the license agreement and continue the installation, enter the number 1 and then enter the number zero (0) to continue. A continuation prompt is displayed.

Note: To cancel the installation after viewing the SiteScope License Agreement, enter the number 1, enter the number zero (0), and then enter the number 3 at the next continuation prompt to cancel the installation.

---

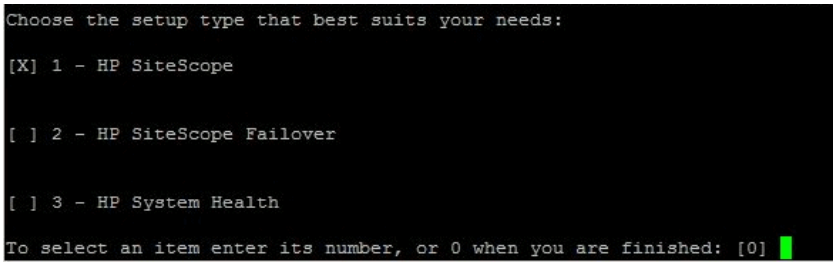
4 The Installation Location selection prompt is displayed.



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.

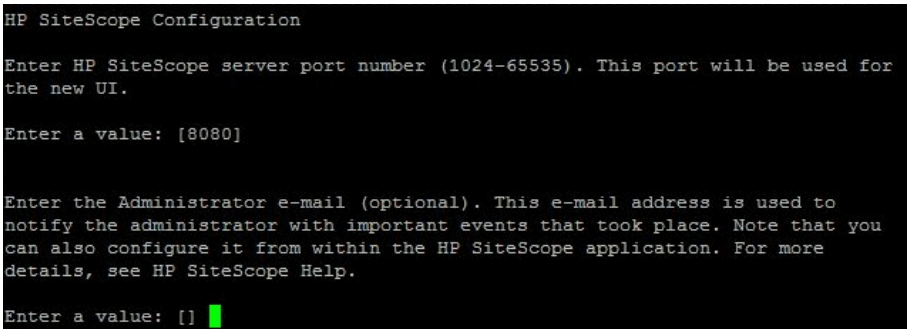
To enter a different installation location, type the location path as a command line entry without square brackets. The installation location must end with a directory called **SiteScope**. Enter 1 to continue to the next step.

5 The SiteScope setup type screen opens.



Choose the type that is suitable for your site. Enter the number of the setup type or accept the default **SiteScope Typical** setup. Enter the number zero (0) to continue.

6 The port and email address prompt is displayed.



Enter the port number you want or accept the default port 8080.

Enter a SiteScope administrator email address. For example, sitescopeadmin@thiscompany.com.

If you do not want to enter an email address at this time, press ENTER to leave this blank and continue to the next step.

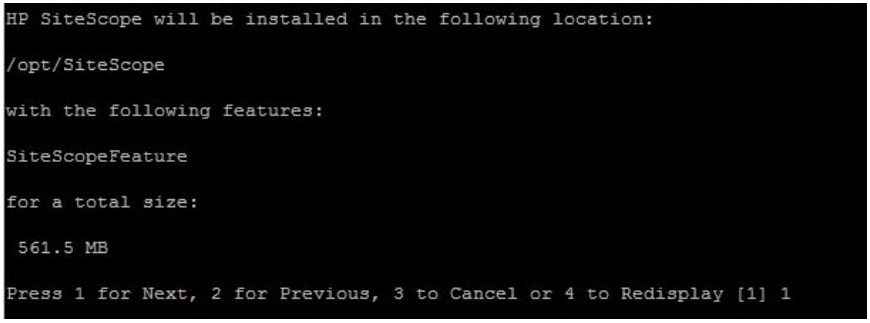
You can enter e-mail information later using the E-mail Preferences page once SiteScope is running.

7 Enter 1 to continue to the next step. The license number prompt is displayed.

8 Enter the license number for SiteScope. If you have an optional license, enter that number in the second text box.

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

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

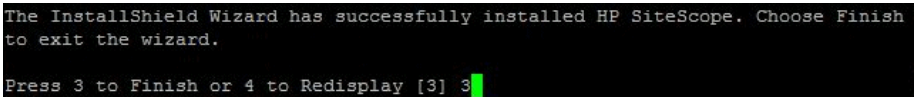


10 Enter 1 to proceed with the installation using the installation location indicated or enter 2 to return to the previous dialogue and make changes. The installation process starts.

11 Make a note of the SiteScope address and port number displayed on the screen. By default, SiteScope tries to answer on port 8080. If another application is using that port number, SiteScope tries another port number (for example, port 8889).

To connect to SiteScope, follow the steps in the section "Connecting to SiteScope" on page 190.

12 Enter 1 to continue to the next step. An installation status message is displayed.



13 Enter 1 to exit the installation script.

Running the Configuration Tool

The Configuration Tool can be run as part of the installation process or independently.

If the installation process detects a previous version of SiteScope, you are asked if you want to export user data. If you choose to export data, you can import that data later.

This section includes the following topics:

Changing SiteScope's Port Number

You can change SiteScope's port number if you can not use the default port of 8080.

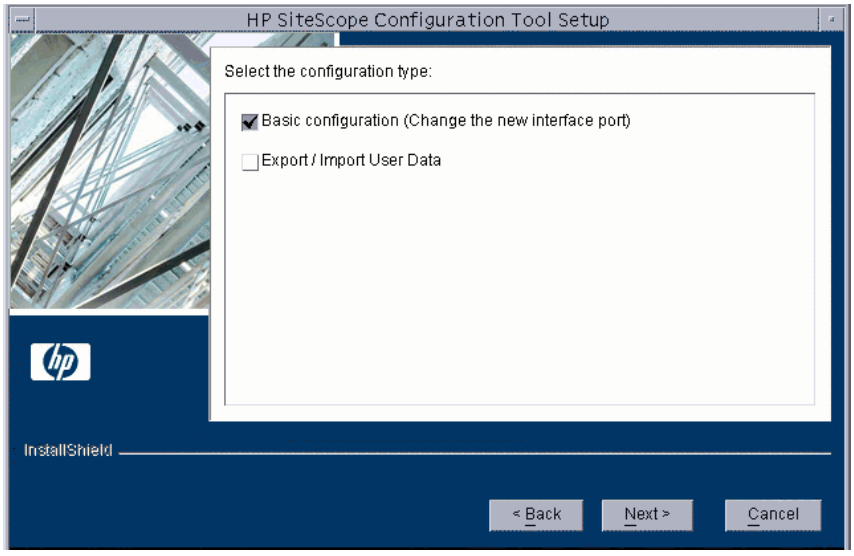
To change SiteScope's port number:

1. On the SiteScope server, do either of the following:
   - **a** In graphic mode, run <SiteScope install Directory>/bin/configTool.sh
   - **b** In console mode, run <SiteScope install Directory>/bin/configTool.sh -console

   The Configuration Tool opens.

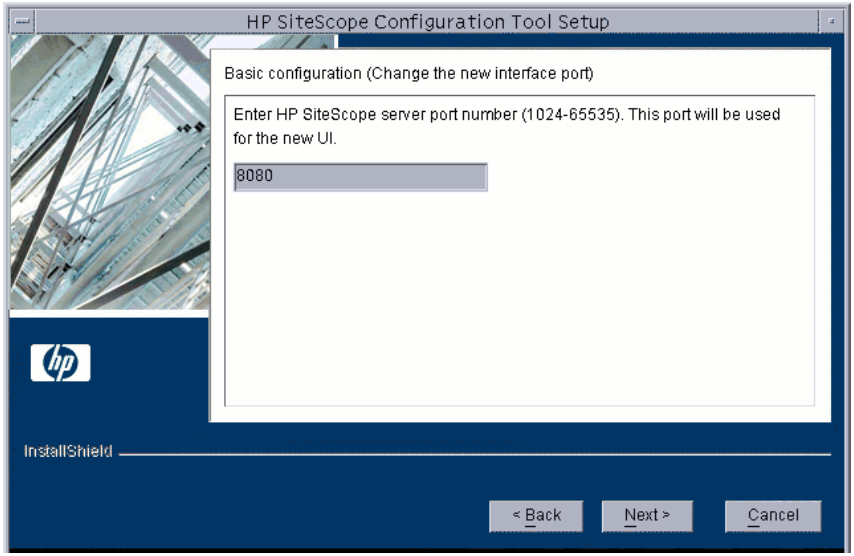
   Click **Next**.

2 Select **Basic Configuration**.



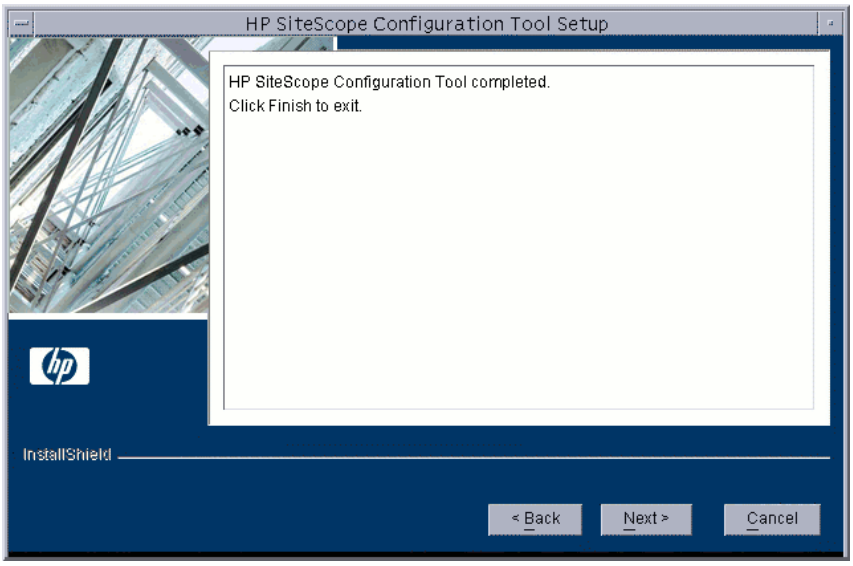
Click **Next**.

3 Enter the port number in the text box.



Click **Next**.

4 The final dialog box opens to show the status.



Click **Finish** to save your changes and exit.

Exporting User Data

You can export SiteScope data such as templates, logs, monitor configuration files, and so forth for later import.

To export user data:

1 Stop the SiteScope service before exporting the data. For details, see "Starting and Stopping the SiteScope Service on Solaris and Linux Platforms" on page 189.

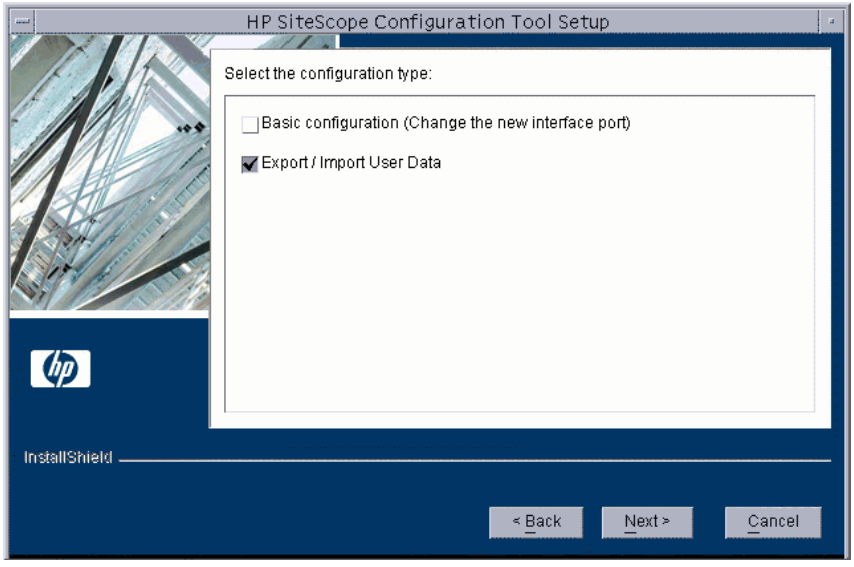
2 On the SiteScope server, do either of the following:

- **a** In graphic mode, run <SiteScope install Directory>/bin/configTool.sh
- **b** In console mode, run <SiteScope install Directory>/bin/configTool.sh -console

The Configuration Tool opens.

Click **Next**.

3 Select **Export/Import User Data**.

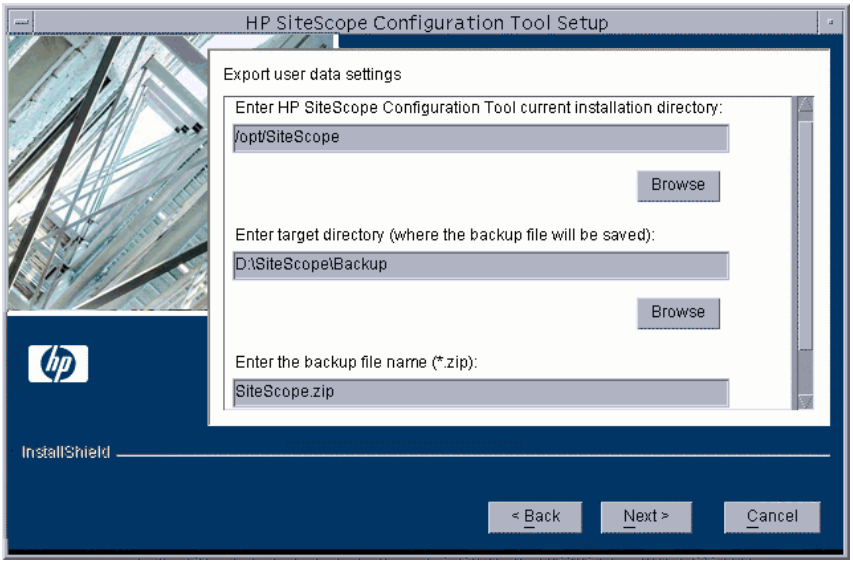


Click **Next**.

4 In the Export/Import User Data dialog box, select **Export User Data**.

Click **Next**.

5 The Export User Data Settings dialog box opens.



- In **Export user data settings**, accept the default directory given in the text box, or enter the full path of the SiteScope installation directory. For example, if you do not want to accept the directory path as listed and the installation directory path is /opt/9_0/SiteScope, enter /opt/9_0/SiteScope.
- In **Enter target directory**, enter the directory to which to export the user data file. The directory must already exist.
- In **Enter the backup file name**, enter a name for the exported user data backup file. The name must end in **.zip**.
- If you also want to export log files, select **Include log files**.

Click **Next** and then **Finish** to complete the export operation.

6 Restart the SiteScope service after exporting the data. For details, see "Starting and Stopping the SiteScope Service on Solaris and Linux Platforms" on page 189.

Importing User Data

You can import SiteScope data such as templates, logs, monitor configuration files, and so forth.

To import user data:

1 Stop the SiteScope service before importing the data. For details, see "Starting and Stopping the SiteScope Service on Solaris and Linux Platforms" on page 189.

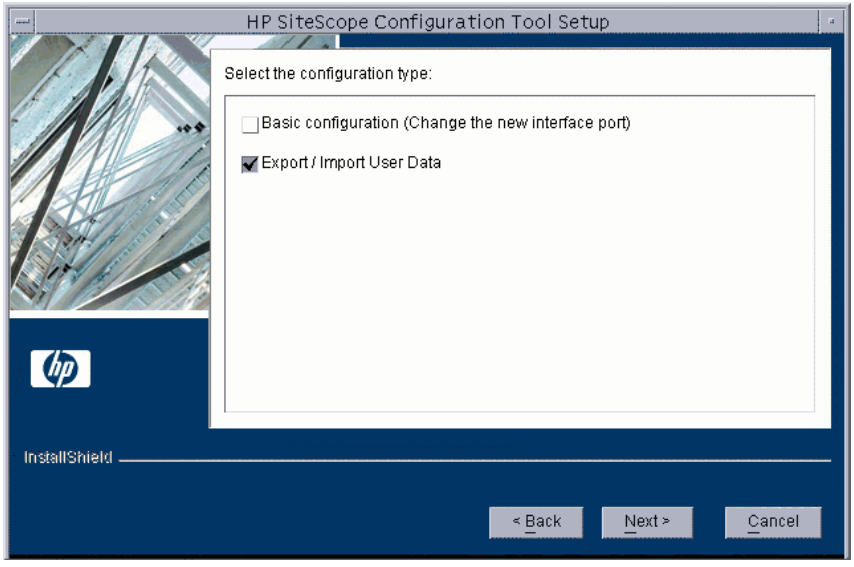
2 On the SiteScope server, do either of the following:

- **a** In graphic mode, run <SiteScope install Directory>/bin/configTool.sh
- **b** In console mode, run <SiteScope install Directory>/bin/configTool.sh -console

The Configuration Tool opens.

Click **Next**.

3 Select **Export/Import User Data**.

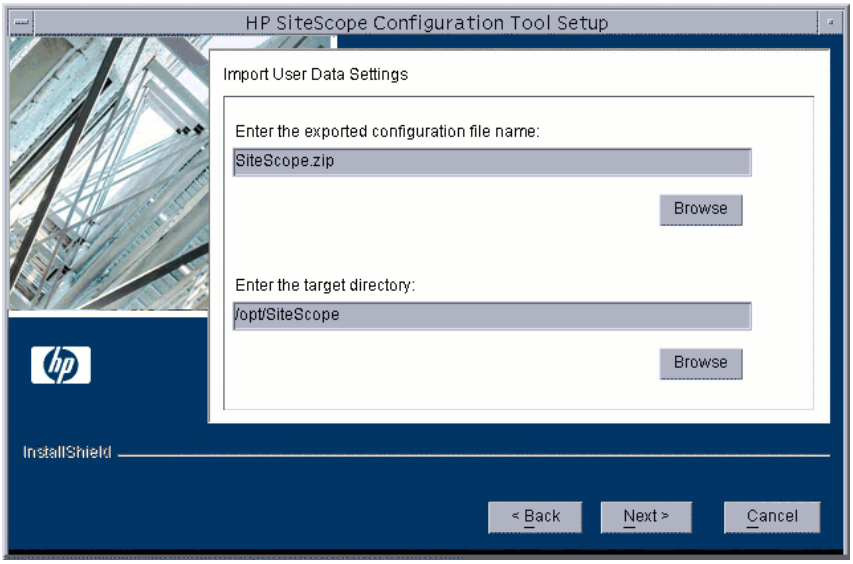


Click **Next**.

4 In the Export/Import User Data dialog box, select **Import User Data**.

Click **Next**.

5 The Import User Data Settings dialog box opens.



- In **Enter the backup file name**, enter the name of the user data file to import.
- In **Enter the target directory**, enter the directory to which to import the user data file.

Click **Next** and then **Finish** to complete the import operation.

6 Restart the SiteScope service after importing the data. For details, see "Starting and Stopping the SiteScope Service on Solaris and Linux Platforms" on page 189.

10

Sizing SiteScope

While the default SiteScope configuration allows running thousands of monitors, sizing the server where SiteScope is installed may be necessary to achieve optimum performance. Since each configuration is different, you should use the SiteScope Capacity Calculator to verify if your configuration requires sizing.

This chapter includes:

About Sizing SiteScope

Proper sizing of the server where SiteScope is to run is the foundation of successful monitoring deployment. To ensure optimal sizing, HP strongly recommends the following SiteScope server environment:

- SiteScope runs as a stand-alone server. For best results, SiteScope should be the only program running on a server. Business Availability Center, BMC, LoadRunner, databases, Web servers, and so forth, should not be on the SiteScope server.
- Only one instance of SiteScope exists and it runs on a single server. Running multiple instances of SiteScope on a single server can cause severe resource problems. This recommendation includes instances of SiteScope used for System Health.

➤ SiteScope Failover needs to be sized just like the primary SiteScope server.

SiteScope Capacity Calculator

SiteScope includes a tool that helps you predict system behavior and perform capacity planning for SiteScope. You enter the CPU and memory details of the system on which SiteScope is running, and the number of monitors of each type and the frequency that they are to run. The calculator then displays the expected CPU usage and memory usage for each monitor type, and the recommended system requirements for the given workload. This enables you to determine whether your configuration requires tuning.

Note: The SiteScope Capacity Calculator is supported in SiteScopes that are running on Windows versions only. For the list of monitors and solution templates supported by the capacity calculator, see "Supported Monitors and Solution Templates" on page 131.

To use the SiteScope Capacity Calculator:

1 Open the SiteScope Capacity Calculator from **<SiteScope root directory>\tools\SiteScope Capacity Calculator.xls** or from the link in the Home page of the SiteScope Documentation Library.

2 In the **Monitor Usage** tab, enter the following information in the **Requirements** section:

- ➤ Average % CPU usage
- ➤ CPU type
- ➤ Memory heap size (in megabytes)

3 In the **Monitors** section, enter the number of monitors for each type, and the update frequency for each monitor.

4 The results and recommendations are displayed in the **Results and Recommendations** section. A difference of 30-40% between the expected results and the actual results should be considered as acceptable.

Supported Monitors and Solution Templates

The following monitors and solution templates are supported by the SiteScope Capacity Calculator:

Monitors

- CPU Monitor
- Database Counter Monitor
- Disk Space Monitor
- DNS Monitor
- Log File Monitor
- Memory Monitor
- Microsoft IIS Server Monitor
- Microsoft SQL Server Monitor
- Microsoft Windows Event Log Monitor
- Microsoft Windows Resources Monitor
- Ping Monitor
- SAP CCMS Monitor
- Script Monitor
- Service Monitor
- Siebel Application Server Monitor
- SNMP by MIB Monitor
- URL Monitor
- WebLogic Application Server Monitor
- WebSphere Application Server Monitor

Solution Templates

- Microsoft Exchange 2003 Solution Template
- Siebel Solution Templates

Sizing SiteScope on Windows Platforms

When sizing SiteScope installed on a Windows platform, you should perform the following sizing steps on SiteScope and on the Windows operating system:

1 Size SiteScope.

We recommend sizing SiteScope first and letting SiteScope run for at least 24 hours before proceeding to the next step. For details, see the procedure "Sizing SiteScope" on page 133.

2 Tune the Windows Operating System.

After sizing SiteScope and waiting at least 24 hours, you need to tune the Windows operating system and then restart the SiteScope server for the parameter changes to take effect. For details, see the procedure "Tuning Microsoft Windows Operating System" on page 134.

3 General Maintenance Recommendations.

In addition, certain general maintenance recommendations should be followed to ensure optimal tuning. For details, see"General Maintenance Recommendations" on page 135.

Important:

- We recommend making backups of any file or parameter that you change, so that it can be restored from that backup if needed.
- If the settings are not effective, do not randomly increase or decrease them. Contact HP Software Support for further analysis and troubleshooting.

Sizing SiteScope

Sizing SiteScope involves checking that monitors use the **Verify error** option only when absolutely necessary. This option should be used on a very small number of monitors, and for monitors with a history of false **no data** alerts due to network issues or server load problems on the remote machine being monitored.

When this feature is enabled, a monitor that fails is immediately run again, bypassing the scheduler before the alert conditions are checked. Large numbers of these extra runs can significantly disrupt the scheduler and cause SiteScope performance to degrade. For monitors failing due to connection problems, verify error can take up to the connection timeout amount of time before the monitor is terminated. During this time, it locks the monitor thread and connection for 2 minutes, by default. This delay can cause other monitors to wait and the failing monitor to skip.

To Size SiteScope:

1 For each monitor, select the **Properties** tab, open the **Monitor Run Settings** panel, and check whether **Verify error** is selected. Clear the check box for monitors that do not require this option.

Tip: For multiple monitors, we recommend using **Global Search and Replace** to perform this task.

---

2 Let SiteScope run for at least 24 hours before tuning the Windows operating system.

Tuning Microsoft Windows Operating System

Tuning Microsoft Windows operating systems involves changing a number of parameters using the Configuration Tool. In addition, certain general maintenance recommendations should be followed to ensure optimal tuning.

To tune Microsoft Windows operating systems:

1 Check that the appropriate Windows Service Pack or Hotfix has been installed on the SiteScope server:

- For Windows 2000, Service Pack 4 must already be installed. For details about increasing file handles on Windows 2000 and for downloading the Service Pack, see http://support.microsoft.com/kb/326591/en-us.
- For Windows XP, Hotfix 327699 must already be installed. For details about increasing file handles on Windows XP and for downloading the Hotfix, see http://support.microsoft.com/kb/327699/en-us.

2 Run the Configuration Tool, and select the **Sizing** option.

This tool increases JVM heap size to 1024 MB, desktop heap size to 2048 MB, and the number of file handles to 18,000. It also disables pop-up warnings for SiteScope executables. For details, see "Running the Configuration Tool" on page 91.

Note: The Configuration Tool supports the default **SiteScope** service name only. If you changed the service name, contact HP Software Support instead of running the Configuration Tool.

---

3 Restart the SiteScope server for the parameter changes to take effect.

General Maintenance Recommendations

Follow these general maintenance recommendations to size SiteScope on Windows.

➤ **Determine appropriate monitor frequency.**

Check the monitor run frequency and ensure that monitors are running at an appropriate interval. For example, most disk monitors do not need to run every 5 minutes. Generally every 15, 30, or even 60 minutes is adequate for all volumes except, perhaps, /var, /tmp, and swap. Reducing monitor frequencies lowers the number of monitor runs per minute, and improves performance and capacity.

➤ **Optimize group structure.**

Group structure should take into account ease of use with SiteScope, and performance optimization for SiteScope. Ideally, the number of top-level groups should be minimized as should the depth of the structure.

Performance can degrade if a group structure has more than 50 top-level groups, or if it is more than 5 levels deep.

➤ **Resolve SiteScope configuration errors.**

Use the health monitors to resolve monitor configuration errors. Even a small number of errors can lead to performance and stability degradation. For more information on resolving these errors, contact HP Software Support.

➤ **Plan the physical location of SiteScope servers.**

SiteScope servers should be physically located as close as possible on the local network to the machines they are monitoring. It is not recommended to monitor over a WAN connection, although in some cases where the connection has sufficient capacity and low latency, this may be acceptable.

Sizing SiteScope on Solaris and Linux Platforms

Sizing SiteScope on Solaris and Linux operating systems involves changing a number of parameters. In addition, certain general maintenance recommendations should be followed to ensure optimal tuning.

1 Tune the Operating System.

Configure the appropriate number of threads for the SiteScope instance and configure the Solaris or Linux operating system parameters. For details, see the procedure "Tuning the Operating System" on page 137.

2 Tune the Java Virtual Machine.

Configure the JVM heap size, thread stack size, and implement parallel garbage collection. For details, see the procedure "Tuning the Java Virtual Machine" on page 139.

3 General Maintenance Recommendations.

In addition, certain general maintenance recommendations should be followed to ensure optimal tuning. For details, see "General Maintenance Recommendations" on page 140.

Tuning the Operating System

Tuning the operating system involves configuring the appropriate number of monitors for the SiteScope instance and configuring the Solaris or Linux operating system parameters.

Configuring the Maximum Number of Running Monitors

You can configure the **Maximum monitor running** setting in **Preferences** > **Infrastructure Preferences** > **Server Settings**. For details, see "Infrastructure Preferences" in the SiteScope Help.

Configuring Solaris or Linux Operating System Parameters

The Solaris or Linux operating system can support large numbers of threads. To enable this feature, perform the following on the SiteScope server.

To configure the Solaris or Linux operating system parameters:

1 Modify the kernel file descriptor limits.

a Edit the **/etc/system** file and add the following line:

```
set rlim_fd_max=8192
```

Note: 1024 is the default (this limit does not apply to user root). The value 8192 is sufficient for even the largest instance of SiteScope. Use this high value rather than experiment with lower values. This avoids the need to restart the machine later if the lower value is not sufficient.

b Restart the server.

2 Modify the user runtime limits.

a In <**SiteScope root directory**>**\bin** directory, add the following line to the SiteScope startup scripts **start-monitor** and **start-service**:

```
ulimit -n 8192
```

b Check that the following parameters have the following minimum values. Contact your UNIX system administrator for more information.

Parameter	Minimum Value
core file size (blocks)	unlimited
data seg size (kbytes)	unlimited
file size (blocks)	unlimited
open files	8192
pipe size (512 bytes)	10
stack size (kbytes)	8192
cpu time (seconds)	unlimited
max user processes	8192
virtual memory (kbytes)	unlimited

You do not need to restart the SiteScope application or the server after modifying the runtime limits.

Tuning the Java Virtual Machine

You should configure the JVM as follows for optimal performance.

To configure the JVM:

1 Increase heap space.

By default, the Java heap space for SiteScope is set to 512 MB. This is insufficient for the normal operation of large instances.

The heap space can be increased up to 1024 MB (this is the recommended heap size for large loads) by modifying **start-service** and **start-monitor** scripts in **<SiteScope root directory>\bin** directory.

2 Decrease thread stack size (-Xss).

Each thread created by SiteScope instantiates a stack with -Xss amount of allocated memory. The default UNIX JRE maximum thread stack size, -Xss, is 512 KB memory per thread.

Unless specified on the Java command line in **<SiteScope root directory>\bin\start-monitor**, the default maximum thread stack size is used. The default size can limit the number of threads by exceeding the available memory.

Instances of 4000 or more monitors can benefit from a -Xss of 128 KB.

General Maintenance Recommendations

There are general maintenance recommendations to size SiteScope on Solaris and Linux platforms.

➤ **Utilize health monitors.**

Utilize health monitors with **Depends on** wherever possible, but especially for all monitors using remote UNIX connections. The health monitor can prevent server performance degradation by detecting if multiple machines become unavailable and lock SSH connection threads.

➤ **Minimize the use of the Verify error feature.**

When the **Verify error** option is enabled in the **Monitor Run Settings** panel, a monitor that fails is immediately run again, bypassing the scheduler before the alert conditions are checked. Large numbers of these extra runs can significantly disrupt the scheduler and cause SiteScope performance to degrade. For monitors failing due to connection problems, verify error can take up to the connection timeout amount of time before the monitor is terminated. During this time, it locks the monitor thread and connection for 2 minutes, by default. This delay can cause other monitors to wait and the failing monitor to skip.

➤ **Use SSH and internal Java libraries.**

Wherever possible, use SSH and Internal Java Libraries option when defining a remote preference with a SSH connection method. Internal Java Libraries is a third-party, Java-based, SSH client. This client significantly improves performance and scalability over Telnet and the host operating system's SSH client. This client supports SSH1, SSH2, Public Key Authentication, and so forth.

In SSH, set **Connection caching enabled**. The **Connection limit** should be adjusted to allow for all monitors running against a particular server to execute in a timely manner.

➤ **Determine appropriate monitor frequency.**

Check the monitor run frequency and ensure that monitors are running at an appropriate interval. For example, most disk monitors do not need to run every 5 minutes. Generally every 15, 30, or even 60 minutes is adequate for all volumes except, perhaps, /var, /tmp, and swap. Reducing monitor frequencies lowers the number of monitor runs per minute, and improves performance and capacity.

➤ **Optimize group structure.**

Group structure should take into account ease of use with SiteScope, and performance optimization for SiteScope. Ideally, the number of top-level groups should be minimized as should the depth of the structure.

Performance can degrade if a group structure has more than 50 top-level groups, or if it is more than 5 levels deep.

➤ **Resolve SiteScope configuration errors.**

Use the health monitors to resolve monitor configuration errors. Even a small number of errors can lead to performance and stability degradation. For more information on resolving these errors, contact HP Software Support.

➤ **Plan the physical location of SiteScope servers.**

SiteScope servers should be physically located as close as possible on the local network to the machines they are monitoring. When monitoring across WAN or slow network links, the network usually becomes the bottleneck. This can require additional time for the monitors to run. It is not recommended to monitor over a WAN connection, although in some cases where the connection has sufficient capacity and low latency, this may be acceptable.

➤ **Use local user accounts.**

Local user accounts are preferred over Directory Service accounts for UNIX Remote Authentication. Local user accounts avoid dependency on a Directory Service server for authentication. This ensures rapid authentication and prevents connection failures if the Directory Service server goes down.

In some cases, very large instances of SiteScope can negatively impact the performance of the Directory Services server. It is recommended that this server be physically close to the servers being monitored.

11

Uninstalling SiteScope

You can uninstall SiteScope from your server machine.

This chapter includes:

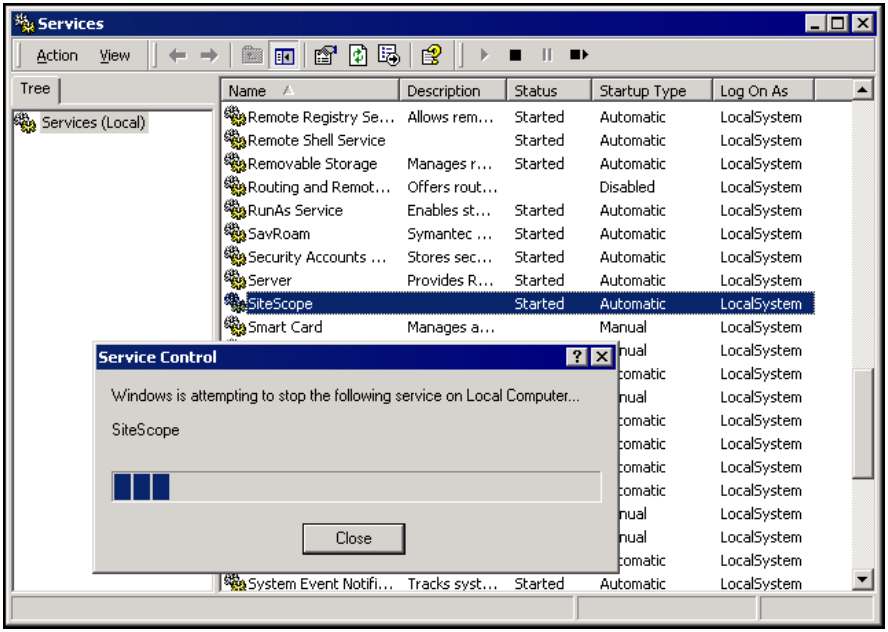
Uninstalling SiteScope on a Windows Platform

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

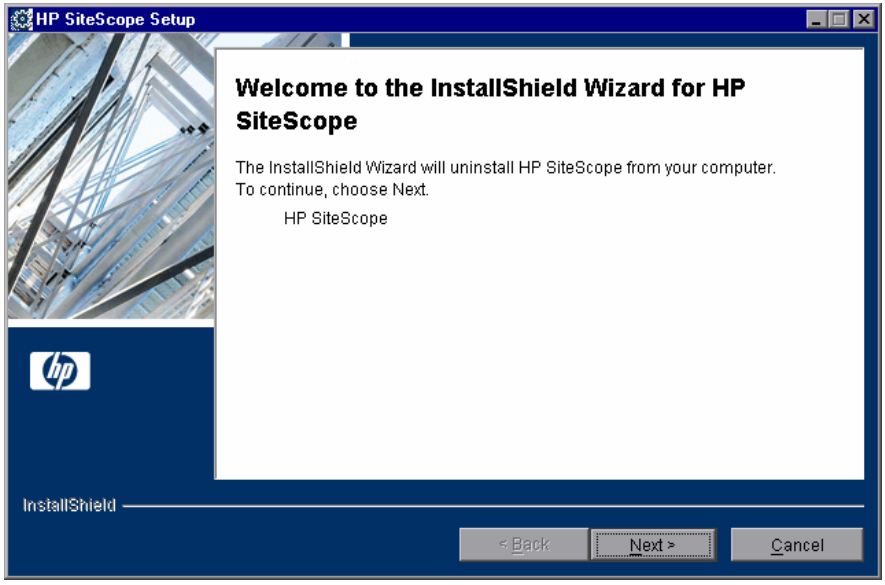
To uninstall SiteScope on a Windows platform:

1 Choose **Start** > **Programs** > **Administrative Tools** > **Services**. The Services dialog box opens.

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.

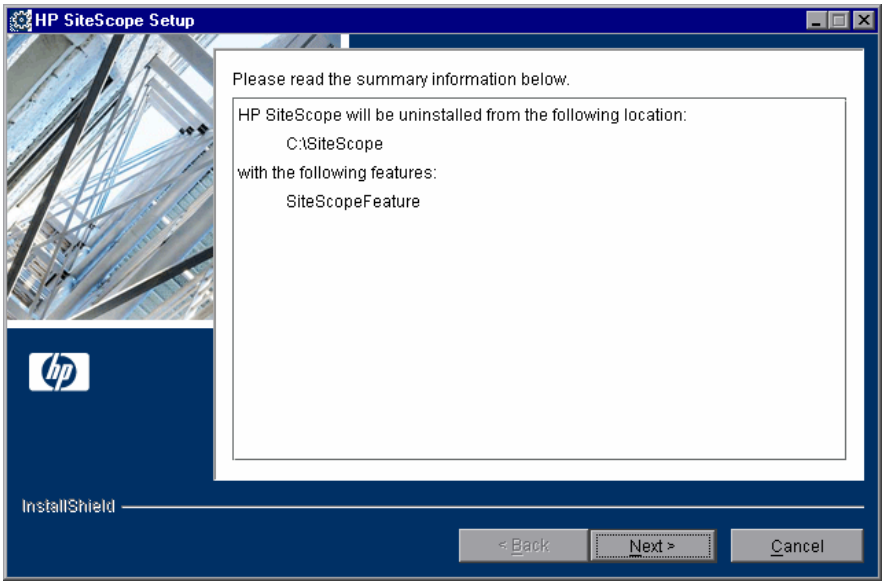


3 Choose **Start** > **Programs** > **HP SiteScope** > **Uninstall HP SiteScope**. The InstallShield Wizard for HP SiteScope begins.



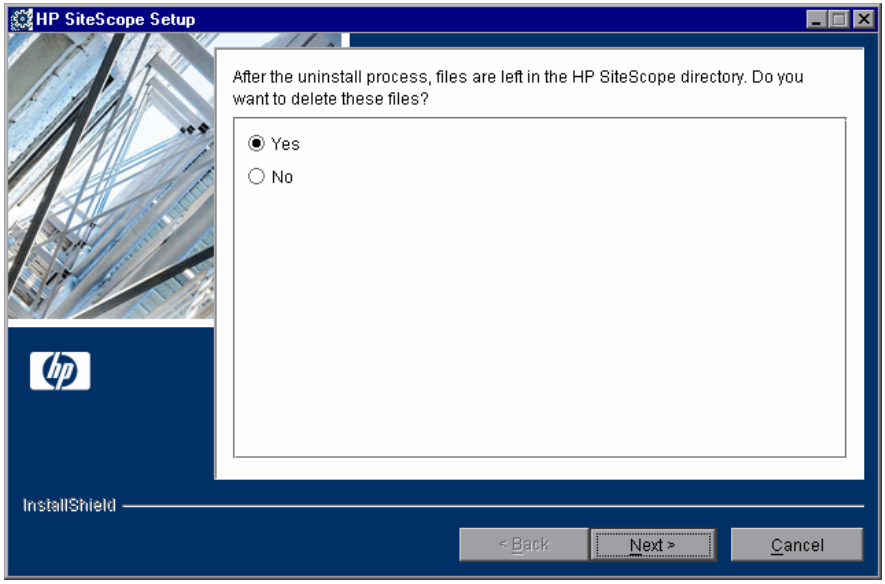
Click **Next** to confirm that you want to uninstall SiteScope.

4 A summary information screen opens.



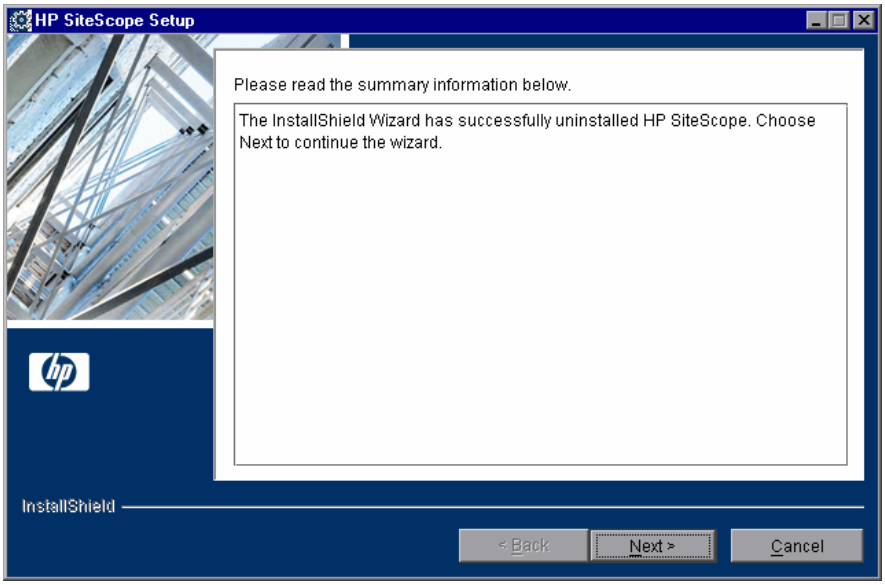
Click **Next** to continue.

5 The uninstall procedure gives the option to delete the HP SiteScope directory files (all files and subdirectories under <**SiteScope root directory**>, but not the root directory itself).



Select an option, and then click **Next** to continue.

6 A screen opens confirming that HP SiteScope was successfully uninstalled.



Click **Next** to complete the uninstall procedure.

7 Restart the server. Failure to restart the server may lead to unexpected problems for other applications.

Uninstalling SiteScope on a Solaris or Linux Platform

For SiteScope running on Solaris or Linux 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.

To uninstall SiteScope on a Solaris or Linux platform:

1. Log in to 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

   At any point during the uninstall procedure, you can return to previous screens to check or change your answers by clicking **Back**.
4. The InstallShield Wizard for HP SiteScope begins. Click **Next** to confirm that you want to uninstall SiteScope.
5. Complete steps 4 - 7 of “Uninstalling SiteScope on a Windows Platform” on page 143.

Part IV

Running SiteScope Securely

12

Hardening the SiteScope Platform

This chapter describes several configuration and set up options that can be used to harden the SiteScope platform.

This chapter includes:

About Hardening the SiteScope Platform

Network and system security has become increasingly important. As a system availability monitoring tool, SiteScope might have access to some system information which could be used to compromise system security if steps are not taken to secure it. You should use the configurations and set up options in this section to protect the SiteScope platform.

Important: There are two Web servers that are active and serving two versions of the SiteScope product interface. To limit all access to SiteScope, you must apply the applicable settings to both the SiteScope Web server and the Apache Tomcat server supplied with SiteScope.

Setting SiteScope User Preferences

SiteScope user profiles are used to require a user name and password in order to access the SiteScope interface. After installation, SiteScope is normally accessible to any user that 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 user name or password defined for it. This is the administrator account. You should define a user name 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. For more information on creating user accounts, see "User Management Preferences" in the SiteScope Help.

Password Encryption

All SiteScope passwords are encrypted using a method called Triple Data Encryption Standard, or TDES. TDES applies the Data Encryption Algorithm on each 64-bit block of text three successive times, using either two or three different keys. As a result, unauthorized users cannot reproduce the original password in a reasonable amount of time.

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 requires that users are authenticated using a certificate. For more information, see "Configuring SiteScope to Use SSL" on page 175.

13

Permissions and Credentials

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

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

Monitor Name	Protocol	User Permissions and Credentials	Notes
Apache Server	HTTP HTTPS	None needed unless required to access the server statistics page.	
BroadVision	Proprietary		
CheckPoint Firewall-1	SNMP	Community string.	This monitor does not support SNMP V3, so the community string passes plain text over the network. The target's SNMP agent may be configured so that the community string can only be used to read a subset of the MIB. The implication for such a configuration is that if an unauthorized person obtained the community string, he would only be able to read OIDs from the agent (but not be able to set them).

Monitor Name	Protocol	User Permissions and Credentials	Notes
Cisco Works	SNMP	Community string or user name/password, depending on SNMP version.	The safest possible configuration for this monitor is running it against an agent configured to use SNMP V3 with authentication (SHA or MD5) and DES encryption for privacy. In this configuration, no unencrypted SNMP data passes over the network. This greatly reduces the risk that a malicious user could compromise the monitored device. It does not take into account security vulnerabilities from implementation bugs in the monitored device's SNMP agent. The riskiest configuration of this monitor is to use SNMP V1 with a community string that has both read and write access on the entire MIB implemented by the agent on the monitored device. In this configuration, a malicious user could obtain the community string by eavesdropping on the network, and then use that community string to reconfigure the device.
Citrix Server	PDH/Perfex	Same as Microsoft ASP Server monitor.	
ColdFusion	Perfex	Same as Microsoft ASP Server monitor.	

Monitor Name	Protocol	User Permissions and Credentials	Notes
COM+	HTTP/ HTTPS		
CPU (Windows)	Perfex	Same as Microsoft ASP Server monitor.	Add the server where SiteScope is running to the Domain Admin group in Active Directory (for Windows 2000 or later). With this option, the SiteScope service is set to log on as a local system account, but the machine where SiteScope is running is added to a group having domain administration privileges. Edit the registry access permissions for all machines in the domain to allow non-admin access. For details on enabling non-admin users to remotely monitor machines with perfmon, see Microsoft Knowledge Base article http://support.microsoft.com/kb/164018/en-us. This option requires changes to the registry on each remote machine that you want to monitor. This means that while the list of servers in the domain includes all machines in the domain, only those whose registry has been modified can be monitored without use of a connection profile.

Monitor Name	Protocol	User Permissions and Credentials	Notes
CPU (Solaris/ Linux)	UNIX/ Linux Shell	Need shell access to the remote server. Supported access protocols are telnet, SSH, and rlogin. It is also necessary for the logged-in user to have permissions to run various executable programs.	It is possible to restrict logged-in users' access by using UNIX group permissions for the various commands that SiteScope would run. A list of the relevant commands for a particular operating system can be found in the **templates.os** files.
Database Counter	JDBC	User credentials are needed to authenticate access to the particular database. Each database has a particular method for providing access control to the particular tables that need to be accessed.	The user needs sufficient permission to execute any specified SQL statements.
Directory	Shell/Perfex	Need shell access to the remote server. Supported access protocols are telnet, SSH, and rlogin. It is also necessary for the logged-in user to have permissions to run various executable programs.	It is possible to restrict logged-in users' access by using UNIX group permissions for the various commands that SiteScope would run. A list of the relevant commands for a particular operating system can be found in the **templates.os** files.
Directory (Windows)	Netbios	Read-only file system access.	Permissions for specific files can be controlled at the operating system level.
Directory (Solaris/ Linux)	File System Access	Read-only file system access to the particular files.	Permissions for specific files can be controlled at the operating system level.
Disk Space (Windows)	Perfex	Same as Microsoft ASP Server monitor.	For Windows 2000, disk counters must be enabled in perfex.

Monitor Name	Protocol	User Permissions and Credentials	Notes
Disk Space (Solaris/ Linux)	Shell	Need shell access to the remote server. Supported access protocols are telnet, SSH, and rlogin. It is also necessary for the logged-in user to have permission to run various executable programs.	It is possible to restrict logged-in users' access by using UNIX group permissions for the various commands that SiteScope would run. A list of the relevant commands for a particular operating system can be found in the **templates.os** files.

Monitor Name	Protocol	User Permissions and Credentials	Notes
F5 Big-IP	SNMP	Community string or user name/password depending on SNMP version.	The safest possible configuration for this monitor is running it against an agent configured to use SNMP V3 with authentication (SHA or MD5) and DES encryption for privacy. In this configuration, no unencrypted SNMP data passes over the network. This greatly reduces the risk that a malicious user could compromise the monitored device. It does not take into account security vulnerabilities from implementation bugs in the monitored device's SNMP agent. The riskiest configuration of this monitor is to use SNMP V1 with a community string that has both read and write access on the entire MIB implemented by the agent on the monitored device. In this configuration, a malicious user could obtain the community string by eavesdropping on the network, and then use that community string to reconfigure the device.
File (Windows)	Netbios	Windows permissions for read-only access to log file.	

Monitor Name	Protocol	User Permissions and Credentials	Notes
File (Solaris/ Linux)	File System Access	Read-only file permission to the target file system.	
FTP	FTP	Valid user name and password for the FTP site with read-only permission to copy the user-specified file. The customer site may allow anonymous logon.	
LDAP	LDAP	Valid user name and password on the LDAP server to do simple authentication. Query or search operations require appropriate permissions. Anonymous authentication also supported in version 7.9.	
Link Check	HTTP/ HTTPS	None needed unless the HTTP/HTTPS site requires a user name/password.	User needs sufficient permission to click on links.
Log File (Windows)	Netbios	Windows permissions for read-only access to log file.	

Monitor Name	Protocol	User Permissions and Credentials	Notes
Log File (Solaris/ Linux)	Shell	Need shell access to the remote server. Supported access protocols are telnet, SSH, and rlogin. It is also necessary for the logged-in user to have permissions to run various executable programs. Read-only file permissions to the target file system.	It is possible to restrict logged-in users' access by using UNIX group permissions for the various command that SiteScope would run. A list of the relevant commands for a particular operating system can be found in the **templates.os** files.
Mail	SMTP	A valid email account and password.	
MAPI	MAPI	User name/password of one or two email accounts to send and receive test emails.	SiteScope must run as local administrator on the SiteScope server. Test email accounts must have local administrator authority in the SiteScope server.
Memory (Windows)	Perfex	Same as Microsoft ASP Server monitor.	
Memory (Solaris/ Linux)	Shell	Need shell access to the remote server. Supported access protocols are telnet, SSH, and rlogin. It is also necessary for the logged-in user to have permissions to run various executable programs.	It is possible to restrict logged-in users' access by using UNIX group permissions for the various commands that SiteScope would run. A list of the relevant commands for a particular operating system can be found in the **templates.os** files.

Monitor Name	Protocol	User Permissions and Credentials	Notes
Microsoft ASP Server	Perfex	Monitoring performance objects on Windows requires that a user have specific access permissions as described in the Microsoft Knowledge Base for article http://support.microsoft.com/kb/300702/en-us and article http://support.microsoft.com/kb/164018/en-us. These articles describe the permissions and security policies that should be granted to the user on the monitored server.	**Perfmon User.** A user that was granted the required privileges to be able to monitor performance objects on Windows servers. **Note:** The **Performance Monitor Users** (on Windows 2000 and Windows 2003), **Power Users**, and **Administrators** groups on Windows servers are already associated with the set of permissions and security policies that are required for a Perfmon User. In other words, any user that belongs to these groups has all required permissions to monitor the performance objects and automatically becomes a Perfmon User. The **Performance Monitor Users** group contains the exact set of privileges whereas the **Power Users** and **Administrators** groups are associated with multiple additional privileges that are not required for performance monitoring.

Monitor Name	Protocol	User Permissions and Credentials	Notes
Microsoft ASP Server (continued)	Perfex (continued)		**SiteScope User.** The user that the SiteScope service logs on as. For SiteScope monitors to be able to collect perfmon data from remote servers, connections must be established to these servers using the credentials of a user defined as a Perfmon User. These connections can be established with the following options: Configure the SiteScope user to be a domain user that is also a user on the remote machines. In the case that the SiteScope User is not defined as a Perfmon User on remote machines, a Remote NT object must be configured in SiteScope using the credentials of a user that is defined as a Perfmon User on the remote machine. Monitors are then configured to use the Remote NT object.
Microsoft IIS Server	Perfex	Same as Microsoft ASP Server monitor.	
Microsoft SQL Server	Perfex	Same as Microsoft ASP Server monitor.	

Monitor Name	Protocol	User Permissions and Credentials	Notes
Microsoft Windows Dialup	MODEM	User name/password to the ISP account being contacted. The account needs sufficient authority to execute its specified test monitors.	
Microsoft Windows Event Log	Perfex	Same as Microsoft ASP Server monitor.	
Microsoft Windows Media Player	File System Access	Read-only file permission to the target file system.	
Microsoft Windows Media Server	Perfex	Same as Microsoft ASP Server monitor.	
Microsoft Windows Performance Counter	Perfex	Same as Microsoft ASP Server monitor.	
Microsoft Windows Resources	PDH	Same as Microsoft ASP Server monitor.	

Monitor Name	Protocol	User Permissions and Credentials	Notes
Network Bandwidth	SNMP	Community string or user name/password depending on SNMP version.	The safest possible configuration for this monitor is running it against an agent configured to use SNMP V3 with authentication (SHA or MD5) and DES encryption for privacy. In this configuration no unencrypted SNMP data passes over the network. This greatly reduces the risk that a malicious user could compromise the monitored device. It does not take into account security vulnerabilities from implementation bugs in the monitored device's SNMP agent. The riskiest configuration of this monitor is to use SNMP V1 with a community string that has both read and write access on the entire MIB implemented by the agent on the monitored device. In this configuration, a malicious user could obtain the community string by eavesdropping on the network, and then use that community string to reconfigure the device.

Monitor Name	Protocol	User Permissions and Credentials	Notes
News	NNTP	A valid user name and password if the news server requires it, with read-only permission to query total number of messages in the news groups.	
Oracle 9i Application Server	HTTP/ HTTPS		
Oracle Database	JDBC	An Oracle user logs in with the ability to execute all the SQL statements found in <**SiteScope root directory**>\ **templates.applications**\ **commands.oraclejdbc**.	
Ping	ICMP	N/A	
Port	TCP	N/A	
Radius	Radius	A valid user name and password on the Radius server. No other permissions are needed.	SiteScope's IP must be added to the list of servers allowed to communicate with the Radius server. It must also be configured to do PAP authentication.
Real Media Player	File System Access	Read-only file permission on the target file system.	
Real Media Server	Perfex	Same as Microsoft ASP Server monitor.	
SAP CCMS	Proprietary	XMI authorization.	Profiles that have XMI authorization are S_A.SYSTEM, PD_CHICAGO, S_WF_RWTEST, and SAP_ALL.

Monitor Name	Protocol	User Permissions and Credentials	Notes
SAP CCMS Alert	Proprietary		
SAP Performance or SAP Work Processes	Proprietary	Still being researched.	
Script (Windows)	Remote shell	Same as Microsoft ASP Server monitor.	
Script (Solaris/ Linux)	Shell	Need shell access to the remote server. Supported access protocols are telnet, SSH, and rlogin. It is also necessary for the logged-in user to have permissions to run various executable programs.	It is possible to restrict logged-in users' access by using UNIX group permissions for the various commands that SiteScope would run. A list of the relevant commands for a particular operating system can be found in the **templates.os** files.
Script on local machine (Solaris, Linux, and Windows)	File System Access/ Perfex	Read-only file permission to the target file system.	
Service (Windows)	Perfex	Same as Microsoft ASP Server monitor.	
Service (Solaris/ Linux)	Shell	Need shell access to the remote server. Supported access protocols are telnet, SSH, and rlogin. It is also necessary for the logged-in user to have permissions to run various executable programs.	It is possible to restrict logged-in users' access by using UNIX group permissions for the various commands that SiteScope would run. A list of the relevant commands for a particular operating system can be found in the **templates.os** files.

Monitor Name	Protocol	User Permissions and Credentials	Notes
Siebel Application Server (previously Siebel Server Manager)	CmdLine	User account must have Siebel Administrator Responsibility privileges to issue Siebel server manager (srvrmgr) commands.	If the srvrmgr client is remote, then a Remote (Windows or UNIX) must be set up with the appropriate user name and password credentials for executing the remote srvrmgr command.
Siebel Log	File System Access	File read-only permission to the target Siebel server file system.	
Siebel Web Server	HTTP/ HTTPS	User name and password are needed if target Siebel Extensions Page is behind third-party, HTML, form-based authentication software.	User must have permission to retrieve the Siebel SWE page.

Monitor Name	Protocol	User Permissions and Credentials	Notes
SNMP	SNMP	Community string or user name/password, depending on the SNMP version.	The safest possible configuration for this monitor is running it against an agent configured to use SNMP V3 with authentication (SHA or MD5) and DES encryption for privacy. In this configuration, no unencrypted SNMP data passes over the network. This greatly reduces the risk that a malicious user could compromise the monitored device. It does not take into account security vulnerabilities from implementation bugs in the monitored device's SNMP agent. The riskiest configuration of this monitor is to use SNMP V1 with a community string that has both read and write access on the entire MIB implemented by the agent on the monitored device. In this configuration, a malicious user could obtain the community string by eavesdropping on the network, and then use that community string to reconfigure the device.

Monitor Name	Protocol	User Permissions and Credentials	Notes
SNMP by MIB	SNMP	Community string or user name and password, depending on the SNMP version.	The safest possible configuration for this monitor is running it against an agent configured to use SNMP V3 with authentication (SHA or MD5) and DES encryption for privacy. In this configuration, no unencrypted SNMP data passes over the network. It greatly reduces the risk that a malicious user could compromise the monitored device. It does not take into account security vulnerabilities from implementation bugs in the monitored device's SNMP agent. The riskiest configuration of this monitor is to use SNMP V1 with a community string that has both read and write access on the entire MIB implemented by the agent on the monitored device. In this configuration, a malicious user could obtain the community string by eavesdropping on the network, and then use that community string to reconfigure the device.

Monitor Name	Protocol	User Permissions and Credentials	Notes
SNMP Trap	SNMP	None, although permissions to configure agents on the network to send traps to SiteScope are required. SiteScope must be running as a privileged user so that it can bind to port 162, a reserved port.	The security risk associated with SNMP V1 and V2 traps is that a malicious user could eavesdrop on the data that is passed in the traps. Using V3 traps with authentication and privacy greatly reduces the chance that data can be used maliciously by eavesdroppers.
SunONE	HTTP/ HTTPS	None, unless using a proxy that requires authentication.	
Tuxedo	Proprietary	PeopleSoft Tuxedo comes with two preconfigured users, **PS** and **VP**, that are monitor-only accounts. No other user can be created or used for SiteScope monitoring.	
URL	HTTP/ HTTPS	None needed for SiteScope. The server may require a valid user name and password.	
URL Content	HTTP/ HTTPS	None needed for SiteScope. The server may require a valid user name and password.	
URL List	HTTP/ HTTPS	None needed for SiteScope. The server may require a valid user name and password.	

Monitor Name	Protocol	User Permissions and Credentials	Notes
URL Sequence	HTTP/ HTTPS	None needed for SiteScope. The server may require a valid user name and password.	
Web Server	Perfex	Same as Microsoft ASP Server monitor.	
Web Server (Solaris, Linux, and Windows)	File System Access	Read-only file permission to the target file system.	
Web Service	HTTP/ HTTPS	Supports basic, digest, and NTLM authentication if required by the target Web service.	
WebLogic Application Server 5.x	SNMP	Community string credential must match the string in the SNMP agent.	
WebLogic Application Server 6.x and above	RMI	Requires a user that belongs to a group with at least monitor role privilege.	
WebSphere Application Server 3.5x	RMI		
WebSphere Application Server 4.5	RMI	Requires a user that belongs to a group with at least monitor role privilege.	
WebSphere Application Server 5.x (SOAP over HTTP)	HTTP/ HTTPS	Requires a user that belongs to a group with at least monitor role privilege.	

Monitor Name	Protocol	User Permissions and Credentials	Notes
WebSphere MQ Status	Proprietary	SiteScope account must be a member of mqm group in the MQ Windows server. In MQ UNIX, the server connection channel used must not require SSL authentication.	
WebSphere Performance Servlet	HTTP/ HTTPS	HTTP authentication via user name and password to the URL of the servlet. Credentials can be customized by the user.	

14

Configuring SiteScope to Use SSL

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

This chapter includes:

About Using SSL in SiteScope

You set a SiteScope server to support SSL by configuring the Web server used to serve 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: To limit all access to SiteScope to HTTPS client connections, you must configure both the SiteScope Web server and the Tomcat server supplied with SiteScope 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 the **<SiteScope install path>\SiteScope\java\bin** directory.

Important: When you create, request, and install a digital certificate, make a note of the parameters and command line arguments that you use in each step of the process. It is very important that you use the same values throughout the procedure.

You can find out more about Keytool at http://java.sun.com/j2se/1.3/docs/tooldocs/win32/keytool.html.

This section includes the following topics:

Using a Certificate from a Certificate Authority

You can use a digital certificate issued by a Certificate Authority. 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 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 root directory**>**groups** directory. You can delete it or simply move it to a different directory.
2. Create a key pair by running the command line listed below from the <**SiteScope root directory**>**java****bin** directory.

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 creates a file called **serverKeystore** in the <**SiteScope root directory**>**groups** directory. SiteScope uses this file to store the certificates used in your secure sessions. Make sure you keep a backup copy of this file in another location.

Guidelines and Limitations

- 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)

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

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

2. To change SiteScope to use a secure connection, you need to add or modify certain settings or configuration files in SiteScope. For details, see "Configuring SiteScope for SSL" on page 180.

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 root directory**>**groups** directory. You can delete it or simply move it to a different directory.
2. Run the following command from the <**SiteScope root directory**>**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 root directory**>**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. For details, see "Configuring SiteScope for SSL" on page 180.

Configuring SiteScope for SSL

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

1 Open the **server.xml** file that is located in the <**SiteScope root directory**>**Tomcat****conf** directory.

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.

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

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

https://<sitescope_server>:8443/sitescope

Part V

Getting Started and Accessing SiteScope

15

Post-Installation Administration

This section includes recommended steps you should perform following SiteScope installation.

This chapter includes:

Post-Installation Administration Checklist

Use this checklist to review the administration tasks you should perform after installing SiteScope.

✔	Step
	Register for SiteScope support. For more information, see "Getting Started Roadmap" on page 17.
	Log in to the SiteScope Web interface using a Web browser. For more information, see "Connecting to SiteScope" on page 190.
	If you are upgrading to SiteScope 10.10 from an earlier version of SiteScope, use the Configuration Tool to transfer monitor and group configuration data from the older SiteScope installation to the new installation. For more information on using the Configuration Tool, see "Running the Configuration Tool" on page 91 (for Windows) or "Running the Configuration Tool" on page 121 (for Solaris or Linux) of the SiteScope Help.
	If you did not enter your SiteScope license information during installation, enter it in the General Preferences page, as described in "General Preferences" of the SiteScope Help. New installations operate with a 10 day evaluation license. For license details, see "SiteScope Licenses" on page 33.

✔	Step
	Create a user name and password for the SiteScope administrator account. This is the default account that is active when the product is installed. It has full privileges to manage SiteScope and is the account that all users who access the product use unless you restrict the account. Create and configure other user accounts based on the requirements of the organization. For details, see "User Management Preferences" in the SiteScope Help. If no user name and password are defined for the administrator user, SiteScope skips the Login page and logs in automatically.
	Configure the SiteScope Email Preferences email server with an administrators email address and specify a mail server that SiteScope can use to forward email messages and alerts to users. For details, see "Email Preferences" in the SiteScope Help.
	Configure connection profiles for the remote servers you want to be able to monitor. Specify the connection method to use in accordance with your security requirements. For details, see "Configure SiteScope to Monitor a Remote Microsoft Windows Server" and "Configure SiteScope to Monitor a Remote UNIX Server" in the SiteScope Help.
	If necessary, adjust Log Preferences to set how many days of monitor data are retained on the SiteScope server. By default, SiteScope deletes logs older than 40 days. If you plan to have monitor data exported to an external database, prepare the database, the necessary drivers, and configure the Log Preferences as applicable. For details, see "Log Preferences" in the SiteScope Help.
	Install middleware drivers for connectivity with remote databases and applications for those monitors that require drivers.
	Configure SiteScope to report to HP Business Availability Center. For details, see "Configuring the Integration" in the SiteScope Help.
	Outline group and monitor organization based on the requirements and constraints identified in your assessment of the business system infrastructure.
	Create and develop templates to help speed the deployment of monitoring using standardized group structure, naming conventions, and configuration settings. For details, see "SiteScope Templates" in the SiteScope Help.

✔	**Step**
	Build dependencies between groups and key monitors to help control redundant alerting. For details, see “Manage a Group – Workflow” in the SiteScope Help.
	Roll out SiteScope to business stakeholders and system administrators.

Once the SiteScope system is up and running with defined users and incoming monitor data, begin the process of educating business and systems users on how to access and use SiteScope reporting and alerting functionality.

16

Getting Started with SiteScope

This chapter explains how to start and stop the SiteScope service, and how to log on to SiteScope for the first time.

This chapter includes:

About Starting the SiteScope Service

The SiteScope process is started on all platforms during installation.

- On Windows platforms, SiteScope is added as a service that is set to restart automatically if the server is rebooted.
- On Solaris and Linux platforms, whenever you reboot the server where SiteScope is installed, you must restart the SiteScope process.

  You can start and stop the SiteScope process manually as necessary using the steps described in this section.

Starting and Stopping the SiteScope Service on Windows Platforms

SiteScope is installed as a service on Microsoft Windows platforms. By default, the SiteScope Service is set to restart automatically whenever the server is rebooted. You can start and stop the SiteScope service manually by using the Services control panel.

To start or stop the SiteScope service using Services control panel:

1. Open the Services control panel by selecting **Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Services**.
2. Select **SiteScope** in the list of services and right-click to display the action menu.
3. Select **Start** or **Stop** as applicable from the action menu.

Netstart and Netstop Commands

You can also start and stop the SiteScope service by using the netstart and netstop commands.

To start the SiteScope service using netstart:

1. Open a command line window on the server where SiteScope is installed.
2. Run the netstart utility using the following syntax:

```
net start SiteScope
```

To stop the SiteScope service using netstop:

1. Open a command line window on the server where SiteScope is running.
2. Run the netstop utility using the following syntax:

```
net stop SiteScope
```

Starting and Stopping the SiteScope Service on Solaris and Linux Platforms

You can start and stop SiteScope manually by using the shell scripts supplied with the product. You can automatically restart SiteScope when a server is rebooted by using an init.d script.

To start the SiteScope process on Solaris and Linux:

1. Open a terminal window on the server where SiteScope is installed.
2. Run the start command shell script using the following syntax:

   <installpath>/SiteScope/start

To stop the SiteScope process on Solaris and Linux:

1. Open a terminal window on the server where SiteScope is running.
2. Run the stop command shell script using the following syntax:

   <installpath>/SiteScope/stop

   In each of the commands above, replace <installpath> with the path where SiteScope is installed. For example, if you installed SiteScope in the /usr directory, the command to stop SiteScope would be:

   /usr/SiteScope/stop

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.

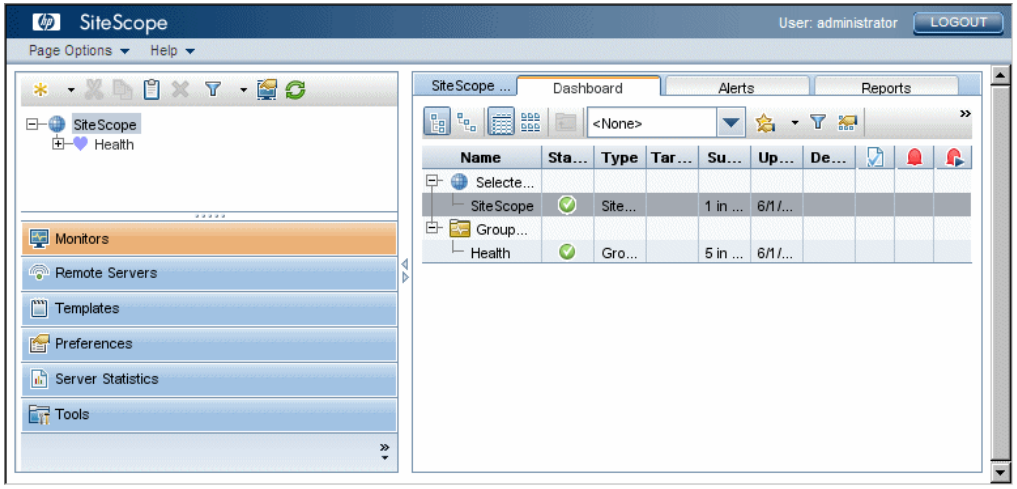
On Windows platforms, the installation process also adds a link to this file in the **Start** > **Programs** menu for SiteScope. The Start menu folder is selected during the installation procedure.

Accessing SiteScope

To access SiteScope, enter the SiteScope address in a Web browser. The default address is: http://localhost:8080/SiteScope.

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



Note:

- To restrict access to this account and its privileges, you need to edit the administrator account profile to include a user login name and login password. SiteScope then displays a login dialogue before SiteScope can be accessed. For information on editing the administrator account profile, see "User Management Preferences" in the SiteScope Help.
- When viewing SiteScope from another machine, it is recommended to use a machine that has Java Runtime Environment (JRE) 6u10 installed.

SiteScope Classic Interface

The SiteScope Classic interface that was available in earlier versions of SiteScope using the URL http://<sitescope_host>:8888, is no longer available for managing SiteScope.

You can still access specific pages in the Classic interface if they are listed in the **_serverFilter** property in the **master.config** file. Pages listed by default include the Monitor Summary and Alert Report pages. If pages are not listed, you can add them to the file. For example, _serverFilter=manage;progress allows access to the Manage Group/Monitor page and the Progress page.

Note: You should not remove SiteScope Classic interface pages that are enabled by default, as this may cause some functionality to fail.

Troubleshooting and Limitations

This section contains troubleshooting and limitations for the following issues when logging on to SiteScope:

- "SiteScope does not start and "Several Java Virtual machines running in the same process caused an error" is displayed" on page 192
- "SiteScope does not start and an error message is displayed" on page 193
- "The SiteScope menu bar opens but the applet fails to start, and you see a blank screen or an "x" image" on page 193

SiteScope does not start and "Several Java Virtual machines running in the same process caused an error" is displayed

This is a known Java defect (http://bugs.sun.com/view_bug.do?bug_id=6516270) that might occur when using Internet Explorer 7.

Possible solution 1: Use a browser other than Internet Explorer 7.

Possible solution 2: Upgrade to Java Runtime Environment 6u10 or later.

Possible solution 3: In the Add or Remove Programs dialog box (**Start** > **Control Panel** > **Add or Remove Programs**), remove all Java/Java Runtime Environment installations except for the latest version.

SiteScope does not start and an error message is displayed

If you encounter an error message such as "The Java Runtime Environment cannot be loaded", or any other unknown error while starting the SiteScope applet, perform the steps below.

After each step, try to reopen SiteScope. If SiteScope fails again, proceed to the next step.

1. Close all the browser's windows.
2. End all remaining browser processes (if any remained) using Windows Task Manager.
3. Clean the local Java applet cache. Select **Start** > **Control Panel** > **Java**, and in the **General** tab, click **Delete Files** and then click **OK**.
4. Clean the local Java applet cache by deleting the content of the following folder: C:\Documents and Settings\<user_name>\Application Data\Sun\Java\Deployment\cache.

The SiteScope menu bar opens but the applet fails to start, and you see a blank screen or an "x" image

This may occur if the Java control panel is not configured to use the Web browser.

Possible solution:

1. Click **Start** > **Control Panel** > **Java**, and in the Java Control Panel, click the **Advanced** tab.
2. Expand the **Default Java for browsers** folder (or **<APPLET> tag support** if you are using Java 5), and make sure that **Microsoft Internet Explorer** and **Mozilla family** is selected.
3. Click **Apply** and then click **OK**.

Part VI

Appendixes

A

Integrating IIS with SiteScope's Tomcat Server

To integrate Internet Information Server (IIS) with the Apache Tomcat server included with SiteScope, you need to make changes to the configuration files used by the Apache Tomcat server and create the virtual directory in the corresponding Web site object in the IIS configuration.

This chapter includes:

Configuring the Apache Tomcat Server Files

To enable IIS integration with the Apache Tomcat server, you must edit the configuration files for the Apache Tomcat server included with SiteScope.

To configure the Apache Tomcat server files:

1. Download the latest version of Java Connector jk from the Apache download site for connector files (http://tomcat.apache.org/download-connectors.cgi).
2. Copy the **isapi_redirect.dll** file to the **<Tomcat installation>\bin\win32** directory. By default, a Tomcat server is installed as part of the SiteScope installation at **C:\SiteScope\Tomcat**. Create the **win32** directory if it does not exist.

3 Perform one of the following:

➤ Create a configuration file in the same directory as the **isapi_redirect.dll** file, and name it **isapi_redirect.properties**. This is an example of the file:

```
# Configuration file for the Jakarta ISAPI Redirector

# The path to the ISAPI Redirector Extension, relative to the website
# This must be in a virtual directory with execute privileges
extension_uri=/jakarta/isapi_redirect.dll

# Full path to the log file for the ISAPI Redirector
log_file=C:\SiteScope\Tomcat\logs\isapi.log

# Log level (debug, info, warn, error or trace)
log_level=info

# Full path to the workers.properties file
worker_file=C:\SiteScope\Tomcat\conf\workers.properties.minimal

# Full path to the uriworkermap.properties file
worker_mount_file=C:\SiteScope\Tomcat\conf\uriworkermap.properties
```

This configuration points to the log file, which is recommended to put under the <**SiteScope root directory**>**Tomcat****logs** directory, and the worker and worker mount files, which should be stored under the <**SiteScope root directory**>**Tomcat****conf** directory.

➤ Add the same configuration entries (see above) to the registry at path: HKEY_LOCAL_MACHINE\SOFTWARE\Apache Software Foundation\Jakarta Isapi Redirector\1.0

4 Create the SiteScope workers file, named **workers.properties.minimal**, under the <**SiteScope root directory**>**Tomcat****conf** directory. This is an example of the SiteScope workers file:

```
# workers.properties.minimal -
#
# This file provides minimal jk configuration
# properties needed to
# connect to Tomcat.
#
# Defining a worker named ajp13w and of type ajp13
# Note that the name and the type do not have to
# match.
worker.list=ajp13w
worker.ajp13w.type=ajp13
worker.ajp13w.host=localhost
worker.ajp13w.port=8009
#END
```

Note: If IIS and Tomcat are not on the same machine, change the host attribute in **workers.properties.minimal** to point to the other machine.

---

5 Create the SiteScope workers mount file under the <**SiteScope root directory**>**Tomcat****conf** directory. This is the example of SiteScope's worker mount file, named **uriworkermap.properties**, as in the configuration example above:

```
# uriworkermap.properties - IIS
#
# This file provides sample mappings for example:
# ajp13w worker defined in workermap.properties.minimal
# The general syntax for this file is:
# [URL]=[Worker name]
/SiteScope=ajp13w
/SiteScope/*=ajp13w
#END
```

The new syntax combines the two rules for SiteScope into one rule:
/SiteScope|/*=ajp13w

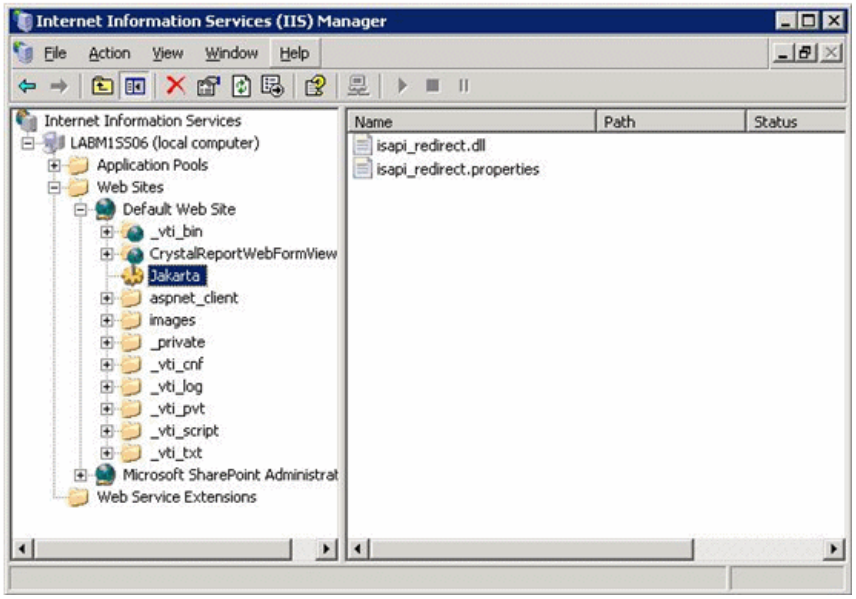
Configuring IIS

After you make changes to the configuration files used by the Tomcat server, you need to create the virtual directory in the corresponding Web site object in the IIS configuration.

To configure IIS:

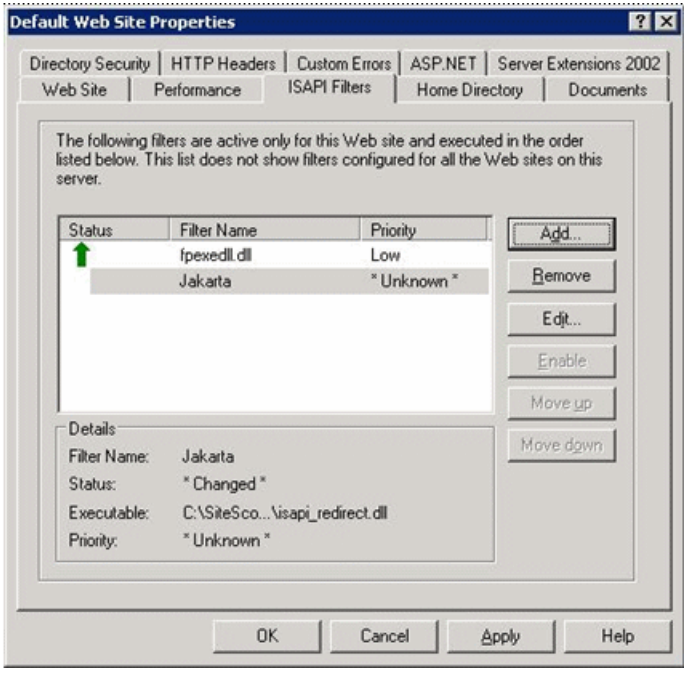
1 From the Windows Start menu, click **Settings** > **Control Panel** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.

2 In the right pane, right-click **<Local Computer name>\Web Sites\<Your Web Site name>**, and click **New\Virtual Directory**. Rename it **Jakarta**, and set **local path** to the directory with **isapi_redirect.dll**.



3 Right click **<Your Web Site name>** and click **Properties**.

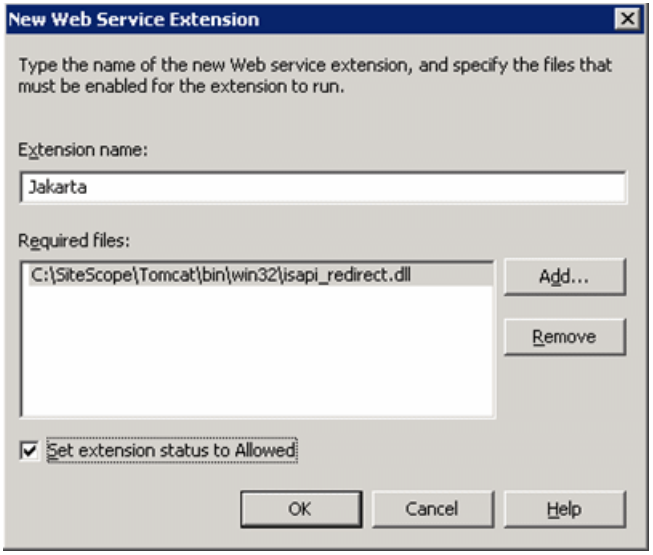
4 Click the **ISAPI Filters** tab, and then click **Add**. In the **Filter Name** column, select **Jakarta**, and browse to **isapi_redirect.dll**. The filter is added, but at this stage it is still inactive.



Click **Apply**.

5 Right-click **<Local Machine name>\Web Service extensions** and click **Add new Web Service Extension**. The New Web Service Extension dialog box opens.

6 In the **Extension name** box, enter the name Jakarta, and under **Required files** browse to the **isapi_redirect.dll** file. Select **Set Extension Status to Allowed**.



Click **OK**.

7 Restart the IIS Web Server, and try to access the application through the Web Service.

B

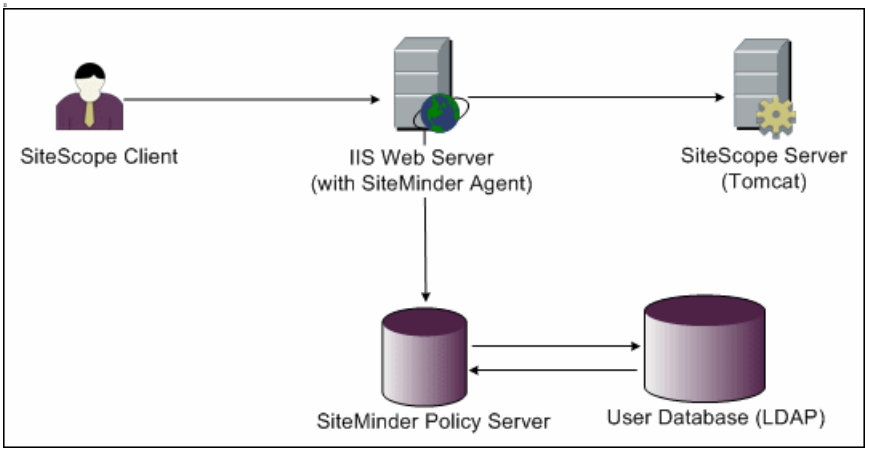
Integrating SiteScope with SiteMinder

SiteScope can be integrated with SiteMinder, a security access management solution, to leverage customer's user and access management configurations.

This chapter includes:

Understanding Integration with SiteMinder

The following diagram illustrates how SiteScope integrates with SiteMinder to authenticate and authorize SiteScope users.



In this architecture, a SiteMinder agent is configured on the IIS Web server which is placed in front of SiteScope's Tomcat application server. The SiteMinder agent must reside on a Web server. The IIS Web server is connected to the SiteMinder policy server that manages all SiteScope users (over a LDAP or any other similar repository).

The SiteMinder agent intercepts all SiteScope's related traffic, and checks the user's credentials. The user's credentials are sent to the SiteMinder policy server for authentication and authorization. If SiteMinder authenticates the user, it sends SiteScope a token (via a special HTTP header) that describes the exact user that managed to log in and pass SiteMinder's authorization.

Note: It is recommended that the SiteScope client, IIS Web server, and the SiteScope's Tomcat application server are configured on the same machine.

Integration Requirements

This section displays the system requirements for integrating SiteScope with SiteMinder.

Operating System	Windows 2000, Windows 2003 Standard/Enterprise SP1
Web Server	IIS 5.0, IIS 6.0
Application Server	Tomcat 5.0.x
Java Connector	Java Connector jk-1.2.21 or later

The Integration Process

This section describes the SiteMinder integration process.

To integrate SiteScope with SiteMinder:

1 Prepare and configure the SiteMinder Policy Server.

Your SiteMinder administrator needs to prepare the SiteMinder policy server for installing the Web agent, install the Web agent on the IIS Web server, and configure the Web agent.

In addition, your SiteMinder administrator needs to configure the SiteMinder policy server. For the recommended SiteMinder configuration details, see "Configuring the SiteMinder Policy Server" on page 206.

2 Configure SiteScope for using SiteMinder.

To enable SiteScope to integrate with SiteMinder, you need to make changes to the configuration files used by the Tomcat server. For details, see "Configuring the Apache Tomcat Server Files" on page 197.

3 Configure IIS.

You need to create the virtual directory in the corresponding Web site object in the IIS configuration. For details, see "Configuring IIS" on page 200.

4 Define permissions for the different SiteScope roles.

After you enable the SiteMinder integration, you must define the permissions for the different roles in SiteScope. For details, see "Defining Permissions for the Different SiteScope Roles" on page 209.

Configuring the SiteMinder Policy Server

You configure the SiteMinder policy server by creating a SiteScope realm object, two SiteScope rules objects for authentication and forwarding the cookie with additional attributes, a SiteScope response object that transfers the additional LDAP attributes to SiteScope, and by adding SiteScope rules and responses to the Security policy object.

Before creating a SiteScope realm object on the policy server, make sure that:

- A special administrator above a domain (that in turn is bound to one or more User Directories) has been configured.
- One or more User Directories objects have been configured. These objects represent the users in the LDAP directory, or any other repository.
- You have defined an authentication scheme.

A domain is connected to one or more of User Directory objects. There is no need to create a special domain for the realm. You can use an existing domain.

To configure the SiteMinder policy server:

1. Log on to SiteMinder Administration.
2. Create a realm and enter the following information:
   - **Name.** Enter a name for the realm. For example, **SiteScope realm**.
   - **Resource Filter.** Enter **/SiteScope**. Everything under SiteScope is part of our realm.

3 Right-click the new realm and click **Create rule under realm**.

- Create a rule for authentication purposes. Enter a meaningful name for the rule, such as **SiteScope rule**. In the **Action** section, select the **Web Agent Action** option and choose all HTTP request schemes (**Get**, **Post** and **Put**).
- Create a second rule for forwarding cookies and other attributes to SiteScope. Enter a meaningful name for the rule, such as **Users role**. In the **Action** section, select the **Authentication events** option and select **OnAuthAccept** from the drop-down list.

4 Create a SiteScope response object to transfer the additional LDAP attributes to SiteScope with the relevant authentication information.

a Right-click **Responses** to open the Response Properties window.

b Enter a meaningful name for the Response. For example, **SiteScope Role**.

c Under the **Attribute List** section, click the **Create** button to open a new window to configure an attribute list.

d In the **Attribute Kind** section, select the **User Attribute** option.

e In the **Attribute Fields** section, choose **SITESCOPE_ROLE** as a variable name, and choose the attribute name to be the chosen field from the predefined User Directory to be sent in the header to SiteScope. This is the User Directory attribute to be sent upon authentication.

Note: If you are using LDAP group objects or a nested group object to define the SiteScope role, special SiteMinder variables should be used for the **Attribute Name** field. You should use the **SM_USERGROUPS** variable for regular groups and **SM_USERNESTEDGROUPS** if you want the **SITESCOPE_ROLE** HTTP header to contain the nested groups' information.

5 Add SiteScope rules and responses to the Security policy object.

a Click the **Policies** option to create a new security policy.

b Enter a meaningful name for the policy. For example, **SiteScope Policy**.

c Click the **Users** tab and add or remove the entities to which the policy applies. (You can choose entities only from the User Directories that are part of the same domain of the realm.)

d Click the **Rules** tab and choose the two rules described in step 3, **Users Role** and **SiteScope Rule**. In addition, add the **SiteScope Role** response that was defined earlier to be the response of the Users Role in step 4.

Configuring SiteScope for Using SiteMinder

To enable SiteScope to integrate with SiteMinder, you need to make changes to the configuration files used by the Tomcat server. For information on configuring the Tomcat server files, see "Configuring the Apache Tomcat Server Files" on page 197.

Configuring IIS

After you make changes to the configuration files used by the Tomcat server, you need to configure IIS. For information on configuring IIS, see "Configuring IIS" on page 200.

Defining Permissions for the Different SiteScope Roles

After you enable the SiteMinder integration, you must define the permissions for the different roles in SiteScope (using the SiteScope regular users permissions model). The association of the users to these roles is done outside of SiteScope, such as in LDAP groups. When a new SiteScope user is added, it only has to be defined in SiteMinder, since the user automatically inherits the permissions from the relevant SiteScope role.

Note: You must ensure that the SiteScope user account used by SiteMinder does not require a password, otherwise SiteMinder is unable to log in. For details on creating user accounts, see "User Management Preferences" in the SiteScope Help.

Logging On to SiteScope

When a user attempts to log on to SiteScope, SiteMinder intercepts the request. If it authenticates the user's credentials, it sends an assigned SiteScope user name and role (group) to SiteScope (for example, User: Fred, Role: Accounting). If SiteScope fails to recognize the name as a valid user name, but it recognizes the role, the user is logged on to SiteScope using the role (in this instance, User: Accounting).

To logon to SiteScope:

Open your Web browser and type the following URL: http://<IIS_machine_name>/SiteScope.

Note: If IIS and SiteScope reside on the same machine, you should connect to the default port 80, and not port 8080.

After SiteMinder successfully authenticates the user and logs on to SiteScope, SiteScope opens directly to the Dashboard view.

Notes and Guidelines

- The names of all users logged in to SiteScope are listed in the audit log, which is located in the <**SiteScope root directory**>**logs** directory. This is the case even when a user is logged in under a role name. For example, if user Fred is logged on under a role because SiteScope did not recognize Fred as a valid user but recognized the role, all operations are still listed with user name Fred in the audit log.
- You can specify a page where the browser is redirected after logging out the SiteMinder environment (this is the page that opens after you click the **LOGOUT** button in SiteScope). To activate the logout page, open the **master.config** file located in <**SiteScope root directory**>**groups**, and add the following line:

  _siteMinderRedirectPageLogout=<url_to_go_to_after_logout>
- The user account that SiteMinder uses to log in to SiteScope must not require a password, otherwise SiteMinder is unable to log in. For details on setting up a user account in SiteScope, see "User Management Preferences" in the SiteScope Help.
- To prevent users trying to access SiteScope directly using the SiteScope URL, you should consider disabling HTTP port 8080 and 8888 on the Tomcat server during SiteScope installation.

Index

K

L

M

N

O

P

R

S

T

U

V

W