HP SiteScope

For the Windows, Solaris and Linux operating systems

Software Version: 11.23

Deployment Guide

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 Notice

© Copyright 2005 - 2013 Hewlett-Packard Development Company, L.P.

Trademark Notices

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

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

iPod is a trademark of Apple Computer, Inc.

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

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

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

UNIX® is a registered trademark of The Open Group.

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 Online 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

HP Software Solutions Now accesses the HPSW Solution and Integration Portal Web site. This site enables you to explore HP Product Solutions to meet your business needs, includes a full list of Integrations between HP Products, as well as a listing of ITIL Processes. The URL for this Web site is **http://h20230.www2.hp.com/sc/solutions/index.jsp**

Contents

Part 1: Introduction to SiteScope

Chapter 1: SiteScope Overview

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. 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 based on 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 trial 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 also acts as a monitoring foundation for other HP offerings such as Business Service Management (BSM), Network Node Manager i (NNMi), HP Software-as-a-Service, and LoadRunner/Performance Center. By starting with SiteScope and adding other HP solutions such as BSM's 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.

SiteScope can also work together with HP Operations Manager (HPOM) products to provide a powerful combination of agentless and agent-based infrastructure management. Serving as an agent of HPOM, SiteScope targets are automatically added to Operations Manager service view maps, which enables HPOM to seamlessly display SiteScope data and monitor status. For event integration, SiteScope alerts and monitor metric status changes are sent directly to HPOM. The combined functionality of agentless and agent-based monitoring provides a powerful and in-depth monitoring solution. For more details on using HPOM products, refer to the HPOM documentation.

Chapter 2: SiteScope Freemium

The SiteScope Freemium edition enables you to use SiteScope with restricted functionality for an unlimited period of time for free. The SiteScope Freemium license provides 250 SiteScope points, and enables you to use SiteScope with partial SiteScope functionality for as long as you want.

You can download and install SiteScope Freemium from the HP SiteScope Product page (hp.com/go/SiteScope). For details on the SiteScope Freemium installation flow, see "SiteScope Freemium Installation Workflow" on page 100.

You can upgrade your SiteScope Freemium installation to a full SiteScope license at any time to expand the monitoring capacity of your initial deployment and to enjoy all the features offered by SiteScope. This provides an efficient and flexible way to scale SiteScope to your environment. For more information on licensing the full version of HP SiteScope, contact your HP Software Sales Representative or visit http://www.hp.com/go/sitescope.

For more information about licensing, see "SiteScope Licenses" on page 38.

The table below shows the features that are available in the SiteScope Freemium edition compared with those available in SiteScope during the free trial period.

Feature	Freemium Version	Full Version / Trial[1]
License duration	Perpetual	**Full:** User-selected duration (paid) **Trial:** 60 days trial
License points	250 points[2]	**Full:** Pay per point and OS instance based license **Trial:** 500 points
Supported platforms	Windows 64-bit only	Various Windows and Linux platforms (32/64-bit)
Monitor types and tools	Available[3]	Available
User templates	Available	Available
Solution templates	Unavailable	Paid (not during the trial period)
Massive and automatic template deployment via CSV or XML	Unavailable	Available
Manage monitors and groups	Unavailable	Available
Dashboard and Multi-View	Limited personalization	Includes: • Dashboard custom filtering • Favorites management

Feature	Freemium Version	Full Version / Trial[1]
Dashboard history view	Unavailable	Available
Alerts	Email only	Includes SNMP, DB, Log, Post, Script, and more...
Over Time reports	• Ad hoc Quick reports • One day data retention	• Server-Centric reports • Management reports (can be scheduled to run daily) • Perpetual data retention (user configurable)
Monitor reports	Available	Available
Alert reports	Limited to the last 24 hours	Available
Baselining	Unavailable	Available
Analytics	Unavailable	Available
User Accounts	One administrator account	• Multiple users and user roles • LDAP integration for user authentication and authorization
Integrations	Unavailable	• Amazon • HP Operations Manager • HP Business Service Management • HP LoadRunner/HP Performance Center • HP Diagnostics • Generic data and events integration
APIs	Unavailable	Available
High Availability	Unavailable	Available
Mobile applications (iPhone and Android)	Unavailable	Available

Feature	Freemium Version	Full Version / Trial[1]
Support model	SiteScope communities	• Full HP support (paid, different levels) • Access to customer support forum • Eligibility for patches and hotfixes

[1] For details about the 60 day trial period, see "Trial License" on page 39.

[2] OS instance based. For details on supported monitors, see "OS Instance Advanced License - Supported Monitors" on page 47.

[3] The following monitors are not available in the Freemium edition because it operates only on a 64-bit Windows system:

- Microsoft Exchange 2003 Mailbox

- Microsoft Exchange 2003 Public Folder

- Microsoft Windows Media Player

- Real Media Player

- Sybase

- Tuxedo

- Web Script

Amazon Web Services monitor is not available because it is a monitor that facilitates integration.

Chapter 3: Getting Started Roadmap

This section 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 sources of assistance, including HP Services and HP Software Support, as well as the SiteScope Help.

3. **Plan your SiteScope deployment.**

   Create a complete deployment plan prior to installing SiteScope software. Use "Deployment Methodology and Planning" on page 15 to assist you. For in-depth deployment planning best practices, consult your HP representative.

4. **Install SiteScope.**

   See "Installation Overview" on page 64 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 164.

5. **Log on 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 188 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.**

   After 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.

Chapter 4: Deployment Methodology and Planning

This chapter includes:

An Enterprise System Monitoring Methodology

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.

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 represent 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 25 or "Sizing SiteScope on Solaris and Linux Platforms" on page 27 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 on 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 be 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).

> **Tip:** 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.

Also, 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.

Considerations for UNIX Environments

SiteScope must be installed on a Solaris or Linux environment by the root user. After SiteScope has been installed, you can create a non-root user account with permissions to run SiteScope (unless the SiteScope Web server is run on a privileged port, in which case it should be run by the root user). For details on configuring a non-root user with permissions to run SiteScope, see "Configuring a Non-Root User Account with Permissions to Run SiteScope" below.

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 a 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 the root user or other highly privileged users.

   Note: Although SiteScope requires 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 on as a different user that has permissions to run the command, or have the permissions changed for the user account that SiteScope is using.

Configuring a Non-Root User Account with Permissions to Run SiteScope

SiteScope must be installed on Linux or Solaris from a root user account. After SiteScope has been installed, you can create a non-root user account with permissions to run SiteScope.

   Note: While SiteScope requires 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.

To create a non-root user account with permissions to use SiteScope:

1. Add a new user: `useradd newuser`

2. Change permissions for the SiteScope installation folder: `chmod 755 /opt/HP/SiteScope/ -R`

3. Change ownership for the SiteScope installation folder: `chown newuser /opt/HP/SiteScope/ -R`

4. Login as the new user: `su newuser`

5. Go to the installation folder: `cd /opt/HP/SiteScope`

6. Run SiteScope: `./start`

Note: To enable the HP Operations Manager event and metrics integration, the HP Operations agent on the SiteScope machine must run under the same user as in SiteScope, namely a non-root user. For details, see Configure an Agent to run Under an Alternative User on UNIX in the HP Operations Manager for UNIX - HTTPS Agent Concepts and Configuration Guide.

Chapter 5: Sizing SiteScope

This chapter includes:

Sizing SiteScope Overview

While the default SiteScope configuration permits 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.

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. BSM, BMC, HP 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 running on Windows versions only, and for monitors and solution templates listed in "Supported Monitors and Solution Templates" on page 23.

To use the SiteScope Capacity Calculator:

1. Before using the calculator, estimate the load on the SiteScope server and use the system requirement recommendations in this guide for determining your hardware needs.

   For details, see "System Hardware Requirements" on page 66.

2. Open the SiteScope Capacity Calculator which is available from:

   - The SiteScope installation folder: **<SiteScope root directory>\tools\SiteScopeCapacityCalculator.xls**

   - Product Manuals page on the HP Software Support site (under Product **SiteScope**, Product version 11.20).

3. Select the **Monitor Usage** tab according to the operating system on which SiteScope is installed (32 or 64-bit).

4. In the **Requirements** section, enter the following information:

   - Average % CPU usage

   - CPU type

   - Memory heap size (in megabytes)

   - For a 64-bit installation, select TRUE if SiteScope is integrated with BSM, or FALSE for a standalone SiteScope.

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

6. 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	
Monitors	• CPU
	• Database Counter
	• Database Query (64-bit only)
	• Directory Monitor (64-bit only)
	• Disk Space
	• DNS Monitor
	• File Monitor (64-bit only)
	• JMX Monitor (64-bit only)
	• Log File Monitor (32-bit only)
	• Memory Monitor
	• Microsoft IIS Server Monitor
	• Microsoft SQL Server Monitor (32-bit only)
	• Microsoft Windows Event Log Monitor (32-bit only)
	• Microsoft Windows Resources Monitor
	• Ping Monitor
	• SAP CCMS Monitor (32-bit only)
	• Service Monitor
	• Siebel Application Server Monitor (32-bit only)
	• SNMP by MIB Monitor
	• UNIX Resources Monitor (64-bit only)
	• URL Monitor
	• URL List Monitor (64-bit only)
	• WebLogic Application Server Monitor (32-bit only)

	• Web Service Monitor (64-bit only)
	• WebSphere Application Server Monitor(32-bit only)
Solution Templates	• Microsoft Exchange 2003 Solution Template (32-bit only)
	• Siebel Solution Templates (32-bit only)

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" below.

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 the next page

3. **General Maintenance Recommendations.**

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

> **Note:**
>
> - 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. Run the Configuration Tool, and select the **Sizing** option.

   This tool increases JVM heap size to 1024 MB (for 32-bit installations) and 4096 MB (for 64-bit installations), desktop heap size to 2048 KB (for 32-bit installations) and 8192 KB (for 64-bit installations), 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 Windows Platforms" on page 138.

   > **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.

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

3. Configure other sizing-related parameters in **Preferences > Infrastructure Preferences** as required.

   > **Tip:** To achieve optimum performance, we recommend using the default values for these settings.

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 the next page.

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 29.

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 29.

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 the Preferences section in Using SiteScope in the SiteScope Help.

> **Tip:** To achieve optimum performance, we recommend using the default value for this setting.

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 Java 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.

- **Use health monitors.**

  Use 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.

  Make sure that connection caching is enabled (in the New/Edit Microsoft Windows/UNIX Remote Server dialog box, expand **Advanced Settings** and clear the **Disable connection caching** check box). The **Connection limit** should be adjusted to enable 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.

Troubleshooting and Limitations

Problem: JVM crashes with an "out of swap space" error.

You can detect an out of swap space error by:

1. Creating a Microsoft Windows Resources monitor to monitor the virtual bytes counter on the target SiteScope server.

2. Configuring the following threshold settings:

32-bit Operating System	64-bit Operating System
Error if >= 1.9 GB	Error if >= 7.9 GB
Warning if >= 1.8 GB	Warning if >= 7.8GB
(The process crashes when its value reaches 2 GB)	(The process crashes when its value reaches 8 GB)

Solution:

1. Reduce the JVM heap size. For details on changing the JVM heap size, see "Running the Configuration Tool on Windows Platforms" on page 138.

2. Reduce the number of threads SiteScope uses by reducing the number of concurrent monitors running (in **Preferences > Infrastructure Preferences > Server Settings > Maximum monitor processes**).

Chapter 6: Understanding Agentless Monitoring

This chapter includes:

SiteScope Monitoring Capabilities Overview

This section 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. 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 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.

SiteScope is a versatile operational monitoring solution that provides many different monitor types for monitoring systems and services at many 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.

Monitor Type	Description
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" below

- "Firewalls and SiteScope Deployment" on page 36

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 using 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, HP-UX, and Solaris.

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

  This category includes monitor types that log on 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 Exchange and Microsoft Windows Dial-up monitors, which are not included in SiteScope for Linux.

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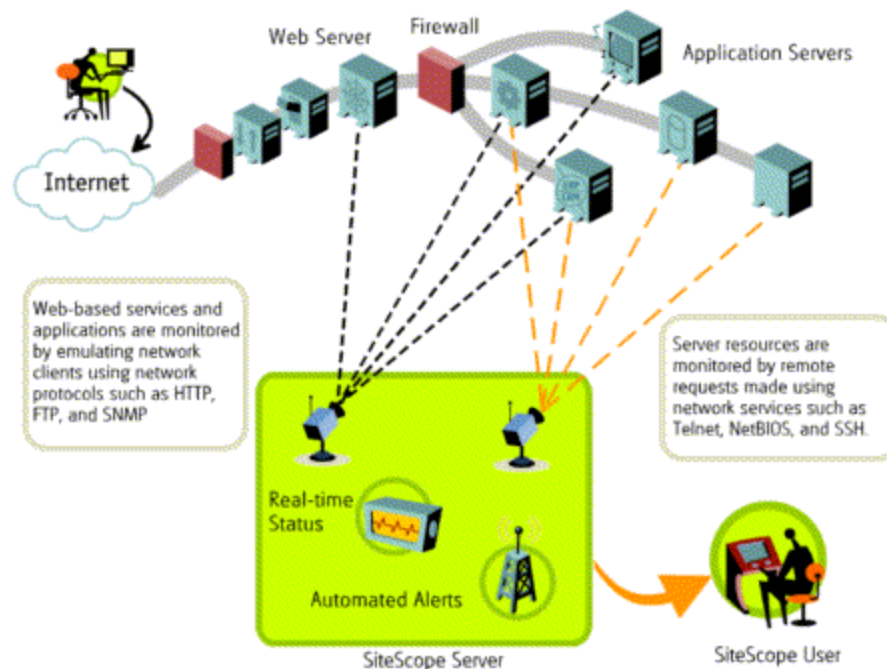
SiteScope Server monitors (for example, CPU, Disk Space, Memory, Service) can be used to monitor server resources on the following platforms:

- Windows

- Solaris (Sparc and x86)

- Linux

- AIX HP-UX (HP-UX 64-bit)

- 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 Solaris or Linux. A Secure Shell server must be installed on each Windows machine that you want to monitor in this way. For more information on enabling this capability, see the SiteScope Monitoring Using

Secure Shell (SSH) section in Using SiteScope in the SiteScope Help.

SiteScope includes an adapter configuration template that enables you to extend SiteScope capabilities to monitor other versions of the UNIX operating system. For more information, see UNIX Operating System Adapters in 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
SiteScope Reports	Port 8888
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

Monitor Permissions and Credentials

User permissions and credentials are needed to access each monitor. For details on the required permissions and credentials, and the corresponding protocol used by each monitor, see the Monitor Permissions and Credentials section in the SiteScope Monitor Reference Guide in the SiteScope Help.

Chapter 7: SiteScope Licenses

This chapter includes:

SiteScope Licensing Overview

SiteScope licensing controls the number of monitors that can be created simultaneously 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.

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.

> **Note:** License keys from versions of SiteScope earlier than 11.00 are not compatible with this version. License key delivery can be fulfilled automatically through https://h30580.www3.hp.com/poeticWeb/portalintegration/hppWelcome.htm.

Understanding SiteScope License Types

To use SiteScope, you must have a valid license. You can install SiteScope using a General license, or use the Freemium or Trial license that is available with each new installation or download of SiteScope. You can also purchase an extension license to extend the trial period under a trial license, or to enable the use of optional monitors and solution templates.

These are the different types of SiteScope licenses:

Type	Description	Duration	Points Displayed
Trial License	During the free trial period, it includes: • All monitors except those monitors which are dependent on Solution Templates that are not bundled with this license. • The following Solution Templates: ▪ Failover ▪ Hadoop ▪ HP Vertica ▪ Microsoft Exchange ▪ Microsoft Lync Server 2010 ▪ Microsoft SharePoint 2010 ▪ SAP ▪ Siebel ▪ VMware Host ▪ VMware Host Performance Troubleshooting **Note:** After the trial period expires or the license is upgraded to a General license, the solution templates listed above and all extension monitors (see "Extension License" on page 42) are no longer available without the applicable SiteScope extension license.	Fixed trial period of up to 60 days. **Note:** The trial period terminates immediately once a perpetual or time-based license is purchased.	500 points

Type	Description	Duration	Points Displayed
Freemium License	Enables partial functionality of SiteScope, with access to all monitors except: • Microsoft Exchange 2003 Mailbox Monitor • Microsoft Exchange 2003 Public Folder Monitor • Microsoft Windows Media Player Monitor • Real Media Player Monitor • Sybase Monitor • Tuxedo Monitor • Web Script Monitor • Amazon Web Services Monitor No solution templates are included. For details, see "SiteScope Freemium" on page 11.	Perpetual.	250 points

Type	Description	Duration	Points Displayed
General License	Enables the standard functionality of SiteScope, based on the number of monitor points included as part of the license. It includes all monitors except: • Extension monitors that require an additional license (see "Extension License" on the next page). • Monitors which are not available when their Solution Templates are not available (see "Monitors Not Available when their Solution Templates are Not Available: " on page 43). Includes access to the Hadoop, HP Vertica, and Failover Monitoring solution templates only.	This license type can be temporary (time-based) or perpetual.	Displays the total number of points purchased with the license.
OS Instance License	System monitors can be licensed by OS instance instead of points. For license details and the list of monitor types supported by this license, see "OS Instance Advanced License" on page 45.	This license type can be temporary (time-based) or perpetual.	Displays the total number of OS/host licenses purchased.

Type	Description	Duration	Points Displayed
Failover License	**SiteScope Failover:** A special license issued by HP enabling the SiteScope instance to act as a failover for another SiteScope installation. The Failover license requires the same number of points as used by the primary SiteScope server. **SiteScope Failover Manager:** While SiteScope Failover Manager is freely available out-of-the-box, it still requires a separate Failover license in case the General license is node locked on the primary SiteScope server. This license is applied on the SiteScope Failover Manager when the primary SiteScope server is down.	This license type can be temporary (time-based) or perpetual.	Displays the total number of points purchased with the SiteScope Failover license.
Extension License	An additional extension license is required to enable each of the solution templates (except Hadoop, HP Vertica, and Failover Monitoring), and the monitors listed below. • COM+ Server • Web Script • WebSphere MQ Status **Note:** Each extension license enables a specific monitor type or solution template.	This license type can be temporary or perpetual.	No points. Each monitor or solution template has its own point consumption. For details, see "License Point Usage For Monitors" on page 47 and "License Point Usage For Solution Templates" on page 56.

Monitors Not Available when their Solution Templates are Not Available:

- All Exchange monitors (Microsoft Exchange Solution Template)

- All Siebel monitors (Siebel Solution Template)

- All SAP monitors (SAP R3 and J2EE Solution Templates)

- All VMware Host monitors and VMware Datastore monitor (VMware Solution Templates)

- Microsoft A/V Conferencing Server (MS Lync Solution Template)

- Microsoft Archiving Server (MS Lync Solution Template)

- Microsoft Director Server (MS Lync Solution Template)

- Microsoft Front End Server (MS Lync Solution Template)

- Microsoft Edge Server (MS Lync Solution Template)

- Microsoft Mediation Server (MS Lync Solution Template)

- Microsoft Monitoring and CDR Server (MS Lync Solution Template)

- Microsoft Registrar Server (MS Lync Solution Template)

Monitors Available Only When SiteScope is Installed on a 32-Bit Environment

The following monitors are available only when SiteScope is installed on a 32-bit environment, or when SiteScope is installed as a 32-bit version in a 64-bit environment using the **HPSiteScope32on64_11.20_setup.exe** installation file (or **HPSiS112x_32on64_11.2x_setup.exe** for a SiteScope 11.2x patch installation):

- Microsoft Exchange 2003 Mailbox Monitor

- Microsoft Exchange 2003 Public Folder Monitor

- Microsoft Windows Media Player Monitor

- Real Media Player Monitor

- Sybase Monitor

- Tuxedo Monitor

- Web Script Monitor

Differences Between General and Extension Licenses

The table below summarizes the differences between General and Extension licenses.

Topic	General License	Extension License
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 extension license key enables extension monitor types for the SiteScope installation on which it is used. The extension license key does not increase the total number of monitor points governed by the General license key. The monitor points used for the creation of extension monitor types are deducted from total monitor points included in the General license key.
	For details on monitor point usage, see "Understanding Monitor Licensing" below.	

SiteScope automatically sends an email notification 7 days before your license is about to expire, and a pop-up message is displayed each time you open SiteScope once the license has expired.

If you need to upgrade or renew your SiteScope license, visit the HP Licensing for Software Portal (https://h30580.www3.hp.com/poeticWeb/portalintegration/hppWelcome.htm).

Understanding Monitor Licensing

Licensing for SiteScope is based on a point system. The number of points consumed by SiteScope depends on the type of license that was purchased and the number and type of monitors being used.

This section includes:

- "Point System" on the next page

- "OS Instance Advanced License" on the next page

- "License Point Usage For Monitors" on page 47

- "License Point Usage For Solution Templates" on page 56

> **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.
>
> - Each license is node locked to avoid possible license confusion and abuse. This means that the license is only valid on a specific machine.

Point System

Licensing for monitor types is based on a point system. A perpetual SiteScope license provides a number of points that you use to create a combination of monitor types.

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 categories based on how many points you need to create 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 object 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 selection costs one point for the explorer instance. Had you selected an additional instance to monitor, it would cost two points, and so forth.

OS Instance Advanced License

System monitors can be licensed per OS instance instead of per number of monitors used. For example, if you are using a CPU, a Disk Space, and a Memory monitor on the same operating

system or host, a single OS instance point is deducted from the license, instead of three monitor points. For the list of supported monitors, see "OS Instance Advanced License - Supported Monitors" on the next page.

SiteScope applies the available OS Instance Advanced licenses to the most monitored hosts/operating system instances (these are the concepts used above)—the ones with the highest number of points consumed by supported monitors monitoring the host/OS. Points consumed by those monitoring are freed, and can be used by other monitors that are not covered by the OS license.

You can view details of OS instance license consumption in **Preferences** > **General Preferences** > **Licenses**. The OS Instance License Usage table includes the OS instances covered by the license, license points used compared to the number of points required, and the number of points saved per host by using the OS Instance Advanced license.

When an OS Instance Advanced license expires or is removed, all monitors belonging to hosts that had used the OS Instance Advanced license, start consuming from the General License point pool. This may lead to a situation where the number of license points used by SiteScope monitors exceeds the number of points available. In this event, SiteScope sends a message that it will shut down within 7 days. To avoid a SiteScope shutdown, you should add more license points or reduce the number of monitors being used. To add more points, contact the HP License Key Delivery Service http://webware.hp.com), and request a new license.

Note:

The SAM license is not affected by the OS Instance Advanced license. SAM points are still counted for monitors reporting to BSM even if they are counted under the OS Instance Advanced license inside SiteScope. This information is displayed in the OS Instance License consumption report (total potential point usage and/or SAM point usage).

When ordering an OS Instance Advanced license in webware, the license name is **HP SiteScope <X> Pts or <Y> OS Instance included w/Operations OS Instance.**

OS Instance Advanced License - Supported Monitors

OS instance based licensing is used for the following monitor types.

• CPU	• Microsoft Windows Performance Counter
• Directory	• Microsoft Windows Event Log
• Disk Space (deprecated)	• Microsoft Registrar Server
• Dynamic Disk Space	• Microsoft Windows Resources
• File	• Microsoft Windows Services State
• HP NonStop Event Log	• Ping
• HP NonStop Resources	• Port
• Memory	• Service
• Microsoft Archiving Server	• Solaris Zones
• Microsoft A/V Conferencing Server	• UNIX Resources
• Microsoft Director Server	• VMware Host CPU
• Microsoft Edge Server	• VMware Host Memory
• Microsoft Front End Server	• VMware Host Network
• Microsoft Hyper-V	• VMware Host State
• Microsoft Mediation Server	• VMware Host Storage
• Microsoft Monitoring and CDR Server	• VMware Performance

License Point Usage For Monitors

The following lists the point usage for each instance of a SiteScope monitor type:

Monitor (A-Z)	Monitor Category	License Point Usage
Amazon Web Services	Virtualization and Cloud	1 point per metric
Apache Server	Application	1 point per metric

Monitor (A-Z)	Monitor Category	License Point Usage
BroadVision Application Server	Application	1 point per metric
Check Point	Application	1 point per metric
Citrix	Application	1 point per metric
ColdFusion Server	Application	1 point per metric
COM+ Server	Application	1 point per metric **Note:** Additional licensing is required to enable this monitor type in the SiteScope interface after the free trial period expires.
Composite	Generic	Computed according to contained monitors **Note:** This monitor is set up at no additional cost in monitor points beyond that of the member monitors which it contains.
CPU	Server	1 point per monitor **Note:** No points are consumed by this monitor if it is running on a host covered by the OS Instance Advanced license. For details, see "OS Instance Advanced License" on page 45.
Custom	Customizable	1 point for every 10 metrics. For example, 41 metrics consume 5 points.
Custom Database	Customizable	1 point for every 10 metrics. For example, 41 metrics consume 5 points.
Custom Log File	Customizable	1 point for every 10 metrics. For example, 41 metrics consume 5 points.
Custom WMI	Customizable	1 point for every 10 metrics. For example, 41 metrics consume 5 points.
Database Counter	Database	1 point per metric
Database Query	Database	1 point per monitor
DB2 8.x and 9.x	Database	1 point per metric
DHCP	Server	1 point per monitor

Monitor (A-Z)	Monitor Category	License Point Usage
Directory	Generic	1 point per monitor **Note:** No points are consumed by this monitor if it is running on a host covered by the OS Instance Advanced license. For details, see "OS Instance Advanced License" on page 45.
Disk Space (Deprecated - replaced by Dynamic Disk Space monitor)	Server	1 point per monitor **Note:** No points are consumed by this monitor if it is running on a host covered by the OS Instance Advanced license. For details, see "OS Instance Advanced License" on page 45.
DNS	Network	1 point per monitor
Dynamic Disk Space	Server	1 point per disk **Note:** No points are consumed by this monitor if it is running on a host covered by the OS Instance Advanced license. For details, see "OS Instance Advanced License" on page 45.
Dynamic JMX	Generic	1 point per monitored object. An object is a path in the tree (not containing the counter name itself) for which at least one direct counter is selected).
e-Business Transaction	Web Transaction	1 point per monitor
F5 Big-IP	Application	1 point per metric
File	Generic	1 point per monitor **Note:** No points are consumed by this monitor if it is running on a host covered by the OS Instance Advanced license. For details, see "OS Instance Advanced License" on page 45.
Formula Composite	Network	1 point per monitor
FTP	Network	1 point per monitor
Generic Hypervisor	Virtualization and Cloud	1 point per host and 1 point per guest
Hadoop	Big Data	1 point per monitored object. An object is a path in the tree (not containing the counter name itself) for which at least one direct counter is selected).
HAProxy	Application	1 point per metric

Monitor (A-Z)	Monitor Category	License Point Usage
HP iLO (Integrated Lights-Out)	Server	1 point per metric
HP NonStop Event Log	Server	1 point per monitor **Note:** No points are consumed by this monitor if it is running on a host covered by the OS Instance Advanced license. For details, see "OS Instance Advanced License" on page 45.
HP NonStop Resources	Server	1 point per object instance **Note:** No points are consumed by this monitor if it is running on a host covered by the OS Instance Advanced license. For details, see "OS Instance Advanced License" on page 45.
HP Vertica JDBC	Big Data	1 point per monitored group. A group is a path in the tree (not containing the counter name itself) for which at least one direct counter is selected).
IPMI	Server	1 point per metric (Maximum: 120)
JMX	Generic	1 point per metric
KVM	Virtualization and Cloud	1 point per host and 1 point per guest
LDAP	Generic	1 point per monitor
Link Check	Web Transaction	1 point per monitor
Log File	Generic	1 point per monitor
Mail	Network	1 point per monitor
MAPI	Network	1 point per monitor
Memory	Server	1 point per monitor **Note:** No points are consumed by this monitor if it is running on a host covered by the OS Instance Advanced license. For details, see "OS Instance Advanced License" on page 45.
Memcached Statistics	Application	1 point per metric

Monitor (A-Z)	Monitor Category	License Point Usage
Microsoft Archiving Server	Media	1 point per metric **Note:** No points are consumed by this monitor if it is running on a host covered by the OS Instance Advanced license. For details, see "OS Instance Advanced License" on page 45.
Microsoft A/V Conferencing Server	Media	1 point per metric **Note:** No points are consumed by this monitor if it is running on a host covered by the OS Instance Advanced license. For details, see "OS Instance Advanced License" on page 45.
Microsoft ASP Server	Application	1 point per metric
Microsoft Director Server	Media	1 point per metric **Note:** No points are consumed by this monitor if it is running on a host covered by the OS Instance Advanced license. For details, see "OS Instance Advanced License" on page 45.
Microsoft Edge Server	Media	1 point per metric **Note:** No points are consumed by this monitor if it is running on a host covered by the OS Instance Advanced license. For details, see "OS Instance Advanced License" on page 45.
Microsoft Exchange	Application	1 point per metric
Microsoft Exchange 2003 Mailbox	Application	3 points per monitor
Microsoft Exchange 2000/2003/2007 Message Traffic	Application	5 points per monitor
Microsoft Exchange 5.5 Message Traffic	Application	5 points per monitor
Microsoft Exchange 2003 Public Folder	Application	5 points per monitor

Monitor (A-Z)	Monitor Category	License Point Usage
Microsoft Front End Server	Media	1 point per metric **Note:** No points are consumed by this monitor if it is running on a host covered by the OS Instance Advanced license. For details, see "OS Instance Advanced License" on page 45.
Microsoft Hyper-V	Virtualization and Cloud	1 point per metric **Note:** No points are consumed by this monitor if it is running on a host covered by the OS Instance Advanced license. For details, see "OS Instance Advanced License" on page 45.
Microsoft IIS Server	Application	1 point per metric
Microsoft Mediation Server	Media	1 point per metric **Note:** No points are consumed by this monitor if it is running on a host covered by the OS Instance Advanced license. For details, see "OS Instance Advanced License" on page 45.
Microsoft Monitoring and CDR Server	Media	1 point per metric **Note:** No points are consumed by this monitor if it is running on a host covered by the OS Instance Advanced license. For details, see "OS Instance Advanced License" on page 45.
Microsoft Registrar Server	Media	1 point per metric **Note:** No points are consumed by this monitor if it is running on a host covered by the OS Instance Advanced license. For details, see "OS Instance Advanced License" on page 45.
Microsoft SQL Server	Database	1 point per metric
Microsoft Windows Dial-up	Network	1 point per monitor
Microsoft Windows Event Log	Server	1 point per monitor **Note:** No points are consumed by this monitor if it is running on a host covered by the OS Instance Advanced license. For details, see "OS Instance Advanced License" on page 45.
Microsoft Windows Media Player	Media	1 point per metric

Monitor (A-Z)	Monitor Category	License Point Usage
Microsoft Windows Media Server	Media	1 point per metric
Microsoft Windows Performance Counter	Server	1 point per monitor **Note:** No points are consumed by this monitor if It is running on a host covered by the OS Instance Advanced license. For details, see "OS Instance Advanced License" on page 45.
Microsoft Windows Resources	Server	1 point per instance **Note:** No points are consumed by this monitor if it is running on a host covered by the OS Instance Advanced license. For details, see "OS Instance Advanced License" on page 45.
Microsoft Windows Services State	Server	1 point per monitor **Note:** No points are consumed by this monitor if it is running on a host covered by the OS Instance Advanced license. For details, see "OS Instance Advanced License" on page 45.
Multi-Log	Generic	1 point per file
Network Bandwidth	Network	1 point per metric
News	Application	1 point per monitor
Oracle 10g Application Server	Application	1 point per metric
Oracle 9i Application Server	Application	1 point per metric (maximum: 7)
Oracle Database	Database	1 point per metric
Ping	Network	1 point per monitor **Note:** No points are consumed by this monitor if it is running on a host covered by the OS Instance Advanced license. For details, see "OS Instance Advanced License" on page 45.
Port	Network	1 point per monitor **Note:** No points are consumed by this monitor if it is running on a host covered by the OS Instance Advanced license. For details, see "OS Instance Advanced License" on page 45.

Monitor (A-Z)	Monitor Category	License Point Usage
Radius	Application	1 point per metric
Real Media Player	Media	1 point per metric
Real Media Server	Media	1 point per metric
SAP CCMS	Application	1 point per metric
SAP CCMS Alert	Application	1 point per metric
SAP Java Web Application Server	Application	1 point per metric
SAP Performance	Application	1 point per metric
SAP Work Processes	Application	1 point per metric
Script	Generic	1 point per monitor up to 4 pattern match metrics; above this, 1 point per additional pattern match metric, that is, #OfMatchValueMetrics-3.
Service	Server	1 point per monitor **Note:** No points are consumed by this monitor if it is running on a host covered by the OS Instance Advanced license. For details, see "OS Instance Advanced License" on page 45.
Siebel Application Server	Application	1 point per metric
Siebel Log	Application	1 point per monitor
Siebel Web Server	Application	1 point per metric
SNMP	Network	1 point per monitor
SNMP by MIB	Network	1 point per metric
SNMP Trap	Network	1 point per monitor

Monitor (A-Z)	Monitor Category	License Point Usage
Solaris Zones	Virtualization and Cloud	1 point for each monitored zone (global or non-global) or physical server. **Note:** No points are consumed by this monitor if it is running on a host covered by the OS Instance Advanced license. For details, see "OS Instance Advanced License" on page 45.
SunONE Web Server	Application	1 point per metric
Sybase	Database	1 point per metric
Syslog	Generic	1 point per monitor
Tuxedo	Application	1 point per metric
UDDI Server	Application	1 point per monitor
UNIX Resources	Server	1 point per instance **Note:** No points are consumed by this monitor if it is running on a host covered by the OS Instance Advanced license. For details, see "OS Instance Advanced License" on page 45.
URL Content	Web Transaction	1 point per monitor
URL List	Web Transaction	1 point per URL
URL Sequence	Web Transaction	1 point per URL (Step)
VMware Datastore	Virtualization and Cloud	1 point per datastore
VMware Host CPU / Memory / Network / State / Storage	Virtualization and Cloud	1 point for each monitored VM or physical server. **Note:** While VMware Host monitors are supported by the OS Instance Advanced license, the license does not cover the ESX host and all VMs being monitored—it can be applied to one ESX host or VM (a separate OS license is required to cover each ESX host or VM). No points are consumed by each host or VM that is covered by the OS license. For details, see "OS Instance Advanced License" on page 45.

Monitor (A-Z)	Monitor Category	License Point Usage
VMware Performance	Virtualization and Cloud	1 point for each monitored VM or physical server. **Note:** No points are consumed by this monitor if it is running on a host covered by the OS Instance Advanced license. For details, see "OS Instance Advanced License" on page 45.
Web Script	Web Transaction	4 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. **Note:** A Web Script monitor can consume more than 4 points if a script run by the monitor has more than 1 transaction.
Web Server	Server	1 point per monitor
Web Service	Generic	1 point per monitor
WebLogic Application Server	Application	1 point per metric
WebSphere Application Server	Application	1 point per metric
WebSphere MQ Status	Application	1 point per instance (that is, channel or queue)
WebSphere Performance Servlet	Application	1 point per metric
XML Metrics	Generic	1 point per metric

License Point Usage For Solution Templates

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

License point usage is based on the solution template cost, which 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 point 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
Hadoop Cluster Monitoring	HDFS solution template: 4 + (Number of files matched by Multi Log monitor) MapReduce solution template: 15 + (Total number of configured job queues) + (Number of files matched by Multi Log monitor)
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
HP Vertica	approximately 18 +10*<node count>
JBoss Application Server 4.x	3
Linux Host	13
Microsoft Exchange 2000	40
Microsoft Exchange 2003	49
Microsoft Exchange 2007	83
Microsoft Exchange 2010	83
Microsoft Exchange 5.5	39
Microsoft IIS 6	98
Microsoft IIS 7.x	79

Solution Template	Typical License Point Usage
Microsoft Lync Server 2010	106 points for one instance of each Lync Server role. (Additional points are used when deploying subtemplates for different machines with the same role.)
Microsoft SharePoint 2010	74
Microsoft SQL Server	18
Microsoft SQL Server 2008 R2	43
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
Siebel Gateway Server for Windows	6
Siebel Web Server for UNIX	19
Siebel Web Server for Windows	19
Solaris Host	13
VMware Capacity Management	Each monitor deployed by the template consumes an amount of points equal to the number of distinct datastores and VM disks currently monitored by it (there are 2 monitors in the solution template). The distinction of the datastores/VM disks is within the monitor. The same datastore monitored by two monitors will be charged 1 point by each monitor. **Example:** If you monitor 6 distinct datastores in the first monitor and 3 distinct VM disks in the second monitor: point consumption = 9

Solution Template	Typical License Point Usage
VMware Host	VMware Host monitors consume an amount of points equal to the number of distinct hosts (ESX) and the VMs currently monitored by it. The solution template includes 5 VMware Host monitors, all of which monitor the ESX host, and 3 of the 5 also monitor VMs on the ESX host. **Example:** If the ESX accommodates X VMs, the license consumption will be as follows: (1 point per ESX + X points for X VMs) * 3 (number of monitors that monitor ESX and VMs) + 2 (number of monitors that monitor ESX only) * 1 point per ESX If X = 4 (for example), license consumption: (1 + 4) * 3 + 2 = 17
VMware Host For Performance Troubleshooting	VMware Host monitors consume an amount of points equal to the number of distinct hosts (ESX) and the VMs currently monitored by it. The solution template includes 5 VMware Host monitors, all of which monitor the ESX host, and 3 of the 5 also monitor VMs on the ESX host. **Example:** If the ESX accommodates X VMs, the license consumption will be as follows: (1 point per ESX + X points for X VMs) * 3 (number of monitors that monitor ESX and VMs) + 2 (number of monitors that monitor ESX only) * 1 point per ESX If X = 4 (for example), license consumption: (1 + 4) * 3 + 2 = 17
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" below

- "Web Process and Content Monitoring" below

- "Application Performance Monitoring " on the next page

- "Network Monitoring" on the next page

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 include the same path with different destination pages. For online services, it may also be necessary to check back-end databases to confirm that data modified using 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 permit 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 using 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 many 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 trial license. To use SiteScope beyond the trial period, you must request and activate a general license key for your copy of SiteScope. For more information on purchasing monitor points, visit the HP Licensing for Software Portal (https://h30580.www3.hp.com/poeticWeb/portalintegration/hppWelcome.htm).

Adding SiteScope Licenses

After you install SiteScope, you can add to your licensing at any time. For information on how to obtain a new or additional monitoring licenses, visit the HP Licensing for Software Portal (https://h30580.www3.hp.com/poeticWeb/portalintegration/hppWelcome.htm).

When you receive your license file from HP, import the license keys into SiteScope using the SiteScope user interface.

To add a license in SiteScope:

1. From a Web browser, open the SiteScope instance you want to modify. The SiteScope service or process must be running.

2. Select **Preferences > General Preferences**, and expand the **Licenses** panel.

3. Enter the path to your SiteScope license file in the **License file** box, or click the **Select** button, and select the license file.

4. Click **Import**. After licenses have been successfully imported, information about the imported licenses is displayed in the licenses table. This includes the license type, description, expiration date, and the total number of monitor points permitted by the license.

Part 2: Before Installing SiteScope

Chapter 8: Installation Overview

There are several planning steps and actions you should consider before you install SiteScope to facilitate the deployment and management of your monitoring environment.

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:**
   >
   > - It is recommended not to install more that one SiteScope on a single machine.
   >
   > - If you plan to use SiteScope Failover Manager to provide backup monitoring availability in case of a SiteScope server failure, you must install SiteScope on a shared resource. For details, see the HP SiteScope Failover Guide located in **<SiteScope root directory>\sisdocs\pdfs\FailoverManager.pdf**.

2. **Obtain the SiteScope installation executable.**

   For details, see "Installation Workflow" on page 98.

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 11.20. Do not install version 11.20 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 "Installation Workflow" on page 98.

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 and Accessing SiteScope" on page 187.

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

   For more information, see "Post-Installation Administration" on page 188.

Chapter 9: Installation Requirements

This chapter includes:

- "System Requirements" below

- "SiteScope Capacity Limitations" on page 71

- "SiteScope Support Matrices" on page 71

System Requirements

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

> **Note:**
> - When using the standard installation programs (**HPSiteScope_11.20_setup.exe** or **HPSiteScope_11.20_setup.bin**), SiteScope is automatically installed as a 32-bit application on 32-bit operating systems or as a 64-bit application on 64-bit operating systems. The **HPSiteScope32on64_11.20_setup.exe** installs SiteScope as a 32-bit application in a 64-bit Windows operating system. Make sure to use the matching installer type also when applying minor-minor releases or patches.
>
> - Running SiteScope on a Solaris platform is now deprecated. The next release is not planned to include a Solaris Installer.
>
> - For troubleshooting and limitations for installing SiteScope on different environments, see "Troubleshooting and Limitations" on page 107.

This section includes the following topics:

- "System Hardware Requirements" on the next page

- "Server System Requirements for Windows" on page 67

- "Server System Requirements for Linux" on page 68

- "Server System Requirements for Solaris" on page 69

- "Client System Requirements" on page 70

System Hardware Requirements

Hardware requirements specifications:

Computer/Processor	1 core / 2000 MHZ minimum
Memory	2 GB minimum 8GB to 16 GB is common for a highly loaded environment
Free Hard Disk Space	10 GB
Network Card	1 physical gigabit Network Interface Card minimum

Virtualization requirements specifications:

- Using VMware and Hyper-V virtual machines is supported for all the supported operating systems (see "Server System Requirements for Windows" on the next page, "Server System Requirements for Linux" on page 68, "Server System Requirements for Solaris" on page 69).

- For better performance and stability, especially in a highly-loaded SiteScope environment, it is recommended to use physical hardware.

- For VMware, VMware tools must be installed on the guest operating system.

Certified Configurations

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

Operating System	Microsoft Windows Server 2003 SP2 Enterprise Edition (32-bit)	Microsoft Windows Server 2003 SP2 Enterprise Edition (64-bit)
System Type	x86-based PC	ACPI Multiprocessor x64-based PC
CPU	4 Intel® Xeon® 5160 physical processors, 3 GHz each	4 Intel® Xeon® 5160 physical processors, 3 GHz each
Total Physical Memory (RAM)	16 GB	16 GB
Java Heap Memory	1024 MB	2048 - 3072 MB
Total Number of Monitors	16,000	24,000
Total Number of Remote Servers	1,250	2,500
Monitor Runs per Minute	2,000	3,500

> **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, remotes connection protocol type, monitor types and distribution by type, monitor frequency, monitor execution time, Business Service Management integration, and Database Logging.
>
> - When working under high load, you should suspend all monitors before connecting to BSM for the first time.

Server System Requirements for Windows

The following Microsoft Windows operating system versions were certified:

System Type	OS Version
32/64-bit	- *Microsoft Windows Server 2003 SP2 Standard/Enterprise Edition - *Microsoft Windows Server 2003 R2 SP2 Enterprise Edition - Microsoft Windows Server 2008 SP1, SP2 Standard/Enterprise Edition
64-bit	- Microsoft Windows Server 2008 R2 SP1 Standard/Enterprise/Datacenter Edition - **Microsoft Windows Server 2012 Standard/Datacenter Edition

* Microsoft Windows Server 2003 support is deprecated and we plan to remove it in the next SiteScope release.

** The HP Operations agent is not available when installing SiteScope 11.23 on a Microsoft Windows Server 2012 environment because the agent version bundled with SiteScope does not support this Windows platform. As a result, the HP Operations Manager Event and Metrics Integration is not supported in SiteScopes running on Windows Server 2012.

Notes and Limitations

Windows Monitors Not Supported by 64-Bit SiteScope

The following monitors are available only when SiteScope is installed on a 32-bit environment, or when SiteScope is installed as a 32-bit version in a 64-bit environment using the **HPSiteScope32on64_11.20_setup.exe** installation file (or **HPSiS112x_32on64_11.2x_setup.exe** for a SiteScope 11.2x patch installation):

- Microsoft Exchange 2003 Mailbox Monitor

- Microsoft Exchange 2003 Public Folder Monitor

- Microsoft Windows Media Player Monitor

- Real Media Player Monitor

- Sybase Monitor

- Tuxedo Monitor

- Web Script Monitor

SiteScope Freemium

The Freemium version of SiteScope is supported only on a 64-bit Windows system.

Server System Requirements for Linux

The following Linux operating system versions were certified:

OS Version	System Type	Notes
Oracle Enterprise Linux 6.0, 6.1	64-bit	The environment must be manually configured before installing SiteScope. For details, see "Installing SiteScope on an Oracle Enterprise Linux Environment" on page 102.
CentOS 6.2	64-bit	The CentOS 6.2 server must be manually configured before installing SiteScope. For details, see "Installing SiteScope on a CentOS 6.2 Environment" on page 103. **Note:** The Operations Manager integration and HP Operations Agent installation are not currently supported in SiteScope 11.2x installed on a CentOS 6.2 server.
Red Hat ES/AS Linux 5.2, 5.4	32-bit	
Red Hat ES/AS Linux 5.5, 5.6, 5.7, 5.8	32/64-bit	

OS Version	System Type	Notes
Red Hat ES/AS Linux 6.0-6.4 (6.0, 6.2, and 6.4 are certified)	64-bit	The Red Hat ES/AS Linux 6.x server must be manually configured before installing the HP Operations agent. For details, see "Installing Dependencies Required by the HP Operations Agent" on page 105. The HP Operations agent is not available when installing SiteScope 11.23 on a Red Hat ES/AS Linux 6.4 environment because the agent version bundled with SiteScope does not support this platform. As a result, the HP Operations Manager Event and Metrics Integration is not supported in SiteScopes running on Red Hat ES/AS Linux 6.4.

Note:

- When SiteScope is installed on Red Hat Linux, the SiteScope Server Health monitor requires valid output of sar -W and sar -B commands for the SwapIns/sec, SwapOuts/sec, PageIns/sec, and PageOuts/sec counters. If these commands do not work, no errors are thrown and these counters are shown as **n/a**. To enable them to run, edit the crontab by adding the command "**/usr/local/lib/sa/sadc -**" to run once a day.

- To be able to monitor CPU and memory usage on SiteScope or a remote server running on a Red Hat Linux environment, the **sysstat** package must be installed on the SiteScope server and on all remote servers being monitored (it is not included out-of-the-box).

- Red Hat Linux 9 with Native POSIX Threading Library (NPTL) is not supported.

Server System Requirements for Solaris

Note: Running SiteScope on a Solaris platform is now deprecated. The next release is not planned to include a Solaris Installer.

The following Solaris operating system versions were certified:

OS Version	System Type	Notes
Solaris 9	32-bit	Supported with latest recommended patch cluster
Solaris 10	32/64-bit	Supported with latest recommended patch cluster

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

Client System Requirements

SiteScope client is supported on all Microsoft Windows operating systems using the following:

Supported Browsers (SiteScope UI)	• Microsoft Internet Explorer 7, 8, 9
	
	• Microsoft Internet Explorer 10
	
	  Note:
	
	  ▪ Alert, Monitor, and Server-Centric Reports are supported in compatibility mode only.
	
	  ▪ There is no support for add-ons, like Java, when Internet Explorer 10 is used from the Start screen. To use SiteScope in Internet Explorer 10, you must switch to Internet Explorer desktop mode and install java. For details, see http://windows.microsoft.com/en-us/internet-explorer/install-java#ie=ie-10.
	
	• Mozilla Firefox 24.0 ESR (this is the latest certified version)
	
	Note:
	
	• The browser must be set to accept third-party cookies and allow session cookies.
	
	• The browser must be set to enable JavaScript execution.
	
	• The browser must allow pop-ups from the SiteScope application.

Supported Browsers (Multi-View)	• Chrome 15 or later (recommended) • Firefox 10 or later (recommended) • Safari 5.1 or later (recommended) • Microsoft Internet Explorer 8, 9, 10 • iPad
Java Plug-in (required to open SiteScope user interface)	• **Supported:** JRE version 6 or 7 (JRE 7 update 45 is the latest certified version) • **Recommended:** JRE 7 **Tip:** Java is installed as part of the SiteScope installation and should not be patched or updated independently.You can check the version of Java by going to **<SiteScope installation directory>\java\bin** and running the following from the command line: `java –server –fullversion`

SiteScope Capacity Limitations

When SiteScope is integrated with BSM, performing 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 Service Management 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 21.

SiteScope Support Matrices

This section includes:

- "HP Business Service Management Integration Support Matrix" below

- "HP Operations Manager (HPOM) Integration Support Matrix" on the next page

- "HP Operations Agent Support Matrix" on page 74

- "HP SiteScope for Load Testing Support Matrix" on page 74

- "HP Network Node Manager i (NNMi) Support Matrix" on page 75

Note: Co-existent deployments of SiteScope with other products are not recommended. HP plans to stop support for co-existent deployments of SiteScope with other products in future versions.

HP Business Service Management Integration Support Matrix

For the most up-to-date version of the support matrix, including the latest certified service packs, check the HP Integrations site (http://support.openview.hp.com/sc/solutions/index.jsp#tab=tab3).

HP SiteScope Version	HP Business Service Management Version				
	9.2x	9.1x	9.0x	8.x	7.x
SiteScope 11.2x	√ (Recommended)	√	√	√	X

HP Operations Manager (HPOM) Integration Support Matrix

For the most up-to-date version of the support matrix, including the latest certified service packs, check the HP Integrations site (http://support.openview.hp.com/sc/solutions/index.jsp#tab=tab3).

HPOM Version	SiteScope 11.2x Integration			
	Events integration	Node discovery Integration	Monitor Discovery Integration	Template Integration
HPOM for Windows 8.1x (with patch OMW_00149)	Supported	Supported	Supported	Not supported
HPOM for Windows 9.0	Supported	Supported with patch OMW_ 00097/98 or later (32-bit/64-bit)	Supported	Supported with patch 159
HPOM for Linux/Solaris 9.0	Supported	Not supported	Supported	Supported
HPOM for Linux/Solaris 9.10	Supported	Supported with patch 9.10.200 or later	Supported	Supported with patch 9.10.210 and hotfix QCCR1A1257 51, or with patches later than 9.10.210

Coexistence Support

If you plan to install HP Operations Manager and SiteScope on the same server, you need to check the support for coexistence of both the products.

HPOM Version	SiteScope Version	
	SiteScope 11.12	SiteScope 11.2x
HPOM for Windows 9.0	Not supported	Supported on Microsoft Windows Server 2008 R2 with patch OMW_00145_6 or later

HPOM for Linux/Solaris 9.00	Supported on Red Hat ES Linux 5.8	• Supported on Red Hat ES Linux 5.8 • Supported on Solaris 10 with patch 119254-43 or 119255-43
HPOM for Linux/Solaris 9.10	Supported on Red Hat ES Linux 5.8 with patch 9.10.210 or later	• Supported on Red Hat ES Linux 5.8 with patch 9.10.220 or later • Supported on Solaris 10 with patch 119254-43 or 119255-43

Note: For HP Operations Manager hardware and software configuration requirements, see the relevant version of the Operations Manager for Windows/UNIX Installation Guide available on the SSO Product Manuals site (http://support.openview.hp.com/selfsolve/manuals).

HP Operations Agent Support Matrix

HP SiteScope Version	HP Operations Agent Version
11.0x	8.60.70
11.1x	8.60.501
11.2x	11.02.011 **Note:** SiteScope 11.23 has been certified with HP Operations agent 11.13.07 (upgraded from 11.02.011).

Note:

- Microsoft Installer 4.5 or later is required for installing the HP Operations agent.

- The HP Operations agent is not supported on SiteScopes installed on Microsoft Windows 2003 with SP1.

- For more information on HP Operations agent installation requirements, see the HP Operations agent documentation available from **<SiteScope root directory>\installation\components\oa\win\paperdocs** or from the HP Software Product Manuals Web site (http://h20230.www2.hp.com/selfsolve/manuals).

HP SiteScope for Load Testing Support Matrix

For the most up-to-date version of the support matrix, including the latest certified service packs, check the HP Integrations site (http://support.openview.hp.com/sc/solutions/index.jsp#tab=tab3).

HP SiteScope Version	HP Performance Center	HP LoadRunner
SiteScope 10.10	9.10, 9.50	9.50
SiteScope 10.11	9.10, 9.50	9.50
SiteScope 10.12	9.50	9.50
SiteScope 10.13	9.50	9.50
SiteScope 10.14	9.50	9.50
SiteScope 11.00	9.50, 11.00	9.50,11.00
SiteScope 11.01	9.50, 11.00	9.50,11.00
SiteScope 11.10	11.00*, 11.50**	11.00, 11.50

SiteScope 11.11	11.00*, 11.50**	11.00, 11.50
SiteScope 11.12	11.00, 11.50***	11.00, 11.50
SiteScope 11.20	11.50	11.50
SiteScope 11.21	11.50	11.50
SiteScope 11.22	11.50	11.50****
SiteScope 11.23	11.50	11.50****

* PC topology integration is not supported.

** PC topology/PAL integration is not supported.

*** PAL integration is not supported.

**** User authentication on the SiteScope side is not supported.

HP Network Node Manager i (NNMi) Support Matrix

For the most up-to-date version of the support matrix, including the latest certified service packs, check the HP Integrations site (http://support.openview.hp.com/sc/solutions/index.jsp#tab=tab3).

Integration	Supported Versions
Event Integration	SiteScope version 11.10 or later NNMi version 9.10 or later (9.21 is the latest certified NNMi version)
Metrics Integration	SiteScope version 11.10 or later NNMi version 9.10 or later NNM iSPI Performance for Metrics version 9.10 or later (9.22 is the latest NNMi certified version)

Chapter 10: Upgrading SiteScope

This chapter includes:

Before Performing the Upgrade

This section describes how to upgrade existing SiteScope installations to SiteScope 11.2x with minimum interruption to your system and operations.

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:

- Install SiteScope on supported Windows, Solaris, or Linux environments as listed in "System Requirements" on page 65. Check the "HP Operations Agent Support Matrix" on page 74 for HP Operations agent prerequisites and installation requirements.

- SiteScope 11.20 must be installed before you can install the latest minor-minor version (for example, 11.23). SiteScope 11.23 can be installed on top of SiteScope 11.2x.

- You can upgrade from SiteScope 10.x or later to SiteScope 11.23 by using the Configuration

Tool to make a backup of your current SiteScope configuration data, uninstalling your current SiteScope version (10.x or 11.x), installing SiteScope 11.20 followed by SiteScope 11.23 on top of it, and then importing the configuration data back into SiteScope. For details, see "Upgrading an Existing SiteScope Installation" below. For versions of SiteScope earlier than 10.00, you must first upgrade to SiteScope 10.x. For versions of SiteScope earlier than 9.00, you must first upgrade to SiteScope 9.x. For upgrade instructions, see the upgrade instructions for the relevant version.

Note: Cross-platform upgrade is not supported. You should avoid importing SiteScope Windows configurations into Linux or Solaris deployments. The same applies for moving from 32- to 64-bit (or opposite).

- Since SiteScope version 10.10, the HTTP method for connecting to a UNIX remote server is no longer supported. 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.

- The custom properties mechanism for adding custom property settings to SiteScope monitors was removed from SiteScope version 10.00, and the filtering functionality was replaced by the Tags mechanism. When upgrading from versions of SiteScope earlier than 10.00, you can convert custom properties to Search/Filter Tags. For details, see "Converting Custom Properties to Search/Filter Tags" on page 80.

- (Applies to the deprecated SiteScope Failover Manager solution) When SiteScope 11.2x is installed on a UNC path (a UNC path is a requirement for SiteScope Failover Manager, Windows only), the patch install/uninstall prompts you to provide the UNC installation path log-on credentials. The patch (MSI) install executes its post-install/pre-remove logic scripts as user "NT AUTHORITY/SYSTEM". This user does not have a mapping to any UNC drive, and failure to provide the correct log-on credentials causes the patch installation to fail. The patch uses these credentials to create a mapping to the UNC installation path for user "NT AUTHORITY/SYSTEM" during the patch installation, and removes the mapping at the end of the installation.

Upgrading an Existing SiteScope Installation

Note: This topic contains instructions for upgrading your version of SiteScope to the latest patch release. For instructions on installing a major or minor version of SiteScope (such as 11.20), see "Installation Workflow" on page 98. For information on upgrading from SiteScope Freemium to the latest version of SiteScope, see "SiteScope Freemium Installation Workflow" on page 100.

It is recommended that you perform the following steps for upgrading your version of SiteScope:

1. **Make sure the SiteScope process/service has been stopped (the installer should automatically stop the process before installation).**

   For more information, see "Starting and Stopping the SiteScope Service on Windows Platform" on page 190 or "Starting and Stopping the SiteScope Process on Solaris and Linux Platforms" on page 191.

2. **Make a backup copy of SiteScope monitor configuration data using the Configuration Tool from your current version of SiteScope.**

   Use the Configuration Tool to make a backup of your current SiteScope installation directory by exporting SiteScope data from your current SiteScope for later import into SiteScope. For more information, see "Backing Up SiteScope Configuration Data" on the next page.

3. **(If using a version of SiteScope earlier than 11.20) Uninstall the current version of SiteScope and install SiteScope 11.20 in a clean directory structure.**

   For information on uninstalling SiteScope, see "Uninstalling SiteScope" on page 158.

   SiteScope 11.20 must be installed before you can install the latest minor-minor version (for example, 11.23). For information on installing SiteScope 11.20, see "Installation Workflow" on page 98.

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

4. **Download and install the latest SiteScope 11.2x minor-minor version and cumulative patch.**

   You can download minor-minor versions and cumulative patches (if available) from the **Downloads** page > **Software Patches** on the HP Software Support web site.

   Minor-minor versions are cumulative; you can install SiteScope 11.23 on top of SiteScope 11.20 directly (you do not need to install SiteScope 11.22).

   a. Go to the SSO site

      http://support.openview.hp.com/selfsolve/patches

   b. Select **SiteScope** and select the most recent 11.2x minor-minor version.

   c. Click **Search** to locate the installation files.

   d. Save the package locally and launch the relevant setup file to install the patch.

   e. Run the installation file and follow the on-screen instructions.

   > **Note:** To install a SiteScope minor-minor version using a silent installation, see "How

    f. Install the latest cumulative/intermediate patch (if available) for the minor-minor version (shown on the HP Support site in the **Software Patches** section for 11.23).

> **Note:** The HP Operations agent is not supported when installing SiteScope 11.23 on a Microsoft Windows Server 2012 environment. As a result, the HP Operations Manager Event and Metrics Integration is not supported in SiteScopes running on Windows Server 2012.

5. **After installation, import the monitor configuration data (from Step 2) using the Configuration Tool.**

   For more information, see .

6. **After importing data from earlier versions of SiteScope, start SiteScope 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 command shell script using the syntax `<installpath>/SiteScope/start` (on Solaris or Linux platforms).

7. **If using SiteScope Failover, upgrade the Failover server with the corresponding SiteScope Failover version.**

   After upgrading the primary server, upgrade the Failover server with the corresponding SiteScope Failover version, and connect the Failover server to the upgraded primary server.

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:\11.20\SiteScope`.

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, server certificates, scripts, and so forth from your current SiteScope for later import into SiteScope. The user data is exported to a **.zip** file.

Alternatively, you can manually back up your SiteScope installation. For details, see .

> **Note:** You should make a backup of the **<SiteScope>\htdocs** directory and copy it to the SiteScope 11.20 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 "Using the SiteScope Configuration Tool" on page 138.

Alternatively, you can have SiteScope export SiteScope data as part of the installation process. For details, see "Installation Workflow" on page 98.

Importing Configuration Data

After upgrading SiteScope, monitor configuration data can be copied from earlier versions of SiteScope using the Configuration Tool. For details, see "Using the SiteScope Configuration Tool" on page 138.

Alternatively, if you manually created a back up, you must delete from the new installation directory all the folders and files that you backed up, and then copy the backed up folders and files to the installation directory. For details, see "Backing up and recovering a SiteScope installation if unable to start SiteScope" on page 196.

Converting Custom Properties to Search/Filter Tags

Custom properties are no longer supported in SiteScope. When upgrading from SiteScope versions earlier than 10.00, you can convert custom properties to Search/Filter Tags by creating a mapping file, and then running the custom properties conversion tool.

To convert custom properties to search/filter tags:

1. In a text editor, create a mapping file by mapping custom properties to search/filter tags using the following format:

   ```
   <Custom Property Name>,<Custom Property Value>-><Tag Name>,<Tag Value>
   ```

   Where:

   `<Custom Property Name>` is the custom property configured in the **master.config** file.

   `<Custom Property Value>` is the value of the given custom property name above.

   `<Tag Name>` is the name of the tag to add to the monitor (the tag must already exist as a Search/Filter Tag in your system).

   `<Tag Value>` is the value of the tag name above that corresponds to the custom property value.

   For example:

```
_custPropSeverity,MINOR->Severity,MINOR
_custPropServiceGroup,Sales->Notification Group,Sales
```

> **Note:** You must not leave empty spaces between the , < > -> characters in the mapping file.

2. Save the file.

3. Open a command line, and enter the following:

   - For Windows environments:

     ```
     <SiteScope root directory>\tools\CustomPropertyToTagTool.bat
     <path to mapping file> <path to SiteScope persistency folder>
     ```

   - For Linux or Solaris environments:

     ```
     <SiteScope root directory>\tools\CustomPropertyToTagTool.sh
     <path to mapping file> <path to SiteScope persistency folder>
     ```

   For example (on a Windows platform):

   ```
   C:\SiteScope\tools\CustomPropertyToTagTool.bat C:\Desktop\configFile2.txt
   C:\SiteScope\persistency
   ```

Upgrading SiteScope 8.9 to SiteScope 9.5.4

It is recommended that you perform the following steps to upgrade from SiteScope 8.9 to SiteScope 9.5.4:

To perform the upgrade:

1. Check the "_version" value in the **master.config** file and persistency. It should be in the format `8.9 17:20:04 2006-11-05 build 257`. If the version looks like "`_version=750`" it should be corrected.

2. Suspend all monitors.

3. Make a backup of the configuration from the SiteScope 8.9 or full SiteScope folder.

4. Install SiteScope 9.5.0.

5. Install SiteScope 9.5.4.

6. Import the configuration.

7. Before starting SiteScope, open **<SiteScope root>\groups\master.config** and perform the following:

   - Add the **_disableHostDNSResolution=true** property.

   - Check that the **_sendRemoteServerDisplayNameToBAC** property is not in the file.

8. Start SiteScope 9.5.4 and wait.

9. Restart SiteScope. Open the SiteScope user interface and check the BAC integration (confirm that you can see the BAC integration settings in **Preferences > Integration Preferences**).

10. Export the configuration with **topazIDs.bat**. Check that targets are the same as in SiteScope 8.9 and no "-1" appears.

Upgrading SiteScope 9.5.4 to SiteScope 10.14

It is recommended that you perform the following steps to upgrade from SiteScope 9.5.4 to SiteScope10.14:

To perform the upgrade:

1. Stop the SiteScope service.

2. Backup the SiteScope 9.5.4 folder (copy it to a temp folder on your system).

3. Export SiteScope configuration from SiteScope 9.5.4:

   - Launch the SiteScope Configuration Tool (**Start > Programs > HP SiteScope > Configuration Tool**) and click **Next**.

   - Select **Export/Import User Data** and click **Next**.

   - Select **Export User data** and click **Next**.

   - Select the location of the SiteScope 9.5.4 installation directory, and a target directory where you want to save exported data. Enter a backup file name. Leave **Include log files** unchecked.

   - After the export is completed, click **Next/Finish**.

   - Copy the third-party libraries and jars that are used for various monitors (for example, SAP client, JDBC drivers) to the temp directory, since these files are not included in the export.

4. Uninstall SiteScope 9.5.4 (**Start > Settings > Control panel > Add or Remove Programs**):

- Uninstall Window launches. Click **Next** twice and uninstall begins.

- After uninstall is complete, click **Finish**.

- Delete any remaining files under the SiteScope directory.

- Confirm that the **SiteScope** service was removed with the uninstall from the Windows services. If the SiteScope service is still displayed, it can be removed manually by running "`sc delete SiteScope`" from command prompt.

5. Reboot the server.

6. Install SiteScope 10.10:

- Run the SiteScope 10.10 installer and click **Next**.

- Accept the license agreement and click **Next**.

- Select a directory for SiteScope 10.10 and click Next (we recommend using the same directory that was used for 9.5.4).

- Select **HP SiteScope** installation type and click **Next**.

- Leave the default port and enter admin email, and then click **Next**.

- Enter the SiteScope 10.10 license, and then click **Next**.

- The summary screen is displayed. Click **Next**.

- After installation is complete, click **Next** (the installer windows closes).

7. Stop the SiteScope service.

8. Set the SiteScope service to run under a monitoring account (local or domain administrator). This step can be skipped, depending on how it was configured for 9.5.4.

9. Install the SiteScope 10.14 patch:

- Run the SiteScope 10.14 installer, and click **Next**.

- Verify the SiteScope service is not running and click **Next**.

- Click **Next** in the License Agreement screen.

- Click **Next** in the Summary screen and 10.14 installation begins.

- After installation is completed, click Next and then click **Finish**.

10. Install hotfixes for SiteScope 10.14.

11. Import data into SiteScope:

- Run the Configuration Tool (**Start > Programs > HP SiteScope > Configuration Tool**) and click **Next**.

- Select **Export/Import User Data** and click **Next**.

- Select **Import User Data** and click **Next**.

- Select the **.zip** file previously exported from the 9.5.4 configuration. Verify the target directory is correct and then click **Next**.

- After import is completed, click **Finish** (the configuration tool closes).

- Restore the third-party libraries and jars that were copied to the temp folder (in step 3).

12. Change data reduction and other parameters in the **master.config** file:

- Open **<SiteScope root>\groups\master.config**.

- Change the line:

  _topazEnforceUseDataReduction=

  to

  _topazEnforceUseDataReduction=false

  > **Note:** If the parameter does not exist, add it so it is set to false.

- Change the line:

  _suspendMonitors=

  to

  _suspendMonitors=true

- Add the parameter:

  _disableHostDNSResolution=true

  > **Note:** All parameters should be added so they are in alphabetical order.

- Save and close the **master.config** file.

13. Launch the SiteScope with your configuration (it will be upgraded during the first run):

- Start SiteScope 10.14.

- Check that all entities that were in the previous configuration are stored in the new SiteScope.

- Check the BAC integration:

  Wait for SiteScope to be started and logged in with the new user interface. Check in SiteScope **Preferences > Integration Preferences** to confirm that you can see the BAC integration settings (for example, the BAC server). If you do not see the integration information on this screen then the data is most likely corrupted. You can confirm this by looking at the BAC integration log (**<SiteScope root>\logs\bac_integration\ bac_ integration.log**). You will see many entries like this:

  ```
  ERROR - Error: TopologyReporterSender Topology Reporter failed to report,
  exception in main loop: Host of origin may not be blank
  ```

- Make sure that you can see your configuration in the user interface, and SiteScope is working fine, and then stop SiteScope.

14. Open the **master.config** file and perform the following:

    - Unsuspend monitors by changing:

      _suspendMonitors=true

      to

      _suspendMonitors=

    - Enable data reduction by changing:

      _topazEnforceUseDataReduction= false

      to

      _topazEnforceUseDataReduction=

    - Save and close the **master.config** file and then start SiteScope again. Log in through the user interface, and check that it is working correctly.

Upgrading SiteScope 10.14 to SiteScope 11.2x

It is recommended that you perform the following steps to upgrade from SiteScope 10.14 to SiteScope 11.2x:

To perform the upgrade:

1. Stop the SiteScope service.

2. Backup the SiteScope 10.14 folder (copy it to a temp folder on your system).

3. Export SiteScope configuration from SiteScope 10.14:

   ▪ Launch the SiteScope Configuration Tool (**Start > Programs > HP SiteScope > Configuration Tool**) and click **Next**.

   ▪ Select **Export/Import User Data** and click **Next**.

   ▪ Select **Export User data** and click **Next**.

   ▪ Select the location of the SiteScope 10.14 installation directory, and a target directory where you want to save exported data. Enter a backup file name. Leave **Include log files** unchecked.

   ▪ After the export is completed, click **Next/Finish**.

   ▪ Copy the third-party libraries and jars that are used for various monitors (for example, SAP client, JDBC drivers) to the temp directory, since these files are not included in the export.

4. Uninstall SiteScope 10.14 (**Start > Settings > Control panel > Add or Remove Programs**):

   ▪ Uninstall Window launches. Click **Next** twice and uninstall begins.

   ▪ After uninstall is complete, click **Finish**.

   ▪ Delete any remaining files under the SiteScope directory.

   ▪ Confirm that the **SiteScope** service was removed with the uninstall from the Windows services. If the SiteScope service is still displayed, it can be removed manually by running "`sc delete SiteScope`" from command prompt.

5. Reboot the server.

6. Install SiteScope 11.20:

   ▪ Run the SiteScope11.20 installer and click **Next**.

   ▪ Accept the license agreement and click **Next**.

   ▪ Select a directory for SiteScope 11.20 and click **Next** (we recommend using the same directory that was used for 10.14).

   ▪ Select **HP SiteScope** installation type and click **Next**.

   ▪ Leave the default port and enter admin email, and then click **Next**. If the default port is taken, enter 8088 instead.

- Leave license blank and click **Next**.

- In the summary screen click **Next**.

- After installation is complete, click **Next** (the installer windows closes).

- Restore third-party libraries and jars that were copied to the temp folder (in step 3).

7. Stop the SiteScope service.

8. Install the latest 11.2x minor-minor version, and any required cumulative/intermediate patches (if available) for the minor-minor version (shown on the HP Support site in the **Software Patches** section for the minor-minor version).

9. Set the SiteScope service to run under a monitoring account. This step can be skipped for module SiteScopes.

10. Import data into SiteScope:

- Run the Configuration Tool (**Start > Programs > HP SiteScope > Configuration Tool**) and click **Next**.

- Select **Export/Import User Data** and click **Next**.

- Select **Import User Data** and click **Next**.

- Click **Next**.

- Select the **.zip** file previously exported from the 10.14 installation, verify the target directory is correct, and then click **Next**.

- After import is completed, click **Finish** (the configuration tool closes).

   Note: Run the Configuration Tool a second time and select the **Sizing** option.

11. Change data reduction and other parameters in the **master.config** file:

- Open the **<SiteScope root>\groups\master.config** file.

- Change the line:

   _topazEnforceUseDataReduction=

   to

   _topazEnforceUseDataReduction=false

> **Note:** If the parameter does not exist, add it so it is set to false.

- Change the line:

  _suspendMonitors=

  to

  _suspendMonitors=true

- Add the parameter:

  _disableHostDNSResolution=true

  > **Note:** All parameters should be added so they are in alphabetical order.

- Save and close the **master.config** file.

12. Enable SiteScope alerts to BSM.

    - Go to the **<SiteScope root>\bin** folder and run the **PersistencyViewer.bat** file.

    - Click the **Select Persistency Path** button, and in the persistency folder, click the **Open** button.

    - In the Filter by type drop-down, look for the class `com.mercury.sitescope.platform.configmanager.MasterConfig`.

      This displays the same list of properties that you can see in the **master.config** file. Look for **_topazAlertEnabled** and verify that it is set to **=1**. Add the property if it is not there.

    - After making changes, click the commit button.

13. Start the SiteScope service. SiteScope upgrades the configuration and then restarts itself. Log in using the user interface and verify the integration to BSM is correct under **Preferences > Integration Settings**.

14. Stop SiteScope.

15. Open the **master.config** file and perform the following:

    - Unsuspend monitors by changing:

      _suspendMonitors=true

      to

      _suspendMonitors=

- Enable data reduction by changing:

  _topazEnforceUseDataReduction= false

  to

  _topazEnforceUseDataReduction=

- Change the parameter:

  _disableHostDNSResolution=false

- Save and close the **master.config** file and then start SiteScope.

Upgrading SiteScope 11.x to SiteScope 11.2x

It is recommended that you perform the following steps to upgrade from SiteScope 11.x to SiteScope 11.2x:

To perform the upgrade:

1. Stop the SiteScope service.

2. Backup the SiteScope 11.x folder (copy it to a temp folder on your system).

3. Export SiteScope configuration from SiteScope 11.x:

   - Launch the SiteScope Configuration Tool (**Start > Programs > HP SiteScope > Configuration Tool**) and click **Next**.

   - Select **Export configuration** and click **Next**.

   - In the Export Configuration screen, select the location of the SiteScope 11.x installation directory, and a target directory where you want to save exported data. Enter a backup file name. Leave **Include log files** unchecked.

   - After the export is completed, click **Next/Finish**.

   - Copy the third-party libraries and jars that are used for various monitors (for example, SAP client, JDBC drivers) to the temp directory, since these files are not included in the export.

4. Uninstall SiteScope 11.x (**Start > Settings > Control panel > Add or Remove Programs**):

   - Uninstall Window launches. Click **Next** twice and uninstall begins.

   - After uninstall is complete, click **Finish**.

   - Delete any remaining files under the SiteScope directory.

- Confirm that the **SiteScope** service was removed with the uninstall from the Windows services. If the SiteScope service is still displayed, it can be removed manually by running "`sc delete SiteScope`" from command prompt.

5. Reboot the server.

6. Install SiteScope 11.20:

   - Run the SiteScope 11.20 installer and click **Next**.

   - Accept the license agreement and click **Next**.

   - Select a directory for SiteScope 11.20 and click **Next** (we recommend using the same directory that was used for 11.x).

   - Select **HP SiteScope** installation type and click **Next**.

   - Leave the default port and enter admin email, and then click **Next**. If the default port is taken, enter 8088 instead.

   - Leave license blank and click **Next**.

   - In the summary screen click **Next**.

   - After installation is complete, click **Next** (the installer windows closes).

   - Restore third-party libraries and jars that were copied to the temp folder (in step 3).

7. Stop the SiteScope service.

8. Install the latest 11.2x minor-minor version, and any required cumulative/intermediate patches (if available) for the minor-minor version (shown on the HP Support site in the **Software Patches** section for the minor-minor version).

9. Set the SiteScope service to run under a monitoring account. This step can be skipped for module SiteScopes.

10. Import data into SiteScope:

    - Run the Configuration Tool (**Start > Programs > HP SiteScope > Configuration Tool**) and click **Next**.

    - Select **Import configuration** and click **Next**.

    - In the Import Configuration screen, select the zip file previously exported from the 11.x installation, verify the target directory is correct, and then click **Next**.

■ After import is completed, click **Finish** (the configuration tool closes).

> **Note:** Run the Configuration Tool a second time and select the **Sizing** option.

11. Change data reduction and other parameters in the **master.config** file:

■ Open the **<SiteScope root>\groups\master.config** file.

■ Change the line:

_topazEnforceUseDataReduction=

to

_topazEnforceUseDataReduction=false

> **Note:** If the parameter does not exist, add it so it is set to false.

■ Change the line:

_suspendMonitors=

to

_suspendMonitors=true

■ Add the parameter:

_disableHostDNSResolution=true

> **Note:** All parameters should be added so they are in alphabetical order.

■ Save and close the **master.config** file.

12. Enable SiteScope alerts to BSM.

■ Go to the **<SiteScope root>\bin** folder and run the **PersistencyViewer.bat** file.

■ Click the **Select Persistency Path** button, and in the persistency folder, click the **Open** button.

■ In the Filter by type drop-down, look for the class
`com.mercury.sitescope.platform.configmanager.MasterConfig`.

This displays the same list of properties that you can see in the **master.config** file. Look for

_topazAlertEnabled and verify that it is set to **=1**. Add the property if it is not there.

- After making changes, click the commit button.

13. Start the SiteScope service. SiteScope upgrades the configuration and then restarts itself. Log in using the user interface and verify the integration to BSM is correct under **Preferences > Integration Settings**.

14. Stop SiteScope.

15. Open the **master.config** file and perform the following:

- Unsuspend monitors by changing:

    _suspendMonitors=true

    to

    _suspendMonitors=

- Enable data reduction by changing:

    _topazEnforceUseDataReduction= false

    to

    _topazEnforceUseDataReduction=

- Change the parameter:

    _disableHostDNSResolution=false

- Save and close the **master.config** file and then start SiteScope.

Upgrading SiteScope Freemium to Full Edition SiteScope

Upgrading from SiteScope Freemium to the full edition of SiteScope enables you to benefit from the additional functionality available in the full edition. For a comparison of the features available in the SiteScope Freemium edition compared with those available in the full edition of SiteScope, see "SiteScope Freemium" on page 11.

To upgrade from SiteScope Freemium to the full edition of SiteScope, you need to purchase and import the SiteScope license and follow the instructions on the screen. For details, see "Adding SiteScope Licenses" on page 62.

Note:

- If you are upgrading from SiteScope Freemium to use SiteScope on an operating system other than Windows 64-bit, or integrating SiteScope with HP Business Service Management (BSM) or HP Operations Manager (HPOM), you need to perform the steps in the section "Upgrading an Existing SiteScope Installation" on page 77.

- When upgrading SiteScope Freemium 11.22 to SiteScope 11.23 (full edition), you must use the Sitescope 32 over 64-bit installer. The installation remains 64-bit as it was before the upgrade.

Troubleshooting and Limitations

This section describes troubleshooting and limitations for SiteScope upgrades.

- "First SiteScope Restart After Upgrade Can Take a Long Time" below

- "SiteScope Fails to Get the Customer ID" on the next page

- "Default Alert Action Is Named According to Action Type" on the next page

- "BSM/ServiceCenter or Service Manager Integration" on the next page

- "Moving SiteScope to a Different Server When Integrated with BSM" on the next page

- "SiteScope Fails to Upgrade" on page 95

- "SSL/Tomcat Configuration File Overwritten After Upgrade from SiteScope 11.21" on page 95

- "Monitors Using Certificates from SiteScope Certificate Management are in Error State After Upgrade from SiteScope 11.21" on page 96

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 on 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 command shell script using the syntax **<installpath>/SiteScope/start** (on Solaris or Linux 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 BSM, 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 BSM 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 BSM. If BSM is down during the restart, SiteScope is unable to retrieve the customer ID, and SiteScope restarts itself again.

Possible Solution: Make sure that any BSM 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.

BSM/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 BSM/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.

Moving SiteScope to a Different Server When Integrated with BSM

This process is relevant if you are moving your SiteScope server to new hardware (with a new host name and IP address) and you are working with the BSM integration. Perform the following steps to minimize the impact on the integration:

1. Make a backup of your current SiteScope installation. For details, see "Backing Up SiteScope Configuration Data" on page 79.

2. Install SiteScope on the new hardware, and import the SiteScope configuration data to the SiteScope installation directory. For details, see "Importing Configuration Data" on page 80.

3. Configure the SiteScope server with the same port number that was used on the old hardware.

4. Perform the following in BSM:

   ▪ Update the relevant fields for the SiteScope profile in the New SiteScope page.

   ▪ Update the information about the SiteScope machine in the HOSTS table.

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.

SSL/Tomcat Configuration File Overwritten After Upgrade from SiteScope 11.21

Problem: After upgrading from SiteScope 11.21, the Tomcat configuration **server.xml** file in the **<SiteScope root directory>\Tomcat\conf** directory is overwritten and any modifications made to that file are removed (for example, changes made when configuring SiteScope to use SSL).

Solution: To restore these modifications, you must reapply them to the **server.xml** file after performing the upgrade.

1. Stop SiteScope.

2. Replace the following files:

Replace File	With
<SiteScope root directory>\ java\lib\security\cacerts	**<SiteScope root directory>\installation\ HPSiS1122\backup\java\lib\security\cacerts**
<SiteScope root directory>\ java\lib\security\java.security	**<SiteScope root directory>\installation\ HPSiS1122\backup\java\lib\security\java.security**
<SiteScope root directory>\ java\lib\security\javaws.policy	**<SiteScope root directory>\installation\ HPSiS1122\backup\java\lib\security\javaws.policy**
<SiteScope root directory>\ java\lib\security\java.policy	**<SiteScope root directory>\installation\ HPSiS1122\backup\java\lib\security\java.policy**

3. Manually reapply all hardening and other customization changes by copying them from

<SiteScope root directory>\installation\HPSiS1122\backup\Tomcat\conf\server.xml to
<SiteScope root directory>\Tomcat\conf\server.xml.

Monitors Using Certificates from SiteScope Certificate Management are in Error State After Upgrade from SiteScope 11.21

Problem: Some monitors, which use certificates from cacerts file, are in error state after upgrading from SiteScope 11.21.

Solution:

1. Stop SiteScope.

2. Replace **<SiteScope root directory>\java\lib\security\cacerts** with **<SiteScope root directory>\installation\HPSiS1122\backup\java\lib\security\cacerts**.

Part 3: Installing SiteScope

Chapter 11: Installation Workflow

SiteScope is installed on a single server, and runs as a single application on Windows platforms, or as a single application or various processes on Solaris or Linux platforms.

This section contains:

- "Installation Version Types" below

- "Installation Flow" on the next page

Installation Version Types

SiteScope is available as a self-extracting executable file and packages folder. For major or minor releases, this file is available on the DVD that comes with the SiteScope media kit, or you can download it from the **Software Updates** page.

For minor-minor and patch releases, you download this file from the **Downloads** page > **Software Patches** on the HP Software Support web site (http://support.openview.hp.com/selfsolve/patches).

Minor-minor versions are cumulative; you can install SiteScope 11.23 on top of SiteScope 11.20 directly (you do not need to install SiteScope 11.22). Every new patch always supersedes the previous patch.

If you want to install the latest possible version, you need to install SiteScope 11.20, then the latest minor-minor version (11.23), then the latest cumulative/intermediate patch for the minor-minor version (shown on the HP Support site in the Patches section for 11.23).

Official Name	Version Type	Example	Installation

Major
Minor
	Full Installer release	10.0, 11.0
		
		10.10, 11.20
		
		Example file name:
		`HPSiteScope_11.20_`
		`setup.exe`
			Install on a clean system, and import previous release configuration. Upgrade is executed on first start up.

Minor-Minor (patch)	Collection of defect fixes from corresponding Major or Minor release	10.11 (on top of 10.10)
		11.01 (on top of 11.00)
		11.23 (on top of 11.20 or 11.2x)
		
		Example file name:
		`HPSiS1122_11.23_`
		`setup.exe`
			Minor-Minor patch is installed on top of its corresponding release. It does not require an upgrade.

Official Name	Version Type	Example	Installation
Cumulative / Intermediate / Public patch	Packages containing official fixes for urgent defects	SS1122130529 SS<ver><date> Example file name: `SS1122130529-11.22.000-WinNT4.0.msi`	Applicable only on top of a single dedicated Major, Minor, or Minor-Minor release.

Installation Flow

> **Note:** This topic contains instructions for installing major or minor releases. For instructions on installing SiteScope patch releases, see "Upgrading an Existing SiteScope Installation" on page 77.

1. **Installation Prerequisites (for Solaris or Linux only).**

   a. Select a suitable installation location and set account permissions. For details, see "Preparing for Solaris or Linux Installation" on page 101.

   b. If you are installing SiteScope on one of the following platforms, you need to manually configure the environment before installing SiteScope:

      ○ **Oracle Enterprise Linux 6.0, 6.1**. For details, see "Installing SiteScope on an Oracle Enterprise Linux Environment" on page 102.

      ○ **CentOS 6.2**. For details, see "Installing SiteScope on a CentOS 6.2 Environment" on page 103.

      ○ **HP Cloud Services (HPCS) instance running on a CentOS 6.2 operating system**. For details, see "Installing SiteScope on an HP Cloud Services Instance Running on CentOS 6.2" on page 103.

      ○ **Red Hat ES/AS Linux 6.0**. For details, see "Installing Dependencies Required by the HP Operations Agent" on page 105.

2. **Install SiteScope 11.20.**

   ▪ For details on installing on Windows, see "Installing Using the Installation Wizard" on page 110.

   ▪ SiteScope for Solaris and SiteScope for Linux have the following installation options:

      ○ User interface executable (installation wizard). For details, see "Installing Using the Installation Wizard" on page 110.

○ Console mode installation script using command line input. For details, see "Installing on Solaris or Linux Using Console Mode" on page 129.

■ You can also install SiteScope using a silent installation. For details, see "Installing SiteScope in Silent Mode" on page 136.

> **Note:**
>
> ○ If there is an existing version of SiteScope installed, you must uninstall it before installing SiteScope 11.20.
>
> ○ If you previously exported SiteScope data using the Configuration Tool (for details, see "Using the SiteScope Configuration Tool" on page 138), you can import the user data **.zip** file.
>
> ○ If you have third-party middleware and drivers, you must copy or install them manually.

3. **Connect to SiteScope.**

   For details, see "Connecting to SiteScope" on page 192.

SiteScope Freemium Installation Workflow

The SiteScope Freemium edition is a version of SiteScope that enables you to try SiteScope for an unlimited period of time for free. SiteScope Freemium can be installed only on a 64-bit Windows platform.

1. **Download the SiteScope Freemium version from the HP SiteScope Product page (hp.com/go/SiteScope).**

2. **Run the SiteScope installation.**

   a. Run **HPSiteScope_11.xx_setup.exe**

   b. Perform the installation procedure in "Installing Using the Installation Wizard" on page 110, starting from step 3.

3. **Connect to SiteScope.**

   For details, see "Connecting to SiteScope" on page 192.

4. **(Optional) Upgrade to a full version of SiteScope.**

   You can upgrade to a full version of SiteScope any time. For details, see "Upgrading SiteScope Freemium to Full Edition SiteScope" on page 92.

Preparing for a 64-Bit SiteScope Installation

SiteScope can execute as a 32-bit or 64-bit application. SiteScope is installed and run as a 64-bit application in the following scenarios:

- Running **HPSiteScope_11.20_setup.exe** on a 64-bit Windows system.

- Running **HPSiteScope_11.20_setup.bin** on a 64-bit Linux or Solaris system.

> **Note:**
>
> - The **HPSiteScope32on64_11.20_setup.exe** installer installs SiteScope as a 32-bit application on a Windows 64-bit system. You can use this version to overcome the limitations of 64-bit SiteScope.
>
> - The Freemium version of SiteScope is supported only on a 64-bit Windows system. To install SiteScope Freemium, run **HPSiteScope_11.xx_setup.exe**.

Before you install SiteScope be aware that:

- Some monitors do not support working with the 64-bit version of SiteScope, so if you plan to work with any one of these monitors, it is recommended to install the SiteScope 32-bit version. For the list of monitors not supported by the 64-bit version of SiteScope, see "Windows Monitors Not Supported by 64-Bit SiteScope" on page 67.

- The 32-bit processes can only access 4 GB of virtual memory, while 64-bit processes can access 8 TB of virtual memory address space and increase the monitoring capacity of SiteScope.

- The SiteScope 64-bit version consumes up to 3 times more memory than the SiteScope 32-bit version. Accordingly, if you are using a SiteScope 64-bit version you should manually increase the JVM heap size on the server, as described in "Using the SiteScope Configuration Tool" on page 138.

Preparing for Solaris or Linux Installation

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

To prepare for installation of SiteScope on Solaris or Linux:

1. Verify that the installation location for the SiteScope application (`/opt/HP/SiteScope`) has access to sufficient disk space for the installation and operation of SiteScope.

2. Create a non-root user account that runs the SiteScope application, and set account permissions to `/opt/HP/SiteScope` for this user. Set the default shell for the account. For

details, see "Configuring a Non-Root User Account with Permissions to Run SiteScope" on page 19.

> **Note:**
>
> - The Solaris and Linux installation directory cannot be changed during installation, and it is not recommended to change it after installation is complete.
>
> - While SiteScope requires 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.
>
> - You can also install SiteScope using a silent installation. For details, see "Installing SiteScope in Silent Mode" on page 136.
>
> - The Freemium version of SiteScope operates only on a 64-bit Windows system.

Installing SiteScope on an Oracle Enterprise Linux Environment

Before SiteScope can be installed on Oracle Enterprise Linux 6.0 or 6.1 (64-bit), the following dependencies must be installed on the environment:

- glibc-2.12-1.25.el6.i686.rpm

- glibc-common-2.12-1.25.el6.i686.rpm

- nss-softokn-freebl-3.12.9-3.el6.i686.rpm

- libXau-1.0.5-1.el6.i686.rpm

- libxcb-1.5-1.el6.i686.rpm

- libX11-1.3-2.el6.i686.rpm

You can install the dependencies, using the `yum` package manager provided in Oracle Enterprise Linux, by running the command:

```
yum install -y glibc glibc-common nss-softokn-freebl libXau libxcb libX11
libXext
```

These dependencies can be found in the default repositories (**/etc/yum.repos.d**) for all Red Hat-based systems.

Installing SiteScope on a CentOS 6.2 Environment

Before installing SiteScope on CentOS 6.2 (64-bit), make sure that one of the following additional libraries is installed on the Linux environment (we recommend using the first option):

- Install glibc.i686 library by executing the command:

```
[root@centos ~]# yum install glibc.i686
```

- Check that any JRE is installed and that paths to it are written correctly:

```
[root@centos ~]# java -version
java version "1.6.0_22"
OpenJDK Runtime Environment (IcedTea6 1.10.6) (rhel-1.43.1.10.6.el6_2-x86_64)
OpenJDK 64-Bit Server VM (build 20.0-b11, mixed mode)
```

If you get a "command not found" error, a JRE should be installed. Use the following command for this:

```
root@centos ~]# yum install java-1.6.0-openjdk
```

Tips for installing SiteScope on a CentOS 6 Server:

Check the hostname of the CentOS 6.2 server and make sure that the host is resolved.

1. Get your hostname by running the hostname command.

2. Run ping <your_hostname>. If the ping request is successful, the host is already resolvable.

3. If that failed, then find your IP using ifconfig.

4. Run echo "<your_ip> <your_hostname>" >> /etc/hosts to add a string with an IP corresponding to your hostname to the hosts file.

5. Run ping <your_hostname> again and make sure that the host is resolved.

   If the hostname does not resolve, this might be the reason that SiteScope does not start.

Installing SiteScope on an HP Cloud Services Instance Running on CentOS 6.2

SiteScope is supported on an HP Cloud Services (HPCS) instance running on a CentOS 6.2 operating system.

Tips for installing SiteScope on HPCS:

- **Check the hostname of the HP Cloud Services server and make sure that the host is resolved.**

    a. Get your hostname by running the hostname command.

    b. Run ping `<your_hostname>`. If the ping request is successful, the host is already resolvable.

    c. If that failed, then find your IP using `ifconfig`.

    d. Run echo "`<your_ip> <your_hostname>`" `>> /etc/hosts` to add a string with an IP corresponding to your hostname to the hosts file.

    e. Run `ping <your_hostname>` again and make sure that the host is resolved.

- **Check the swap size.**

    a. Run the free command and make sure that the swap is created.

    b. If you see that the swap is absent:

    ```
    [root@centos ~]# free | grep Swap
    Swap: 0 0 0
    ```

    run the following commands:

    Create a 2 GB file:

    ```
    [root@centos ~]# dd if=/dev/zero of=/swapfile bs=1M count=2048
    ```

    Initialize it as the swap:

    ```
    [root@centos ~]# mkswap /swapfile
    ```

    Enable it:

    ```
    [root@centos ~]# swapon /swapfile
    ```

    c. Check the swap again:

    ```
    root@centos ~]# free | grep Swap
    Swap: 2097144 0 2097144
    ```

- **Install additional libraries.**

    For details, see "Installing SiteScope on a CentOS 6.2 Environment" on the previous page.

Security Group Configuration

IP Protocol	From Port	To Port	Type	CIDR IPS
tcp	8080	8080	IPs	0.0.0.0/0
tcp	22	22	IPs	0.0.0.0/0
tcp	8888	8888	IPs	0.0.0.0/0
icmp	-1	-1	IPs	0.0.0.0/0

Installing SiteScope on HPCS

To install SiteScope on HPCS:

1. Change the current directory to the location where the SiteScope installer is located, and run the SiteScope installer:

   ```
   [root@centos ~]# sh ./HPSiteScope_11.20_setup.bin -i console
   ```

2. Install SiteScope using the console mode. For details, see "Installing on Solaris or Linux Using Console Mode" on page 129.

3. After installation is finished run SiteScope:

   ```
   [root@centos ~]# /opt/HP/SiteScope/start
   ```

4. Wait for a couple of minutes until the SiteScope service is started, and then check that the necessary processes are running:

   ```
   [root@centos ~]# ps -ef | grep SiteScope | grep -v grep |awk '{print $3}
   '84758477
   ```

   The last command shows the process IDs of the SiteScope processes. If there are two processes, the SiteScope server has started successfully.

Notes and limitations

The Operations Manager integration is currently not supported in SiteScope 11.2x installed on a CentOS 6.2 server.

Installing Dependencies Required by the HP Operations Agent

When installing the HP Operations agent on the SiteScope server, you should perform the following:

1. Before the HP Operations agent can be installed, you should install the following dependencies on the environment:

   On Red Hat ES Linux 6.0 (64-bit):

   ■ Install **compat-libstdc++-33-3.2.3-69.el6.i686.rpm** on the Red Hat Enterprise Linux 6 x64 node.

   > **Note:** To install SiteScope with the HP Operations agent on RHEL x64 in graphics mode, you must run the installer with the machine default JRE.
   >
   > ./<PRODUCT_NAME>_<VERSION>_setup.bin LAX_VM /usr/bin/java $@
   >
   > For example:
   >
   > ./HPSiteScope_11.20_setup.bin LAX_VM /usr/bin/java $@

   ■ Install **compat-libstdc++-33-3.2.3-69.el6.ppc64.rpm** on the Red Hat Enterprise Linux 6 PPC node.

   You can install the dependencies, using the yum package manager provided in Red Hat Enterprise Linux, by running the command:

   `yum install compat-libstdc++-33-3.2.3-69.el6.i686.rpm` or

   `yum install compat-libstdc++-33-3.2.3-69.el6.ppc64.rpm`

   On SunOS:

   ■ Install SunOS **patch 119254-43** or **119255-43**.

   ■ Make sure that the IP address of the system is mapped to the system's host name.

   > **Note:** For additional requirements for installing and using the HP Operations agent, see the Operations Agent Installation Guide on the HP Software Support Web site (http://support.openview.hp.com/selfsolve/manuals).

2. After installing the HP Operations agent, you should check the installation status in the log files.

   ■ SiteScope log. This just shows whether the installation passed successfully or not.

   Log file name: **HPSiteScope_config_tool.log**

   Log file location:

- **win- %temp%** on Windows platforms

- **/temp** or **/var/temp** on UNIX/Linux platforms

  (search for results of "installOATask")

- HP Operations agent log files.

  Log file name: **oainstall.log**, **oapatch.log**

  Log file location:

  - **%ovdatadir%\log** on Windows platforms

  - **/var/opt/OV/log/** on UNIX/Linux platforms

Troubleshooting and Limitations

This section describes the following troubleshooting and limitations for installing SiteScope.

- "SiteScope might not install on 64-bit Linux using console mode" below

- "SiteScope does not install on 64-bit Linux in graphic mode" below

- "SiteScope service not installed when SiteScope is installed on a 64-bit Microsoft Windows Server 2003" on the next page

- "SiteScope might not install on Windows if %TEMP% and %TMP% point to a directory containing an empty space" on the next page

- "HP Operations agent does not install on 32-bit Windows" on the next page

- "Error installing the HP Operations agent - check the log files" on page 109

- "After uninstalling SiteScope, a subsequent SiteScope installation fails" on page 109

SiteScope might not install on 64-bit Linux using console mode

Installing SiteScope on Linux Red Hat 64-bit environments using console mode may fail if there are too many X sessions opened.

Workaround: Close some of the X sessions, or clear the DISPLAY variable.

SiteScope does not install on 64-bit Linux in graphic mode

The SiteScope installer might not work on Linux Red Hat 64-bit environments using the installation wizard.

Workaround: Install SiteScope using the console mode instead.

SiteScope service not installed when SiteScope is installed on a 64-bit Microsoft Windows Server 2003

The SiteScope service fails to install on a 64-bit Microsoft Windows Server 2003 on which McAfee Antivirus software is running.

Workaround: Shut down the McAfee Antivirus software and then reinstalled SiteScope.

SiteScope might not install on Windows if %TEMP% and %TMP% point to a directory containing an empty space

Installing SiteScope on a Microsoft Windows machine might fail if the environment variables %TEMP% and %TMP% point to a directory containing an empty space. For example, `C:\Documents and Settings\Default User\Local Settings\Temp`.

Workaround: Change the environment variables %TEMP% and %TMP% to point to a directory path that does not contain an empty space. For example, **C:\Temp**.

HP Operations agent does not install on 32-bit Windows

If the HP Operations agent fails to install on a 32-bit Windows machine, rename all the **.msi** files in **<SiteScope root directory>\install\components\oa\win32** to their original names (see list below), and then reinstall the agent.

For example, `HPOvAgtEx-06.20.105-WinNT4.0-release.msi` should be renamed `HPOvAgtEx.msi`.

HPOvAgtEx.msi	HPOvAgtEx.msi HPOvLcja.msi
HPOvBbc.msi	HPOvBbc.msi HPOvLcko.msi
HPOvConf.msi	HPOvConf.msi HPOvLczC.msi
HPOvCtrl.msi	HPOvCtrl.msi HPOvPacc.msi
HPOvDepl.msi	HPOvDepl.msi HPOvPCO.msi
HPOvEaAes.ms	HPOvEaAes.ms HPOvPerlA.msi
HPOvEaAgt.msi	HPOvEaAgt.msi HPOvSecCC.msi
HPOvEaAja.msi	HPOvEaAja.msi HPOvSecCo.msi
HPOvEaAko.msi	HPOvEaAko.msi HPOvXalanA.msi
HPOvEaAzC.msi	HPOvEaAzC.msi HPOvXercesA.msi
HPOvLces.msi	HPOvLces.msi HPOvXpl.msi

Error installing the HP Operations agent - check the log files

If you encounter an error while installing the HP Operations agent or you want to see the installation status, you can check the log files as described in "Installing Dependencies Required by the HP Operations Agent" on page 105.

After uninstalling SiteScope, a subsequent SiteScope installation fails

After uninstalling SiteScope, a subsequent installation cannot be completed and the following message is displayed: "Please enable windows scripting host". This occurs because Windows is unable to resolve the %SystemRoot% variable in the PATH environment variable (even though %SystemRoot% does appear in the path).

Workaround: Replace the %SystemRoot% variable in the PATH environment variable with the actual path to **C:\Windows\system32**.

Chapter 12: Installing Using the Installation Wizard

Use the following steps to install SiteScope on supported Windows, Solaris, or Linux environments using the installation wizard. For the list of supported environments, see "System Requirements" on page 65.

The installation wizard automatically executes if X11 libraries have already been installed on the server. If these libraries are not installed, you can either:

- Install SiteScope in graphic mode on a machine without an X11 server. For details, see "Installing SiteScope Using the Installation Wizard on a Machine Without X11 Server" on page 127.

- Install SiteScope on Solaris or Linux platforms in console mode. For details, see "Installing on Solaris or Linux Using Console Mode" on page 129.

> **Note:** You can also install SiteScope using a silent installation. For details, see "Installing SiteScope in Silent Mode" on page 136.

To install SiteScope:

1. Obtain the SiteScope installation program. The SiteScope installation program file can be accessed from one of the following locations:

   - The SiteScope release media (for major or minor releases).

   - The Software Patches page on the HP Software Support Online web site at http://support.openview.hp.com/selfsolve/patches. Go to **Software Support Online > Downloads > Software Patches** and select **SiteScope** as the product.

     > **Note:** The most recent versions of SiteScope are posted here.

   - The Downloads page in BSM Platform Administration.

2. Run the SiteScope installation according to your operating system.

   For Windows:

   a. Determine which executable you need to use. For details, see "Preparing for a 64-Bit SiteScope Installation" on page 101.

○ **HPSiteScope_11.20_setup.exe**

This installer automatically determines which SiteScope version to install. On a 32-bit operating system, SiteScope is installed as a 32-bit application. On a 64-bit operating system, SiteScope is installed as a 64-bit application.

○ **HPSiteScope32on64_11.20_setup.exe**

This installer is for 64-bit Windows operating systems only. SiteScope is installed as 32-bit application. This installation allows monitors that are not supported on the 64-bit Windows operating system to be supported. See "Windows Monitors Not Supported by 64-Bit SiteScope" on page 67.

b. Enter the location from which you are installing SiteScope according to your operating system and architecture, followed by the executable name.

For example:

```
<DVD_ROOT>\Windows_Setup\SiteScope\
HPSiteScope_11.20_setup.exe
```

or

```
<DVD_ROOT>\Windows_Setup\SiteScope\
HPSiteScope32on64_11.20_setup.exe
```

For Linux or Solaris:

a. Log in to the server as user **root**.

b. Run the installer by entering: **./HPSiteScope_11.20_setup.bin**.

> **Note:** 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 wizard gives you an error message and then exits the installation. Change to install mode using the **change user** command. For details, refer to the Microsoft support site (http://support.microsoft.com/kb/320185).

3. The Choose Locale screen is displayed.

Click **OK** to continue with the installation. The Initialization screen is displayed.
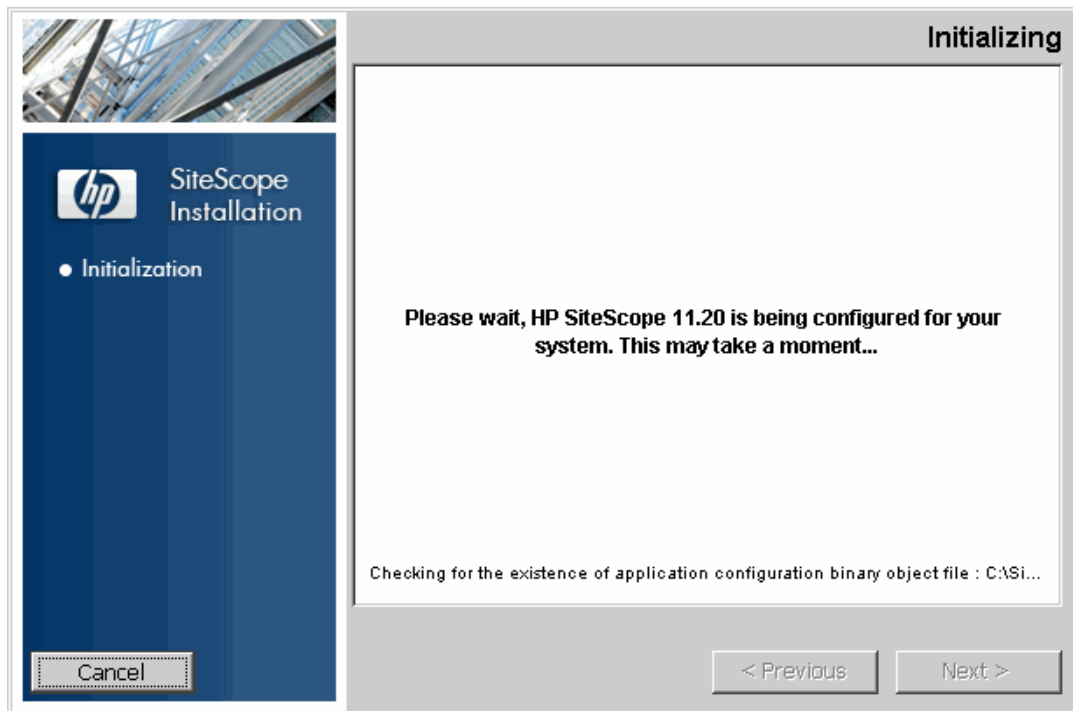
If the Installer detects any anti-virus program running on your system, it prompts you to examine the warnings before you continue with the installation.

4. Read the warnings, if any, that appear in the **Application requirement** check warnings screen and follow the instructions as described in the screen.

If the installer detects an anti-virus program you can try installing SiteScope without disabling the anti-virus program.
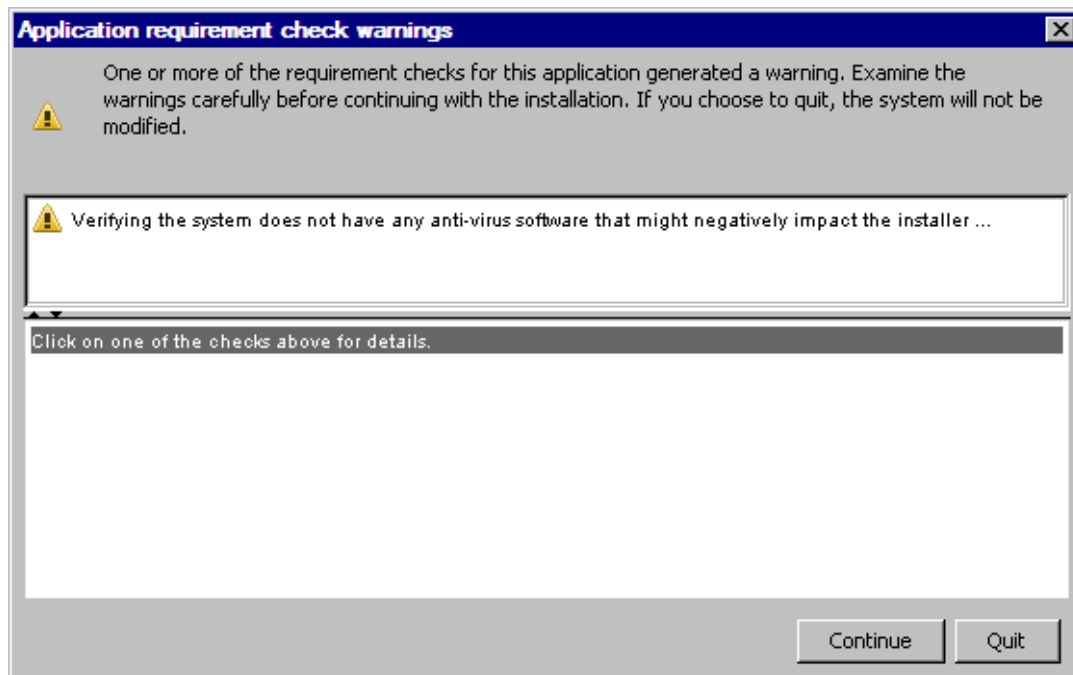
Click **Continue** to continue with the installation.

5. In the Introduction (Install) screen that opens, click **Next**.
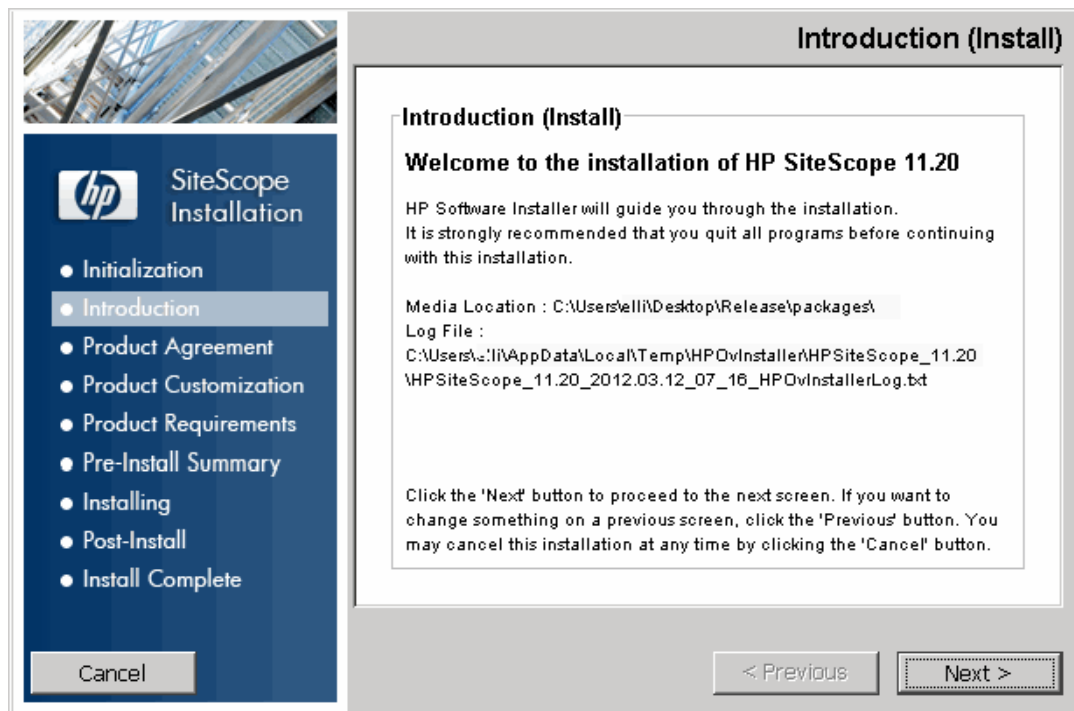
6. The License Agreement screen opens.
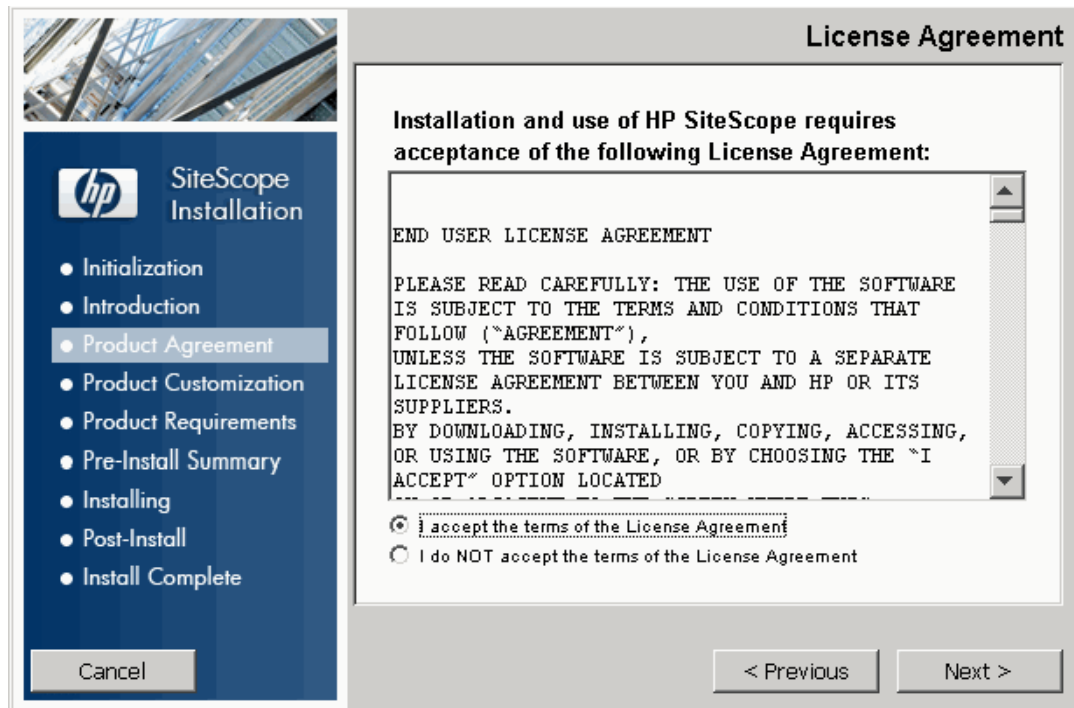
Read the SiteScope License Agreement.

To install SiteScope, select **I accept the terms of the License Agreement**, and then click
Next.

7. If you are installing SiteScope Freemium, skip to step 8.

    In the Product Customization screen, select the SiteScope setup type.
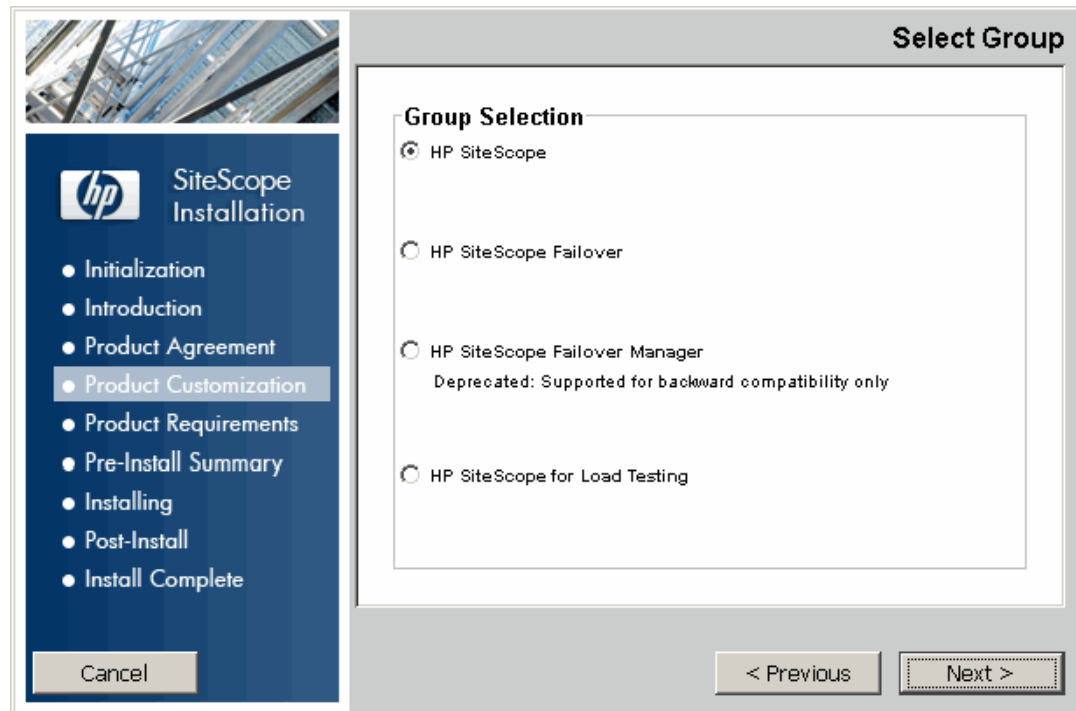
- **HP SiteScope.** This is the standard SiteScope installation.

- **HP SiteScope Failover.** This installation provides a backup for monitoring infrastructure
  availability if a primary SiteScope server fails. This is the classic SiteScope Failover
  (automated mirroring) solution that was reinstated as a replacement for SiteScope Failover
  Manager.

- **HP SiteScope Failover Manager.** This installation enables you to use the SiteScope
  Failover Manager (shared drive architecture) solution as a backup for monitoring
  infrastructure availability if a primary SiteScope server fails.

  Note: This option is deprecated and is available for backward compatibility only. While
  SiteScope Failover is still supported, HP plans to stop supporting it in the future, and
  recommends that you evaluate the SiteScope Failover solution instead.

- **HP SiteScope for Load Testing.** This setup type is used with an HP LoadRunner or HP

Performance Center installation only. It enables users to define and use SiteScope monitors on a LoadRunner or Performance Center application. SiteScope provides additional monitoring that complements the native LoadRunner and Performance Center monitors. For more details, see the relevant LoadRunner or Performance Center documentation.

> **Note:** This installation option is not available when installing on Solaris or Linux platforms.

Click **Next** to continue.

8. The Select Features screen opens, displaying the HP SiteScope folder.
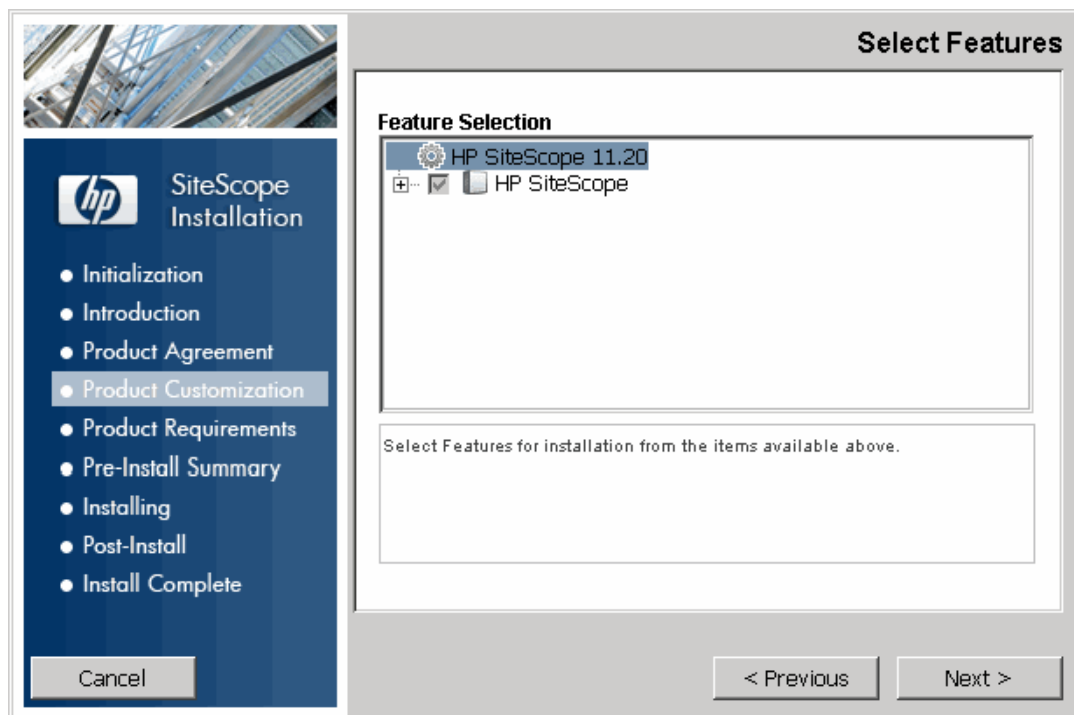
Click **Next** to continue.

9. If installing on Solaris or Linux platforms, SiteScope is automatically installed in the **/opt/HP/SiteScope/** folder. Skip to step 10.

The Choose the folders screen opens.
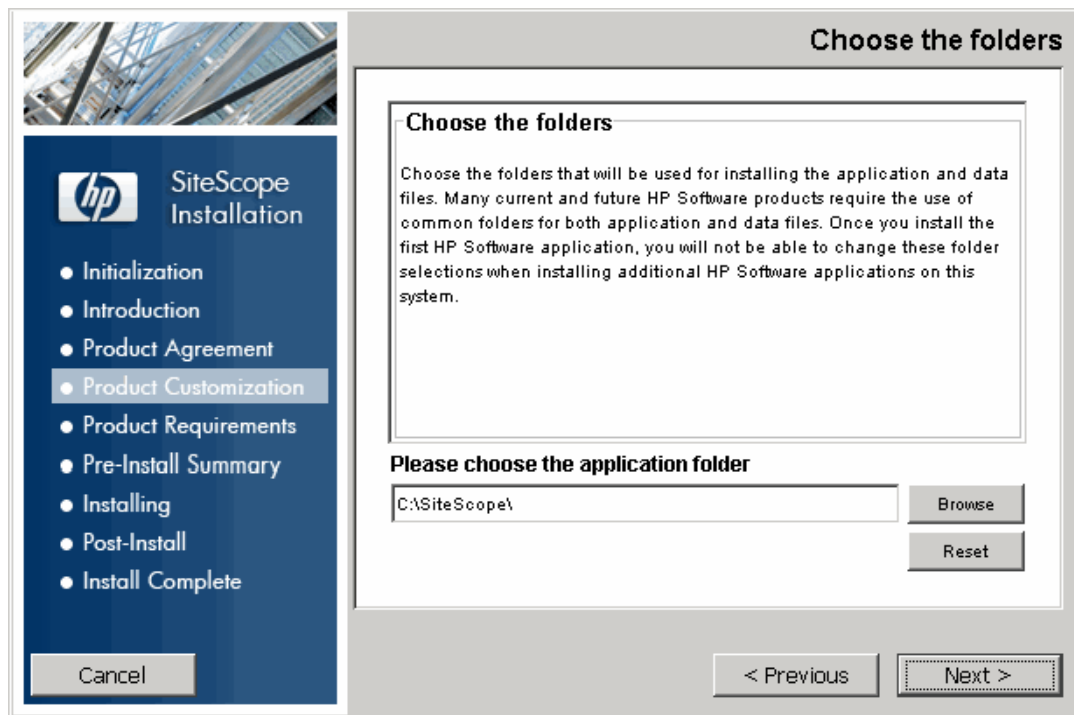
Accept the default directory location, or click **Browse** to select another directory. If you select another directory, the installation path must not contain spaces or non-Latin characters in its name, and must end with a folder named **SiteScope** (the folder name is case sensitive). To restore the default installation path, click **Reset**.

Note for SiteScope Failover Manager users: The SiteScope Failover Manager option is deprecated and is available for backward compatibility only.

If you plan to use SiteScope Failover Manager to provide a backup monitoring availability, you must install SiteScope as a shared resource.

- On Windows, you must install SiteScope using the UNC path of the SiteScope installation folder. For example, \\lab1\users\SiteScopes\Version_11.20\Build_2000\SiteScope

- On Linux or Solaris, you must mount the shared resource to the **/opt/HP/SiteScope** folder.

Click **Next** to continue.

10. The Install Checks screen opens and runs verification checks.
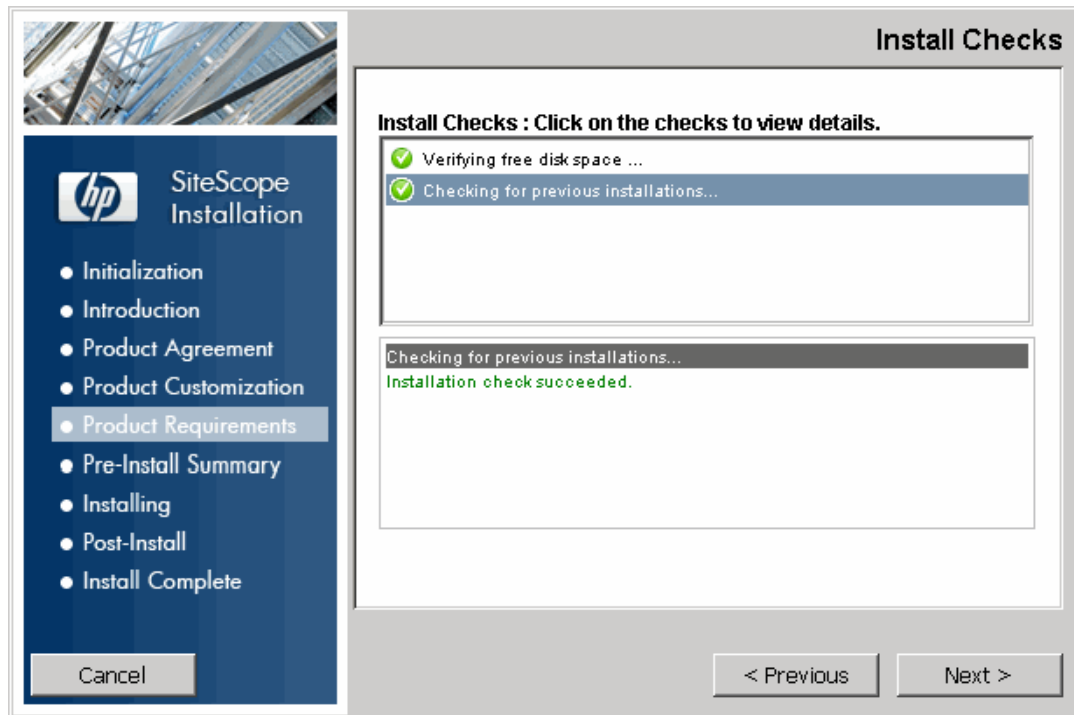
Click **Next** after the free disk space verification completes successfully.

If the free disk space verification is not successful, do the following:

- Free disk space, for example by using the Windows Disk Cleanup utility.

- Repeat steps 9 and 10.

11. In the Pre-Install Summary screen, click **Install**.
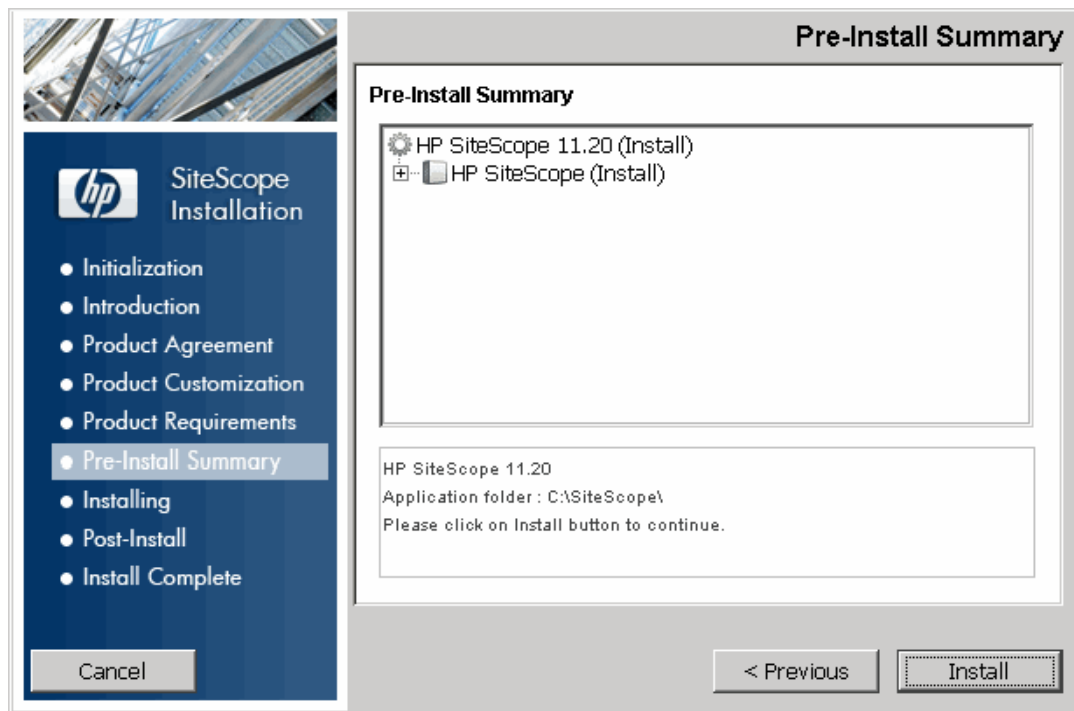
12. The Installing screen opens and the installer selects and installs the required SiteScope software components. Each software component and its installation progress is displayed on your screen during installation.

13. After installing the SiteScope components, the Introduction screen of the SiteScope Configuration Wizard opens.
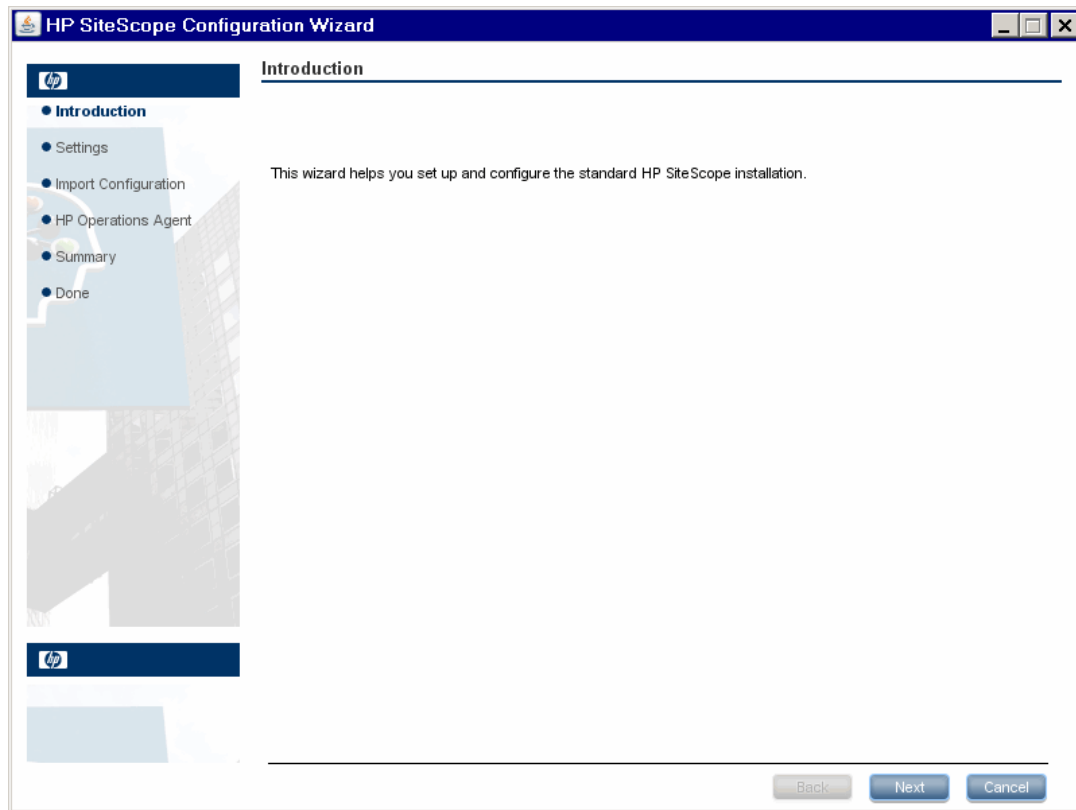
Click **Next**.

14. The Settings screen of the SiteScope Configuration Wizard opens.

Enter the required configuration information and click **Next**:

- **Port.** The SiteScope port number. If the port number is already in use (an error message is displayed), enter a different port. If necessary, you can change the port later using the Configuration Tool. The default port is 8080.

  Note: If you plan to use SiteScope Failover Manager to monitor more than one primary SiteScope from a single Failover machine, each primary SiteScope installation must be configured to answer on a unique port number. You can check the ports used by the SiteScope server using the SiteScope Configuration Wizard. For details, see "Running the Configuration Tool on Windows Platforms" on page 138.

- **License file.** Enter the path to the license file, or click **Select** and select the SiteScope license key file. A license must be purchased if intending to use SiteScope beyond the 60-day trial period. It is not necessary to enter license information at this point to use SiteScope during the free trial period.

  Note:

- License keys from versions of SiteScope earlier than 11.00 are not compatible with this version. License key delivery can be fulfilled automatically through http://webware.hp.com.

- If you are installing a Freemium license, license keys are not relevant.

- **Use local system account** (not applicable for Solaris or Linux installations). By default, SiteScope is installed to run as a Local System account. This account has extensive privileges on the local computer, and has access to most system objects. When SiteScope is running under a Local Systems account, it attempts to connect to remote servers using credentials of the server as configured in SiteScope.

- **Use this account** (not applicable for Solaris or Linux installations). Select to change the user account of the SiteScope service. You can set the SiteScope service to log on as a user with domain administration privileges. This gives SiteScope access privileges to monitor server data within the domain. Enter an account and password (and confirm the password) that can access the remote servers.

> **Note:**
> When SiteScope is installed to run as a custom user account, the account used must have **Log on as a service** rights. To grant a user logon service access:
>
> i. In Windows Control Panel, double-click **Administrative Tools**.
>
> ii. Double-click Local Security Policy, and select **Local Policies > User Rights Assignment > Log On as a Service**.
>
> iii. Click **Add User or Group**, and select the user you want to grant logon service access to, and click **OK**.
>
> iv. Click **OK** to save the updated policy.

- **Service name** (not applicable for Solaris or Linux installations). The name of the SiteScope service. If the machine has a previous version of SiteScope installed, enter another name for the SiteScope service. The default service name is `SiteScope`.

- **Start SiteScope service after install** (not applicable for Solaris or Linux installations). Automatically starts the SiteScope service after the installation is complete.

15. The Import Configuration screen opens, enabling you to import existing SiteScope configuration data to the new SiteScope installation.
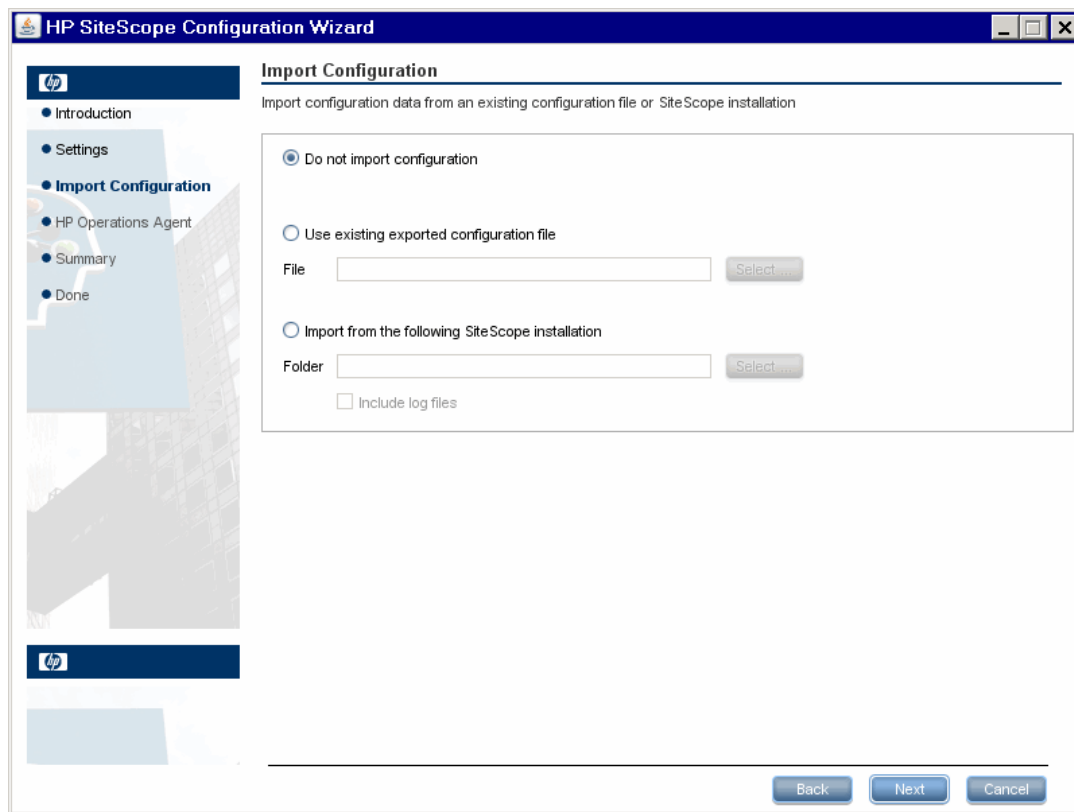
Select one of the following options and click **Next**:

- **Do not import configuration data.**

- **Use existing exported configuration file.** Enables you to use SiteScope data such as templates, logs, monitor configuration files, and so forth, from an existing exported configuration file. SiteScope data is exported using the Configuration Tool, and is saved in **.zip** format. Click the **Select** button and navigate to the user data file that you want to import.

- **Import from the following SiteScope installation.** Click the **Select** button and navigate to the SiteScope installation folder from which you want to import configuration data.

  ○ **Include log files.** Enables you to import log files from the selected SiteScope installation folder.

Note: When moving configuration data from one SiteScope installation to another, make sure that SiteScope server from which you are taking configuration data is in the same time zone as the SiteScope server to which the data is being imported.

16. The HP Operations Agent screen opens. The agent is required to enable SiteScope to send

events and to act as a data storage for metrics data if SiteScope is integrated with an HP Operations Manager or BSM Gateway server.

> **Note:**
>
> - If you are installing the Freemium license, the HP Operations Agent screen does not open. Skip to step 17.
>
> - The HP Operations Agent is not required when graphing metrics data to Performance Graphing using the profile database in BSM. The profile database is the recommended option, because it is a more robust and scalable data source, and does not require configuration of the HP Operations Integration.
>
>   For details on reporting metrics data, see Integrating SiteScope with HP Operations Manager Products in the SiteScope Help. You can check the HP Software Integrations site to see if a more updated version of this guide is available (for Windows: http://support.openview.hp.com/sc/solutions/integrations.jsp?intid=39; for UNIX: http://support.openview.hp.com/sc/solutions/integrations.jsp?intid=628)

Select one of the following options and click **Next**:

- **Do not install HP Operations Agent.** The HP Operations agent is not installed.

- **Install HP Operations Agent.** Select to install the HP Operations agent on the SiteScope server.

> **Note:**
>
> - If you install SiteScope and the HP Operations agent on a machine that already has the agent installed, SiteScope overrides it and upgrades the current agent.
>
> - The HP Operations agent is supported on SiteScopes running on the environments listed in "HP Operations Agent Support Matrix" on page 74. Consequently, the SiteScope integration with HPOM and BSM is only supported on these environments.
>
> - If you encounter problems installing the HP Operations agent on a 32-bit Windows machine, see "Troubleshooting and Limitations" on page 107.

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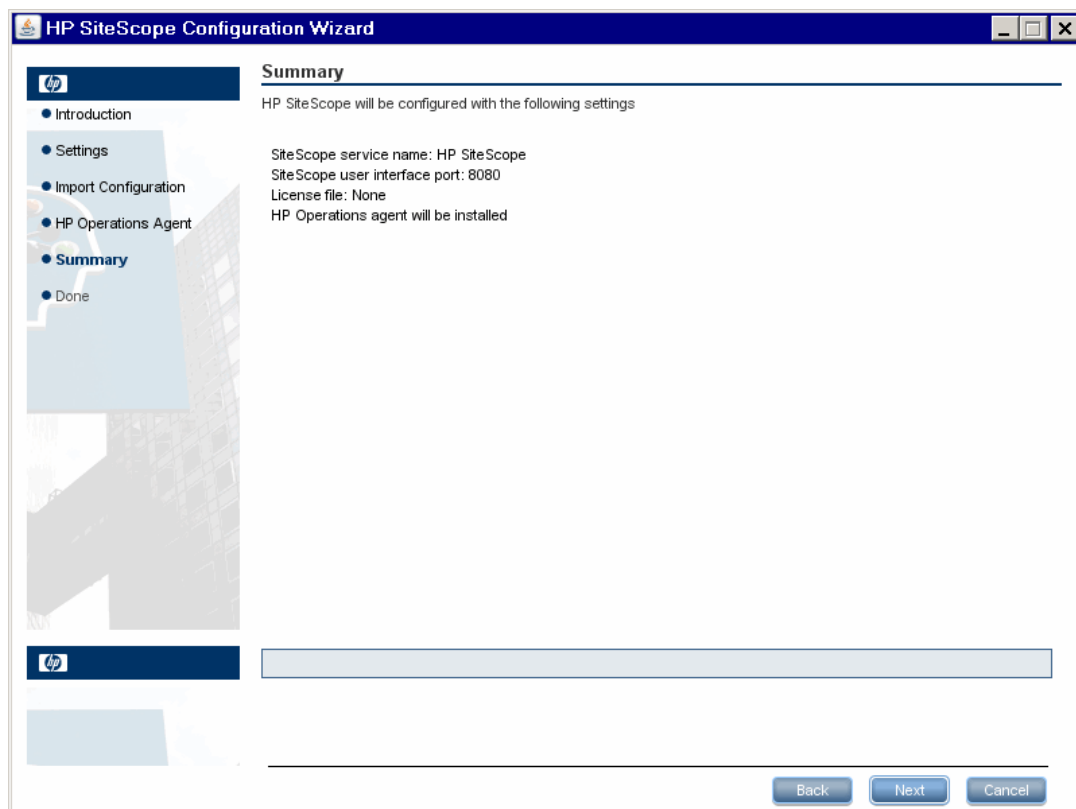
Check that the information is correct and click **Next** to continue, or **Back** to return to previous screens to change your selections.

18. The Done screen opens.
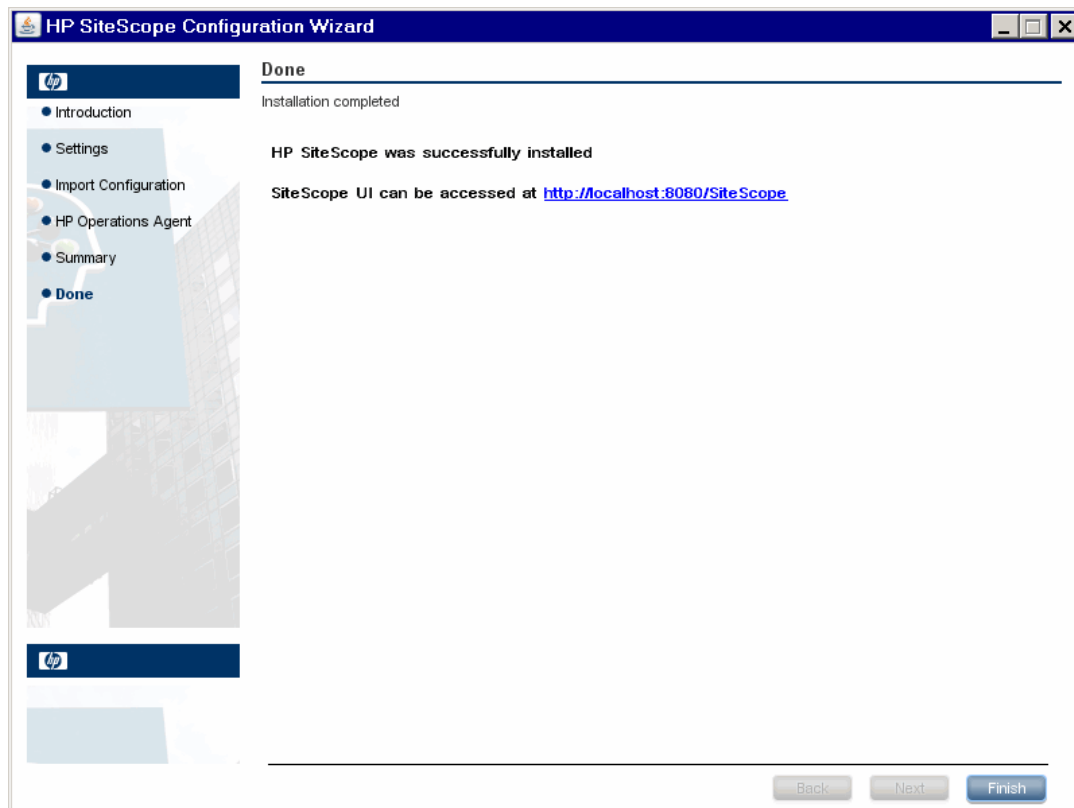
To access the SiteScope user interface, click the connection address for this installation of SiteScope.

> **Note:** If you did not select Start SiteScope service after install in the Configuration Settings screen, you need to start the SiteScope service before you can connect to SiteScope. For details, see "Getting Started with SiteScope" on page 190.

Click **Finish** to close the SiteScope Configuration Wizard.

19. When the installation finishes, the Installation Complete window opens displaying a summary of the installation paths used and the installation status.
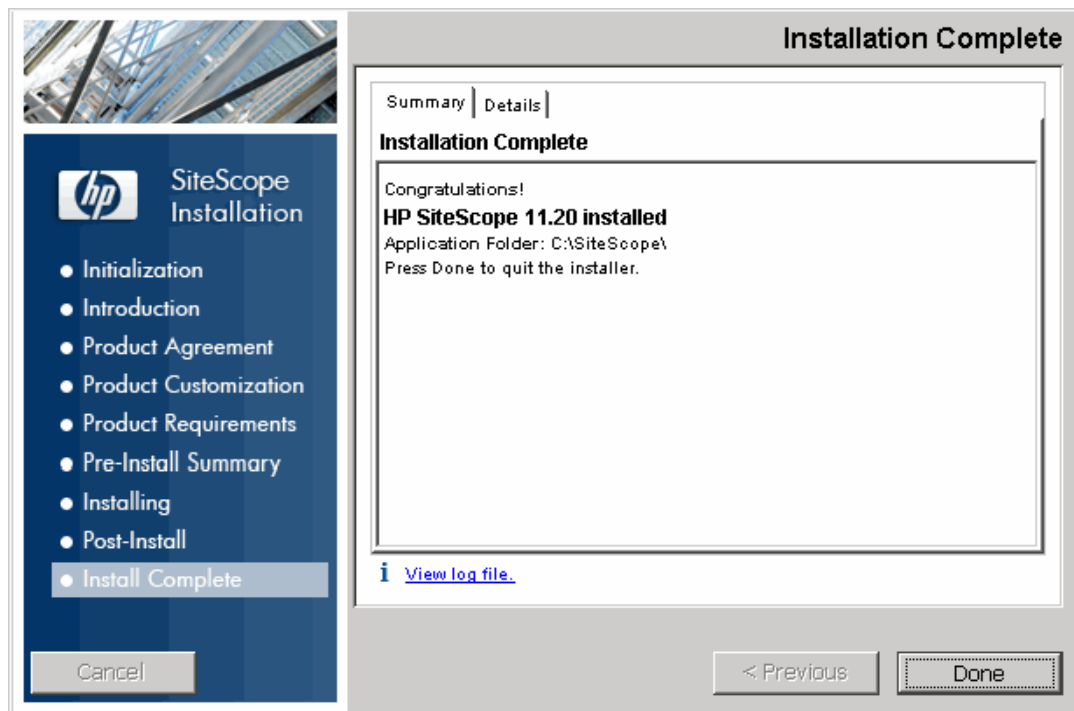
If the installation was not successful, review the installation log file for any errors by clicking the **View log file** link in the **Installation Complete** window to view the log file in a web browser.

For more information about the installed packages, click the **Details** tab.

Click **Done** to close the installation program.

If the installation program determines that the server must be restarted, it prompts you to restart the server.

20. For the latest available functionality, download and install the latest SiteScope patch from the same location from which you installed SiteScope. For information on accessing the SiteScope interface, see "Connecting to SiteScope" on page 192.

21. After installing SiteScope on a Linux or Solaris environment, 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.

Installing SiteScope Using the Installation Wizard on a Machine Without X11 Server

You can install SiteScope using the installation wizard on a machine that does not have an X11 server either by:

- Using a VNC server (on many Linux and Solaris systems, a VNC server is installed by default).

- Editing the DISPLAY environment variable to make the programs use X server on another machine.

To install SiteScope on a machine without X11 using a VNC server:

1. In command line, run vncserver. If it runs, select a password and note the display that the VNC server uses (usually `:1`).

2. Connect to your SiteScope machine using VNC client using the format: hostname:display. For example, `sitescope.company.name:1`

3. In the console that opens, navigate to the SiteScope installation directory and run the installation as usual.

To install SiteScope on a machine without X11 by redirecting X:

1. Run any Linux or Solaris system with an X server, or install an X server on Windows (for example, `xming`).

2. Check that X access control permits your SiteScope machine to connect. On Linux or Solaris platforms, consult man `xhost`. On Windows platforms, see the documentation for X server implementation.

3. Run **export DISPLAY=x-server.machine.name:display** on your SiteScope machine (display is usually `0`).

4. Navigate to the SiteScope installation directory in the same shell, and run the installation as usual.

Chapter 13: Installing on Solaris or Linux 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 using the user interface.

Note: Running SiteScope on a Solaris platform is now deprecated. The next release is not planned to include a Solaris installer.

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. To install the full edition of SiteScope, run the following command:

   ```
   HPSiteScope_11.20_setup.bin -i console
   ```

   The installation script initializes the Java Virtual Machine to begin the installation.

3. The Choose Locale screen is displayed.

   ```
   Preparing to install...
   Extracting the JRE from the installer archive...
   Unpacking the JRE...
   Extracting the installation resources from the installer archive...
   Configuring the installer for this system's environment...
   Preparing CONSOLE Mode Installation...


   ===============================================================================
   Choose Locale...
   ---------------

      1- Deutsch
    ->2- English
      3- Fran?ais

   CHOOSE LOCALE BY NUMBER:
   ```

   Enter the number to select the desired locale, and press ENTER to continue.

4. A confirmation screen is displayed.

   Press ENTER to continue.

5. The Introduction screen is displayed.

```
================================================================================
Introduction
------------


Welcome to the installation for HP SiteScope 11.20
HP Software Installer will guide you through the installation. It is strongly
recommended that you quit all programs before continuing with this
installation.

Application Media Location :
/install/SiteScope/3497/SiteScope/LinuxSetup/packages/
Installation Log File : /tmp/HPOvInstaller/HPSiteScope_11.20/HPSiteScope_11.20_
2012.03.16_18_58_HPOvInstallerLog.txt
Respond to each prompt to proceed to the next step in the installation.
If you want to change something on a previous step, type 'back'.
You may cancel this installation at any time by typing 'quit'.

PRESS <ENTER> TO CONTINUE: █
```

Press ENTER to continue with the installation.

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

```
PRESS <ENTER> TO CONTINUE:


Additional License Authorizations:
Additional license authorizations and restrictions applicable to your software
product are found at:  http://www.hp.com/go/SWLicensing


I accept the terms of the License Agreement (Y/N): Y█
```

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 Y.

> **Note:** To cancel the installation after viewing the SiteScope License Agreement, enter N.

7. The SiteScope setup type screen opens.

```
================================================================================

Install Groups are combined sets of features.
If you want to change something on a previous step, type 'back'.
You may cancel this installation at any time by typing 'quit'.



  ->1- HP SiteScope: ()
    2- HP SiteScope Failover: ()
    3- HP SiteScope Failover Manager: (Deprecated: Supported for backward compatibili
ty only)

Please select one of the following groups ...:
```

Choose the type that is suitable for your site. Enter the number of the setup type, and then press ENTER to continue.

8. The Select Features screen opens.

```
================================================================================
Select Features
--------------

Install Features represent a group of functionality
If you want to change something on a previous step, type 'back'.
You may cancel this installation at any time by typing 'quit'.



  ->1- HP SiteScope(Required)

Please Select Features(Use a comma to separate your choices)
    : 1
```

Enter the number 1 (required) to install SiteScope.

Press ENTER to continue with the installation.

9. The Install Requirements screen opens.

```
================================================================================
Install Requirements Checks
------------------------

================================================================================
 Verifying : Verifying free disk space ...  [Completed]
 Verifying : Checking for previous installations...  [Completed]
================================================================================
Performing checks ...
Details :  performing checks ... please wait
Executing initialize action :
Install check requirements successfully completed
If you want to change something on a previous step, type 'back'.
You may cancel this installation at any time by typing 'quit'.

Please hit Enter to continue:
```

Press ENTER to continue with the installation.

10. The Pre-Installation Summary screen opens.

```
================================================================================
Pre-Installation Summary
------------------------

Review the following before continuing:

Application Name
    HP SiteScope

Application Shortname
    HPSiteScope

Application Revision
    11.20

Application Directory
    /opt/HP/SiteScope/

Data Directory
    /var/opt/HP/SiteScope/

If you want to change something on a previous step, type 'back'.
You may cancel this installation at any time by typing 'quit'.


PRESS <ENTER> TO CONTINUE: █
```

Press ENTER to continue with the installation.

11. The Install Features screen opens and the installation process starts.

```
================================================================================
Install Features
----------------

Checking the status of packages


Checking the installation status of selected packages


Processing of 9 packages (Using Native rpm) scheduled.
Completed checking the installation status of all packages.
This process might take a while. Please do not interrupt...
```

When the installation process is complete, the post-installation configuration screen opens.

12. The port prompt is displayed.

```
================================================================================
Installing...
-------------


 [================|================|================|================]
 [----------------|----------------|----------------|----------------]
 : ==============================================================================
------------------------------------------------------------
Enter the HP SiteScope port number
Port [8080]
PRESS <1> to accept the value [8080], or <2> to change the value
```

Enter the number 1 to accept the default port 8080, or enter number 2 to change the port, and then enter a different number in the change port prompt.

> **Note:** If you plan to use SiteScope Failover Manager to monitor more than one primary SiteScope from a single Failover machine, each primary SiteScope installation must be configured to answer on a unique port number. You can check the ports used by the SiteScope server using the SiteScope Configuration Wizard. For details, see "Running the Configuration Tool on Solaris or Linux Platforms" on page 144.

Press ENTER to continue with the installation.

13. The license file path prompt is displayed.

```
Enter the path to license file
File name []
PRESS <1> to accept the value [], or <2> to change the value
```

Enter the number 1 to leave the license file path empty (it is not necessary to enter license information at this point to use SiteScope during the free trial period), or enter the number 2, and then enter the license file path in the next text box.

> **Note:** License keys from previous versions of SiteScope are not compatible with this version. License key delivery can be fulfilled automatically through http://webware.hp.com.

Press ENTER to continue with the installation.

14. The Import Configuration Data screen opens.

```
Import configuration data from an existing configuration file or SiteScope
installation
->1 - Do not import: ()
  2 - Import from file: ()
  3 - Import from folder: ()
```

Enter the number 1 if you do not want to import data.

Enter the number 2 to use SiteScope data such as templates, logs, monitor configuration files, and so forth, from an existing exported configuration file. If you select this option, enter the path to the configuration file in the next text box.

Enter the number 3 to import configuration data from a SiteScope installation directory. If you select this option, enter the path to the SiteScope installation folder from which you want to import configuration data.

Press ENTER to continue with the installation.

> **Note:** When moving configuration data from one SiteScope installation to another, make sure that SiteScope server from which you are taking configuration data is in the same time zone as the SiteScope server to which the data is being imported.

15. The Install HP Operations Agent screen opens. The HP Operations agent is required if SiteScope is integrated to send events and metrics to an HP Operations Manager or BSM Gateway server.

> **Note:** The HP Operations Agent is not required when graphing metrics data to Performance Graphing using the profile database in BSM. The profile database is the recommended option, because it is a more robust and scalable data source, and does not require configuration of the HP Operations Integration.
>
> For details on reporting metrics data, see Integrating SiteScope with HP Operations Manager Products in the SiteScope Help. You can check the HP Software Integrations site to see if a more updated version of this guide is available (for Windows: http://support.openview.hp.com/sc/solutions/integrations.jsp?intid=39; for UNIX: http://support.openview.hp.com/sc/solutions/integrations.jsp?intid=628)

```
Install HP Operations Agent
->1 - Do not install: ()
  2 - Install: ()
```

Enter the number 1 if you do not want to install the HP Operations agent.

Enter the number 2 to install the HP Operations agent on the SiteScope server. The agent is required to enable SiteScope to send events and act as a data storage for metrics data when SiteScope is integrated with an HP Operations Manager or BSM Gateway server.

> **Note:**

> ■ If you install SiteScope and the HP Operations agent on a machine that already has the agent installed, SiteScope overrides it and upgrades the current agent.
>
> ■ The HP Operations agent is supported on SiteScopes running on the environments listed in the SiteScope Support Matrices section in "HP Operations Agent Support Matrix" on page 74. Consequently, the SiteScope integration with HPOM and BSM is supported on these environments only.

Press ENTER to continue with the installation.

16. The console displays the installation parameters for confirmation.

```
HP SiteScope will be configured with the following settings
SiteScope user interface port: 8080
License file: None
HP Operations agent will not be installed
Press <1> to continue, or <2> to change values:
```

Enter 1 to proceed with the installation using the parameters indicated or enter 2 to return to make changes, and then press ENTER.

The installation process completes. An installation status message is displayed.

```
================================================================================
Installation Complete
--------------------

Congratulations!
HP SiteScope 11.20
The installation has been successfully completed.
Application Directory: /opt/HP/SiteScope/

View log file./tmp/HPOvInstaller/HPSiteScope_11.20/HPSiteScope_11.20_2012.03.16
_18_58_HPOvInstallerLog.txt
[root@VMAMQA297 /]#
```

17. After installing SiteScope, 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.

   For details on creating a non-root user that runs the SiteScope application, and setting account permissions, see "Configuring a Non-Root User Account with Permissions to Run SiteScope" on page 19.

18. To connect to SiteScope, follow the steps in the section "Starting and Stopping the SiteScope Process on Solaris and Linux Platforms" on page 191.

Chapter 14: Installing SiteScope in Silent Mode

This chapter includes:

- "About Installing SiteScope in Silent Mode" below

- "Running a Silent Installation" below

About Installing SiteScope in Silent Mode

You can install SiteScope using a silent installation. A silent installation runs the entire setup process in the background without requiring you to navigate through the setup screens and input your selections. Instead, all configuration parameters are allocated values you define in a response file. To run silent installations for different configurations, you can create multiple response files.

Notes and Limitations

Before running a silent installation, consider the following issues:

- When running an installation in silent mode, no messages are displayed. Instead, you can view installation information in the log files, including information on whether the installation was successful. The installation log files can be found under:

  - **%tmp%\HPOvInstaller\HPSiteScope_11.20** on Windows platforms (**%tmp%\HPOvInstaller\HPSiteScopeFreemium_11.22** for SiteScope Freemium on Windows platforms)

  - **/tmp/HPOvInstaller/HPSiteScope_11.20** on Solaris or Linux platforms

- The SiteScope installation path (`prodInstallDir=<Installation_path>`) must not contain spaces or non-Latin characters in its name, and must end with a folder named **SiteScope** (the folder name is case sensitive).

Running a Silent Installation

You run a silent installation using the **ovinstallparams.ini** file. Since this file has a very specific format, you should create the silent installation file using the sample **ovinstallparams.ini** file.

> **Note:** The sample **ovinstallparams.ini** file is available only after installing SiteScope from the **<SiteScope installation directory>\examples\silent_installation** folder.

How to run a silent installation for SiteScope 11.20:

1. Navigate to the **ovinstallparams.ini** file located in the **<SiteScope installation directory>\examples\silent_installation** folder.

2. Make a copy of the file, and then modify it to meet your installation needs.

3. Copy the file to the setup folder where the SiteScope installation file (**HPSiteScope_11.20_ setup.exe**, **HPSiteScope32on64_11.20_setup.exe**, or **HPSiteScope_11.20_setup.bin**) is located.

4. Run the installer from the command line with the **-i silent** flag. In Windows, specify **Wait** mode. For example:

`start /wait HPSiteScope_11.20_setup.exe -i silent` (Windows)

or

(For SiteScope Freemium) `start /wait HPSiteScopeFreemium_11.22_setup.exe -i silent` (Windows)

or

`HPSiteScope_11.20_setup.bin -i silent` (Linux or Solaris)

How to run a silent installation for a SiteScope 11.2x minor-minor version (patch):

1. Run the installer from the command line with **-i silent** flag. (The **oviinstallparams.ini** (answers) file is not required, unlike in a regular installation.)

   For example, to install SiteScope 11.23 in silent mode, run the command:

   - For Windows: **HPSiS1123_11.23_setup.exe -i silent**

   - For UNIX: **HPSiS1123_11.23_setup.bin -i silent**

To uninstall SiteScope in silent mode:

Linux or Solaris:

`/opt/HP/SiteScope/installation/bin/uninstall.sh -i silent`

Windows:

`%SITESCOPE_HOME%\installation\bin\uninstall.bat -i silent`

Chapter 15: Using the SiteScope Configuration Tool

This chapter includes:

-

-

-

-

Running the Configuration Tool on Windows Platforms

The Configuration Tool is a convenient utility for moving configuration data from one SiteScope installation to another. You can export SiteScope data such as templates, logs, monitor configuration files, scripts, server certificates, and so forth from your current SiteScope for later import into SiteScope. You can also use the wizard to optimize SiteScope's performance by making sizing changes in the Windows Registry keys, to change the ports assigned to SiteScope, and to install and uninstall the HP Operations Agent.

If you exported SiteScope data during the installation process, you can import the data using the Configuration Tool. Alternatively, you can export data from your current SiteScope independently using the Configuration Tool. If you have created or modified monitor configuration files in previous versions of SiteScope, you may need to import them to the current SiteScope directory.

Note:

- You must stop the SiteScope service before exporting or importing the data, and restart the service after exporting or importing the data. For details, see .

- When moving configuration data from one SiteScope installation to another, make sure that the SiteScope server from which you are taking configuration data is in the same time zone as the SiteScope server to which the data is being imported.

- When importing configurations to the same version of SiteScope, you must rename or delete all template example containers so as to import the new template examples.

- The inclusion of server certificates and scripts when exporting data is supported in the Configuration Tool. For details on how to include server certificates and scripts when exporting data from earlier versions of SiteScope, see .

- If you import configuration data from a Freemium edition of SiteScope, the Freemium license in the license file is not included in the imported data. Similarly, if you export configuration from a Freemium edition of SiteScope, the Freemium license is not included in

the exported data. For details about the Freemium license, see "Freemium License" on page 40.

To run the SiteScope Configuration Tool:

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

2. Select the actions that you want to perform, and then click **Next**.

Introduction

This wizard enables you to make sizing changes to the SiteScope server, change the ports assigned to SiteScope, move configuration data from one SiteScope installation to another, and install/uninstall the HP Operations agent.

Select the actions that you want to perform.

☐ Sizing

☐ Change ports

☐ Import configuration

☐ Export configuration

☐ HP Operation Agent

- **Sizing.** Enables optimizing SiteScope's performance by increasing JVM heap size, desktop heap size, and the number of file handles in the Windows Registry keys. For details, see step 3.

  > **Note:** If you start SiteScope by running the **go.bat** file in the **<SiteScope installation>\bin directory**, open the **go.bat** file and increase the **–Xmx512m** parameter to **–Xmx1024m** (for 1GB) or higher, as required, up to a maximum of **–Xmx8192m** (for 8GB).

- **Change port.** Enables changing any of the ports used by the SiteScope server. For details, see step 4.

- **Import configuration.** Enables importing configuration data from an exported configuration data (**.zip**) file, or from an existing SiteScope installation. For details, see step 5.

- **Export configuration.** Enables exporting SiteScope data such as templates, logs, and monitor configuration files from your current SiteScope for later import into SiteScope. For details, see step 6.

- **HP Operations Agent.** Enables installing and unstalling the HP Operations Agent. The

agent enables SiteScope or SiteScope Failover to send events and act as a data storage for metrics data when SiteScope is integrated with an HP Operations Manager or BSM Gateway server. For details, see step 7.

3. If you selected the **Sizing** option, the Sizing screen opens listing the parameters in the Windows Registry (the example below is for a 32-bit installation).

Sizing

Clicking on the next button changes the following parameters in the registry:

1. Increases the JVM heap size
2. Increases the desktop heap size to 2048 KB
3. Increases the number of file handles to 18,000
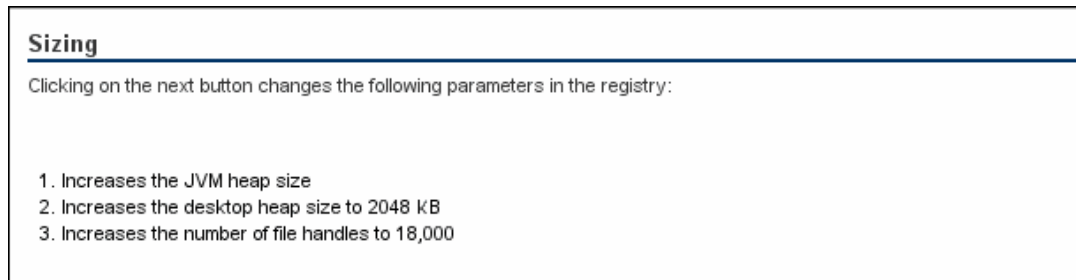
You can optimize SiteScope's performance by making changes in the following Windows Registry keys:

- **JVM heap size.** The value is changed from 512 MB to 1024 MB for 32-bit installations, and to 4096 MB for 64-bit installations. 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 KB to 2048 KB for 32-bit installations, and to 8192 KB for 64-bit installations. For more details on Desktop heap size, refer to http://support.microsoft.com/kb/126962.

> **Note:** Sizing changes can be made only if the physical memory of the SiteScope server is larger than the maximum JVM heap size (Xmx) that the Configuration Tool has configured (1 GB for a 32-bit installation and 4 GB for a 64-bit installation).

Click **Next** to complete the sizing operation.

- **File handles.** The value is increased from 10,000 to 18,000 file handles. For more details on changing file handles, refer to http://support.microsoft.com/kb/326591.

4. If you selected the **Change ports** option, the Change Ports screen opens.

Modify the ports used by the SiteScope server as required. Port numbers must be numeric and should be in the 1-65534 range. A port is mandatory for all components except Classic user interface.

Note: It is recommended to use ports in the 28000-28100 range so as not to interfere with ports used by other Business Service Management products.

Click **Next** to complete the change port operation.

Note: After completing the port change operation, the port is updated in the **Start > All Programs > HP SiteScope > Open HP SiteScope** link.

5. If you selected the **Import Configuration** option, the **Import Configuration** screen opens.

> **Note:**
>
> - You must stop the SiteScope service before importing the data, and restart the service after importing the data. For details, see "Starting and Stopping the SiteScope Service on Windows Platform" on page 190.
>
> - If you are importing configuration data from a Freemium edition of SiteScope, the Freemium license in the license file is not included in the imported data.

- If you select **Use existing exported configuration file**, enter the name of the user data file to import.

- If you select **Import the following SiteScope installation**, enter the SiteScope installation directory from which to import the user data file. If you also want to import log files, select **Include log files**.

Click **Next** to complete the import operation.

6. If you selected the **Export Configuration** option, the Export Configuration screen opens.

Export Configuration

Export configuration data from an existing SiteScope.

It is recommended that you stop SiteScope before processing.

From SiteScope folder	C:\SiteScope Select ...
To file	
☐ Include log files	

- In **From SiteScope folder**, accept the default directory given in the 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:\SiteScope11_0\SiteScope`, enter `D:\SiteScope11_0\SiteScope`.

- In **To file**, enter the directory to which to export the user data file (the directory must already exist) and the 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**.

> **Note:**

■ You must stop the SiteScope service before exporting the data, and restart the service after exporting the data. For details, see "Starting and Stopping the SiteScope Service on Windows Platform" on page 190.

■ 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 11.20 directory after an upgrade, so that you can see old reports.

■ If you are exporting configuration data from a Freemium edition of SiteScope, the Freemium license is not included in the exported data.

Click **Next** to complete the export operation.

If you are installing SiteScope Freemium, skip to step 8.

7. If you selected the **HP Operations Agent** option, the Install/Uninstall HP Operations Agent screen opens.

HP Operations Agent

Install/Uninstall HP Operations Agent

The HP Operations agent is required to integrate SiteScope event and metrics data with HP Operations Manager and BSM. The agent sends events and acts as a data storage for metrics data that can be made available to HP Operations Manager and BSM applications.

Install HP Operations Agent   ☐

Uninstall HP Operations Agent   ☐

■ **Install HP Operations Agent.** Select to install the HP Operations agent on the SiteScope server. The agent is required to enable SiteScope to send events and act as a data storage for metrics data if SiteScope is integrated with an HP Operations Manager or BSM Gateway server.

Note: The HP Operations Agent is not required when graphing metrics data to Performance Graphing using the profile database in BSM. The profile database is the recommended option, because it is a more robust and scalable data source, and does not require configuration of the HP Operations Integration.

For details on reporting metrics data, see Integrating SiteScope with HP Operations Manager Products in the SiteScope Help. You can check the HP Software Integrations site to see if a more updated version of this guide is available (for Windows: http://support.openview.hp.com/sc/solutions/integrations.jsp?intid=39; for UNIX: http://support.openview.hp.com/sc/solutions/integrations.jsp?intid=628)

■ **Uninstall HP Operations Agent.** Select to uninstall the HP Operations agent from the SiteScope server.

Click **Next** to complete the install/uninstall operation.

> **Note:** If you install the HP Operations agent on a machine that already has the agent installed, SiteScope overrides it and upgrades the current agent.

8. The Summary screen opens, displaying the configuration status.

   Click **Finish** to close the wizard.

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

Running the Configuration Tool on Solaris or Linux Platforms

The Configuration Tool is a convenient utility for moving configuration data from one SiteScope installation to another. You can export SiteScope data such as templates, logs, monitor configuration files, scripts, server certificates, and so forth from your current SiteScope for later import into SiteScope. You can also use the wizard to change any of the ports used by the SiteScope server, and to install and unistall the HP Operations agent.

If you exported SiteScope data during the installation process, you can import the data using the Configuration Tool. Alternatively, you can export data from your current SiteScope independently using the Configuration Tool. If you have created or modified monitor configuration files in previous versions of SiteScope, you may need to import them to the current SiteScope directory.

> **Note:**
>
> ● You can also run the configuration Tool on Solaris or Linux platforms in console mode. For details, see "Running the Configuration Tool on Solaris or Linux Using Console Mode" on page 149.
>
> ● When moving configuration data from one SiteScope installation to another, make sure that SiteScope server from which you are taking configuration data is in the same time zone as the SiteScope server to which the data is being imported.
>
> ● The inclusion of server certificates and scripts when exporting data is supported by the SiteScope Configuration Tool. For details on how to include server certificates and scripts when exporting data from earlier versions of SiteScope, see "Upgrading an Existing SiteScope Installation" on page 77.
>
> ● The SiteScope 64-bit version consumes up to 3 times more memory than the SiteScope 32-

bit version. Accordingly, if you are using a SiteScope 64-bit version you should manually increase the JVM heap size on the server:

a. Open the **SiteScope/bin/start-service** file for editing.

b. In the last line, increase parameter **-Xmx512m** to **-Xmx2048m** (for 2GB) or to a higher value, as required, up to a maximum of **-Xmx8192m** (for 8GB).

To run the SiteScope Configuration Tool:

1. On the SiteScope server, do either of the following:

   a. In graphic mode, run `<SiteScope install Directory>/bin/config_tool.sh`

   b. In console mode, run `<SiteScope install Directory>/bin/config_tool.sh -i console`

   The SiteScope Configuration Wizard opens.

   Click **Next**.

2. Select the actions that you want to perform in the Introduction screen, and then click **Next**.

   ### Introduction

   This wizard enables you to change the ports assigned to SiteScope, move configuration data from one SiteScope installation to another, and install/uninstall the HP Operations Agent.

   Select the actions that you want to perform.

   ☐ Change ports

   ☐ Import configuration

   ☐ Export configuration

   ☐ HP Operations Agent

   - **Change port.** Enables changing any of the ports used by the SiteScope server. For details, see step 3.

   - **Import Configuration.** Enables importing configuration data from an exported configuration data (**.zip**) file, or from an existing SiteScope installation. For details, see step 5.

   - **Export Configuration.** Enables exporting SiteScope data such as templates, logs, and monitor configuration files from your current SiteScope for later import into SiteScope. For

details, see step 4.

- **HP Operations Agent.** Enables installing and unstalling the HP Operations agent. The agent enables SiteScope or SiteScope Failover to send events and act as a data storage for metrics data when SiteScope is integrated with an HP Operations Manager or BSM Gateway server. For details, see step 6.

3. If you selected the **Change ports** option, the Change Ports screen opens.

Change Ports

You can change any of the ports used by the SiteScope server

It is recommended to use ports in the 28000-28100 range so as not to interfere with ports used by other Business Service Management products.

SiteScope user interface	8080
Tomcat shutdown	28005
Tomcat AJP connector	28009
SSL	8443
JMX console	28006
Classic user interface	8888
Classic user interface (secure)	

Modify the ports used by the SiteScope server as required. Port numbers must be numeric and should be in the 1-65534 range. A port is mandatory for all components except Classic user interface.

> **Note:** It is recommended to use ports in the 28000-28100 range so as not to interfere with ports used by other Business Service Management products.

Click **Next** to complete the change port operation.

4. If you selected the **Export Configuration** option, the Export Configuration screen opens.

Note: You must stop the SiteScope service before exporting the data, and restart the service after exporting the data. For details, see "Starting and Stopping the SiteScope Process on Solaris and Linux Platforms" on page 191.

- In **From SiteScope folder**, accept the default directory given in the 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 **To file**, enter the directory to which to export the user data file (the directory must already exist) and the 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** to complete the export operation.

5. If you selected the **Import Configuration** option, the Import Configuration screen opens.

> **Note:** You must stop the SiteScope service before importing the data, and restart the service after importing the data. For details, see "Starting and Stopping the SiteScope Process on Solaris and Linux Platforms" on page 191.

- If you select **Use existing exported configuration file**, enter the name of the user data file to import.

- If you select **Import the followingSiteScope installation**, enter the SiteScope installation directory to which to import the user data file.

- If you also want to import log files, select **Include log files**.

Click **Next** to complete the import operation.

6. If you selected the **HP Operations Agent** option, the HP Operations Agent screen opens.

HP Operations Agent

Install/Uninstall HP Operations Agent

The HP Operations agent is required to integrate SiteScope event and metrics data with HP Operations Manager and BSM. The agent sends events and acts as a data storage for metrics data that can be made available to HP Operations Manager and BSM applications.

Install HP Operations Agent ☐

Uninstall HP Operations Agent ☐

- **Install HP Operations Agent.** Select to install the HP Operations agent on the SiteScope server. The agent is required to enable SiteScope to send events and act as a data storage for metrics data if SiteScope is integrated with an HP Operations Manager or BSM server .

> **Note:** The HP Operations Agent is not required when graphing metrics data to Performance Graphing using the profile database in BSM. The profile database is the recommended option, because it is a more robust and scalable data source, and does not require configuration of the HP Operations Integration.
>
> For details on reporting metrics data, see Integrating SiteScope with HP Operations Manager Products in the SiteScope Help. You can check the HP Software Integrations site to see if a more updated version of this guide is available (for Windows: http://support.openview.hp.com/sc/solutions/integrations.jsp?intid=39; for UNIX: http://support.openview.hp.com/sc/solutions/integrations.jsp?intid=628)

- **Uninstall HP Operations Agent.** Select to uninstall the HP Operations agent from the SiteScope server.

Click **Next** to complete the install/uninstall operation.

> **Note:** If you install the HP Operations agent on a machine that already has the agent installed, SiteScope overrides it and upgrades the current agent

7. The Summary screen opens.

Click **Finish** to close the wizard.

Running the Configuration Tool on Solaris or Linux Using Console Mode

You can run the Configuration Tool using a command line or console mode. Use this option if you are configuring SiteScope on a remote server, or for any other reason that prevents the use of the user interface.

To run the Configuration Tool on Solaris or Linux using the console mode:

1. Run the following command:

    `/bin/config_tool.sh -i console`

2. The configuration selection screen is displayed.

```
# pwd
/opt/HP/SiteScope/bin
# ./config_tool.sh -i console
This wizard enables you you to change the ports assigned to SiteScope,
move configuration data from one SiteScope installation to another,
and install/uninstall the HP Operations agent

Select the actions that you want to perform.
-------------------------------------------------------------
-------------------------------------------------------------
Please select one of the options

->1 - Export: ()
  2 - Import: ()
  3 - Change ports: ()
  4 - HP Operations Agent: ()

:
```

Choose the configuration action that you want to perform.

- Enter the number 1 to export SiteScope data.

- Enter the number 2 to import configuration data from an exported configuration data (.zip) file, or from an existing SiteScope installation.

- Enter the number 3 to change any of the ports used by the SiteScope server.

- Enter the number 4 to install or uninstall the HP Operations agent.

Press ENTER to continue.

3. If you selected the **Export** option, the Export Configuration screen opens.

```
Select the actions that you want to perform.
-------------------------------------------------------------
-------------------------------------------------------------
Please select one of the options

->1 - Export: ()
  2 - Import: ()
  3 - Change ports: ()
  4 - HP Operations Agent: ()

: 1
-------------------------------------------------------------
SiteScope source folder
Folder name []
PRESS <1> to accept the value [], or <2> to change the value
2
Folder name:
/opt/HP/SiteScope
Folder name [/opt/HP/SiteScope]:
PRESS <1> to accept the value [/opt/HP/SiteScope], or <2> to change the value
1
-------------------------------------------------------------
Exported configuration target file name
File Name [SiteScope.zip]
PRESS <1> to accept the value [SiteScope.zip], or <2> to change the value
1

Configuration completed
```

- For the **SiteScope source folder**:

  ○ Enter the number 1 to accept the default directory given in [ ].

  ○ Enter the number 2 to change the value, and then 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/HP/SiteScope, enter
    /opt/HP/SiteScope.

  Press ENTER to continue with the installation.

- For **Exported configuration target file name**:

  ○ Enter the number 1 to export the data to a file named **SiteScope.zip**.

  ○ Enter the number 2 to change the name for the exported user data file. The name must
    end in **.zip**.

  Press ENTER to complete the export operation.

4. If you selected the **Import** option, the Import Configuration screen opens.

```
Select the actions that you want to perform.
-----------------------------------------------------------
-----------------------------------------------------------
Please select one of the options

->1 - Export: ()
  2 - Import: ()
  3 - Change ports: ()
  4 - HP Operations Agent: ()

: 2
-----------------------------------------------------------
Import configuration data from an existing configuration file or SiteScope installati
on

->1 - Do not import: ()
  2 - Import from file: ()
  3 - Import from folder: ()

: 2
-----------------------------------------------------------
Enter the name of the imported configuration file
File name [1]:
PRESS <1> to accept the value [1], or <2> to change the value
2
File name:
SiteScope.zip
File name [SiteScope.zip]:
PRESS <1> to accept the value [SiteScope.zip], or <2> to change the value
1

Configuration completed
```

Select the configuration data option:

- Enter the number 1 if you do not want to import configuration data.

- Enter the number 2 to import configuration data from a file. If you select this option:

  ○ Enter the number 1 to accept the default file name given in [ ].

  ○ Enter the number 2 to change the value, and enter the name of the file from which to
    import configuration data. Enter the number 1 to accept the name.

- Enter the number 3 to import configuration data from a SiteScope installation directory. If
  you select this option:

  ○ Enter the number 1 to accept the default directory given in [ ].

  ○ Enter the number 2 to change the value, and enter the SiteScope installation directory
    from which to import the user data file. Enter the number 1 to accept the name.

  Press ENTER to complete the import operation.

5. If you selected the **Change Ports** option, the Change Ports screen opens.

```
Please select one of the options

->1 - Export: ()
  2 - Import: ()
  3 - Change ports: ()
  4 - HP Operations Agent: ()

: 3
-------------------------------------------------------------
SiteScope user interface port
Port [8080]
PRESS <1> to accept the value [8080], or <2> to change the value
1
-------------------------------------------------------------
Tomcat shutdown port
Port [28005]
PRESS <1> to accept the value [28005], or <2> to change the value
1
-------------------------------------------------------------
Tomcat AJP connector port
Port [28009]
PRESS <1> to accept the value [28009], or <2> to change the value
1
-------------------------------------------------------------
SSL port
Port [8443]
PRESS <1> to accept the value [8443], or <2> to change the value
1
-------------------------------------------------------------
JMX console port
Port [28006]
PRESS <1> to accept the value [28006], or <2> to change the value
1
-------------------------------------------------------------
Classic user interface port
Port [8888]
PRESS <1> to accept the value [8888], or <2> to change the value
1
-------------------------------------------------------------
Classic user interface (secure) port
Port []
PRESS <1> to accept the value [], or <2> to change the value
1

Configuration completed
```

Modify the ports used by the SiteScope server as required. Port numbers must be numeric and should be in the 1-65534 range. A port is mandatory for all components except Classic user interface.

> **Note:** It is recommended to use ports in the 28000-28100 range so as not to interfere with ports used by other BSM products.

Press ENTER to complete the change port operation.

6. If you selected the **HP Operations Agent** option, the HP Operations Agent screen opens.

```
Please select one of the options

->1 - Export: ()
  2 - Import: ()
  3 - Change ports: ()
  4 - HP Operations Agent: ()

: 4
--------------------------------------------------------------
Please select one of the options

->1 - Install HP Operation Agent: ()
  2 - Uninstall HP Operation Agent: ()

: 1
--------------------------------------------------------------
Install HP Operations Agent

->1 - Do not install: ()
  2 - Install: ()

: 2

Configuration completed
```

Select one of the following options:

- Enter the number 1 to install the HP Operations agent on the SiteScope server. The agent is required to enable SiteScope to send events and act as a data storage for metrics data if SiteScope is integrated with an HP Operations Manager or BSM Gateway server.

  Note: The HP Operations Agent is not required when graphing metrics data to Performance Graphing using the profile database in BSM. The profile database is the recommended option, because it is a more robust and scalable data source, and does not require configuration of the HP Operations Integration.

  For details on reporting metrics data, see Integrating SiteScope with HP Operations Manager Products in the SiteScope Help. You can check the HP Software Integrations site to see if a more updated version of this guide is available (for Windows: http://support.openview.hp.com/sc/solutions/integrations.jsp?intid=39; for UNIX: http://support.openview.hp.com/sc/solutions/integrations.jsp?intid=628)

- Enter the number 2 to uninstall the HP Operations agent from the SiteScope server.

  Note: If you install the HP Operations agent on a machine that already has the agent installed, SiteScope overrides it and upgrades the current agent.

Press ENTER to complete the HP Operations agent install/uninstall operation.

  Note: The SiteScope 64-bit version consumes up to three times more memory than the SiteScope 32-bit version. Accordingly, if you are using a SiteScope 64-bit version you

should manually increase the JVM heap size on the server as follows:

a. Open the **SiteScope/bin/start-service** file for editing.

b. In the last line, increase parameter **-Xmx512m** to **-Xmx2048m** (for 2GB) or to a higher value, as required, up to a maximum of **-Xmx8192m** (for 8GB).

Running the Configuration Tool in Silent Mode

You can run the SiteScope Configuration Tool in silent mode. This enables you to make a backup copy of SiteScope configuration data from your current version of SiteScope, without having to navigate through the Configuration Tool screens and input your selections. Instead, all configuration parameters are allocated values you define in a response file.

Notes and Limitations

Before running a silent configuration, consider the following issues:

- When running a configuration in silent mode, no messages are displayed. Instead, you can view configuration information in the log files, including information on whether the configuration was successful. The configuration log files can be found under:

  - **%tmp%\HPSiteScope_config_tool.log** on Windows platforms

  - **/tmp/HPSiteScope_config_tool.log** on Solaris or Linux platforms

- When moving configuration data from one SiteScope installation to another, make sure that the SiteScope server from which you are taking configuration data is in the same time zone as the SiteScope server to which the data is being imported.

- When importing configurations to the same version of SiteScope, you must rename or delete all template example containers so as to import the new template examples.

- You must stop the SiteScope service before exporting or importing the data, and restart the service after exporting or importing the data. For details, see "Starting and Stopping the SiteScope Service on Windows Platform" on page 190 and "Starting and Stopping the SiteScope Process on Solaris and Linux Platforms" on page 191.

- If you selected the export configuration option:

  - 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 directory after an upgrade, so that you can see old reports.

  - The inclusion of server certificates and scripts when exporting data is supported in the Configuration Tool. For details on how to include server certificates and scripts when

exporting data from earlier versions of SiteScope, see "Upgrading an Existing SiteScope Installation" on page 77.

- If you selected the sizing option (available on Windows platforms only):

  - Sizing changes can be made only if the physical memory of the SiteScope server is larger than the maximum JVM heap size (Xmx) that the Configuration Tool has configured (1 GB for a 32-bit installation and 4 GB for a 64-bit installation).

  - If you start SiteScope by running the **go.bat** file in the **<SiteScope installation>\bin directory**, open the **go.bat** file and increase the **–Xmx512m** parameter to **–Xmx1024m** (for 1GB) or higher, as required, up to a maximum of **–Xmx8192m** (for 8GB).

- If you selected the change ports option, it is recommended to use ports in the 28000-28100 range so as not to interfere with ports used by other Business Service Management products.

- If you selected the HP Operations Agent option and you install the HP Operations agent on a machine that already has the agent installed, SiteScope overrides it and upgrades the current agent.

- When SiteScope is running on Solaris or Linux platforms using the SiteScope 64-bit version (which consumes up to 3 times more memory than the SiteScope 32-bit version), you should manually increase the JVM heap size on the server as follows:

  a. Open the **SiteScope/bin/start-service** file for editing.

  b. In the last line, increase parameter **-Xmx512m** to **-Xmx2048m** (for 2GB) or to a higher value, as required, up to a maximum of **-Xmx8192m** (for 8GB).

Running Silent Configuration

You run a silent configuration using the **configtoolparams.txt** file. Since this file has a very specific format, you should create the silent configuration file using the sample file located in the **<SiteScope installation directory>\examples\silent_config** folder.

To run a silent configuration for SiteScope (for SiteScope 11.22 or later):

1. Navigate to the **configtoolparams.txt** file located in the **<SiteScope installation directory>\examples\silent_config** folder.

2. Make a copy of the file, and save it to a location of your choice.

3. Open the file, modify it to meet your configuration needs (follow the instructions in the sample file), and then save the file.

4. Run the configuration from the command line with the **-i silent** and the **-f <answers file>** flag.

   For example:

   ```
   config_tool -i silent -f c:\configtoolparams.txt (Windows)
   ```

or

`./config_tool.sh -i silent -f /opt/configtoolparams.txt` (Linux or Solaris)

Chapter 16: Uninstalling SiteScope

This chapter includes:

Uninstalling SiteScope on a Windows Platform

You can uninstall SiteScope 11.20 and any minor-minor versions (patches) installed on top of it, or a SiteScope minor-minor version only from your server machine. For SiteScope running on Windows platforms, the SiteScope installation includes a program to uninstall the SiteScope software from your computer.

This section includes:

How to Uninstall SiteScope and Any Minor-Minor Versions Installed on Top of it

1. Stop the SiteScope service.

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

   b. 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.

2. Uninstall SiteScope.

   a. Choose **Start > All Programs > HP SiteScope > Uninstall HP SiteScope**.

   b. On the Choose Locale screen, choose the language you want to have displayed, and click OK.

   c. On the Application Maintenance screen, Select **Uninstall** and click **Next**.

   d. In the Pre-Uninstall Summary screen, click **Uninstall**.

   e. The HP SiteScope Configuration Wizard opens. Specify whether to uninstall the HP Operations Agent ((not applicable for SiteScope Freemium). Click **Next**.

Each software component and its uninstallation progress are displayed on your screen during the uninstallation operation.

> **Note:** If SiteScope is installed on the same machine as HP Operations Manager, when uninstalling SiteScope you should clear the option to uninstall the HP Operations agent.

After the uninstallation process is complete, the Uninstall Complete window opens showing you a summary of the uninstallation process.

    f. In the Uninstall Complete window, click **Done** to close the uninstallation program.

    From the **View log file** link, you can access the uninstallation log file that opens in a Web browser. For details on the removed packages, click the Details tab

3. When the uninstall process is complete, restart the machine if requested.

How to Uninstall a SiteScope Minor-Minor Version

1. Stop the SiteScope service.

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

    b. 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.

2. Select **Control Panel > Add/Remove Programs > Change or Remove Programs**, and make sure the **Show Updates** option is selected to ensure that the minor-minor version is displayed beneath the root entry. For example, for SiteScope 11.23, select **HP SiteScope 11.23**, click the **Change/Remove** button, and follow the uninstall wizard instructions listed in step 2 above.

3. When the uninstall process is complete, restart the machine if requested.

Uninstalling SiteScope on a Solaris or Linux Platform

You can uninstall SiteScope 11.20 and any minor-minor versions (patches) installed on top of it, or a SiteScope minor-minor version only from your server machine. 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.

This section includes:

- "How to Uninstall SiteScope and Any Minor-Minor Versions Installed on Top of it" below

- "How to Uninstall a SiteScope Minor-Minor Version" on page 162

How to Uninstall SiteScope and Any Minor-Minor Versions Installed on Top of it

1. Log on 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.

   ```
   $
   $ ./stop
   Stopped SiteScope process (6252)
   Stopped SiteScope monitoring process (6285)
   $
   ```

3. If you work in X Windows mode, run the following command:
   /opt/HP/SiteScope/installation/bin/sis_uninstall.sh

4. If you work in console mode, you should:

   - Uninstall SiteScope 11.2x by running the command (for example, for SiteScope 11.23):
     /opt/HP/SiteScope/Uninstall/HPSiS1123/setup.bin -i console

   - Uninstall SiteScope 11.20 by running the command:
     /opt/HP/SiteScope/Uninstall/HPSiteScope/setup.bin -i console

5. The HP Software Installer starts. Specify the Locale and press ENTER.

```
Preparing to install...
Extracting the JRE from the installer archive...
Unpacking the JRE...
Extracting the installation resources from the installer archive...
Configuring the installer for this system's environment...
Preparing CONSOLE Mode Installation...


===============================================================================
Choose Locale...
----------------


    1- Deutsch
  ->2- English
    3- Fran?ais

CHOOSE LOCALE BY NUMBER: 2
===============================================================================
HP Software Installer
---------------------



PRESS <ENTER> TO CONTINUE: 2
```

6. Type 1 and press ENTER to confirm that you want to uninstall SiteScope.

```
===============================================================================
Maintenance Selection
---------------------

Modify, repair or uninstall the application
If you want to change something on a previous step, type 'back'.
You may cancel this installation at any time by typing 'quit'.



  ->1- Uninstall       Uninstall the application from your computer.

Please select one of the options...: 1
```

7. The uninstallation process begins. If HP Operations Agent is installed, you are prompted to
    uninstall it. Type 2 and press ENTER to uninstall HP Operations Agent:

```
  : -------------------------------------------------------------
Uninstall HP Operations Agent
->1 - Do not uninstall: ()
  2 - Uninstall: ()
```

8. The package uninstall status messages are displayed and then the uninstall completes:

```
===============================================================================
Uninstallation Complete
-----------------------



The uninstallation has been successfully completed.
```

How to Uninstall a SiteScope Minor-Minor Version

1. Stop SiteScope by running the **stop** shell script included in the **/opt/HP/SiteScope**. An example command line to stop the SiteScope is: **/opt/HP/SiteScope/stop**

2. Run the uninstall command (for example, for SiteScope 11.23):

   - In graphic mode: **/opt/HP/SiteScope/Uninstall/HPSiS1123/setup.bin**

   - In console mode: **/opt/HP/SiteScope/Uninstall/HPSiS1123/setup.bin -i console**

   - In silent mode: **/opt/HP/SiteScope/Uninstall/HPSiS1123/setup.bin -i silent**

3. When the uninstall process is complete, restart the machine if requested.

Part 4: Running SiteScope Securely

Chapter 17: Hardening the SiteScope Platform

This chapter includes:

- "Overview" below

- "Setting SiteScope User Preferences" below

- "Password Encryption" below

- "Using Transport Layer Security (TLS) to Access SiteScope" on the next page

Overview

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

As a system availability monitoring tool, SiteScope might have access to system information that could be used to compromise system security if steps are not taken to secure it. You should use the configurations and setup options in this section to protect the SiteScope platform.

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

Setting SiteScope User Preferences

SiteScope user profiles are used to require a user name and password to access the SiteScope interface. After installation, SiteScope is normally accessible to any user who has HTTP access to the server on which 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 the User Management Preferences section in Using SiteScope in the SiteScope Help.

Password Encryption

All SiteScope passwords are encrypted using a method called Triple Data Encryption Standard (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, it is extremely difficult for unauthorized users to reproduce the original password.

Using Transport Layer Security (TLS) to Access SiteScope

You can configure SiteScope to use TLS to control access to the product interface. For more information, see "Configuring SiteScope to Communicate Over a Secure Connection" on page 166.

> **Note:** Transport Layer Security (TLS) is the new name for Secure Sockets Layer (SSL). The SiteScope user interface still includes references to SSL. The terms are used interchangeably in SiteScope.

Chapter 18: Configuring SiteScope to Communicate Over a Secure Connection

This chapter includes:

- "Configuring SiteScope to Require a Secure Connection" below

- "Configuring Smart Card Authentication" below

- "Configuring SiteScope to Verify Certificate Revocation" on page 168

Configuring SiteScope to Require a Secure Connection

You can configure SiteScope to require secure access to its interfaces (UI and API). You do this by:

1. Obtaining the server certificate issued to the FQDN of the SiteScope server.

2. Configuring SiteScope to respond to access requests only over a secure channel.

You can do this by either:

- Using the Hardening Tool to configure SiteScope to perform this configuration (recommended method). For details, see "How to Use the Hardening Tool to Configure SiteScope to Require a Secure Connection" on page 174.

- Manually configuring SiteScope to use TLS. For details, see "Manually Configuring SiteScope for Using a Secure Connection" on page 213.

Configuring Smart Card Authentication

Smart cards are physical devices used to identify users in secure systems. These cards can be used to store certificates which verify the user's identity and allow access to secure environments.

SiteScope supports user authentication using smart cards. If smart card authentication is configured, you cannot log in to SiteScope without a valid smart card.

SiteScope can be configured to use these certificates in place of the standard model of each user manually entering a user name and password. You define a method of extracting the user name from the certificate stored on each card.

When SiteScope is configured for smart card authentication, users can log in to SiteScope only with a valid smart card. The option of logging in by manually typing in your username and password is locked for all users unless smart card configuration is disabled.

If smart card authentication is configured in BSM and you want to integrate SiteScope with BSM, you must configure SiteScope smart card authentication to authenticate the BSM client certificate.

For details, see "Configuring SiteScope to Connect to a BSM Server That Requires a Secure Connection" on page 170.

Similarly, if SiteScope is configured for smart card authentication and you want to allow BSM to communicate with SiteScope, you must first configure BSM to authenticate with the client certificate in SiteScope. For details, see "Configuring SiteScope to Connect to a BSM Server That Requires a Secure Connection" on page 170.

Note: If smart card enforcement is enabled, the only supported browser is Internet Explorer running on a Windows operating system.

If smart card enforcement is disabled, but client certificate authentication is enabled, to use SiteScope in Firefox, see "Using Firefox When Client Certification is Enabled" on page 168.

Tip: For more information about smart cards, see the Smart Card Authentication Configuration Guide (http://support.openview.hp.com/selfsolve/document/KM00444967/binary/BSM_923_SmartCardGuide.pdf).

Configuring SiteScope to Require Client Certificate Authentication

If you have configured SiteScope to work over TLS (see "Configuring SiteScope to Require a Secure Connection" on the previous page), you can then configure SiteScope and SiteScope public API client to require client certificate authentication.

You do this by using the Hardening Tool. For details, see "How to Use the Hardening Tool to Configure SiteScope and SiteScope Public API Client Certificate Authentication" on page 180.

Chapter 19: Advanced Hardening Configuration

This chapter includes:

- "Configuring SiteScope to Verify Certificate Revocation" below

- "Using Firefox When Client Certification is Enabled" below

- "Importing Certificate Authority Certificates into SiteScope TrustStores" on the next page

- "Disabling JMX Remote Access" on the next page

- "Restoring a Backed Up Configuration" on the next page

Configuring SiteScope to Verify Certificate Revocation

You use the Hardening Tool to configure SiteScope to verify revocation of client certificates. For details, see "How to Use the Hardening Tool to Configure SiteScope to Verify Certificate Revocation" on page 176.

Using Firefox When Client Certification is Enabled

If smart card enforcement is disabled, but client certificate authentication is enabled, to open the SiteScope user interface in Firefox, you must:

1. Import your personal certificate into Firefox, as follows:

   a. In Firefox, go to **Tools** > **Options** > **Advanced** > **Encryption** > **View Certificates**. The Certificate Manager dialog box opens.

   b. Click **Import...** and open your personal certificate in **.pfx** (or **.p12**) file format. The Password Entry dialog box opens.

   c. Enter the password used to encrypt this certificate backup and click **OK**. The certificate appears in the Certificate Manager dialog box, confirming that the certificate is added to Firefox.

2. Import your personal certificate into the client JRE, as follows:

   a. In the JRE, open the Java Control Panel.

   b. Go to **Security** > **Certificates** and select Client Authentication as the Certificate type.

   c. Click **Import** and open the client certificate that you imported into Firefox.

   d. Click **OK**. The personal certificate appears in the JRE.

3. Enter the SiteScope URL in Firefox. The User Identification Request dialog box opens. Select the personal certificate that you created in step 1 to present as identification.

Importing Certificate Authority Certificates into SiteScope TrustStores

For SiteScope to trust a client certificate, SiteScope must trust the Certificate Authority that issued the client certificate. For SiteScope to trust a Certificate Authority, the Certificate Authority's certificate must be stored in the SiteScope server and main TrustStores.

The SiteScope server TrustStore is responsible for authentication of all incoming connection request from clients (API and browsers).

The SiteScope main TrustStore is a Certificate Authority Java TrustStore that is located in the Java directory in the SiteScope install directory. This TrustStore is responsible for SiteScope certificate management.

You use the Hardening Tool to import Certificate Authority certificates into SiteScope server and main TrustStores. For details, see "How to Use the Hardening Tool to Import Certificate Authority Certificates into SiteScope TrustStores" on page 177.

Disabling JMX Remote Access

JMX has remote access to the SiteScope server by default. You can disable that access.

> **Note:** To fully secure SiteScope, it is recommended that you disable JMX remote access.

You use the Hardening Tool to configure JMX remote access. For details, see "How to Use the Hardening Tool to Configure JMX Remote Access" on page 181.

Restoring a Backed Up Configuration

When you run the Hardening Tool, the existing SiteScope configuration is automatically backed up. To restore a backed up configuration, see "How to Use the Hardening Tool to Restore a Backed Up Configuration" on page 181.

Chapter 20: Configuring SiteScope to Communicate With BSM Over a Secure Connection

This chapter includes:

- "Configuring SiteScope to Connect to a BSM Server That Requires a Secure Connection" below

- "Configuring SiteScope to Connect to a BSM Server That Requires a Client Certificate" below

- "Configuring BSM to Connect to SiteScope When SiteScope Requires a Client Certificate" below

Configuring SiteScope to Connect to a BSM Server That Requires a Secure Connection

To configure SiteScope to connect to a BSM server that requires a secure connection, you must establish trust to enable secure communication between SiteScope and BSM. This means that SiteScope must trust the Certificate Authority that issued the BSM server certificate. For SiteScope to trust a Certificate Authority, the Certificate Authority's certificate must be stored in the SiteScope server and main TrustStores. For details, see "Importing Certificate Authority Certificates into SiteScope TrustStores" on page 169.

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

You can configure SiteScope to connect to a BSM server that requires a client certificate. This involves importing the BSM server certificate into a SiteScope keystore.

We recommend that you do this by using the Hardening Tool. For details, see "How to Use the Hardening Tool to Configure SiteScope to Connect to a BSM Server That Requires a Client Certificate" on page 178.

It is also possible use the manual procedures in "Configuring SiteScope to Connect to a BSM Server That Requires a Client Certificate" on page 221.

Configuring BSM to Connect to SiteScope When SiteScope Requires a Client Certificate

In BSM, perform the following steps on both the Gateway and Data Processing Servers:

1. Copy the file **<SiteScope Home>\templates.certificates\BSMClientKeystore** from the SiteScope machine file to any folder on the BSM machine.

2. Stop BSM.

3. Edit **<HP BSM root directory>\EjbContainer\bin\product_run.bat** and add the following:

```
set SECURITY_OPTS=-Djavax.net.ssl.keyStore=FULL_PATH_TO_COPIED_
BSMClientKeyStore_File -Djavax.net.ssl.keyStorePassword=PASSWORD_FOR_
BSMClientKeyStore_File -Djavax.net.ssl.keyStoreType=JKS

set JAVA_OPTS=%JAVA_OPTS% %SECURITY_OPTS%
```

where `FULL_PATH_TO_COPIED_BSMClientKeyStore_File` is a keystore path, and `PASSWORD_` `FOR_BSMClientKeyStore_File` is the keystore password.

4. Restart BSM.

5. Configure BSM and SiteScope in System Availability Management (SAM) Administration.

6. Change the **Gateway Server name/IP address** property in **SAM Administration > New/Edit SiteScope > Distributed Settings** to the Fully Qualified Domain Name (FQDN) of the secure reverse proxy.

Chapter 21: Using the Hardening Tool

The Hardening Tool is a command-line tool that enables you to configure SiteScope to perform a full or partial hardening of SiteScope.

> **Note:** Each time the tool runs, it performs a full backup of the existing SiteScope configuration, enabling you to roll back to a backed up configuration. For details, see "How to Use the Hardening Tool to Restore a Backed Up Configuration" on page 181.

You can use the Hardening Tool to perform the following tasks:

- "How to Run the Hardening Tool" below

- "How to Use the Hardening Tool to Configure SiteScope to Require a Secure Connection" on page 174

- "How to Use the Hardening Tool to Configure SiteScope to Verify Certificate Revocation" on page 176

- "How to Use the Hardening Tool to Import Certificate Authority Certificates into SiteScope TrustStores" on page 177

- "How to Use the Hardening Tool to Configure SiteScope to Connect to a BSM Server That Requires a Client Certificate" on page 178

- "How to Use the Hardening Tool to Configure SiteScope and SiteScope Public API Client Certificate Authentication" on page 180

- "How to Use the Hardening Tool to Configure JMX Remote Access" on page 181

- "How to Use the Hardening Tool to Restore a Backed Up Configuration" on page 181

How to Run the Hardening Tool

This topic describes how to open and run the Hardening Tool. To perform the other tasks described in the topics in this chapter, you must first perform the steps in this topic.

1. (Optional) If you want to enable LDAP user authentication, configure LDAP integration before running the tool:

    a. Configure the LDAP server on SiteScope. For details, see "How to Set Up SiteScope to Use LDAP Authentication" in the Using SiteScope Guide in the SiteScope Help.

    b. Create a new role in SiteScope user management for LDAP users.

    c. Change the SiteScope administrator login name to the email address of a user located in LDAP. Do not enter a password.

2. Stop the SiteScope service:

   Windows:

   - If you are running SiteScope from **go.bat**, close the command-line terminal or press **CTRL+C**.

   - If you are running SiteScope as a service:

        i.   In Windows Explorer, search for **services**. The Component Services window opens.

        ii. In the left pane, select **Services (Local)**.

        iii. In the services list in the center pane, select **HP SiteScope**.

        iv. In the area to the left of the service list, click **Stop the service**.

   Linux:

   Run the command line:

   ```
   cd /opt/HP/SiteScope/
   ./stop
   ```

   > **Caution:** Do not run the Hardening Tool when SiteScope is running.

3. Start the tool by running the command line:

   Windows:

   ```
   <SiteScope Installation directory>\tools\SiteScopeHardeningTool>
   runSSLConfiguration.bat
   ```

   Linux:

   ```
   cd <configuration tool directory>
   ./runSSLConfiguration.sh
   ```

   The Hardening Tool opens.

4. When prompted in the tool, select the option "SiteScope hardening configuration". The existing SiteScope configuration is automatically backed up.

5. When prompted, enter a backup description to allow easy recognition in case you want to restore that backup in the future. To restore a backed up configuration, see "How to Use the Hardening Tool to Restore a Backed Up Configuration" on page 181.

   > **Note:** When using the Hardening Tool, the Tomcat configuration **server.xml** file in the

> **/opt/HP/SiteScope/Tomcat/conf** directory is overwritten and any modifications made to that file before running the tool are removed. To restore these modifications, you must reapply them to this file after running the tool.

6. Select one or a combination of the tasks listed in the tool.

   For details on using the Hardening Tool to perform configuration tasks, see the other topics in this chapter.

> **Note:** Changes in configuration take effect only after you exit the Hardening Tool.

How to Use the Hardening Tool to Configure SiteScope to Require a Secure Connection

You can use the Hardening Tool to configure SiteScope to require a secure connection (https), as follows:

1. Run the Hardening Tool. For details, see "How to Run the Hardening Tool" on page 172.

2. When prompted in the tool, select the option "Configuring SiteScope Standalone to work over SSL (https)".

   Alternatively, if you want to perform all the hardening configuration tasks available in the tool, select the option "Full SiteScope hardening configuration (all of the configuration options)".

3. Confirm that you want to configure SiteScope to work over SSL.

4. Select one of the following methods to create the SiteScope server keystore to hold the SiteScope server certificate:

   - **Import a server keystore in .jks format.**

     The tool prompts you to select an alias in which the key for SiteScope SSL authentication is located.

     > **Note:** If you later configure SiteScope and SiteScope public API client for client certificate authentication (see "Configuring SiteScope to Require Client Certificate Authentication" on page 167), SiteScope uses this alias to export the key to the client TrustStore of the SiteScope API.

     Follow the instructions in the tool.

   - **Create a server keystore by signing a request on a certified Certificate Authority**

server.

Selecting this option creates a new keystore and generates a key request to a certificate authority for a signed certificate. The generated certificate is then imported into the keystore.

The tool prompts you to enter server keystore parameters. We recommend that for the Common Name, you enter your machine's URL (for example, `yourserver.domain.com`), and for the alias name, your machine's name (for example, `yourserver`).

- **Import a server keystore from a server certificate in .pfx format.**

Selecting this option creates a keystore from a certificate in **.pfx** format. This certificate must contain its private key.

The Hardening Tool automatically ensures that the keystore password and the private key are the same each time a keystore is created.

5. Enter a username property for the client certificate. The default username is `Other Name`.

The server certificate is imported to the server keystore. The certificate alias appears in the tool.

6. Confirm if you want to enable SiteScope client authentication.

If you enable client TLS authentication, SiteScope performs full client TLS authentication upon the TLS handshake and extracts a client certificate. This client certificate is checked against the SiteScope user management system.

7. Confirm if you want to enable smart card enforcement.

If you enable smart card enforcement, SiteScope verifies that the client certificate originates from a hardware device. For more details about smart card enforcement, see "Configuring Smart Card Authentication" on page 166.

8. Enter a password for the SiteScope server TrustStore. The default password is `changeit`.

For SiteScope to trust a client certificate, SiteScope must trust the Certificate Authority that issued the client certificate. For SiteScope to trust a Certificate Authority, the Certificate Authority's certificate must be stored in the SiteScope server and main TrustStores. To import Certificate Authority certificates into SiteScope TrustStores, see "How to Use the Hardening Tool to Import Certificate Authority Certificates into SiteScope TrustStores" on page 177.

How to Use the Hardening Tool to Configure SiteScope to Verify Certificate Revocation

You can use the Hardening Tool to configure SiteScope to verify revocation of client certificates using the following methods:

- **Certificate Revocation List (CRL)**

  Enables you to verify client certificate revocation through a CRL list. The URL of the CRL list is located in the client certificate properties. The list is downloaded to the local server. You are prompted to enter a life time of the CRL list cached on the local server.

  The following table describes the CRL lifetime:

CRL value	Description
-1	The CRL is cached locally and reloaded only if changed on the server. This value is recommended for better performance.
0	The CRL is reloaded with each verification request.
≥1	The CRL lifetime in seconds. At the expiration of this time, the CRL is reloaded.

- **Online Certificate Status Protocol (OCSP)**

  Enables you to verify client certificate revocation through a connection to a remote server. SiteScope passes the serial number of the client certificate to the remote server and waits for a response. The default OCSP responder URL is located in the client certificate properties, but you can override this URL.

You can verify client certificate revocation via a CRL, or via a CRL and the OCSP.

To verify client certificate revocation:

1. Run the Hardening Tool. For details, see "How to Run the Hardening Tool" on page 172.

2. Select the option "Configure SiteScope SSL certificate revocation verification via CRL and OCSP".

3. Follow the instructions in the tool.

   The Tool prompts you to activate the forward HTTP proxy.

   If you activate the forward HTTP proxy, all certificate revocation requests are redirected through the proxy server to CRL and OCSP URLs.

   Changes in configuration take effect only after you exit the Hardening Tool.

How to Use the Hardening Tool to Import Certificate Authority Certificates into SiteScope TrustStores

For more information about importing Certificate Authority certificates into SiteScope TrustStores, see "Importing Certificate Authority Certificates into SiteScope TrustStores" on page 169.

To import Certificate Authority certificates into SiteScope TrustStores:

1. Prerequisites

   Before importing Certificate Authority certificates into SiteScope TrustStores, you must configure SiteScope to work over TLS by importing a SiteScope server certificate into the SiteScope server keystore. For details, see "How to Use the Hardening Tool to Configure SiteScope to Require a Secure Connection" on page 174.

2. Run the Hardening Tool. For details, see "How to Run the Hardening Tool" on page 172.

3. When prompted in the tool, select the option "Import CA certificates into SiteScope main and server trustStores".

4. Follow the instructions in the tool.

Tips:

- The tool accepts file paths in regular Windows format only. In UNIX format, where a blank space in a file path is preceded by a backslash ("\") to indicate that a blank space follows, you should remove the backslash.

Format	File path
Windows	**/user/temp dir/certificate.cer**
UNIX	**/user/temp\ dir/certificate.cer** change to: **/user/temp dir/certificate.cer**

- Changes in configuration take effect only after you exit the Hardening Tool.

How to Use the Hardening Tool to Configure SiteScope to Connect to a BSM Server That Requires a Client Certificate

You use the Hardening Tool to configure client TLS authentication for BSM integration. The tool enables you to configure SiteScope to allow BSM to integrate with SiteScope. You can also use this tool to configure SiteScope Failover for TLS with client certificate authentication. In both cases, you must follow the procedure described below.

> **Note:** Before configuring TLS Client Authentication for BSM integration, you must configure SiteScope to work over TLS by importing a SiteScope server certificate into the SiteScope server keystore. For details, see "How to Use the Hardening Tool to Configure SiteScope to Require a Secure Connection" on page 174.
>
> If you have not already done this, the Hardening Tool prompts you to perform a full SiteScope hardening configuration.

To configure client TLS client authentication for BSM integration:

1. Run the Hardening Tool. For details, see "Using the Hardening Tool" on page 172.

2. Select the option "Configure SiteScope client certificate authentication for BSM Integration".

3. Follow the instructions in the tool.

   a. When prompted, enter a full path in **.cer** format to the Certificate Authority certificate that issued the BSM server certificate. The BSM server certificate is imported into the SiteScope TrustStore.

   b. When prompted, confirm that you trust the BSM server certificate. The BSM server certificate is imported to the keystore.

   c. When prompted, select one of the following methods to create the SiteScope server keystore to hold the SiteScope server certificate:

      ○ **Import a server keystore in .jks format.**

        The tool prompts you to select an alias in which the key for SiteScope TLS authentication is located.

        > **Note:** If you later configure SiteScope and SiteScope public API client for client certificate authentication (see "Configuring SiteScope to Require Client Certificate Authentication" on page 167), SiteScope uses this alias to export the key to the client TrustStore of the SiteScope API.

○ **Create a server keystore by signing a request on a certified Certificate Authority server.**

Selecting this option creates a new keystore and generates a key request to a certificate authority for a signed certificate. The generated certificate is then imported into the keystore.

The tool prompts you to enter server keystore parameters. We recommend that for the Common Name, you enter your machine's URL (for example, `anyserver.domain.com`), and for the alias name, your machine's name (for example, `anyserver`).

○ **Import a server keystore from a server certificate in .pfx format.**

Selecting this option creates a keystore from a certificate in **.pfx** format. This certificate must contain its private key.

The Hardening Tool automatically ensures that the keystore password and the private key are the same each time a keystore is created.

d. When prompted, enter the password for the client keystore that will be used to authenticate BSM. SiteScope creates the BSM client certificate keystore.

e. When prompted, enter the password for the Discovery Agent **TrustStore MAMTrustStoreExp.jks**. The default password is `logomania`. We highly recommend that you do not change the default password.

During the configuration process, SiteScope automatically imports the BSM server certificate into SiteScope TrustStore.

f. When prompted, confirm that you trust the BSM server certificate.

The BSM server certificate is imported into the SiteScope keystore.

Tips:

■ The tool accepts file paths in regular Windows format only. In UNIX format, where a blank space in a file path is preceded by a backslash ("\") to indicate that a blank space follows, you should remove the backslash.

Format	File path
Windows	**/user/temp dir/certificate.cer**
UNIX	**/user/temp\ dir/certificate.cer** change to: **/user/temp dir/certificate.cer**

- Changes in configuration take effect only after you exit the Hardening Tool.

How to Use the Hardening Tool to Configure SiteScope and SiteScope Public API Client Certificate Authentication

You use the Hardening Tool to configure SiteScope and SiteScope public API client for client certificate authentication as follows:

1. Run the Hardening Tool. For details, see .

2. Select the option "Configure SiteScope and SiteScope public API client for client certificate authentication".

3. Follow the instructions in the tool.

Tips:

- If you enable LDAP user authentication for SiteScope public APIs, the username extracted from the API client certificate is authenticated by the LDAP server.

- When you are prompted to add a client certificate signing authority to the SiteScope server TrustStore, the certificate is imported into SiteScope server TrustStore and main TrustStore. Created API configuration files are placed under the script directory in the **API_Configuration** directory.

- The tool accepts file paths in regular Windows format only. In UNIX format, where a blank space in a file path is preceded by a backslash ("\") to indicate that a blank space follows, you should remove the backslash.

Format	File path
Windows	**/user/temp dir/certificate.cer**
UNIX	**/user/temp\ dir/certificate.cer** change to: **/user/temp dir/certificate.cer**

- Changes in configuration take effect only after you exit the Hardening Tool.

How to Use the Hardening Tool to Configure JMX Remote Access

You can use the Hardening Tool to enable or disable JMX remote access to the SiteScope server as follows:

1. Run the Hardening Tool. For details, see "How to Run the Hardening Tool" on page 172.

2. Select the option "Configure JMX remote access".

3. Follow the instructions in the tool.

> **Tip:** Changes in configuration take effect only after you exit the Hardening Tool.

How to Use the Hardening Tool to Restore a Backed Up Configuration

When you run the Hardening Tool, the existing SiteScope configuration is automatically backed up. You can use the Hardening Tool to restore a backed up configuration as follows:

1. Run the Hardening Tool. For details, see "How to Run the Hardening Tool" on page 172.

2. Select the option "Restore SiteScope configuration from backup".

3. Follow the instructions in the tool.

> **Tips:**
>
> - Backup names contain the time and date of the backup.
>
> - Changes in configuration take effect only after you exit the Hardening Tool.

Hardening Tool Limitations/Troubleshooting

This section describes troubleshooting and limitations when working with the Hardening Tool.

Limitations

If SiteScope is installed on a non-English operating system, you cannot use the Hardening Tool to configure SiteScope for using TLS. In that case, use the manual procedure described in the appendix section of the HP SiteScope Deployment Guide.

Troubleshooting

- The Hardening Tool does not accept file paths in UNIX format.

  Cause: The tool accepts file paths in regular Windows format only.

  Solution: In UNIX format, where a blank space in a file path is preceded by a backslash ("\") to indicate that a blank space follows, you should remove the backslash.

Format	File path
Windows	**/user/temp dir/certificate.cer**
UNIX	**/user/temp\ dir/certificate.cer** change to: **/user/temp dir/certificate.cer**

- Upon exiting the tool, an error message appears notifying that there was a problem copying to a file.

  Cause: This happens when the configuration tool cannot find one of the created configuration files. This occurs when the tool is not run from the command line. In this case, the created files are not placed in the configuration tool directory.

  Solution:

  a. In the configuration tool directory, delete any created libraries (for example, **API_ Configuration**, **tmp_<number>**, **BSM_Int**).

  b. Open a command line terminal.

  c. Go to configuration tool directory through the command line.

  d. Run the configuration tool from the command line. For details, see "Using the Hardening Tool" on page 172.

- After configuring SiteScope authentication, SiteScope does not provide an option for an authentication certificate when accessing SiteScope through a web browser and login fails.

  Cause: SiteScope TrustStores do not contain the certificates of certificate signing authorities (CA certificates). This causes SiteScope not to request client certificates that were signed by those certificate signing authorities.

  Solution: Import CA certificates into SiteScope main and server TrustStores and add the needed CA certificates. For details, see "Importing Certificate Authority Certificates into SiteScope TrustStores" on page 169.

- SiteScope public API call exits with `NumberFormatException`.

  Cause: API call executed with `-useSSL` parameter set to false.

  Solution: Run API call with `-useSSL` parameter set to true.

- SiteScope public API call exits with `ConnectException: Connection refused`.

  Cause: API call tries to connect to a port that is not a TLS port.

  Solution: Set the `-port` parameter to TLS authentication port 8443.

- SiteScope public API call fails with `(500) Internal Server Error`.

  Cause: The `-login` parameter is not set to the correct TLS username.

  Solution: Set the `-login` parameter to `SITESCOPE_CERTIFICATE_AUTHENTICATED_USER`.

- SiteScope displays the following message when you try to access SiteScope through a browser: "The user is not valid SiteScope user. Please contact SiteScope administrator".

  Cause: Client TLS authentication and Smart Card enforcement are enabled while configuring SiteScope for TLS authentication, but LDAP server is not set in SiteScope user management.

  Solution 1:

  a. Run the Hardening Tool.

  b. Restore the SiteScope configuration that was backed up before running the tool (for details, see).

  c. Configure the LDAP server.

  d. Run the Hardening Tool again.

  Solution 2:

  a. Open the **master.config** file at **<SiteScope root directory>\groups** and change the value of the following properties to false:

     - _clientCertificateAuthEnabled

     - _clientCertificateAuthIsAPIRealLDAPUserRequired

     - _clientCertificateAuthSmartCardEnforcementEnabled

  b. Restart SiteScope.

  c. Configure the LDAP server.

  d. Open the **master.config** file.

  e. Change the above properties to their original values.

  f. Restart SiteScope.

Chapter 22: Configuration of USGCB (FDCC) Compliant Desktop

The United States Government Configuration Baseline (USGCB), formerly known as the Federal Desktop Core Configuration (FDCC), is a standard for desktop configuration that provides guidance on improving and maintaining effective configuration settings focusing primarily on security.

SiteScope is certified with USGCB (FDCC) compliant clients. To enable compliancy, you must add the SiteScope URL to the trusted sites security zone and to the pop-up allow list. It is also recommended to allow file downloads.

For more information on USGCB (FDCC), see:

- http://usgcb.nist.gov/usgcb/microsoft_content.html

- http://nvd.nist.gov/fdcc/index.cfm

Prerequisites:

Install the latest JRE version supported by SiteScope as listed in the "Client System Requirements" on page 70.

How to Enable Group Policy Editor (gpedit.msc) in Windows 7:

1. Add the SiteScope URL to the Trusted sites security zone:

   a. Open the Group Policy Editor by running the command: `run gpedit.msc`.

   b. Navigate to: **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Internet Explorer** > **Internet Control Panel** > **Security Page**:

      i. In the setting panel on the right, double-click **Site to Zone Assignment List**, select the **Enabled** option, and click **Show**. In the Show Content dialog box, click **Add**.

      ii. In the **Enter the name of the item to be added** box, enter the name of the SiteScope server. For example, `http://MySiteScope.com`. If you are using SiteScope over HTTPS, enter `https://MySiteScope.com`.

      iii. In the **Enter the value if item to be added** box, enter the number to denote the zone type:

Value	Zone Type	Description
1	Intranet zone	Sites on your local network
2	Trusted Site Zone	Sites that have been added to your trusted sites

Value	Zone Type	Description
3	Internet zone	Sites that are on the Internet
4	Restricted Sites zone	Sites that have been specifically added to your restricted sites

2. Add the SiteScope URL to the Pop-up allow list.

   a. Open the Group Policy Editor by running the command: `run gpedit.msc`.

   b. Navigate to: **Computer Configuration > Administrative Templates > Windows Components > Internet Explorer**:

      i. In the setting panel on the right, double-click **Pop-up allow List**, select the **Enabled** option, and click **Show**. In the Show Content dialog box, click **Add**.

      ii. In the **Enter the name of the item to be added** box, enter the name of the SiteScope server. For example, `http://MySiteScope.com`. If you are using SiteScope over HTTPS, enter `https://MySiteScope.com`.

3. Allow file downloads (optional, used for log grabber and release notes).

   a. Open the Group Policy Editor by running the command: `run gpedit.msc`.

   b. Navigate to: **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Internet Explorer** > **Security Features** > **Restrict File Download**, and in the setting panel on the right, double-click **Internet Explorer Process**, and select the **Disabled** option.

Part 5: Getting Started and Accessing SiteScope

Chapter 23: Post-Installation Administration

This chapter includes recommended steps you should perform after installing SiteScope.

✓	Step
	Register for SiteScope support. For more information, see "Getting Started Roadmap" on page 14.
	Log on to the SiteScope Web interface using a Web browser. For more information, see "Connecting to SiteScope" on page 192.
	If you are upgrading 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 "Using the SiteScope Configuration Tool" on page 138.
	If you did not enter your SiteScope license information during installation, enter it in the General Preferences page, as described in the General Preferences section of Using SiteScope in the SiteScope Help. New installations operate with a 60 day trial license. For license details, see "SiteScope Licenses" on page 38.
	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 the User Management Preferences section in Using SiteScope 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 the Email Preferences section in Using SiteScope 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 the Remote Servers section in Using SiteScope 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 the Log Preferences section in Using SiteScope in the SiteScope Help.

✓	Step
	Install middleware drivers for connectivity with remote databases and applications for those monitors that require drivers.
	When using SiteScope as a data collector for Business Service Management (BSM), configure the BSM integration. For details, see the Working with BSM section in Using SiteScope in the SiteScope Help.
	When using SiteScope to send events or report metrics for use in HP Operations Manager (HPOM) or Operations Management in BSM, configure the HP Operations Manager integration. For details, see "Integrating SiteScope with HP Operations Manager Products" in the HP Software Integrations site: • For HPOM for Windows, http://support.openview.hp.com/sc/solutions/integrations.jsp?intid=39 • For HPOM for UNIX, http://support.openview.hp.com/sc/solutions/integrations.jsp?intid=628
	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 the User-Defined Templates and Solution Templates sections in Using SiteScope in the SiteScope Help.
	Build dependencies between groups and key monitors to help control redundant alerting. For details, see the Working with SiteScope Groups section in Using SiteScope in the SiteScope Help.
	Roll out SiteScope to business stakeholders and system administrators.

After 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.

Chapter 24: Getting Started with SiteScope

This chapter includes:

- "Starting the SiteScope Service Overview" below

- "Starting and Stopping the SiteScope Service on Windows Platform" below

- "Starting and Stopping the SiteScope Process on Solaris and Linux Platforms" on the next page

- "Connecting to SiteScope" on page 192

- "SiteScope Classic Interface" on page 193

- "Troubleshooting and Limitations" on page 193

Starting the SiteScope Service Overview

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 Platform

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 Process 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.

> **Note:** While SiteScope must be installed on Solaris or Linux from a root user account, after it has been installed it can be run from a non-root user account. For details, see "Configuring a Non-Root User Account with Permissions to Run SiteScope" on page 19.

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`

   (Alternatively, on Linux/UNIX machines you can run `service sitescope start` in any directory.)

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`

   `(Alternatively, on Linux/UNIX machines you can run service sitescope stop in any directory.)`

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.

On Windows platforms, the installation process also adds a link to SiteScope in the **Start** > **All 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 > All Programs > HP SiteScope > Open HP SiteScope**. If the SiteScope port is changed after installing SiteScope, the port is updated in the **Open HP SiteScope** link.

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.
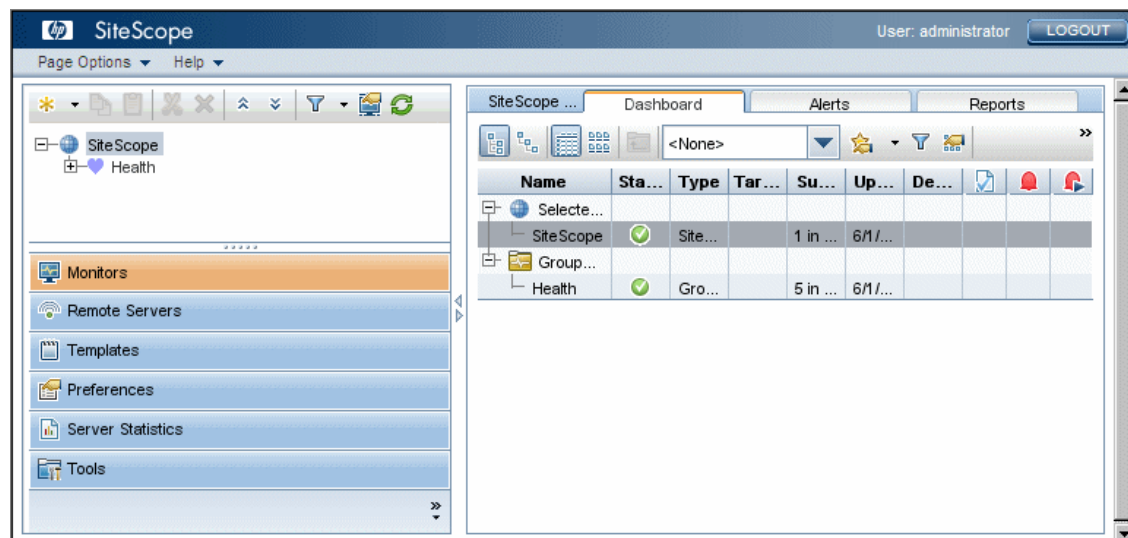
Note:

- To restrict access to this account and its privileges, you need to edit the administrator account profile to include a user login name and password. SiteScope then displays a login dialogue before SiteScope can be accessed. For information on editing the administrator account profile, see the User Management Preferences section in Using SiteScope in the SiteScope Help.

- When viewing SiteScope from another machine, it is recommended to use a machine that has Java Runtime Environment 1.6.0_26 or later 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.

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 an error message is displayed" on the next page

- "SiteScope applet loading fails with a "NoClassDefFound" exception" on the next page

- "Problems loading applet from a 64-bit machine" on the next page

- "For SiteScope installed on Solaris: "SiteScope failed to start as a background process" error is displayed when the stop and start commands are used" on page 195

- "For SiteScope installed on Solaris: "Shutting down SiteScope reason scheduled restart..." error is displayed shortly after starting SiteScope" on page 195

- "SiteScope hangs when opening the same SiteScope server on more than one tab in a browser window" on page 196

- "The SiteScope menu bar opens but the applet fails to start, and you see a blank screen, an error, or an "x" image" on page 196

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**. In the **General** tab, click **Settings > 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`.

SiteScope applet loading fails with a "NoClassDefFound" exception

If applet loading fails with a "NoClassDefFound" exception, select the **Keep temporary files on my computer** option in your client Java configuration (**Control Panel > Java > General Tab > Temporary Internet Files > Settings**).

If security issues require it, delete the temporary files manually when you finished using the SiteScope applet:

1. Close the SiteScope applet.

2. Select **Start > Control Panel > Java > General tab**.

3. In the **Temporary Internet Files** section, click **Settings**, and then click **Delete Files**.

Problems loading applet from a 64-bit machine

When running SiteScope on a 64-bit machine, make sure to use a browser version that matches your JRE:

JRE	Browser
64-bit JRE	- Internet Explorer (64-bit)
	- Internet Explorer (64-bit)
32-bit JRE	- Internet Explorer (32-bit)
	- Internet Explorer (32-bit)

For SiteScope installed on Solaris: "SiteScope failed to start as a background process" error is displayed when the stop and start commands are used

This issue could occur because SiteScope was not shut down properly before you tried to start it again. In some environments, if you start SiteScope and then immediately stop it, SiteScope is not stopped properly.

There are two possible solutions to this issue:

Possible solution 1 (to avoid this issue before starting SiteScope):

1. Manually kill the SiteScope process.

2. Run `ps -e | grep SiteScope` to get the SiteScope process ID.

3. Run `kill -9 <SiteScope's process ID>`.

Possible solution 2 (if you started SiteScope, and immediately want to stop it):

1. Before you stop SiteScope, go to the **<SiteScope root directory>\groups** folder and make sure that a file named **monpid** appears there.

2. If it does not appear, wait a couple of minutes until it is created.

3. Stop SiteScope.

For SiteScope installed on Solaris: "Shutting down SiteScope reason scheduled restart..." error is displayed shortly after starting SiteScope

SiteScope keeps restarting with "Shutting down SiteScope reason scheduled restart...." error written to the **<SiteScope root directory>\logs\Error.log** file.

The following error is written to the **<SiteScope root dir>\logs\tomcat.log** file:

```
<Date> [http-8080-Processor18] (PoolTcpEndpoint.java:441) ERROR - Endpoint
ServerSocket[addr=0.0.0.0/0.0.0.0,port=0,localport=8080] ignored exception:
java.net.SocketException: Too many open files
```

Possible solution:

On the Solaris server on which SiteScope is installed, edit the **/etc/security/limits.conf** file by adding your new limit for the user running Tomcat. For example:

```
root hard nofile 5120
root soft nofile 4096
```

For details on the **/etc/security/limits.conf** settings, see http://ss64.com/bash/limits.conf.html.

SiteScope hangs when opening the same SiteScope server on more than one tab in a browser window

When opening the same SiteScope server user interface in more than one tab of a browser window, SiteScope hangs when trying to navigate between the SiteScope server tabs.

Possible solution:

- Close the redundant tabs, and make sure that only one tab is open for the same SiteScope server user interface.

- Alternatively, open a new browser window.

The SiteScope menu bar opens but the applet fails to start, and you see a blank screen, an error, 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**. In the **General** tab, click **Network Settings**, select the **Direct Connection** option, and then click **OK**.

2. In the **Advanced** tab, expand the **Default Java for browsers** folder (or **<APPLET> tag support** if you are using Java 5). Make sure that **Microsoft Internet Explorer** and **Mozilla family** are selected. Click **Apply** and then click **OK**.

3. Restart your browser.

Backing up and recovering a SiteScope installation if unable to start SiteScope

To recover the SiteScope configuration data if SiteScope goes down and you are unable to restart it, you should make a backup of your current SiteScope installation directory and all of the subdirectories within the directory before installing a new version of SiteScope. You can back up the current SiteScope installation using the Configuration Tool to export SiteScope data to a **.zip** file, or you can manually back up the required files.

After reinstalling SiteScope, the monitor configuration data can be copied into SiteScope using the Configuration Tool (if you used the tool to make a backup of your installation directory), or by deleting from the new installation directory all the folders and files that you backed up, and then copying the backed up folders and files to the installation directory.

To back up the SiteScope installation:

1. Stop SiteScope.

   > **Note:** Although it is not mandatory to stop SiteScope, it is recommended to do so before making a back up.

2. Make a backup of your current SiteScope installation directory either by:

   - Using the Configuration Tool to export your configuration into a **.zip** file. For details, see "Using the SiteScope Configuration Tool" on page 138.

   - Copy the following folders and files from the SiteScope installation to your backup destination:

Directory	Description
\cache	Contains data samples that were not reported to Business Service Management if Business Service Management was down.
\conf\ems	Contains key configuration and control files used with Integration monitor types. This is only applicable if you use SiteScope as an agent reporting to another Business Service Management application.
\conf\integration	Contains topology files used for integrations with Business Service Management.
\discovery\scripts\custom	Contains custom discovery scripts.
\groups	Contains monitor, alert, report, and other critical configuration data needed for SiteScope operation.
\htdocs	Contains scheduled reports and user-customized style sheets for the SiteScope interface. Backup this directory and copy it to the SiteScope directory (within the same SiteScope versions) to avoid damaging the report pages and to see old reports. This folder cannot be backed up when the configuration is imported into a newer SiteScope version.
\logs	Contains a number of logs including date coded logs of monitoring data. Selectively back up the most recent monitoring data log files along with the other log types in this directory. You may also want to back up the **error.log**, **RunMonitor.log, access.log**, **alert.log**, and **monitorCount.log** logs for historical continuity.

Directory	Description
\persistency	This is the main persistency directory of the product. All the defined monitors, groups, alerts, templates, and many other SiteScope entities are found in this directory.
\scripts	Contains scripts used by Script monitors.
\scripts.remote	Contains command scripts used by Script monitors to trigger other scripts on remote servers.
\templates.*	Includes data and templates used to customize monitor function, alert content, and other features. The group of subdirectories all begin with the name templates. **Example:** templates.mail, templates.os, templates.webscripts
\WEB-INF\lib\peregrine.jar	File that might have been altered (regenerated) when configuring the HP Service Manager integration.

To recover the SiteScope installation:

1. Perform a new installation of SiteScope. For details, see "Installation Workflow" on page 98.

2. After installing SiteScope:

   - If you used the Configuration Tool to make a backup of your current SiteScope installation directory, use the Configuration Tool to import the previously created **.zip** file. For details, see "Using the SiteScope Configuration Tool" on page 138.

   - If you manually created a back up, delete all the folders and files listed above from the new installation directory, and then copy the backed up folders and files to the installation directory.

SiteScope does not open in Firefox

Problem: SiteScope does not open in the Firefox browser if smart card enforcement is disabled, but client certificate authentication is enabled.

Solution: To open SiteScope in the Firefox browser when smart card enforcement is disabled, but client certificate authentication is enabled, see "Using Firefox When Client Certification is Enabled" on page 168.

Appendixes

Appendix 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 section includes:

- "Configuring the Apache Tomcat Server Files" below

- "Configuring IIS" on page 203

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 from:

   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**.

     Example of the isapi_redirect.properties 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 it 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.

> **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:

- **worker.ajp13w.port** depends on the Tomcat version being used. Open **<SiteScope root
  directory>\Tomcat\conf\server.xml** and search for the string <Connector port= to
  determine the port which this Tomcat version is using.

- If you are configuring SiteScope to integrate with SiteMinder, modify the redirect port in the
  <!-- Define an AJP 1.3 Connector on port 8009 --> section of the **server.xml** file from:

```
<!--    <Connector port="18009"
URIEncoding="UTF-8" enableLookups="false" redirectPort="8443" protocol="AJ
P/1.3" /> -->
```

to

```
<Connector port="18009"
URIEncoding="UTF-8" enableLookups="false" redirectPort="80" protocol="AJP/
1.3" />
```

- 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.

> **Example of the SiteScope workers 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`

Tomcat log output is written to the **<SiteScope root dir>\logs\tomcat.log** file. Settings for the log file can be configured from the **<SiteScope root dir>\Tomcat\common\classes\log4j.properties** file.

Troubleshooting

Problem: When upgrading from and earlier version of SiteScope, the Tomcat configuration **server.xml** file in the **<SiteScope root directory>\Tomcat\conf** directory is overwritten and any modifications made to that file are removed (for example, changes made when configuring SiteScope to use SSL).

Solution: To restore these modifications, you must reapply them to the **server.xml** file after performing the upgrade.

a. Stop SiteScope.

b. Replace the following files:

| Replace File	With
<SiteScope root directory>\java\lib\security\cacerts	**<SiteScope root directory>\installation\HPSiS1122\backup\java\lib\security\cacerts**
<SiteScope root directory>\java\lib\security\java.security	**<SiteScope root directory>\installation\HPSiS1122\backup\java\lib\security\java.security**
<SiteScope root directory>\java\lib\security\javaws.policy	**<SiteScope root directory>\installation\HPSiS1122\backup\java\lib\security\javaws.policy**
<SiteScope root directory>\java\lib\security\java.policy	**<SiteScope root directory>\installation\HPSiS1122\backup\java\lib\security\java.policy**

c. Manually reapply all hardening and other customization changes by copying them from **<SiteScope root directory>\installation\HPSiS1122\backup\Tomcat\conf\server.xml** to **<SiteScope root directory>\Tomcat\conf\server.xml**.

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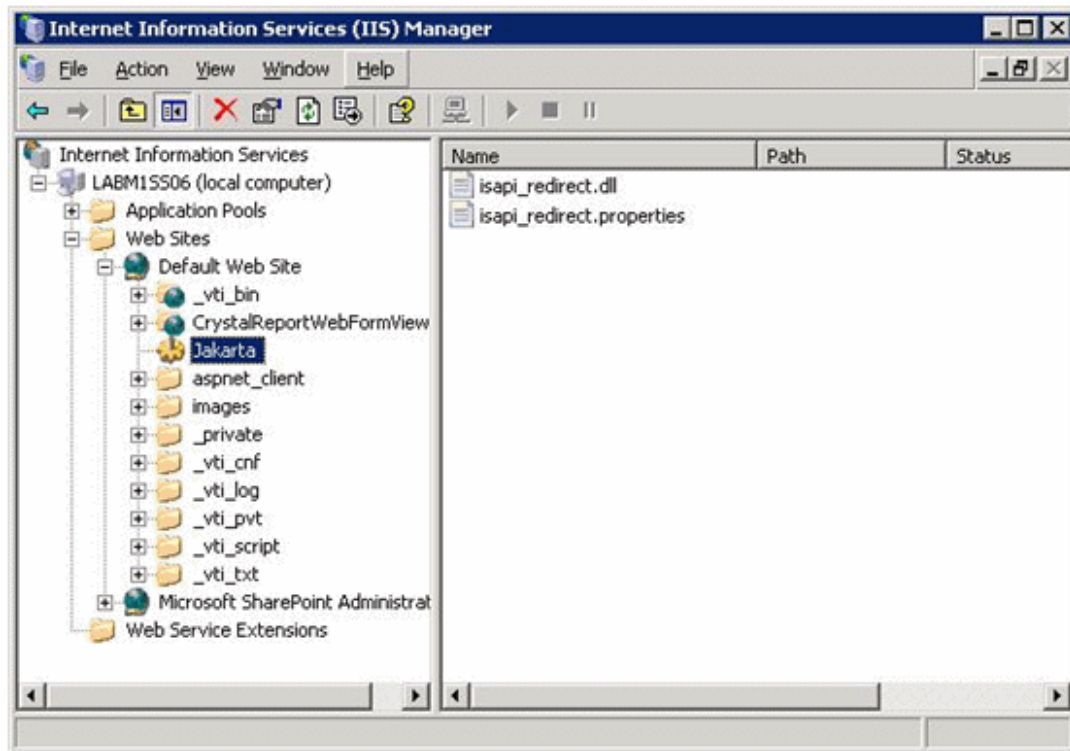
3. Right click **<Your Web Site name>** and click **Properties**.

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.
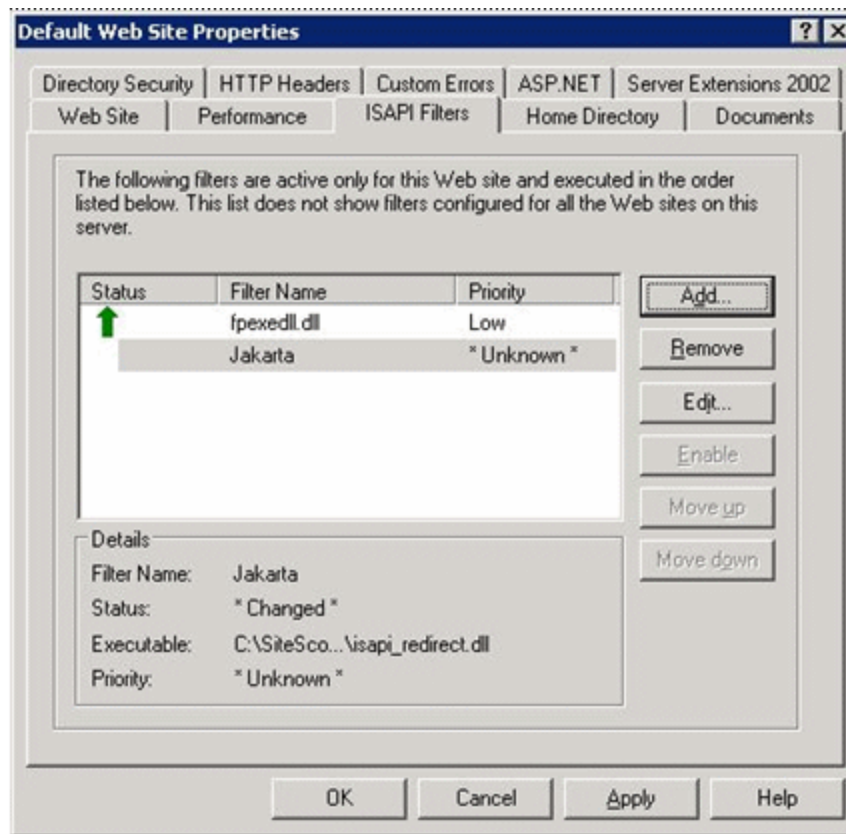
Click **Apply**.

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**.

New Web Service Extension

Type the name of the new Web service extension, and specify the files that must be enabled for the extension to run.

Extension name:

Jakarta

Required files:

C:\SiteScope\Tomcat\bin\win32\isapi_redirect.dll

Add...

Remove

☑ Set extension status to Allowed

OK   Cancel   Help
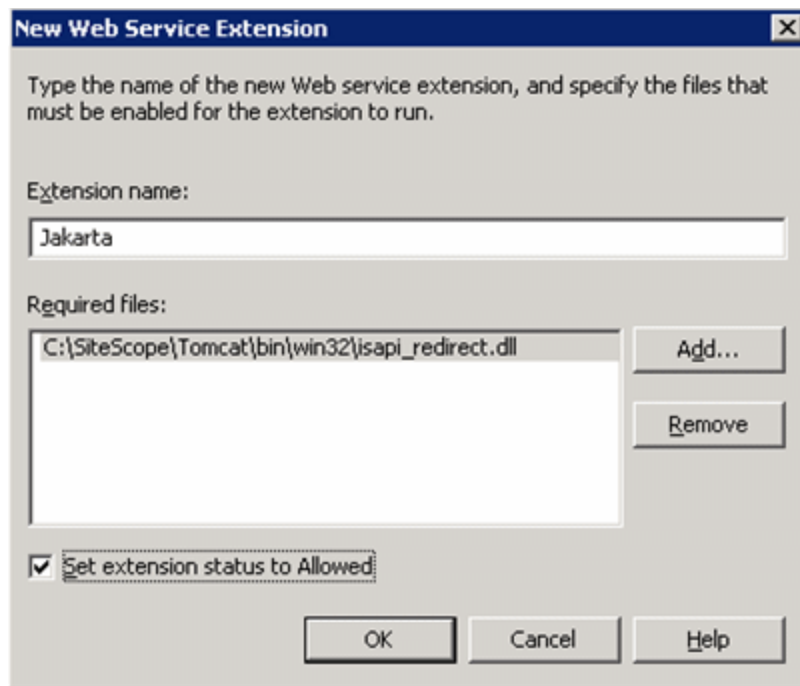
Click **OK**.

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

Appendix 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 section includes:

Understanding Integration with SiteMinder

The following diagram illustrates how SiteScope integrates with SiteMinder to authenticate and authorize SiteScope users.
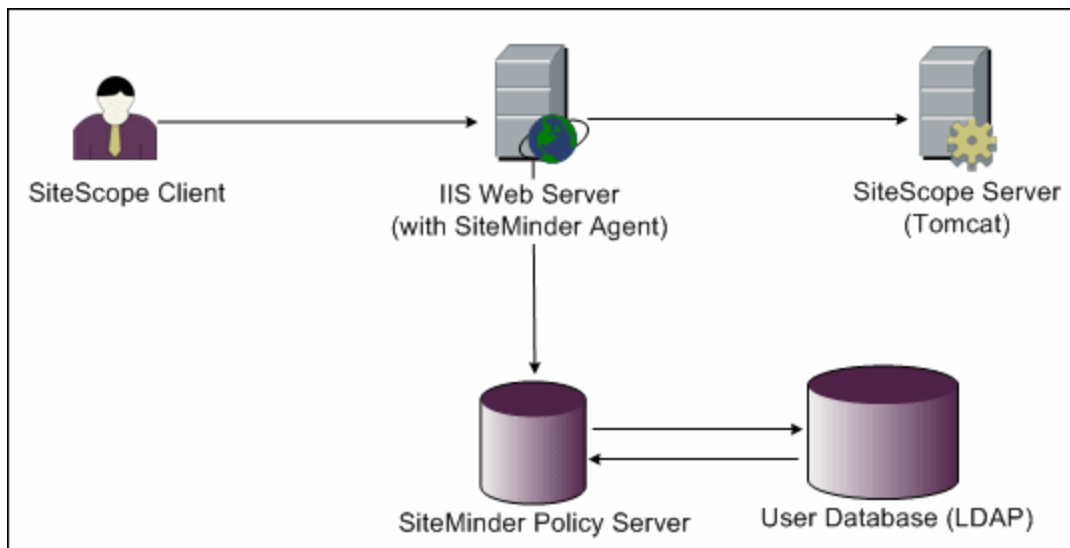
In this architecture, a SiteMinder agent is configured on the IIS Web server which is placed in front of SiteScope's Tomcat application server. The SiteMinder agent must reside on a Web server. The

IIS Web server is connected to the SiteMinder policy server that manages all SiteScope users (over an 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 (using a special HTTP header) that describes the exact user that managed to log on 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 minimum system requirements for integrating SiteScope with SiteMinder.

Operating System	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

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 the next page.

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 200.

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 203.

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 211.

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 on 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 200.

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 203.

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 on. For details on creating user accounts, see the User Management Preferences section in Using SiteScope 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 enable 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 on to SiteScope must not require a password, otherwise SiteMinder is unable to log on. For details on setting up a user account in SiteScope, see the User Management Preferences section in Using SiteScope 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.

- To prevent users from being logged out of SiteScope after 30 minutes of inactivity in the Web browser, change the "`_keepAliveFromJSP=`" property to "`=true`" in the **master.config** file.

Appendix C: Manually Configuring SiteScope for Using a Secure Connection

You can manually configure SiteScope to using a secure connection to restrict access to the SiteScope interface.

We recommend that you use the Hardening Tool to configure SiteScope for using SSL. For details, "Using the Hardening Tool" on page 172.

This section includes:

- "Preparing SiteScope for Using TLS" below

- "Configuring SiteScope for TLS on Tomcat" on page 217

- "Configuring SiteScope for Mutual TLS Configuration" on page 219

- "Configuring SiteScope to Connect to BSM Server With TLS Deployment" on page 220

- "Configuring SiteScope to Connect to a BSM Server That Requires a Client Certificate" on page 221

- "Configuring the Topology Discovery Agent in SiteScope When BSM Server Requires a Client Certificate" on page 224

Preparing SiteScope for Using TLS

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 enables 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.

> **Caution:** 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.

> **Note:**
>
> - SiteScope uses keystores and truststores in JKS format only.
>
> - To prepare the SiteScope Classic interface for use with TLS, you must configure both the Tomcat server (see "Configuring SiteScope for TLS on Tomcat" on page 217) and the classic interface engine (refer to the instructions in "Accessing SiteScope Reports and Classic User Interface Using HTTPS" on page 228).

You can find out more about keytool at the Oracle web site
(http://docs.oracle.com/javase/7/docs/technotes/tools/windows/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 use a certificate from a certificate authority:

1. Obtain the root certificate (and any other intermediate certificate) from a certificate authority.

2. Import the root certificate (and any other intermediate certificate) to **<SiteScope root directory>\java\lib\security\cacerts** from the user interface or by running the following command:

    ```
    keytool -import -alias yourCA -file C:\CAcertificate.cer -keystore
    ..\lib\security\cacerts -storepass changeit
    ```

3. 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.

4. Create a key pair by running the following command line from the **<SiteScope root directory>\java\bin directory**:

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

    > **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.
    >
    > - The `serverKeystore` string used when generating the certificates must be typed in the same case as specified in the documentation, otherwise it will fail when using SiteScope Failover with SSL.

> ▪ The private key password and keystore password must be the same to avoid getting an
>   `IOException: Cannot recover key` error.

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`)

ST = 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.

5. Create a certificate request for this keystore by running the following command from the **<SiteScope root directory>\java\bin** directory:

```
keytool -certreq -alias yourAlias -file ..\..\groups\sis.csr -keystore
..\..\groups\serverKeystore -storepass passphrase
```

This command creates a file named **sis.csr** in the **<SiteScope root directory>\groups** directory. Use this file to request a certificate from your certificate authority.

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**. Use the following steps to import the certificate for use with SiteScope.

6. 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
```

> **Note:** To avoid `keytool error: java.lang.Exception: Failed to establish chain from reply` when importing the certificate from a certificate authority, you should import the root certificate (and any other intermediate certificate) from a certificate authority to **<SiteScope root directory>\java\lib\security\cacerts** using Certificate Management from the user interface or by running the following command:
>
> ```
> keytool -import -alias yourCA -file C:\CAcertificate.cer -keystore
> ..\lib\security\cacerts -storepass changeit
> ```

7. 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 TLS on Tomcat" on the next page.

Using a Self-Signed Certificate

Alternatively, you can generate a self-signed certificate to configure SiteScope using one of the following:

- **SSL Tool.** For details, see "To use the SSL Tool:" below.

- **Manual configuration.** Use the `-selfcert` option to have the Keytool utility generate a self-signed certificate. For details, see "To manually generate a self-signed certificate:" on the next page.

> **Note:** We recommend using the SSL Tool in most cases. However, you should use manual configuration if you are configuring SiteScope to use SSL on a Windows platform and do not have the `%SITESCOPE_HOME%` variable (for example, SiteScope has already been launched from another location using the **go.bat** command) or on a Linux platform if you have SiteScope installed not in **/opt/HP/SiteScope/ directory**.

To use the SSL Tool:

1. Enter the following to stop the SiteScope service:

```
cd /opt/HP/SiteScope/
./stop
```

2. Enter the following to run the SSL Tool:

```
cd /opt/HP/SiteScope/tools/SSL/
```

```
./ssl_tool.sh
```

3. Follow the instructions in the SSL Tool.

To manually generate 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.

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

   > **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.
   >
   > - The `serverKeystore` string used when generating the certificates must be typed in the same case as specified in the documentation, otherwise it will fail when using SiteScope Failover with SSL.

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, ST=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 TLS on Tomcat" below.

5. Optionally, you can export the certificate for use in BSM by running the following command:

   ```
   keytool -exportcert -alias yourAlias -file <SiteScope root
   directory>\certificate_name.cer -keystore ..\..\groups\serverKeystore
   ```

   When prompted, enter your keystore password.

Configuring SiteScope for TLS on Tomcat

To enable TLS 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.

Note:

- If there are other HP products installed on the same server as SiteScope, you might need to change port 8443 to another port to avoid conflict.

- Tomcat log output is written to the **<SiteScope root directory>\logs\tomcat.log** file. Settings for the log file can be configured from the **<SiteScope root directory>\Tomcat\common\classes\log4j.properties** file.

- You can strengthen security on the Tomcat server by disabling weak ciphers. To do so, open **<SiteScope root directory>\Tomcat\conf\server.xml**, and change the existing list to the following:

  <Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
  maxThreads="150" scheme="https" secure="true" clientAuth="false"

```
sslProtocol="TLS" ciphers="SSL_RSA_WITH_RC4_128_SHA, TLS_RSA_WITH_
AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_
DSS_WITH_AES_128_CBC_SHA, SSL_RSA_WITH_3DES_EDE_CBC_SHA,
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA, SSL_DHE_DSS_WITH_3DES_
EDE_CBC_SHA"/>]
```

By default, Tomcat looks for a **.keystore** file in the SiteScope user's home directory.

For more information on enabling TLS for the Tomcat server, see
http://tomcat.apache.org/tomcat-5.5-doc/ssl-howto.html.

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

   `https://<SiteScope_server>:8443/SiteScope` (the link is case sensitive)

Configuring SiteScope for Mutual TLS Configuration

Perform the following steps if the SiteScope server requires a client certificate from the client.

1. SiteScope should be configured with TLS For details, see "Configuring SiteScope for TLS on
   Tomcat" on page 217.

2. Configure the Tomcat server to request a client certificate by locating the following section of
   the **<SiteScope root directory>\Tomcat\conf\server.xml** configuration file:

```
<Connector port="8443"
      maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
      enableLookups="false" disableUploadTimeout="true"
      acceptCount="100" debug="0" scheme="https" secure="true"
      sslProtocol="TLS"
      keystoreFile="..\groups\serverKeystore"
      keystorePass="changeit"
```

and adding the following attributes, and changing `clientAuth="true"`:

```
       truststoreFile="..\java\lib\security\cacerts"
      truststorePass="changeit"
      truststoreType="JKS"
      clientAuth="true"
/>
```

3. Import the root certificate of the certificate authority that issues client certificates to your

organization to the SiteScope truststore (**<SiteScope root directory>\java\lib\security\cacerts**) by running the command:

```
C:\SiteScope\java\>keytool -import -trustcacerts -alias <your alias> -keysto
re ..\lib\security\
    cacerts -file <certificate file>
```

4. Create a client certificate, or use an existing one to import it to the browser.

5. Restart SiteScope, and access it using the following link:

    `https://<server>:8443/SiteScope` (the link is case sensitive)

> **Note:**
>
> Calls to the SiteScope SOAP API also require a certificate. Add the following to your Java code to respond with a client certificate:
>
> `System.setProperty("javax.net.ssl.keyStore",<pathname to client certifica te keystore in JKS format>);`
>
> `System.setProperty("javax.net.ssl.keyStorePassword", <password of client certificate keystore>);`
>
> (Optional) `System.setProperty("javax.net.ssl.trustStore", <pathname to truststore in JKS format>);`
>
> or use the following JVM arguments:
>
> `-Djavax.net.ssl.keyStore=<pathname to client certificate keystore in JKS format>`
>
> `-Djavax.net.ssl.keyStorePassword=<password of client certificate keystor e>`
>
> (Optional) `-Djavax.net.ssl.trustStore=<pathname to truststore in JKS format>`

Configuring SiteScope to Connect to BSM Server With TLS Deployment

To connect SiteScope to a BSM server with an TLS deployment, perform the following:

1. Connect to the SiteScope server.

2. Import the CA root certificate or BSM server certificate into SiteScope using Certificate Management in the SiteScope user interface. For details, see the Certificate Management section in the Using SiteScope Guide in the SiteScope Help.

3. If BSM is configured with a load balancer, import the certificates of Load Balance Core and Center URLs into SiteScope using Certificate Management in the SiteScope user interface. For details, see the Certificate Management section in the Using SiteScope Guide in the SiteScope Help.

4. For details on how to import the certificate into BSM, see the Using SSL with SiteScope section in the BSM Hardening Guide in the BSM Documentation Library.

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

To connect SiteScope to a BSM server that requires a client certificate, perform the following:

1. Connect to the SiteScope server.

2. Import the CA root certificate or BSM server certificate into SiteScope using Certificate Management in the SiteScope user interface. For details, see the Certificate Management section in the Using SiteScope Guide in the SiteScope Help.

3. If you obtained the client certificate in JKS format, copy it to the **<SiteScope root directory>\templates.certificates** folder, and continue from step 11.

> **Note:**
>
> - Make sure that the private key password is at least 6 characters long, and that the private key and keystore passwords are the same.
>
> - In addition, make sure that the above keystore contains the CA certificate that issued it.

If you obtained the client certificate in some other format, perform the steps below.

4. Create a keystore under **<SiteScope root directory>/templates.certificates** by running the following command from the **<SiteScope root directory>\java\bin** directory:

```
keytool -genkey -keyalg RSA -alias sis -keystore
<SiteScope root directory>\templates.certificates\.ks -storepass
<your_keystore_password>
```

> **Example:**
>
> ```
> keytool -genkey -keyalg RSA -alias sis -keystore C:\SiteScope\templates.c
> ertificates\.ks -storepass changeit
> What is your first and last name?
> ```

```
[Unknown]: domain.name
What is the name of your organizational unit?
[Unknown]: dept
What is the name of your organization?
[Unknown]: XYZ Ltd
What is the name of your City or Locality?
[Unknown]:  New York
What is the name of your State or Province?
[Unknown]:  USA
What is the two-letter country code for this unit?
[Unknown]:  US
Is CN=domain.name, OU=dept, O=XYZ Ltd, L=New York, ST=USA, C=US correct?
[no]:  yes


Enter key password for <SiteScope>
```

Press ENTER to use the same password as the keystore password.

5. Create a certificate request for this keystore by running the following command from the **<SiteScope root directory>\java\bin** directory:

```
keytool -certreq -alias sis -file c:\sis.csr -keystore
<SiteScope root directory>\templates.certificates\.ks -storepass
<your_keystore_password>
```

Example:

```
keytool -certreq -alias sis -file c:\sis.csr -keystore
C:\SiteScope\templates.certificates\.ks -storepass changeit
```

6. Have your certificate authority sign the certificate request. Copy/paste the contents of the **.csr** file into your Certificate Authority Web form.

7. Download the signed client certificate in BASE-64 format to **<SiteScope root directory>\templates.certificates\clientcert.cer**.

8. Download the certificate authority certificate in BASE-64 format to c:\.

9. Import the certificate authority certificate into the JKS keystore by running the following command:

```
keytool -import -alias ca -file c:\ca.cer -keystore
<SiteScope root directory>\templates.certificates\.ks -storepass
<your_keystore_password>
```

Example:

```
keytool -import -alias ca -file c:\ca.cer -keystore C:\SiteScope\template
s.certificates\.ks -storepass changeit
Owner: CN=dept-CA, DC=domain.name
Issuer: CN=dept-CA, DC=domain.name
Serial number: 2c2721eb293d60b4424fe82e37794d2c
Valid from: Tue Jun 17 11:49:31 IDT 2008 until: Mon Jun 17 11:57:06 IDT 2
013
Certificate fingerprints:
MD5:   14:59:8F:47:00:E8:10:93:23:1C:C6:22:6F:A6:6C:5B
SHA1: 17:2F:4E:76:83:5F:03:BB:A4:B9:96:D4:80:E3:08:94:8C:D5:4A:D5
Trust this certificate? [no]:  yes
Certificate was added to keystore
```

10. Import the client certificate into the keystore by running the following command:

```
keytool -import -alias sis -file
<SiteScope root directory>\templates.certificates\certnew.cer -keystore
<SiteScope root directory>\templates.certificates\.ks -storepass
<your_keystore_password>
```

Example:

```
keytool -import -alias sis -fil
c:\SiteScope\templates.certificates\certnew.cer -keystore
C:\SiteScope\templates.certificates\.ks -storepass changeit
```

The certificate reply is installed in the keystore **<SiteScope root directory>\java\bin**
directory.

11. Check the keystore contents by running the following command from the **<SiteScope root
directory>\java\bin** directory, and enter the keystore password:

```
keytool -list -keystore <SiteScope root directory>\templates.certificates\.ks
```

Example:

```
keytool -list -keystore C:\SiteScope\templates.certificates\.ks
Enter keystore password:  changeit

Keystore type: jks
Keystore provider: SUN
```

```
Your keystore contains 2 entries
ca, Mar 8, 2009, trustedCertEntry,
Certificate fingerprint (MD5): 14:59:8F:47:00:E8:10:93:23:1C:C6:22:6F:A6:
6C:5B
sis, Mar 8, 2009, keyEntry,
Certificate fingerprint (MD5): C7:70:8B:3C:2D:A9:48:EB:24:8A:46:77:B0:A3:
42:E1


C:\SiteScope\java\bin>
```

12. To use this keystore for client certificate, add the following lines to the **<SiteScope root directory>\groups\master.config** file:

    _urlClientCert=<keystoreName>

    _urlClientCertPassword=<keystorePassword>

    > **Example:**
    >
    > _urlClientCert=.ks
    > _urlClientCertPassword=changeit

13. Save the changes to the file.

14. In **SiteScope Preferences > Integration Preferences > BSM Preferences Available Operations**, click **Reset** to delete all BSM related settings from the SiteScope server and all SiteScope configurations from BSM.

15. Restart the SiteScope server.

16. In BSM, select **Admin > System Availability Management Administration**, and click the **New SiteScope** button to add the SiteScope instance.

    > **Note:** If the connection between SiteScope and BSM fails, check the **<SiteScope root directory>\log\bac_integration.log** for errors.

Configuring the Topology Discovery Agent in SiteScope When BSM Server Requires a Client Certificate

After configuring SiteScope to connect to the BSM Gateway server using a client certificate (see "Configuring SiteScope to Connect to a BSM Server That Requires a Client Certificate" on page 221), you need to perform the following steps for discovery to report topology to the BSM server.

1. Create a folder named **security** in **<SiteScope root directory>\WEB-INF\classes** (if it does not exist).

2. Move **MAMTrustStoreExp.jks** and **ssl.properties** from **<SiteScope root directory>\WEB-INF\classes** to the **<SiteScope root directory>\WEB-INF\classes\security** folder.

3. Import the CA root certificate (or BSM server certificate) into the discovery trust store (**MAMTrustStoreExp.jks**) with password (the default password for the discovery trust store is **logomania**, which encrypted, is: [22,-8,116,-119,-107,64,49,93,-69,57,-13,-123,-32,-114,-88,-61]):

```
keytool -import -alias <your_CA> -keystore <SiteScope root directory>\WEB-INF\classes\security\MAMTrustStoreExp.jks -storepass <your_keystore_password>
```

> **Example:**
>
> ```
> keytool -import -alias AMQA_CA -file c:\ca.cer -keystore
> C:\SiteScope\WEB-INF\classes\security\MAMTrustStoreExp.jks -storepass
> logomania
> ```

> **Note:** The private key password must be at least 6 characters, and the password for the private key and password for the keystore must be the same.

4. Check the contents of TrustStore using the following command:

```
<SiteScope root directory>\java\bin>keytool -list -keystore <SiteScope root directory>\WEB-INF\classes\security\MAMTrustStoreExp.jks -storepass <your_keystore_password>
Keystore type: <Keystore_type>
Keystore provider: <Keystore_provider>
Your keystore contains 2 entries mam, Nov 4, 2004,
trustedCertEntry,Certificate fingerprint (MD5):
<Certificate_fingerprint> amqa_ca, Dec 30, 2010, trustedCertEntry,Certificate
fingerprint (MD5):
<Certificate_fingerprint>
```

> **Example:**
>
> ```
> C:\SiteScope\java\bin>keytool -list -keystore C:\SiteScope\WEB-INF\classes\security\MAMTrustStoreExp.jks -storepass logomania
>
> Keystore type: JKS
> Keystore provider: SUN
>
> Your keystore contains 2 entries
> ```

```
mam, Nov 4, 2004,trustedCertEntry,
Certificate fingerprint (MD5):
C6:78:0F:58:32:04:DF:87:5C:8C:60:BC:58:75:6E:F7
amqa_ca, Dec 30, 2010, trustedCertEntry,
Certificate fingerprint (MD5):
5D:47:4B:52:14:66:9A:6A:0A:90:8F:6D:7A:94:76:AB
```

5. Copy the SiteScope client keyStore (.ks) from **<SiteScope root directory>\templates.certificates** to **<SiteScope root directory>SiteScope\WEB-INF\classes\security**.

6. In the **ssl.properties** file, update the **javax.net.ssl.keyStore** property to the keyStore name. For example, `javax.net.ssl.keyStore=.ks`.

7. Change the SiteScope client keyStore password to match the Discovery password for keystore (default is `logomania`).

```
keytool -storepasswd -new <Discovery_keystore_password> -keystore
<SiteScope root directory>\WEB-INF\classes\security\.ks -storepass
<your_keystore_password>
```

Example:

```
keytool -storepasswd -new logomania -keystore C:\SiteScope\WEB-INF\classe
s\security\.ks -storepass changeit
```

8. Change private key password to match Discovery password for keystore:

```
keytool -keypasswd -alias sis -keypass <your_keystore_password> -new
<Discovery_keystore_password> -keystore <SiteScope root directory>\WEB-
INF\classes\security\.ks -storepass <your_keystore_password>
```

Example:

```
keytool -keypasswd -alias sis -keypass changeit -new logomania -keystore
C:\SiteScope\WEB-INF\classes\security\.ks -storepass logomania
```

9. Verify keystore using new password:

```
keytool -list -v -keystore <SiteScope root directory>\WEB-
INF\classes\security\.ks -storepass <your_keystore_password>
```

Example:

```
keytool -list -v -keystore C:\SiteScope\WEB-INF\classes\security\.ks -
storepass logomania
```

10. Restart the SiteScope server.

11. In BSM, select **Admin > System Availability Management Administration**, and click the **New SiteScope** button to add the SiteScope instance. In the Profile Settings pane, make sure to select the **BSM Front End Use HTTPS** check box.

12. Check the topology appears in **BSM > Admin > RTSM Administration > IT Universe Manager > System Monitors** view.

Troubleshooting

- Check the **bac-integration.log** located in **<SiteScope root directory>\logs\bac_integration** for the following errors:

```
2010-12-30 11:03:06,399 [TopologyReporterSender] (TopologyReporterSender.j
ava:364)
 ERROR - failed to run main topology agent. topologyCommand=TopologyComman
d
{commandType=RUN_SCRIPT, …
java.lang.IllegalArgumentException: cannot find script with name=create_mo
nitor.py
at com.mercury.sitescope.integrations.bac.topology.dependencies.Dependenci
esCrawler.
findDependencies(DependenciesCrawler.java:60)
at com.mercury.sitescope.integrations.bac.topology.dependencies.
ScriptDependenciesFinder.find(ScriptDependenciesFinder.java:80)
at com.mercury.sitescope.integrations.bac.topology.TopologyReporterSender.
getDependencies(TopologyReporterSender.java:552)
at com.mercury.sitescope.integrations.bac.topology.TopologyReporterSender.
send(TopologyReporterSender.java:347)
at com.mercury.sitescope.integrations.bac.topology.TopologyReporterSender.
run(TopologyReporterSender.java:304)
at java.lang.Thread.run(Thread.java:619)
```

- Verify that the certificate and Keystore passwords are identical.

Appendix D: Accessing SiteScope Reports and Classic User Interface Using HTTPS

You can setup the SiteScope web server to use an SSL connection with access via the https protocol. The steps you need to take to do this are described in this section.

This section describes:

- "About Working with Certificates in SiteScope" below

- "Using a Certificate from a Certificate Authority" below

- "Using a Self-Signed Certificate" on page 231

About Working with Certificates in SiteScope

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 the parties they communicate with. This is installed in **<SiteScope install path>\SiteScope\java\bin** directory.

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

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

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

Using a Certificate from a Certificate Authority

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

To use a certificate from a Certificate Authority:

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

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

2. Next, you must create a key pair. To do this, you need to run the command line listed below from the **<SiteScope root>\java\bin** directory.

> **Note:** Values in italics are variables that you fill in with information specific to your organization.
>
> 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=yourComp
anyName, L=yourLocation, S=yourState, C=yourCountryCode" -alias yourAlias -k
eypass keypass -keystore ..\..\groups\serverKeystore -storepass passphrase -
keyalg "RSA" -validity valdays
```

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

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 will 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.

3. Create a certificate request file. To do this, run the following command also from the **<SiteScope root>\java\bin** directory:

```
keytool -certreq -alias yourAlias -file ..\..\groups\filename.csr -keypass k
eypass -keystore ..\..\groups\serverKeystore -storepass passphrase -keyalg "
RSA"
```

This command will generate a .csr to be used as a request file. You need to send this file to a Certificate Authority (CA) along with your request for a certificate. After you receive your certificate from a Certificate Authority (the reply should include a file called **cert.cer**), you need to import this certificate into the KeyStore file you created in the steps above. The file should be called **serverKeystore**. Use the following steps to import the certificate.

4. To import the certificate data into the KeyStore file, run the following command also from the **SiteScope\java\bin** directory:

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

5. To change SiteScope to use a secured connection, you need to add or modify the following parameters in the **<SiteScope root>\groups\master.config** file:

```
_httpSecurePort=8899
```

The number you use for the **_httpSecurePort** parameter can be set to any available port number. It is recommended that you use a port number other than 8888, which is the default port for the accessing SiteScope using HTTP (unsecured).

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

_httpPort=

_httpSecurePort=8899

_httpSecureKeyPassword=passphrase

_httpSecureKeystorePassword=keypass

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

6. Save the changes to the **master.config** file.

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

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

```
http://server_IP_address:8888
```

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

```
https://server_IP_address:8899
```

Using a Self-Signed Certificate

Alternatively, you also can generate a self signed certificate. To do this, you use the -selfcert option to have the Keytool utility generate a self-signed certificate.

To use a self-signed certificate:

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

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

2. Next, run the following command from the **<SiteScope root>\java\bin** directory.

   > **Note:** Values in italics are variables that you fill in with information specific to your organization
   >
   > 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=yourComp
   anyName, L=yourLocation, S=yourState, C=yourCountryCode" -alias yourAlias -k
   eypass keypass -keystore ..\..\groups\serverKeystore -storepass passphrase -
   keyalg "RSA" -validity valdays
   ```

3. Next run the following command, also from the **SiteScope\java\bin** directory:

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

4. To change SiteScope to use a secured connection, you need to add or modify the following parameters in the **<SiteScope root>\groups\master.config** file:

   ```
   _httpSecurePort=8899
   ```

   The number you use for the **_httpSecurePort** parameter can be set to any available port number. It is recommended that you use a port number other than 8888, which is the default port for the accessing SiteScope using HTTP (unsecured).

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

_httpPort=

_httpSecurePort=8899

_httpSecureKeyPassword=passphrase

_httpSecureKeystorePassword=keypass

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

5. Save the changes to the **master.config** file.

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

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

`http://server_IP_address:8888`

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

`https://server_IP_address:8899`

We appreciate your feedback!

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Deployment Guide (SiteScope 11.23)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to SW-doc@hp.com.