HPE SiteScope

Software Version: 11.40

Deployment Guide

Go to **HELP CENTER ONLINE**
http://sitescope-help.saas.hpe.com

Hewlett Packard
Enterprise

Document Release Date: August 2017 | Software Release Date: August 2017

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise Development LP 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. HPE 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 HPE 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

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: https://softwaresupport.hpe.com.

This site requires that you register for an HPE Passport and sign in. To register for an HPE Passport ID, go to https://softwaresupport.hpe.com and click **Register**.

Support

Visit the HPE Software Support Online web site at: https://softwaresupport.hpe.com

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

HPE 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 HPE 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 HPE Passport user and sign in. Many also require a support contract. To register for an HPE Passport ID, go to: https://softwaresupport.hpe.com and click **Register**.

To find more information about access levels, go to: https://softwaresupport.hpe.com/web/softwaresupport/access-levels.

HPE Software Solutions & Integrations and Best Practices

Visit **HPE Software Solutions Now** at https://softwaresupport.hpe.com/km/KM01702710 to explore how the products in the HPE Software catalog work together, exchange information, and solve business needs.

Visit **Hewlett Packard Enterprise Self-Solve Knowledge Search** at https://softwaresupport.hpe.com/group/softwaresupport to access a wide variety of best practice documents and materials.

Contents

Part 1: Plan your Deployment

Chapter 1: Deployment Methodology

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 HPE 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 20 or "Sizing SiteScope on Linux Platforms" on page 22 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 Linux Environments

SiteScope must be installed on a 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 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`
7. Update the **/etc/init.d/sitescope** file with the command to run as a non-root user. For example, add “`su sitescope –c`” in front of the `start/stop` command.

Chapter 2: 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, HPE 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. APM, BMC, HPE 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 the 64-bit monitors and solution templates listed in "Supported Monitors and Solution Templates" on page 19.

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 85.
2. Open the SiteScope Capacity Calculator which is available from:
   - The SiteScope installation folder: **<SiteScope root directory>\tools\SiteScopeCapacityCalculator.xls**
   - The HPE Software Support site.
3. Select the **Monitor Usage** tab according to the operating system on which SiteScope is installed.
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 APM, 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:

- 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)

Note: The SiteScope 32-bit monitors are deprecated and will not work after performing an upgrade to SiteScope 11.40. For more details, see "Migrate from 32-Bit to 64-Bit SiteScope" on page 177.

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 HPE 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 4096 MB, desktop heap size to 8192 KB, and the number of file handles to 18,000. It also disables pop-up warnings for SiteScope executables. For details, see "Run the Configuration Tool on Windows Platforms" on page 186.

   > **Note:** The Configuration Tool supports the default SiteScope service name only. If you changed the service name, contact HPE 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 HPE 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 Linux Platforms

Sizing SiteScope on 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 Linux operating system parameters. For details, see the procedure "Tuning the Operating System" below.

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 24.

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 25.

Tuning the Operating System

Tuning the operating system involves configuring the appropriate number of monitors for the SiteScope instance and configuring the 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 Linux Operating System Parameters

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

To configure the 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:**
      >
      > - Since this path can vary on different Linux platforms, you should add the corresponding path according to your Linux platform.
      > - `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

Parameter	Minimum Value
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 4096 MB (this is the recommended heap size for large loads) by modifying **start-service** and **start-monitor** scripts in **<SiteScope root directory>\bin** directory.

   We recommend setting the minimum heap size to equal maximal heap in order to enhance performance on SiteScope startup. For example, change `-Xmx4096m –Xms512m` to `-Xmx4096m –Xms4096m`.

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 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 HPE 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:

   Error if >= 7.9 GB

   Warning if >= 7.8GB

   (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 "Run the Configuration Tool on Windows Platforms" on page 186.
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 3: 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.
Web Process and Content	Monitors availability of key URLs, the function of key Web-based processes, and monitors key text content.

Monitor Type	Description
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 the next page

SiteScope Monitoring Methods

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

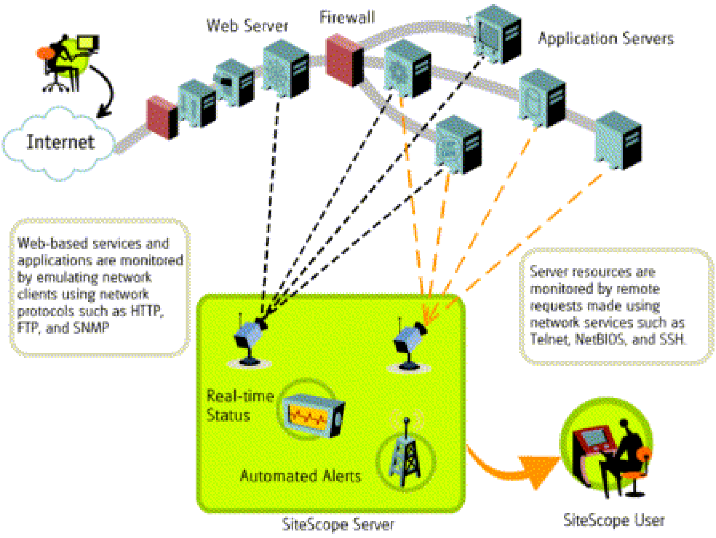
- **Standards-based network protocols.**

  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.

  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.


Web Server
Firewall
Application Servers
Internet
Web-based services and applications are monitored by emulating network clients using network protocols such as HTTP, FTP, and SNMP
Server resources are monitored by remote requests made using network services such as Telnet, NetBIOS, and SSH.
Real-time Status
Automated Alerts
SiteScope Server
SiteScope User

SiteScope Server monitors (for example, CPU, Disk Space, Memory, Service) can be used to monitor server resources on the following platforms: Windows, AIX, CentOS, FreeBSD, HP iLO, HP-UX, HP/UX, HP/UX64-bit, Linux, MacOSX, NonStopOS, OPENSERVER, Red Hat Enterprise Linux, SCO, SGI Irix, Solaris Zones, Sun Fire X64 ILOM, Sun Solaris, SunOS, Tru64 5.x,Tru64 Pre 4.x (Digital), and Ubuntu Linux.

> **Note:** An SSH connection is required to monitor server resources (for example, CPU utilization, memory) on Windows machines from a SiteScope running on 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 Monitor Reference Guide in the SiteScope Help.

Chapter 4: SiteScope Licenses

SiteScope licensing controls the number of monitors that can be created simultaneously and the types of monitors that can be used. Since SiteScope licensing is based on the monitoring requirements it 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 HPE products and are eligible for free updates and upgrades. You are also given access to the HPE Software Support web site. You can use this access to search for technical information in the HPE Software Self-solve knowledge base as well as downloading updates to the SiteScope documentation.

This chapter includes:

Capacity-based (OSi) License Model

SiteScope licensing controls the number of monitors that can be created simultaneously and the types of monitors that can be used. The number of SiteScope monitors that you can create is based on two factors:

- The monitoring capacity you have purchased for the specific license capacity types (OS Instance, URL, Transaction).
- Types of SiteScope monitors you want to use.

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 HPE products and are eligible for free updates and upgrades.

You are also given access to the HPE Software Support site. You can use this access to search for technical information in the Self-Solve Knowledge Search as well as downloading updates to the SiteScope documentation.

Licensing Model for Monitors

The licensing entitlement model used by SiteScope changed from a point-based model to a capacity-type model that is based on the types of objects SiteScope is monitoring. There are three types of monitored objects: Operating System instances (OSi), Transactions for monitors that run VuGen scripts, and URLs.

The license capacity types that are available are dependent on the installation type and on the SiteScope edition you choose. This means that you can flexibly scale a SiteScope deployment to meet the needs of your organization and the requirements of your infrastructure.

For details of the licensing mechanism, see:

- "Instant-On License" below
- "License Edition " on the next page
- "License Capacity Type" on page 34

Licensing Model for Solution Templates

Solution templates no longer require a separate license for each solution. Instead, all solution templates are automatically available with the Premium, Ultimate, and System Collector edition license. License consumption for a solution template is calculated according to the monitors deployed from the solution template.

Instant-On License

To use SiteScope, you must have a valid license. A license is automatically activated (instantly-on) according to the setup type you selected.

- **HPE SiteScope.** The *Community* edition license is instantly available upon a regular SiteScope installation. This free edition, provides limited SiteScope functionality for an unlimited period of time. You can upgrade your SiteScope edition at any time to expand the monitoring capacity of your initial deployment and to enjoy all the features offered by SiteScope. For the list of SiteScope editions that are available, see "License Edition " on the next page.
- **HPE SiteScope for Load Testing.** The *Load Testing* edition license is instantly available upon HPE SiteScope for Load Testing installation. This setup type is used with an LoadRunner or Performance Center installation only.

> **Note:** For a SiteScope Failover installation, the *Failover* edition license is provided with the Premium, Ultimate, and System Collector editions at no additional cost. After installing SiteScope Failover, you need to import the Failover license file.

License Edition

You can upgrade your initial SiteScope deployment by selecting the SiteScope edition and capacity model (see "License Capacity Type" on the next page) according to the type of environment you want to monitor.

You can select from the following editions:

License Edition	Description
Trial Edition	SiteScope provides a free, one-time trial license that gives you full SiteScope functionality during a 30-day period. For details, see "Trial Edition" on page 44.
Premium/Ultimate Edition	Provides full SiteScope functionality, including integrations, SiteScope APIs, SiteScope Failover, and the use of enterprise monitors and templates. Premium and Ultimate editions have the same functionality, and differ only in the integrations with which they are bundled. For details, contact your HPE sales representative. For more details, see "Premium/Ultimate Edition" on page 46.
System Collector	A version of SiteScope provided with Operations Manager Integration that enables SiteScope monitors to be used on OM applications. For details, see "System Collector Edition" on page 48.
Load Testing	A version of SiteScope provided with LoadRunner and Performance Center that enables users to define and use SiteScope monitors on a LoadRunner or Performance Center application. For details, see "Load Testing Edition" on page 50.

For a comparison of the features available in each edition, see "Feature Comparison Table" on page 39.

For license purchase inquiries (or if you require additional capacity), contact your HPE sales representative or use the “Contact Us” link in the HPE SiteScope Product page. If you own a license and require a license key file, use the HPE Licensing for Software Portal.

License Capacity Type

The table below contains an explanation of the different capacity types, the rules used to calculate license usage, and the monitors supported by each license capacity type:

Capacity Type	**Description**
OSi License	**Monitors Supported:** All monitors except URL, URL Content, URL List, URL Sequence, Web Script, Web Service, Link Check, XML Metrics, and free monitors (Composite, Formula Composite, Amazon Web Services, e-Business Transaction, and Integration monitors).
	License Consumption: Generally, one OSi license instance is consumed for every monitored remote server, regardless of the number of monitors configured for that remote server. 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 is deducted from the license. **Exceptions:** • Custom monitor, SNMP Trap, and Microsoft Windows Dial-Up consume one OS instance per 15 monitors. • Dynamic Docker monitor consumes one OS instance license per monitored cluster and one for each monitored node. • HPE Vertica JDBC monitor consumes one OS instance per monitored server and one OS instance per monitored node. • Solaris Zones monitor consumes one OS instance per monitored server property and one OS instance per monitored zone. • VMware Datastore monitor consumes one OS instance per datastore. • VMware Host monitors consume one OS instance license per monitored host and one OS instance license for each monitored virtual machine. Note that VMware best practices recommend that you set the object name (in vSphere) of a VM guest to be the same as the server name (or machine name) of the guest itself. Where you set the names this way, SiteScope uses only one OS Instance for all monitors of the same server. Where the vSphere object name is different from the guest server name, SiteScope uses one OS instance for all VMware monitors with the guest server name, and one OS instance for all monitors with the vSphere object name. **Note:** OS instances are not aggregated between different editions because the cost of an OS instance license differs for each edition type. However, OS instances are aggregated between OS licenses of the same edition (for example if you have multiple Premium edition licenses each containing OS instances).

Capacity Type	Description
URL License	**Monitors Supported:** URL, URL Content, URL List, URL Sequence, Web Service, Link Check, XML Metrics. **License Consumption:** • Each monitored URL or URL step consumes one URL license instance. • URL licenses are aggregated between editions, except Community, Trial, and Load Testing edition which have their own URL license.
Transaction License	**Monitors Supported:** Web Script monitors that use VuGen script transactions. **License Consumption:** • One transaction license instance is consumed per VuGen script transaction. Note that the "/Total/Status" counter also consumes one transaction license instance when it is selected in the Web Script monitor. • Transaction licenses are aggregated between edition, except for Community and Load Testing editions which do not support monitoring transactions.

Importing and Upgrading Your License

When you install SiteScope, it includes a free Community edition license.

To extend SiteScope beyond the features included in the Community edition, you must purchase the SiteScope edition with the capacity types (OSi, URL, and Transaction) you require, and then import the license file key into SiteScope.

You can import a SiteScope license:

- During installation using the SiteScope Configuration Wizard, or
- Post-installation using the General Preferences page (see "Importing SiteScope Licenses" on page 78), an API, or the SiteScope Configuration Tool (see Using the SiteScope Configuration Tool).

When you import an edition license that is higher in the hierarchy, it upgrades the functionality of the active edition according to the edition of the imported license. For details on upgrading a license, see Upgrading the SiteScope Edition License.

You can also increase license capacity for the Premium, Ultimate, and System Collector editions. For details, see Increasing the License Capacity.

License Expiration

Edition License Expiration

For time-based licenses, SiteScope send a warning message to users 7 days before the license is due to expire.

If an edition license expires, the license is automatic downgraded to the previous valid license in the edition hierarchy (see "Upgrading the SiteScope License Edition"). Otherwise, the Community edition becomes active. This is also the case where a user removes a license.

SiteScope functionality is immediately reduced according to the features that are available within the active edition definition.

> **Note:** A user cannot remove the Community or Load Testing edition license from the Installed Licenses table in **Preferences > General Preferences > Licenses**.

Capacity License Expires

When the capacity of an OSi, URL, or Transaction license is exceeded, SiteScope:

1. Opens a dialog box displaying a warning message.
2. Sends a message to the user that the license capacity has been exceeded. SiteScope sends a daily notification for a period of up to 7 days.

If the user has not removed the extra monitors or increased the license capacity within this time, SiteScope suspends all monitors—even for monitor types for which the capacity was not exceeded. While monitors are suspended, you are still able to remove monitors from SiteScope.

Downgrade to Community License

When a commercial license expires and no other commercial edition exists or is valid, the Community edition license automatically becomes the activate license. Any functionality not supported in the Community edition is immediately disabled.

The table below shows how a license downgrade impacts functionality:

Feature	Description
Monitors	If the Community edition license capacity is exceeded, all monitors are suspended, and a message is displayed in the user interface. Any created monitors not allowed in Community edition stop running and are disabled (for example, enterprise monitors and Amazon Web Services monitor).

Feature	Description
User accounts	Users lose the ability to log in with other user accounts (regular or LDAP) or to edit other user accounts. This does not apply to the SiteScope Administrator account.
Data retention	While all daily logs will be kept on the file system, users can see report and analytics data for the last 30 days only.
Alerts	Alert actions not allowed in Community edition are stopped and disabled (only Email and Event Console alert actions are allowed).
Reports	Scheduled reports are not sent, and only Quick Reports can be activated from the user interface.
APIs	All public and private SiteScope APIs are blocked.
Integrations	All integrations are stopped and disabled.
SiteScope Failover	SiteScope Failover gets an error message and stops synchronizing data from the primary SiteScope.

Licensing Notes and Limitations

Community Edition

The Community edition will not be released with every SiteScope minor or minor-minor version release. For details on version types, see "Installation Version Types" in the Deployment Guide.

SiteScope integrated with APM

- If SiteScope is configured to send data to APM and the SiteScope license expires, SiteScope stops sending all data (including topology) to APM. When you renew the SiteScope license, you must clear the **Disable all logging to Application Performance Management** check box in **Preferences > Integration Preferences > APM Integration > APM Integration Main Settings** to enable logging and data flow to APM, since SiteScope automatically disables logging to APM on license expiration.
- If you delete a monitor from SiteScope after your SiteScope Premium, Ultimate, or System Collector edition license expires (and therefore, the integration with APM is disabled), the monitor is not removed from APM. You need to manually remove the monitor from the **SiteScope Topology Upgrade Compliancy** view in APM in **RTSM Administration > IT Universe Manager**.

SiteScope Editions Overview

SiteScope is available in various editions which provide different functionalities.

SiteScope is installed with a built-in **Community** edition license which provides limited SiteScope functionality at no cost, for an unlimited period of time. In addition, there is free, one-time **Trial** edition which provides full functionality of SiteScope during a 30-day period.

> **Note:** The SiteScope (Community Edition) image is also available on the Docker Hub. For details, see "SiteScope Image on the Docker Hub" below.

You can extend SiteScope beyond the features included in the Community edition, by upgrading to one of the various commercial editions: **Premium**, **Ultimate**, or **System Collector**. There is also a free **Load Testing** edition that is instantly available upon installing SiteScope for Load Testing. The Community, Premium, and Ultimate editions are available to any user, whereas the System Collector and Load Testing editions are provided with Operations Manager Integration and LoadRunner/Performance Center respectively.

You can add SiteScope functionality and capacity by importing additional licenses. This provides an efficient and flexible way to scale SiteScope to meet the needs of your organization and the requirements of your infrastructure. For details on purchasing a license or additional license capacity, contact your HPE sales representative or use the “Contact Us” link in the HPE SiteScope Product page.

For more information about licensing, see "Capacity-based (OSi) License Model" on page 31.

SiteScope Image on the Docker Hub

The SiteScope (Community Edition) version image is also available on the Docker Hub. Docker Hub repositories let you share images with co-workers, customers, or the Docker community at large.

You can access the SiteScope image from https://hub.docker.com/r/hpsoftware/sitescope/.

To install the image:

Run this image using the following command:

```
docker run -d -p 8080:8080 -p 8888:8888 --name <<containerName>>
hpsoftware/sitescope:<<version>>
```

Where `containerName` is the name to be assigned to the running SiteScope container and `version` is the version of SiteScope, for example 11.40.

To access SiteScope:

Enter the SiteScope address in a Web browser to access SiteScope. The default address is as follows:

```
http://<<HOST_NAME>>:8080/SiteScope
```

Where `HOST_NAME` is the host name or IP address of the machine running the SiteScope docker container. SiteScope opens to the Dashboard view.

Feature Comparison Table

The table below shows the features that are available in the various SiteScope editions.

Feature	**SiteScope Editions**			**Available with HPE Products Only**	
	Community	**Trial**	**Premium/ Ultimate**	**System Collector**	**Load Testing**
License Duration	Instant-on (perpetual)	30 days	Term or perpetual	Term or perpetual	Instant-on (perpetual)
License Entitlement Model	25 OSIs 25 URLs (Fixed capacity)	25 OSIs 25 URLs 10 Transactions (Fixed capacity)	OSIs, URLs, Transactions (Quantity determined by user)	OSIs (Quantity determined by user)	25 OSIs 25 URLs (Fixed capacity)
Node Locked[1]	x	x	✓	✓	x
Support Model	SiteScope communities	Web/Phone	Web/Phone	Web/Phone	Email
User Accounts	1	Unlimited	Unlimited	Unlimited	Unlimited
Data Retention	30 days [2]	30 days [2]	Unlimited	Unlimited	Unlimited
Alerts	Email, Event Console only	✓	✓	✓	✓
Reporting	Quick Reports only	✓	✓	✓	✓
Multi-View, Event Console	✓	✓	✓	✓	✓
Analytics	✓	✓	✓	✓	✓
Monitor Types	All monitors except those listed in "Monitors Not Included in Community Edition" on page 41.	All monitors	All monitors	All monitors	All monitors except Web Script and Integration monitors

Feature	SiteScope Editions			Available with HPE Products Only	
	Community	**Trial**	**Premium/ Ultimate**	**System Collector**	**Load Testing**
Solution Templates	Apache Cassandra, Apache Tomcat, Hadoop Cluster Monitoring, MS Exchange 2010, MS Exchange Server 2013, MS Lync Server 2010, MS SharePoint 2010, VMware Capacity Management	All solution templates	All solution templates	All solution templates	HPE Quality Center, HPE QuickTest Professional, HPE Service Manager, HPE Vertica, Operating System Host (AIX, Linux, Microsoft Windows, Solaris)
User-Defined Templates	✔ Except for deploying via CSV or XML file	✔	✔	✔	✔
APIs	x	✔	✔	✔	✔
Integrations	x	✔	✔	✔	Generic Data Integration
High Availability (Failover)	x	x	✔	✔	x
Updates and Patches	x	x (Possible to update via patches)	✔	✔	✔
Supported Platforms (Installation)	Various Windows and Linux 64-bit platforms (see for the list of supported versions).				Windows platforms only
Multi-Lingual UI Support	10 Languages (see the list of supported languages in the Internationalization section of the Using SiteScope Guide).				

[1] Some license editions are node locked to avoid license abuse. This means that the license is valid on a specific machine only.

[2] Configuring the number of daily logs in the log preferences will not have any effect on the number of daily logs retained.

Monitors Not Included in Community Edition

- Active Directory Replication monitor
- Azure monitor
- Amazon Web Services monitor
- COM+ Server monitor
- HPE Vertica JDBC monitor
- Integration monitors - HPE Service Manager, NetScout Event, Technology Database Integration, Technology Log File Integration, Technology SNMP Trap Integration, Technology Web Service Integration
- Microsoft Azure monitor
- Microsoft Exchange monitors - Microsoft Exchange 2007 Message Traffic, Microsoft Exchange, Microsoft Exchange Base (Deprecated monitors: Microsoft Exchange 5.5/2000/2003 Message Traffic, Microsoft Exchange 2003 Mailbox, Microsoft Exchange 2003 Public Folder)
- Microsoft Lync monitors - Archiving Server, A/V Conferencing Server, Director Server, Edge Server, Front End Server, Mediation Server, Monitoring and CDR Server, Registrar Server
- Oracle Database Solution Templates - Oracle 10g Application Server, Oracle 9i Application Server, Oracle Database monitor
- SAP monitors - SAP CCMS, SAP CCMS Alert, SAP Java Web Application Server, SAP MAI Alert, SAP Performance, SAP Work Processes
- Siebel monitors - Siebel Application Server, Siebel Log, Siebel Web Server
- VMware Datastore monitor
- VMware Host monitors - VMware Host CPU, VMware Host Memory, VMware Host Network, VMware Host State, VMware Host Storage
- WebLogic Application Server monitor
- Web Script monitor
- WebSphere monitors - WebSphare Application Server, WebSphare MQ Status, WebSphere Performance Servlet monitor

Community Edition

The Community edition provides limited SiteScope functionality for free, an unlimited period of time. This edition is automatically activated after performing a regular SiteScope installation.

> **Note:** The Community edition will not be released with every SiteScope minor or minor-minor version release. For details on version types, see the "Installation Version Types" in the Deployment Guide.

The table below shows some of the main differences between the Community edition and the SiteScope commercial editions.

Feature	Description
License Duration	**Community edition:** This edition never expires. It can be overridden by any other edition after importing the license file, and it is re-activated when no other commercial edition exists or is valid. **Commercial edition:** Term or perpetual. For details on what happens when a commercial edition license expire, see "License Expiration" on page 36.
Capacity	**Community edition:** This edition has a fixed capacity for monitoring up to 25 OS instances and 25 URLs (the capacity cannot be extended). If this capacity is exceeded during a monitor run, all monitors are suspended and an error is displayed in the log. For example, OSi capacity consumption for Dynamic VMware monitors can change during the monitor run according to the number of discovered VMs. **Commercial edition:** User can purchase OS instances, URLs, and Transaction license capacity according to their monitoring requirements.
User Management	**Community edition:** One user account (Administrator). **Commercial edition:** Unlimited users and user roles and support for LDAP integration for authentication and authorization.
Solution Templates & Monitors	**Community edition:** • Solution templates and their dependent monitors are not available. • The monitors listed in "Monitors Not Included in Community Edition" on the previous pageare not available. • All other monitors are available. **Commercial edition:** All monitors and solution templates are available.

Feature	Description
Data Retention	**Community edition:** - Historical monitor data is retained for 30 days only (but log files are not deleted). Configuring the number of daily logs in the log preferences will not have any effect on the number of daily logs retained. - Quick Reports display data for the past 30 days. **Commercial edition** Unlimited
Alert Actions	**Community edition:** Only Email and Event Console alert actions are enabled. **Commercial edition:** All alert actions are enabled.
APIs	**Community edition:** Not supported. **Commercial edition:** Supported
Integrations	**Community edition:** Not supported. **Commercial edition:** Supported
High Availability (Failover)	**Community edition:** Not supported. If you attempt to connect a SiteScope Failover machine to SiteScope using the Community edition, an exception is returned from the primary SiteScope to the Failover SiteScope and displayed in the user interface. A corresponding message is also written to the error.log of the primary SiteScope. **Commercial edition:** Supported
Template Deployment	**Community edition:** CSV template deployment (via the user interface) and automatic template deployment is not supported. **Commercial edition:** Fully supported
Upgrade	You can upgrade the Community edition to the Premium, Ultimate, or System Collector edition. For details, see "Importing and Upgrading Your License" on page 35.

Trial Edition

Below are the specifications for using the SiteScope Trial edition.

Feature	**Description**
Edition Type	A free, one-time trial license.
Edition Duration	30 days
Capacity	When activated from Community edition, the Trial license includes a capacity for monitoring up to 25 OS instances, 25 URLs, and 10 transactions. **Note:** The capacity for a Trial license is fixed, and cannot be extended or renewed.
Functionality	Full SiteScope functionality. For details, see "Feature Comparison Table" on page 39.
Node locked	No
Activation	Available when using the Community edition, by selecting **Preferences > General Preferences > Licenses > Trial Edition**. It can be started only once; thereafter the button is permanently disabled.
Deactivate	Select **Preferences > General Preferences > Licenses**. In the Installed Licenses table, select the **Trial** row, and click **Remove License**. This returns SiteScope to the previous edition (or Community edition, if no other editions were purchased).
Upgrade	You can override the Trial edition with the Premium, Ultimate, or System Collector edition. For details, see "Importing and Upgrading Your License" on page 35.
Expiration	The license automatically expires after 30 days, and SiteScope returns to the Community edition. Functionality is reduced according to the functionality of the currently active license edition.

Commercial Editions

SiteScope includes the following commercial editions. The tables that follow list the specifications for using these editions.

For the list of features available in each edition, see "Feature Comparison Table" on page 39.

- "Premium/Ultimate Edition" on the next page
- "System Collector Edition" on page 48

Premium/Ultimate Edition

Feature	Description
Edition Type	Commercial edition.
Edition Duration	Term or perpetual
Capacity	Purchase the OSi, URL, and Transaction capacity that you require (there is no minimum capacity). For license purchase inquiries (or if you require additional capacity), contact your HPE sales representative or use the “Contact Us” link in the HPE SiteScope Product page.
Functionality	Full SiteScope functionality
Node locked	Yes (the license is valid on a specific machine only)
Activation	After purchasing a license, select **Preferences > General Preferences > Licenses**, and enter the path to your SiteScope license file in the **License file** box, or click the **Select** button, and select the license file.
Deactivate	Select **Preferences > General Preferences > Licenses**. In the Installed Licenses table, select the **Premium/Ultimate** row, and click **Remove License**. When deleting a Premium or Ultimate edition license, you should also delete all Premium or Ultimate edition capacity type rows (OSi, URL, and Transaction). This returns SiteScope to the previous edition, or Community edition, if no other editions were purchased.
Upgrade	You can override the Premium edition with the Ultimate or System Collector edition. For details, see "Importing and Upgrading Your License" on page 35.
Expiration	A license expires when the time-period for all capacity types in the active edition comes to an end. SiteScope sends a notification message to the user 7 days before the license is due to expire, and displays this information in the Licenses panel. Upon expiration, SiteScope automatically downgrades the edition (and functionality) to the previous commercial edition, if any, in the hierarchy. Otherwise, the Community edition becomes the active edition.

Feature	Description
Capacity Downgrade	When the OSi, URL, or Transaction capacity is exceeded, SiteScope: 1. Opens a dialog box with a warning message. 2. Sends a daily message (for up to 7 days) warning the user to remove the extra monitors, or to increase the license capacity. After the capacity has been exceeded for 7 days, SiteScope suspends all monitors.

System Collector Edition

Feature	**Description**
Edition Type	A version of SiteScope that is provided with Operations Manager Integration.
Edition Duration	Term or perpetual
Capacity	Purchase the OSi capacity that you require (there is no minimum capacity). For license purchase inquiries (or if you require additional capacity), contact your HPE sales representative or use the “Contact Us” link in the HPE SiteScope Product page.
Functionality	Full SiteScope functionality.
Node locked	Yes (the license is valid on a specific machine only)
Activation	After purchasing a license, select **Preferences > General Preferences > Licenses**, and enter the path to your SiteScope license file in the **License file** box, or click the **Select** button, and select the license file.
Deactivate	Select **Preferences > General Preferences > Licenses**. In the Installed Licenses table, select the **System Collector** row, and click **Remove License**. When deleting a System Collector edition license, you should also delete all System Collector edition capacity type rows (OSi, URL, and Transaction). This returns SiteScope to the previous edition, or Community edition, if no other editions were purchased.
Upgrade	While you cannot override a System Collector license, you can import a Premium, or Ultimate edition license to increase your URL and Transaction capacity. For details, see "Importing and Upgrading Your License" on page 35. System Collector OSi will be aggregated with Premium or Ultimate. **Note: Note**: To aggregate System Collector OSi license with other OSi license editions (Premium or Ultimate), import **only** the System Collector OSi license on Premium or Ultimate license.

Feature	Description
Expiration	A license expires when the time-period for the OS instance capacity in the active edition comes to an end. SiteScope sends a notification message to the user 7 days before the license is due to expire, and displays this information in the Licenses panel. Upon expiration, SiteScope automatically downgrades the edition (and functionality) to the previous commercial edition, if any, in the hierarchy. Otherwise, the Community edition becomes the active edition.
Capacity Downgrade	When the OSi, URL, or Transaction capacity is exceeded, SiteScope: 1. Opens a dialog box with a warning message. 2. Sends a daily message (for up to 7 days) warning the user to remove the extra monitors, or to increase the license capacity. After the capacity has been exceeded for 7 days, SiteScope suspends all monitors.

Load Testing Edition

Below are the specifications for using the SiteScope Load Testing edition in LoadRunner or Performance Center.

Feature	**Description**
Edition Type	A freely available version of SiteScope that is provided with LoadRunner and Performance Center.
Edition Duration	Perpetual
Capacity	25 OS instances, 25 URLs **Note:** Refer to the price guide for the available quantity if you want to increase the capacity.
Functionality	See "Feature Comparison Table" on page 39.
Node locked	No
Activation	Automatically activated after installing SiteScope for Load Testing .
Deactivate	A user cannot remove the Load Testing edition license.
Upgrade	You can upgrade Load Testing edition to Premium, Ultimate, or System Collector edition. For details, see "Importing and Upgrading Your License" on page 35. **Note:** Upgrading a Load Testing edition requires additional configuration as described in "Upgrading a Load Testing Edition to Premium, Ultimate, or System Collector Edition" on page 1.
Expiration	Not applicable (the license is perpetual)
Capacity Downgrade	When the license capacity is exceeded, SiteScope: 1. Opens a dialog box with a warning message. 2. Sends a daily message (for up to 7 days) warning the user to remove the extra monitors. After the capacity has been exceeded for 7 days, SiteScope suspends all monitors.

Failover Edition

Below are the specifications for using the SiteScope Failover edition.

Feature	**Description**
Edition Type	SiteScope Failover provides redundancy and automatic backup protection if a SiteScope server experiences availability issues. The Failover Edition license is provided with the Premium, Ultimate, and System Collector editions at no additional cost.
Edition Duration	SiteScope Failover is dependent on there being a primary SiteScope with a Premium, Ultimate, or System Collector edition license.
Functionality	Full SiteScope functionality
Activation	After installing SiteScope Failover, you need to import the Failover license. It only starts to work after the Failover server is synchronization with a primary SiteScope server (with Premium, Ultimate, or System Collector edition license).
Deactivate	Select **Preferences > General Preferences > Licenses**. In the Installed Licenses table, select the **Failover** row, and click **Remove License**. When deleting a Failover edition license, you should also delete all Failover edition capacity type rows (OSi, URL, and Transaction).
Expiration / Capacity Downgrade	SiteScope Failover is dependent on there being a primary SiteScope with a Premium, Ultimate, or System Collector edition license. Upon expiration of the primary SiteScope edition license, the Failover license also expires and there is no active edition on the SiteScope Failover machine.

Simple Monitors Bucket

The simple monitors bucket is a generic bucket for all simple monitors where 10 simple monitors consume one OSi license. The license consumption is calculated based on the total number of simple monitors that are deployed across hosts where 10 simple monitors = One OSi. Previously, the license bucket was based on monitor type, for example 10 ping monitors = one OSi or 10 Port monitors = One OSi. However, the current bucket is a generic one where 10 simple monitors consume one OSi.

Example 1

Previously if you had a Ping monitor then you would get one Ping bucket that consumes one OSi license. If you added a Port monitor, you would consume one more OSi for one Port bucket. Now with the generic bucket, all simple monitors will be calculated under one bucket, where one bucket lets you consume any of the 10 simple monitors for one OSi license. So in this case, the Port monitor and the Ping monitor will consume just one OSi license whereas previously you consumed 2 OSi licenses.

The simple monitors that can be pooled under one bucket are

- Ping Monitor
- Port Monitor
- DNS Monitor
- FTP Monitor
- SNMP Monitor
- SNMP Trap Monitor
- Browsable SNMP Monitor
- Network Bandwidth Monitor

The simple monitors bucket is dynamic where monitors are added or deleted from the bucket based on the monitors being deployed. If a regular monitor is deployed on a host, then the simple monitors running on the same host share the OSi license consumed by the regular monitor and free up the simple monitors bucket. There is no limit to the number of simple monitors that can share the OSi with the regular monitor on the same host.

Example 2

If you have 3 Ping monitors and 4 Port monitors, your license consumption previously would be 2 OSis (one Ping bucket and one Port bucket). If you deployed a CPU monitor, the license consumption would become 3 OSis (One ping bucket, One port bucket and One CPU). But now with the generic bucket, the license consumption would be one simple bucket with both the Ping and Port monitors consuming it. When you deploy a CPU monitor on the same host where the simple monitors are deployed, the simple monitors share the same OSi license with the CPU monitor and therefore, the simple monitors bucket is dynamically freed up. Therefore, the total license consumption is just one OSi.

Simple Bucket Monitors - License Consumption Scenarios

Scenario 1

Host	**A**	**B**	**C**	**D**
Monitors	Ping	Ping	Ping	Ping
OS Total consumption 11.32	One OSi (for one Ping bucket (4/10))			
OS Total consumption 11.40	One OSi (for one Simple bucket(4/10))			

Scenario 2

Host	A	B	C	D	E
Monitors	Ping	Ping	Ping	Ping	Ping
	Port	Port	Port	Port	
OS Total consumption 11.32	Two OSi (for one Ping bucket (5/10) and one Port bucket (4/10))				
OS Total consumption 11.40	One OSi (for one Simple bucket (9/10))				

Scenario 3

Host	A	B	C	D	E	F
Monitors	Ping	Ping	Ping	Ping	Ping	Ping
	Port	Port	Port	Port	Port	
OS Total consumption 11.32	2 OSis (for 1 ping bucket (6/10) and 1 port bucket (5/10))					
OS Total consumption 11.40	2 OSis (for 2 simple Sbuckets (10/10 + 1/10))					

Scenario 4

Host	A	B	C	D	E
Monitors	Ping				
	Port				
	CPU				
OS Total consumption 11.32	3 OSis (for 1 CPU monitor, 1 Ping bucket (1/10) and 1 Port bucket (1/10))				
OS Total consumption 11.40	1 OSi (for 1 CPU monitor, no simple bucket consumption)				

Scenario 5

Host	A	B	C	D	E

Monitors		Ping	Ping		
	Port	Port	Port	Port	
	CPU				
OS Total consumption 11.32	3 OSis (for 1 CPU monitor, 1 Ping bucket (2/10) and 1 Port bucket (4/10))				
OS Total consumption 11.40	2 OSis (for 1 CPU monitor and 1 Simple bucket (5/10))				

Scenario 6

Host	**A**	**B**	**C**	**D**	**E**	F
Monitors	Ping	Ping	Ping	Ping	Ping	Ping
	Port	Port	Port	Port	Port	Port
	CPU	CPU	CPU	CPU		
OS Total consumption 11.32	6 OSis (for 4 CPU monitors, 1 Ping bucket (6/10) and 1 Port bucket (6/10))					
OS Total consumption 11.40	5 OSis (for 4 CPU monitors and 1 simple bucket(4/10))					

Scenario 7

Monitors	300 Ping
	300 Port
	100 CPU
OS Total consumption 11.32	160 OSis (for 100 CPU monitors, 30 Ping buckets and 30 Port buckets)
OS Total consumption 11.40	120 OSis (for 1 CPU monitor and 2 simple buckets)

Points-based License Model

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" below
- "OS Instance Advanced License" on the next page
- "License Point Usage For Monitors" on page 57
- "License Point Usage For Solution Templates" on page 68

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

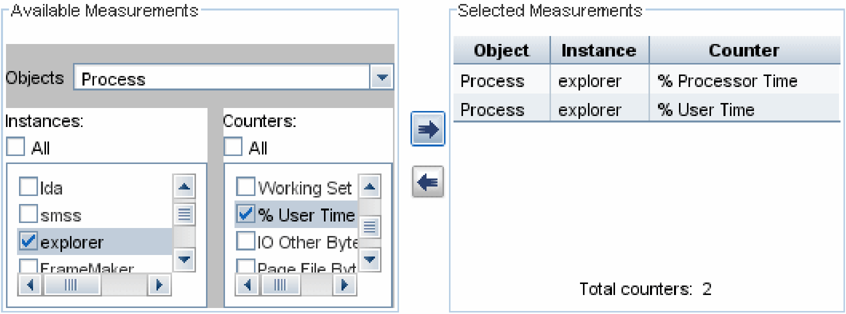
Licensing for monitor types is based on a point system. A perpetual SiteScope license provides a number of points that you use to create a combination of monitor types.

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.



Available Measurements

Objects: Process

Instances:
□ All
□ Ida
□ smss
☑ explorer
□ FrameMaker

Counters:
□ All
□ Working Set
☑ % User Time
□ IO Other Byte
□ Page File Byt

Selected Measurements

Object	Instance	Counter
Process	explorer	% Processor Time
Process	explorer	% User Time

Total counters: 2

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 HPE License Key Delivery Service http://www.hpe.com/software/entitlements), 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 APM 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 **HPE 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
- Directory
- Disk Space (deprecated)
- Dynamic Disk Space
- File
- HPE NonStop Event Log
- HPE NonStop Resources
- Memory
- Microsoft Archiving Server
- Microsoft A/V Conferencing Server
- Microsoft Director Server
- Microsoft Edge Server
- Microsoft Front End Server
- Microsoft Hyper-V
- Microsoft Mediation Server
- Microsoft Monitoring and CDR Server
- Microsoft Windows Performance Counter
- Microsoft Windows Event Log
- Microsoft Windows Resources
- Microsoft Windows Services State
- Microsoft Registrar Server
- Ping
- Port
- Service
- Solaris Zones
- UNIX Resources
- VMware Host CPU
- VMware Host Memory
- VMware Host Network
- VMware Host State
- VMware Host Storage
- 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
BroadVision Application Server	Application	1 point per metric
Check Point	Application	1 point per metric
Citrix	Application	1 point per metric

Monitor (A-Z)	Monitor Category	License Point Usage
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 56.
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 56.
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 56.
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 56
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 56.
Formula Composite	Network	1 point per monitor
FTP	Network	1 point per monitor

Monitor (A-Z)	Monitor Category	License Point Usage
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
HPE iLO (Integrated Lights-Out)	Server	1 point per metric
HPE 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 56.
HPE 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 56.
HPE 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

Monitor (A-Z)	Monitor Category	License Point Usage
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 56.
Memcached Statistics	Application	1 point per metric
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 56.
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 56.
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 56.
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 56.

Monitor (A-Z)	Monitor Category	License Point Usage
Microsoft Exchange (2007/2010)	Application	1 point per metric
Microsoft Exchange Base (2010/2013)	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
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 56.
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 56.
Microsoft IIS Server	Application	1 point per metric

Monitor (A-Z)	Monitor Category	License Point Usage
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 56.
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 56.
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 56.
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 56
Microsoft Windows Media Player	Media	1 point per metric
Microsoft Windows Media Server	Media	1 point per metric

Monitor (A-Z)	Monitor Category	License Point Usage
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 56.
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 56.
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 56.
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 56.

Monitor (A-Z)	Monitor Category	License Point Usage
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 56.
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 56
Siebel Application Server	Application	1 point per metric
Siebel Log	Application	1 point per monitor

Monitor (A-Z)	Monitor Category	License Point Usage
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
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 56.
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 56.
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)

Monitor (A-Z)	Monitor Category	License Point Usage
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 56.
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 56.
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)

Monitor (A-Z)	Monitor Category	License Point Usage
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 HPE 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)
HPE Quality Center Application Server for UNIX	11

Solution Template	Typical License Point Usage
HPE Quality Center Application Server for Windows	11
HPE Quality Center 10.0 License Status	12
HPE Quality Center 9.2 License Status	6
HPE QuickTest Professional License Server	3
HPE Service Manager for UNIX	48
HPE Service Manager for Windows	12
HPE Vertica	approximately 18 +10*<node count>
JBoss Application Server 4.x	3
JBoss Application Server 7.1 - 7.3	Approximately 15 points on the JBoss Application Server + 1 point for each application deployed
Linux Host	13
Microsoft Exchange 5.5	39
Microsoft Exchange 2000	40
Microsoft Exchange 2003	49
Microsoft Exchange 2007	83
Microsoft Exchange 2010	83
Microsoft Exchange Server 2013: Client Access Server Role	64 points (+/- 1 to 6 points, as some Microsoft Windows Resources monitors contain counter's regex)
Microsoft Exchange Server 2013: Mailbox Server Role	60 points (+/- 1 to 6 points, as some Microsoft Windows Resources monitors contain counter's regex)
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

Solution Template	**Typical License Point Usage**
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
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

Solution Template	Typical License Point Usage
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

Point-based License Model

You can install SiteScope using a General license 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: • The following Solution Templates: • *Failover • *Hadoop • *HPE Vertica • Microsoft Exchange • Microsoft Lync Server 2010 • Microsoft SharePoint 2010 • SAP • Siebel • All VMware solution templates • All monitors except those monitors which are dependent on Solution Templates that are not bundled with this license. **Note:** After the trial period expires or the license is upgraded to a General license, the solution templates listed above (except *) and all extension monitors (see "Extension License" on the next page) 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
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" below). • Monitors which are not available when their Solution Templates are not available (see "Monitors Not Available when their Solution Templates are Not Available: " on the next page). Includes access to the Hadoop, HPE 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 56.	This license type can be temporary (time-based) or perpetual.	Displays the total number of OS/host licenses purchased.
Extension License	An additional extension license is required to enable each of the solution templates (except Hadoop, HPE 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 57 and "License Point Usage For Solution Templates" on page 68.

Type	Description	Duration	Points Displayed
Failover License	**SiteScope Failover:** A special license issued by HPE 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.

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 "Points-based License Model" on page 55.	

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, contact a regional support center listed here: https://h22244.www2.hpe.com/mysoftware/contact/getLicenseCenter.

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" on the next page
- "Web Process and Content Monitoring" on the next page

- "Application Performance Monitoring " below
- "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

Importing SiteScope Licenses

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

To import a license into 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 the license has been successfully imported, information about the imported license is displayed in the Installed Licenses table. This includes the license edition, capacity type and details (capacity available, used, and remaining), expiration date, and the license status.

> **Note:** After upgrading to SiteScope 11.40, it might take a short period of time before the Licensing panel is updated with the current licenses.

Migrate License Model

SiteScope 11.40 version works with the capacity-base (OSi) license by default. However, with this version of SiteScope you have the ability to work with the points-based license if you have a valid points-based license.

This section includes the following topics:

- "Important Notes on License Migration" below
- "License Migration Scenarios" below
- "Steps to Migrate to Points-based License " on the next page
- Troubleshooting

Important Notes on License Migration

- You are allowed to use only one license model (Capacity (OSi) or points-based)
- When you switch to the points-based license, only the points-based license will work.
- After migration, the capacity of your points-based license will remain unchanged.
- License Expiration
  - After migration, the expiry of your license will be that of your points-based license expiry date.
  - If your points-based license has an unlimited expiry date, you can continue to have unlimited expiry after migration.
- Freemium 11.2x license cannot be imported to the points-based license in 11.40.
- 11.2x , 11.3x or 11.40 license is locked to the IP of SiteScope server.
- If you are a LoadRunner or Performance Center user with SiteScope 11.40 , you must use LoadTesting edition that comes with the Instant-on 25 OSI and URL licenses. You cannot migrate to the point-based model.

License Migration Scenarios

Scenario 1 – Import SiteScope 11.24 configuration to SiteScope 11.40.

Consider you are an existing SiteScope user who bought a point-based license on August 31, 2016 with one year validity and 500 points. Your license expires on August 31, 2017. The following points are applicable:

- You are entitled to use SiteScope version 11.40 from the day of the software release.
- You can download and install version 11.40, import your existing 11.2x configuration into 11.40 and upgrade the configuration.
- You can migrate your license to use the points-based license.

- After migration, SiteScope continues to use points-based license instead of 11.40 license. SiteScope interprets your license as follows:
  - License expiration will be as per your points-based license. In this case, the license expiry is August 31, 2017.
  - After your license expires on August 31, 2017, you can choose to purchase the points-based license or the capacity-based license.

Scenario 2 – SiteScope 11.24 License expires after migration to 11.40 mode.

Consider you have a valid 11.24 license with an expiry date of September 15, 2017. You have downloaded SiteScope 11.40 on August 31, 2017 and have migrated to the point-based model. Your license expiry will be based on your 11.24 license. After September 15, 2017 your license expires. You can choose to purchase the points-based license or the capacity-based license.

Scenario 3 – Valid Failover license migration

Consider you have a failover license with 500 points and one year validity with license expiry on August 1, 2017. The following points are applicable in this scenario:

- You are entitled to use SiteScope version 11.40 from the day of the software release and can migrate license to point-based model.
- After license migration, you must reconfigure the failover parameters.
- After license migration, SiteScope continues to use point-based license instead of 11.40 license. SiteScope interprets your license as follows:
  - License edition will be automatically set to Failover edition.
  - License expiration will be as per your point-based license. In this case, the license expiry is August 1, 2017.

Scenario 4 – Migrating license of SiteScope that is integrated with APM

Consider you have an existing SiteScope setup that is integrated with APM. You have a valid point-based license and want to move to 11.40 configuration with the point-based license model.

- You are entitled to use SiteScope version 11.40 from the day of the software release.
- You can download and install version 11.40, import your existing configuration into 11.40 and upgrade the configuration.
- You can migrate license to use point-based model.
- After license migration, you must reconfigure the APM Integration.

Steps to Migrate to Points-based License

Prerequisites

- You must have a valid SiteScope points-based license.
- SiteScope 11.40 must be installed.

To migrate to points-based license, follow these steps:

1. Stop the SiteScope service.
2. Browse to the `master.config`file located in <SiteScope_directory>SiteScope\groups directory.
3. Open the `master.config` file in edit mode.
4. Modify the value of the point-based license parameter as `_use112xLicense=true`.
5. Start the SiteScope service.
6. Import a valid point-based license. For details to import a license, see the "Importing SiteScope License" in the SiteScope Deployment Guide.

License is migrated to the points-based model.

Verify License Migration

You can verify if you have migrated successfully to the points-based license model using any of the following options:

- License Usage Monitor under SiteScope Health monitor shows the availability and usage of points-based license information on the dashboard.
- The Active edition information in the **About SiteScope** page (**Help** > **About SiteScope**) displays the points-based license information.
- The Licenses panel in General Preferences (**Preferences** > **General Preferences**) displays the license edition, status, and capacity details of the points-based license.

Part 2: Install SiteScope

Chapter 5: Installation Overview

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 Linux platforms.

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 than one SiteScope on a single machine.
   > - If you plan to use SiteScope Failover to provide backup monitoring availability in case of a SiteScope server failure, see the HPE SiteScope Failover Guide located in **<SiteScope root directory>\sisdocs\pdfs\SiteScopeFailover.pdf**.

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

   For details, see "Installation Flow" on page 93.

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 11.40. Do not install version 11.40 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 Flow" on page 93.

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 "Post-Installation: Getting Started" on page 185.

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

   For more information, see "Post-Installation Administration" on page 204.

Chapter 6: Installation Requirements

This chapter includes:

- "System Requirements" below
- "SiteScope Capacity Limitations" on page 90
- "SiteScope Integration Matrix " on page 90

System Requirements

This section includes the following topics:

- "System Hardware Requirements" on the next page
- "Server System Requirements for Windows" on page 86
- "Server System Requirements for Linux" on page 86
- "Client System Requirements" on page 88

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 minimum
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 the next page).
- 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 APM.

Operating System	Microsoft Windows Server 2012 R2 (64-bit)
System Type	ACPI Multiprocessor x64-based PC
CPU	4 physical Intel Xeon (R) x5650 processors @2.67 GHz each
Total Physical Memory (RAM)	16 GB
Java Heap Memory	8192 MB
Total Number of Monitors	24,000
Total Number of Remote Servers	2,500
Monitor Runs per Minute	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 APM for the first time.

Server System Requirements for Windows

The following Microsoft Windows operating system versions have been certified:

- Microsoft Windows Server 2016 (Dual core)
- Microsoft Windows Server 2012 R2 Data Center
- Microsoft Windows Server 2012 R2 Standard Edition
- Microsoft Windows Server 2012 Standard/Datacenter Edition
- Microsoft Windows Server 2008 R2 SP1 Standard/Enterprise/Datacenter Edition

SiteScope installation on Amazon Web Services (AWS) and Azure

SiteScope can be installed on Amazon Web Services (AWS) and Azure on the platform versions listed above. You must have a static public IP address to use the SiteScope permanent license on AWS and Azure.

Server System Requirements for Linux

The following Linux 64-bit operating system versions have been certified:

- openSUSE 42.2
- Oracle Enterprise Linux (OEL) 6.0 – 6.5, 7.0
- Red Hat ES/AS Linux 5.5-5.8, 6.0 – 6.8, 7.0, 7.1, 7.2, 7.3, 7.4
- CentOS 6.2, 7.0, 7.2, 7.3

Note:

- The OEL and CentOS environments must be manually configured before installing SiteScope. For details, see the chapters "Installation Prerequisites - Linux", "Installing SiteScope on an Oracle Enterprise Linux Environment" and "Installation Prerequisites -

CentOS 6.2" in the SiteScope Deployment Guide.

- If you plan to integrate SiteScope with OM or APM, you need to configure dependencies on the Red Hat ES Linux 6.0 (64-bit) environment before installing the Operations Agent (the agent is required for sending events and storing metrics data to OM or APM). For details on configuring the dependencies and installing the agent, see the Integrating SiteScope with Operations Manager Products Guide available in the SiteScope Help or on the HPE Software Integrations site.
- 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. Since the binary path can vary on 32- and 64-bit systems and on different Linux platforms, you should add the corresponding path according to your Linux platform.
- To be able to monitor CPU and memory usage on SiteScope or a remote server running on Red Hat Linux or openSUSE 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).
- To view certain report elements on SiteScope for Linux, it is necessary that an X Window system be installed and running on the server where SiteScope is running.

SiteScope installation on Amazon Web Services (AWS) and Azure

SiteScope can be installed on Amazon Web Services (AWS) and Azure on the system versions listed above. You must have a static public IP address to use the SiteScope permanent license on AWS and Azure.

Client System Requirements

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

Supported Browsers: SiteScope UI	• Microsoft Internet Explorer 10, 11 Internet Explorer 10 is supported with the following limitation: 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. Internet Explorer 10 and 11 are supported with the following limitation: Alert, Monitor, and Server-Centric Reports are supported in compatibility mode with **Document mode: quirks** only; the default **Document mode: IE5 quirks** is not supported. To enable **quirks** mode, open the Alert, Monitor, or Server-Centric report, and press `F12`. In the Developer Tools, select **Document Mode > Quirks**. • Google Chrome browsers that support NPAPI (latest certified version): 59.0.3071.115 (Official Build) (64-bit). **Note:** ◦ To enable NPAPI in Chrome, enter `chrome://flags/#enable-npapi` in your URL bar, click the **Enable** link for the **Enable NPAPI configuration** option, and then click the **Relaunch** button at the bottom of the configuration page. For details, see https://java.com/en/download/faq/chrome.xml. ◦ Due to a browser specific limitation, the Page Options and Help links do not work in Google Chrome. • Mozilla Firefox (latest certified version): ESR 52.2.1 (32-bit) **Prerequisites:** The browser must be set to enable JavaScript execution, allow pop-ups from the SiteScope application, and accept third-party cookies and allow session cookies.
Supported Browsers: Unified Console	• Internet Explorer 10, 11 • Google Chrome browsers (latest certified version): 59.0.3071.115 (Official Build) (64-bit) • Mozilla Firefox (latest certified version): ESR 52.2.1 (32-bit) • Safari (latest certified version): 9.0 for Mac • iPad 3 with Safari (iOS 9 with latest updates) • Android tablet with Chrome 34.0.1847 (or with any latest default browser of Android) Full HD display

Supported Browsers: SiteScope Multi-View Page in MyBSM	• Internet Explorer 10, 11
Java Plug-in (required to open SiteScope user interface)	• JRE version 8 (JRE 8 update 131 is the latest certified version) **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`

Supported Open SSH Versions

SiteScope Version	**Open SSH Versions**
11.40	7.3 p1, 7.4 p1, 7.5 p1

SiteScope Capacity Limitations

- When SiteScope is integrated with APM, 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 Application Performance Management integration properties for over 2,500 monitors at one time.
- We do not recommend creating more than 1000 remote servers that use an SSH connection (assuming the default parameter settings, such as run frequency, number of connections, and so forth, are used). If you need to monitor more than 1000 remote servers using SSH, you should add another SiteScope server.

> **Tip:** SiteScope includes a tool that helps you predict system behavior and perform capacity planning for SiteScope. For details, see "SiteScope Capacity Calculator" on page 17.

SiteScope Integration Matrix

SiteScope supports integrations with the following products:

- Application Performance Management (APM), previously BSM
- Operations Manager i (OMi)
- Operations Manager for Windows
- Operations Manager for Unix
- Performance Dashboard
- Load Runner
- Operations Bridge Analytics (OBA)
- Operations Bridge Reporter (OBR), previously SHR
- Performance Center
- Performance Manager
- Service Manager
- Diagnostics
- Operations Orchestration (OO)
- Cloud Service Automation (CSA)

- Continuous Delivery Automation (CDA)
- HPE Codar

For supported versions, refer to the integration matrix on the Aztec portal: https://softwaresupport.hpe.com/group/softwaresupport/search-result/-/facetsearch/document/KM01663677?lang=en&cc=us&hpappid=202392_SSO_PRO_HPE#S

For integrations with OMi, OBR and other integrations that use Operations Agent, refer to the SUMA matrix for the supported OA versions.

https://softwaresupport.hpe.com/group/softwaresupport/search-result/-/facetsearch/document/KM323488

Chapter 7: Installation Workflow

This chapter contains instructions for installing major or minor releases. For instructions on installing a minor-minor release or intermediate patch, or upgrading from an existing version of SiteScope, follow the instructions in "Upgrade an Existing SiteScope Installation" on page 175.

This chapter includes:

Installation Version Types

SiteScope is installed and run as a 64-bit application. It is available as a self-extracting executable file and packages folder. For major or minor releases, this file is available in the SiteScope installer package (zip file).

For minor-minor and patch releases, you download this file from the **Software Patch** section on the HPE Software Support site.

> **Note:** SiteScope minor-minor and patch releases should be installed on top of standard SiteScope installations only; not on non-standard installations such as SiteScope Failover or System Health.

If you want to install the latest possible version, you need to install SiteScope 11.40, then the latest minor-minor version, if available, then the latest intermediate patch for the minor-minor version (shown on the HPE Support site in the Patches section for latest minor-minor version), if available.

Official Name	Version Type	Example	Installation
Major Minor	Full Installer release	10.0, 11.0 10.10, 11.40 Example file name: `HPESiteScope_11.40_setup.exe`	Install on a clean system, and import previous release configuration. Upgrade is executed on first start up.

Official Name	Version Type	Example	Installation
Minor-Minor (patch)	Collection of defect fixes from corresponding Major or Minor release	11.01 (on top of 11.00) 11.24 (on top of 11.20 or 11.2x) 11.33 (on top of 11.30) Example file name: `HPESiS1133_11.33_setup.exe`	Minor-Minor patch is installed on top of its corresponding release. It does not require an upgrade.
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

This topic contains instructions for installing SiteScope 11.40 only. For instructions on upgrading from an existing version of SiteScope, follow the instructions in "Upgrade an Existing SiteScope Installation" on page 175.

1. **Installation Prerequisites (for Linux only).**
   a. Select a suitable installation location and set account permissions. For details, see "Installation Prerequisites - Linux" on page 96.
   b. If you are installing SiteScope on one of the following Linux platforms, you need to manually configure the environment before installing SiteScope:

Platform	Installation Prerequisites
Oracle Enterprise Linux 6.0, 6.1	See "Install Dependencies on an Oracle Enterprise Linux 6.0, 6.1 Environment" on page 98.
CentOS 6.2	See "Installation Prerequisites - CentOS 6.2" on page 98.

Platform	Installation Prerequisites
Cloud Services instance running on a CentOS 6.2 operating system	See "Install SiteScope on an Cloud Services Instance Running on CentOS 6.2" on page 99.
Red Hat ES/AS Linux 6.0	If you plan to integrate SiteScope with OM or APM, you need to configure dependencies on the Red Hat ES Linux 6.0 (64-bit) environment before installing the Operations Agent (the agent is required for sending events and storing metrics data to OM or APM). For details on configuring the dependencies and installing the agent, see the Integrating SiteScope with Operations Manager Products Guide available in the SiteScope Help or on the HPE Software Integrations site.

2. **Download SiteScope 11.40.**

   a. Download the platform specific installer package (**SiteScope_11.40_Windows.zip** or **SiteScope_11.40_Linux.zip**) to the machine where you want to install SiteScope. SiteScope is available via HPE Systems as follows:

Customer	Download Options
For Evaluating Customers	Link for electronic download evaluation HPE Software Partner Central for HPE Authorized Software Partners (The above links require HPE Passport accounts. Register for an HPE Passport at http://h20229.www2.hpe.com/passport-registration.html.)
For New Customers	Electronic Software Download. Customer receives a link via email where the software can be downloaded; this link is specific to the order.

Customer	Download Options
For Existing Customer Updates	https://h20575.www2.hpe.com/usbportal/softwareupdate.do **Prerequisites:** i. You need an HPE Passport account to access the above link, and a Support Agreement ID (SAID) to receive updates through the SSO Portal. To register for an HPE Passport, see http://h20229.www2.hpe.com/passport-registration.html. For details on activating your SAID, see the FAQ on the Software Support Online site. ii. A new license key is required for the software upgrade. Contact your HPE support renewal rep to request product contract migration first. Once contract migration is completed, go to the My Software Updates portal (https://h20575.www2.hpe.com/usbportal/softwareupdate.do) and click the **Get Licensing** tab to get the new license key(s). **To download software updates:** i. Select **My software updates**. ii. Expand **Application Performance Management**, select the HPE SiteScope 11.40 Software E-Media you require, and click **Get software updates**. iii. In the Selected Products tab, click **Get Software** for the product update(s) you want, and follow the instructions on the site to download the software.

b. Extract the compressed file into an appropriate directory.

3. **Install SiteScope 11.40.**

   Install SiteScope using one of the following installation options:

Operating System	Installation Options
Windows	• User interface executable (installation wizard). For details, see "Install Using the Installation Wizard" on page 103. • Silent installation. For details, see "Install SiteScope in Silent Mode" on page 127.

Operating System	Installation Options
Linux	• User interface executable (installation wizard). For details, see "Install Using the Installation Wizard" on page 103. • Console mode installation script using command line input. For details, see "Install on Linux Using Console Mode" on page 122. • Silent installation. For details, see "Install SiteScope in Silent Mode" on page 127.

> **Note:**
>
> - Console mode installation is not supported for Windows installations.
> - If there is an existing version of SiteScope installed, you must uninstall it before installing SiteScope 11.40.
> - If you previously exported SiteScope data using the Configuration Tool (for details, see "Run the SiteScope Configuration Tool" on page 186), you can import the user data **.zip** file.
> - If you have third-party middleware and drivers, you must copy or install them manually.

4. **Install and Configure the Operations Agent (required if integrating SiteScope with OM or APM)**

   For details on installing and configuring the agent, see the Integrating SiteScope with Operations Manager Products Guide available in the SiteScope Help or on the HPE Software Integrations site.

5. **Install Microsoft hotfixes.**

   To improve SiteScope scalability and performance, we recommend installing Microsoft hotfixes. For more information, see "Install Microsoft Hotfixes" on page 206.

6. **Connect to SiteScope.**

   For details, see "Connecting to SiteScope" on page 209.

Installation Prerequisites - Linux

Before installing SiteScope on an Oracle Enterprise Linux platform, you need to perform the following:

- Verify that the installation location for the SiteScope application (`/opt/HP/SiteScope`) has at least 2.5 GB of free disk space for the installation and operation of SiteScope.

  In addition, the Linux installer requires full access to the default temporary directory (the `/tmp` directory). If this directory is restricted in any way (for example because of security requirements), you should choose a different temporary directory with full access before running the installer.

You can change this directory by running the command:

```
export IATEMPDIR=/new/tmp/dir
```

```
export _JAVA_OPTIONS=-Djava.io.tmpdir=/new/tmp/dir
```

where `/new/tmp/dir` is the new Installer's working directory.

- 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 15.
- If installing SiteScope on an Oracle Enterprise Linux 6.0 or 6.1 environment, install the dependencies as described in "Install Dependencies on an Oracle Enterprise Linux 6.0, 6.1 Environment" on the next page.

> **Note:**
>
> - The 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 "Install SiteScope in Silent Mode" on page 127.

Tips for installing SiteScope on an Oracle Enterprise Linux 7 platform:

Check the hostname of the Oracle Enterprise Linux 7 server and make sure that the host is resolved.

1. Get your hostname by running the hostname command.
2. Run ping `<FQDN>`. If the ping request is successful, the host is already resolvable.
3. If that failed, then find your IP using `ifconfig`.
4. Run echo "`<IP Address> <FQDN> <shortname>" >> /etc/hosts` to add a string with an IP corresponding to your hostname to the hosts file.
5. Run `ping <FQDN>` 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.

Install Dependencies on an Oracle Enterprise Linux 6.0, 6.1 Environment

Before SiteScope can be installed on Oracle Enterprise Linux 6.0 or 6.1, 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.

Installation Prerequisites - CentOS 6.2

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** and **libXp.i686** libraries by executing the command:

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

> **Note:** Usually CentOS installation has all the libraries already installed. In this case, the installer uses glibc.i686 as soon as JRE depends on glibc and libXp. Since SiteScope has its own java, the JRE is required for running the installer only.

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.

Install SiteScope on an Cloud Services Instance Running on CentOS 6.2

SiteScope is supported on an Cloud Services instance running on a CentOS 6.2 operating system.

Tips for installing SiteScope on Cloud Services:

1. **Check the hostname of the 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.
2. **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
```

3. **Install additional libraries.**

   For details, see "Installation Prerequisites - CentOS 6.2" on page 98.

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

Install SiteScope on Cloud Services

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

   ```
   [root@centos ~]# sh ./HPSiteScope_11.40_setup.bin -i console
   ```

2. Install SiteScope using the console mode. For details, see "Install on Linux Using Console Mode" on page 122.
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 11.40 installed on a CentOS 6.2 server.

Troubleshooting and Limitations

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

- "SiteScope might not install on Linux using console mode" below
- "Error installing the Operations Agent - check the log files" below
- "After uninstalling SiteScope, a subsequent SiteScope installation fails" below

SiteScope might not install on Linux using console mode

[Installing SiteScope on Linux Red Hat 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.

Error installing the Operations Agent - check the log files

If you encounter an error while installing the Operations Agent or you want to see the installation status, you can check 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")
- 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

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 8: Install Using the Installation Wizard

Use the following steps to install SiteScope on supported Windows or Linux environments using the installation wizard. For the list of supported environments, see "System Requirements" on page 84.

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 "Install SiteScope Using the Installation Wizard on a Machine Without X11 Server" on page 121.
- Install SiteScope on Linux platforms in console mode. For details, see "Install on Linux Using Console Mode" on page 122.

> **Note:**
>
> - You can also install SiteScope using a silent installation. For details, see "Install SiteScope in Silent Mode" on page 127.
> - If you are planning on upgrading an existing version of SiteScope, follow the procedures in "Upgrade an Existing SiteScope Installation" on page 175.
> - The option to install the Operations Agent directly from within SiteScope was removed from the Configuration Wizard and the Configuration Tool. Instead, you must manually install and configure the agent. The agent is required for sending events and storing metrics data if SiteScope is integrated with OM or APM (except when graphing metrics data to Performance Graphing using the profile database in APM). For details on installing and configuring the agent, see the Integrating SiteScope with Operations Manager Products Guide available in the SiteScope Help or on the HPE Software Integrations site.

To install SiteScope:

1. Obtain the SiteScope installation package.
   a. Download the platform specific installer package (**SiteScope_11.40_Windows.zip** or **SiteScope_11.40_Linux.zip**) to the machine where you want to install SiteScope.

SiteScope is available via HPE Systems as follows:

Customer	Download Options
For Evaluating Customers	Link for electronic download evaluation HPE Software Partner Central for HPE Authorized Software Partners **Note:** The above links require HPE Passport accounts. Register for an HPE Passport at http://h20229.www2.hpe.com/passport-registration.html.
For New Customers	Electronic Software Download. Customer receives a link via email where the software can be downloaded; this link is specific to the order.
For Existing Customer Updates	https://h20575.www2.hpe.com/usbportal/softwareupdate.do **Prerequisites:** i. You need an HPE Passport account to access the above link, and a Support Agreement ID (SAID) to receive updates through the SSO Portal. To register for an HPE Passport, see http://h20229.www2.hpe.com/passport-registration.html. For details on activating your SAID, see the FAQ on the Software Support Online site. ii. A new license key is required for the software upgrade. Contact your HPE support renewal rep to request product contract migration first. Once contract migration is completed, go to the My Software Updates portal (https://h20575.www2.hpe.com/usbportal/softwareupdate.do) and click the **Get Licensing** tab to get the new license key(s). **To download software updates:** i. Select **My software updates**. ii. Expand **Application Performance Management**, select the HPE SiteScope 11.40 Software E-Media you require, and click **Get software updates**. iii. In the Selected Products tab, click **Get Software** for the product update(s) you want, and follow the instructions on the site to download the software.

b. Extract the compressed file into an appropriate directory.

2. Run the SiteScope installation according to your operating system. Note that SiteScope is installed and run as a 64-bit application only.

   For Windows:

   a. Run **HPSiteScope_11.40_setup.exe**.

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

For example:

```
<SiteScope_Installation>\HPSiteScope_11.40_setup.exe
```

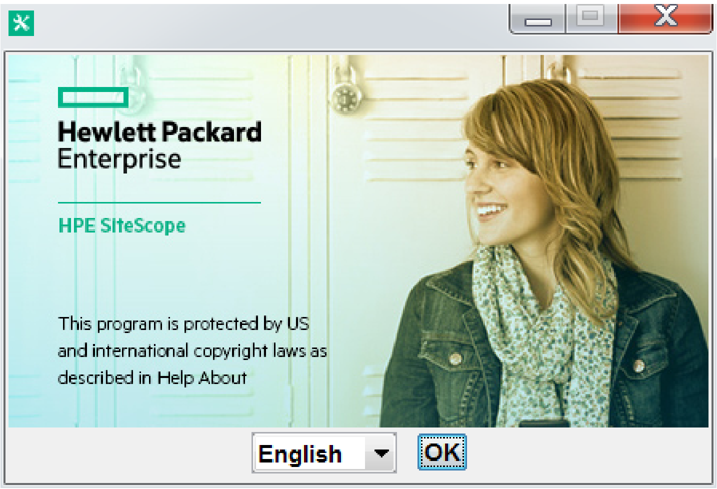
For Linux:

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

b. Run the installer by entering: **./HPSiteScope_11.40_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. Select a language for installing SiteScope from the languages listed. The installer shows a different set of languages depending on the OS Locale. For the list of languages supported in the SiteScope user interface, see the Internationalization in SiteScope section of the Using SiteScope Guide.


Hewlett Packard
Enterprise
HPE SiteScope
This program is protected by US and international copyright laws as described in Help About
English
OK

Click **OK** to continue with the installation. The Initialization screen is displayed.

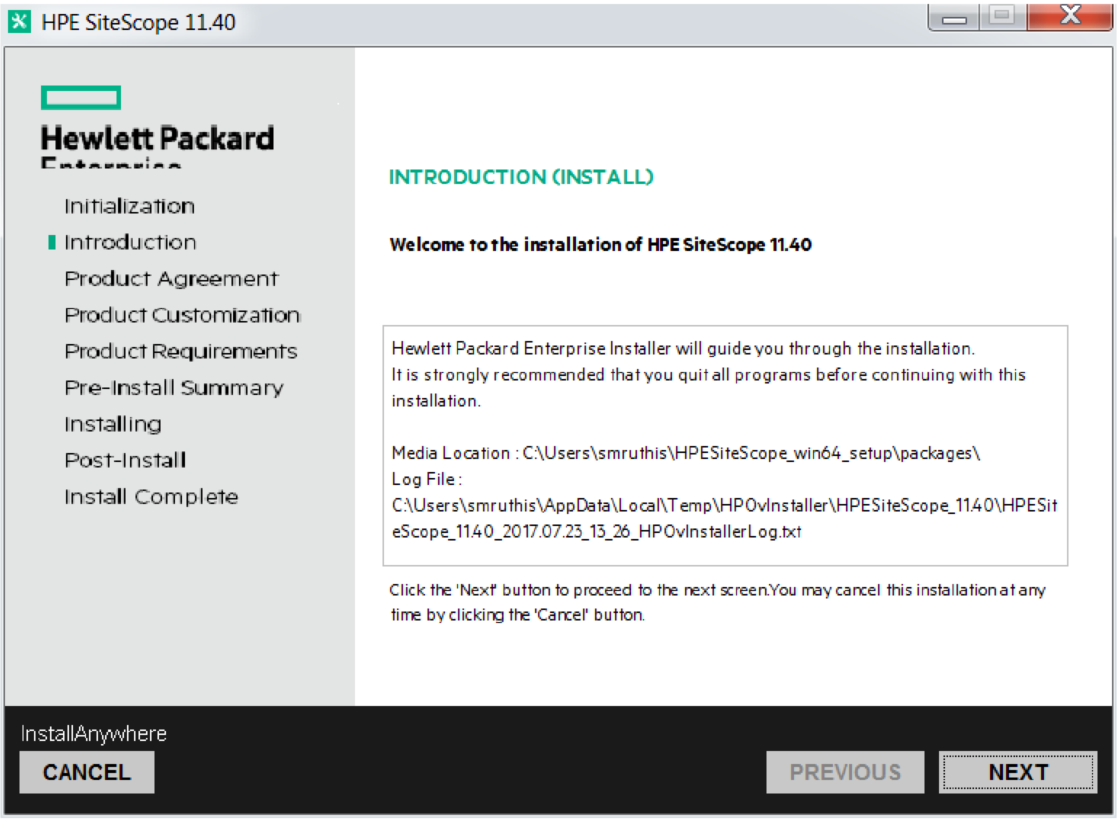
If the Installer detects any anti-virus program running on your system, it prompts you to examine the warnings before you continue with the installation.

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. Click **Next** on the Introduction (Install) screen.



INTRODUCTION (INSTALL)

Welcome to the installation of HPE SiteScope 11.40

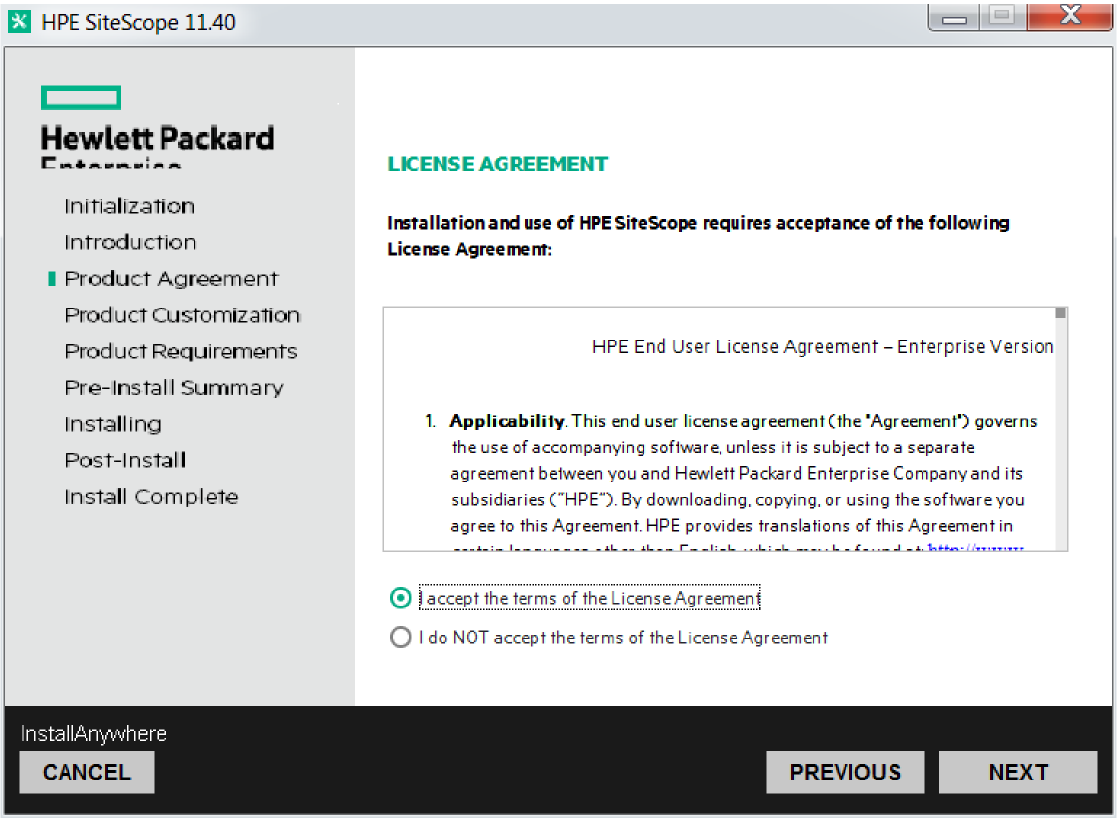
Hewlett Packard Enterprise Installer will guide you through the installation.
It is strongly recommended that you quit all programs before continuing with this installation.

Media Location : C:\Users\smruthis\HPESiteScope_win64_setup\packages\
Log File :
C:\Users\smruthis\AppData\Local\Temp\HPOvInstaller\HPESiteScope_11.40\HPESiteScope_11.40_2017.07.23_13_26_HPOvInstallerLog.txt

Click the 'Next' button to proceed to the next screen.You may cancel this installation at any time by clicking the 'Cancel' button.

The License Agreement screen is displayed.

6. Read the SiteScope License Agreement and select **I accept the terms of the License Agreement**. Click **Next**.



LICENSE AGREEMENT

Installation and use of HPE SiteScope requires acceptance of the following License Agreement:

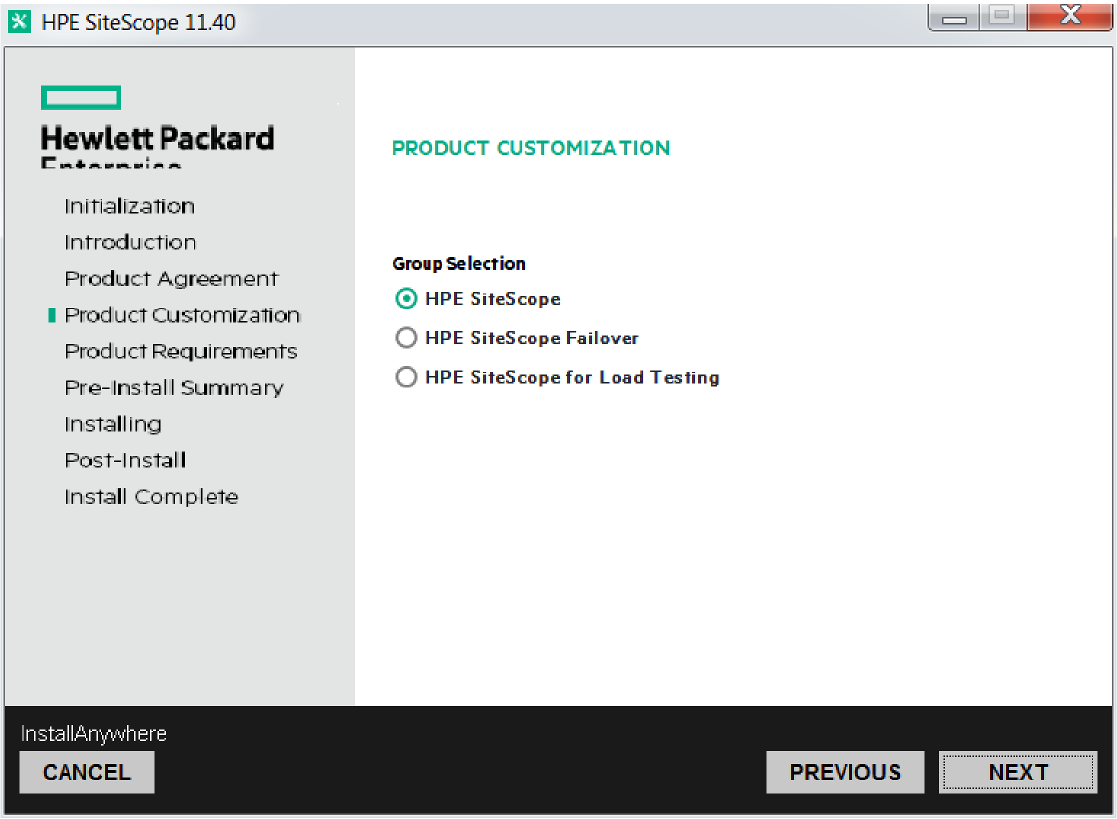
HPE End User License Agreement – Enterprise Version

1. **Applicability**. This end user license agreement (the "Agreement") governs the use of accompanying software, unless it is subject to a separate agreement between you and Hewlett Packard Enterprise Company and its subsidiaries ("HPE"). By downloading, copying, or using the software you agree to this Agreement. HPE provides translations of this Agreement in certain languages other than English, which may be found at: http://www.

● I accept the terms of the License Agreement

○ I do NOT accept the terms of the License Agreement

7. On the Product Customization screen, select the SiteScope setup type.



PRODUCT CUSTOMIZATION

Group Selection

● HPE SiteScope

○ HPE SiteScope Failover

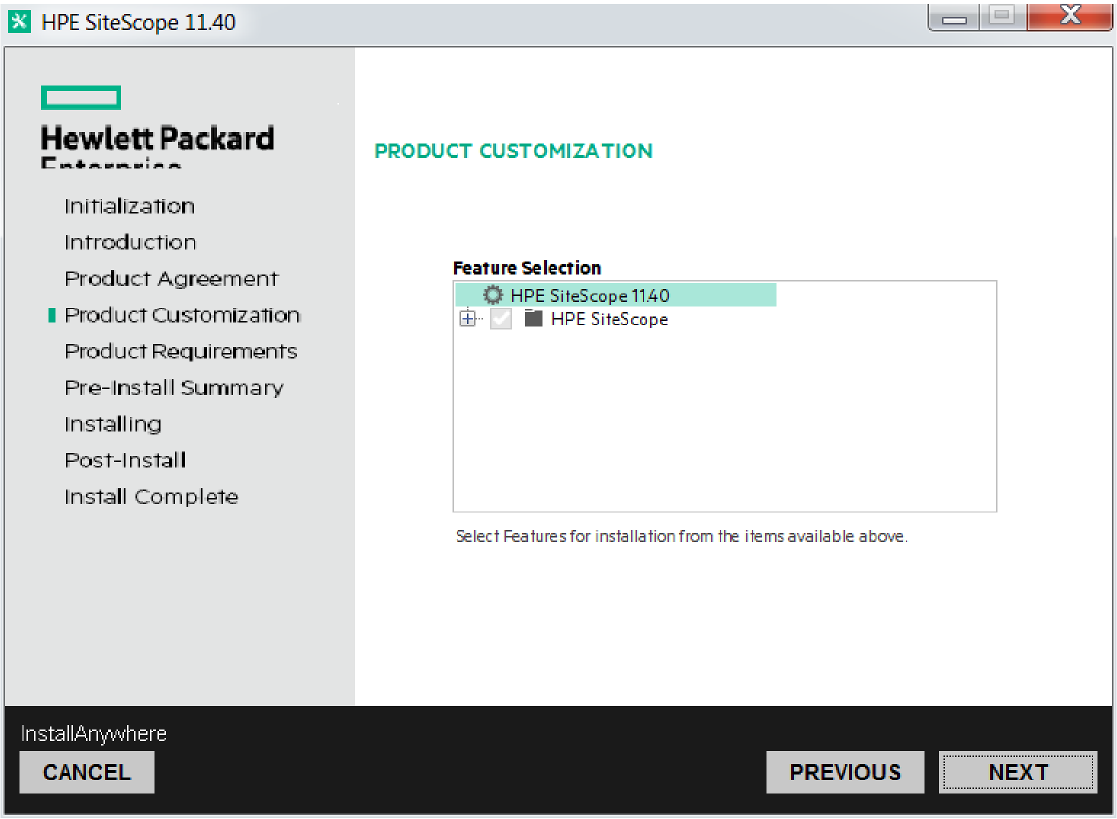
○ HPE SiteScope for Load Testing

- **HPE SiteScope.** This is the standard SiteScope installation.
- **HPE SiteScope Failover.** This installation provides a backup for monitoring infrastructure availability if a primary SiteScope server fails.
- **HPE SiteScope for Load Testing.** This setup type is used with an HPE LoadRunner or HPE 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 Linux platforms.

Click **Next** to continue.

8. On the Feature Selection screen, click **Next**.



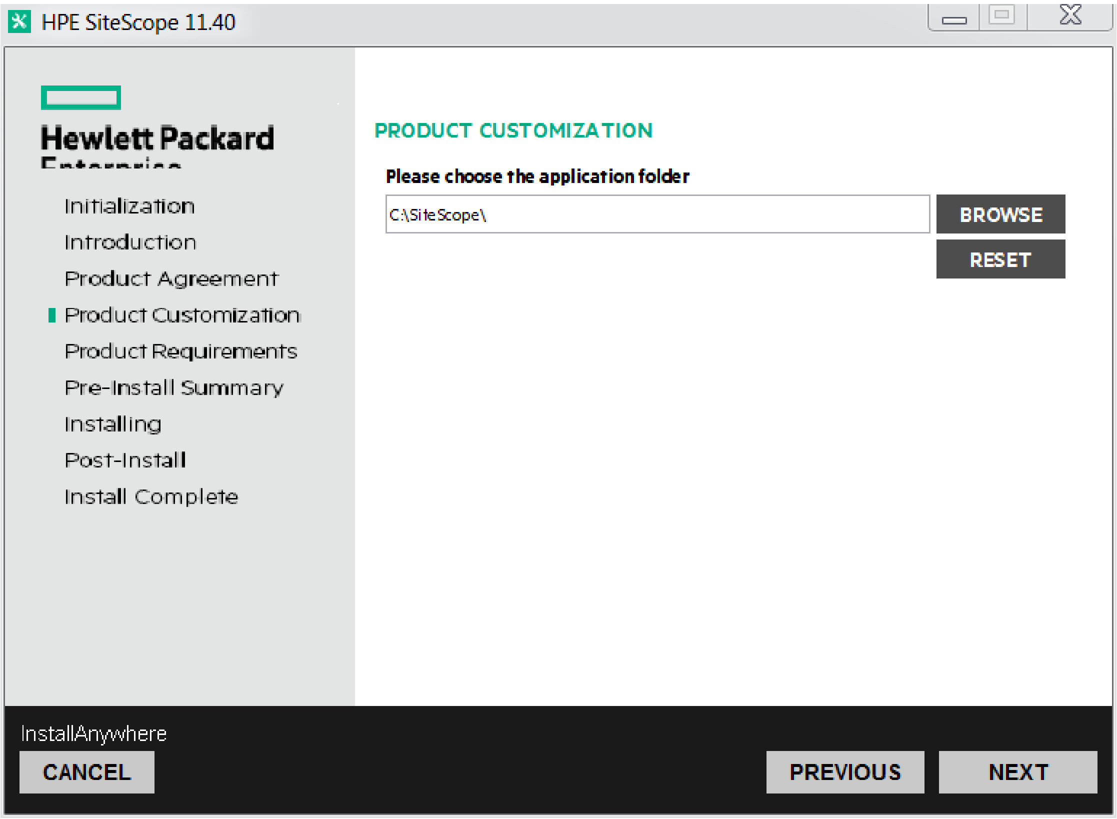
Feature Selection

HPE SiteScope 11.40

☑ HPE SiteScope

Select Features for installation from the items available above.

9. If installing on Linux platforms, SiteScope is automatically installed in the **/opt/HP/SiteScope/** folder. Skip to step 10. The Choose the folders screen is displayed.

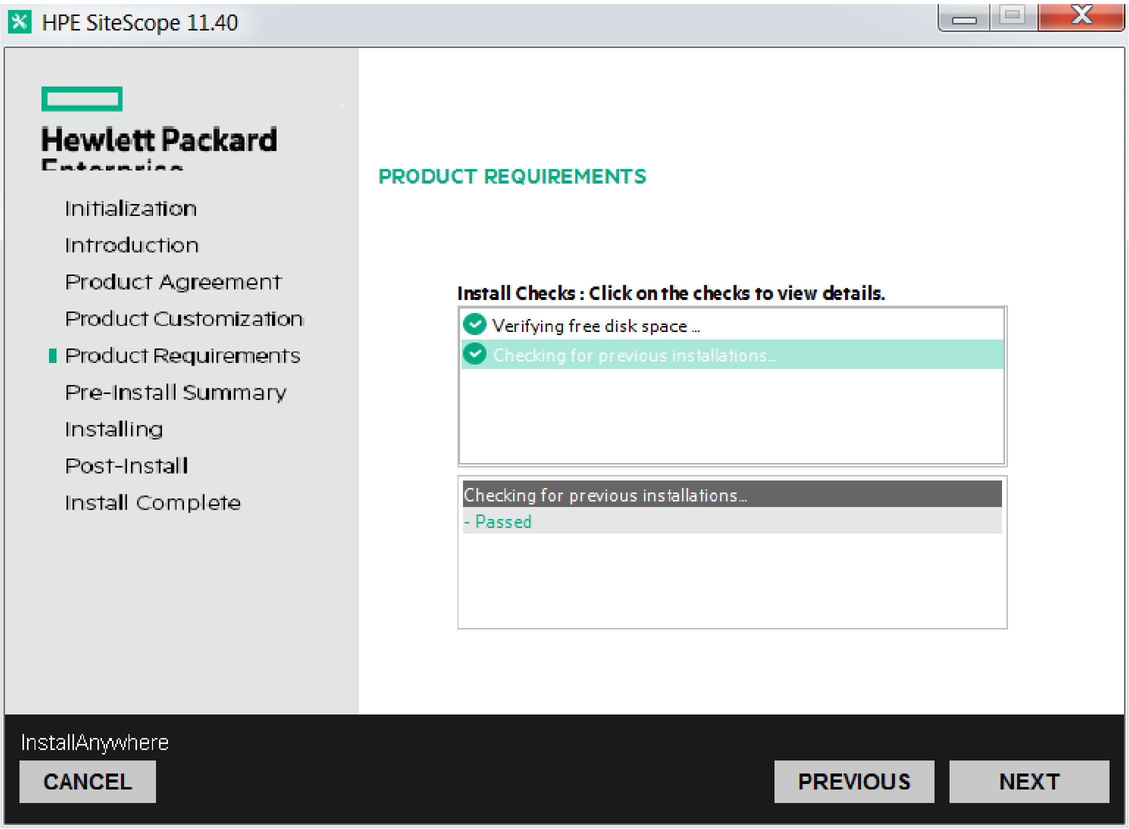


Please choose the application folder

C:\SiteScope\

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**.

Click **Next** to continue. The Install Checks screen opens and runs verification checks.



Install Checks : Click on the checks to view details.

✓ Verifying free disk space ...
✓ Checking for previous installations...

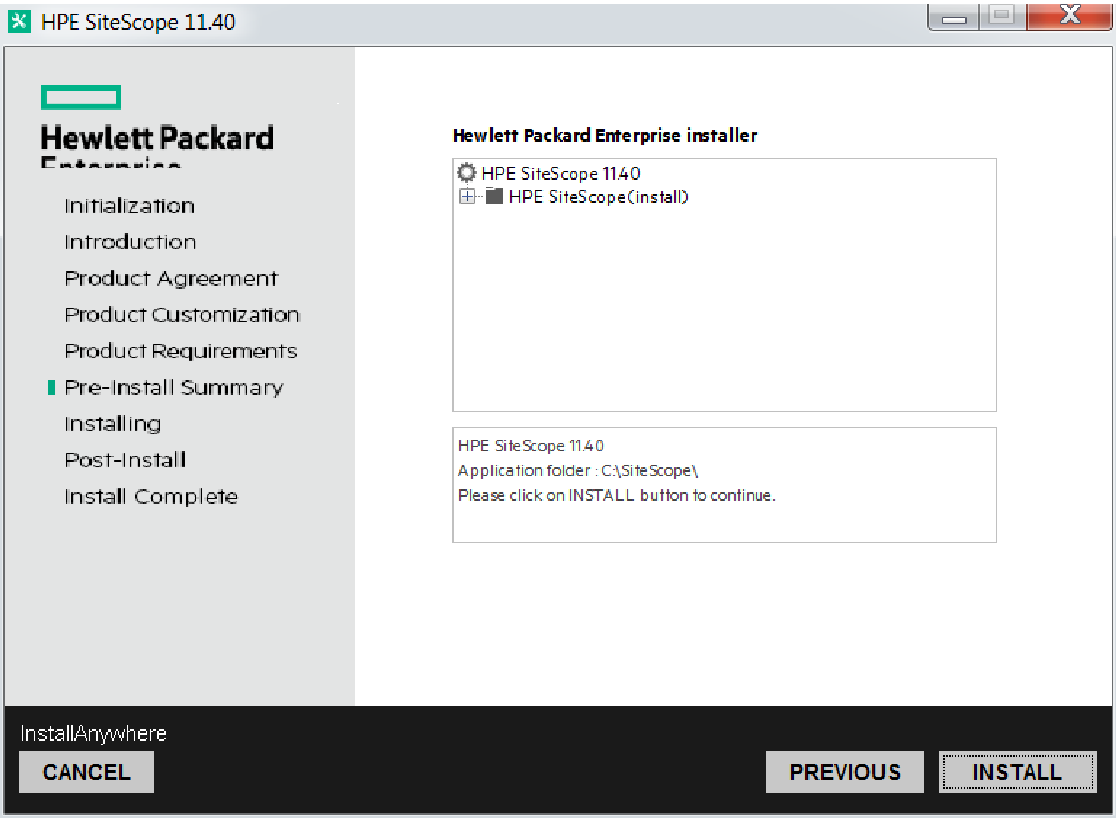
Checking for previous installations...
- Passed

10. 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. On the Pre-Install Summary screen, click **Install**.

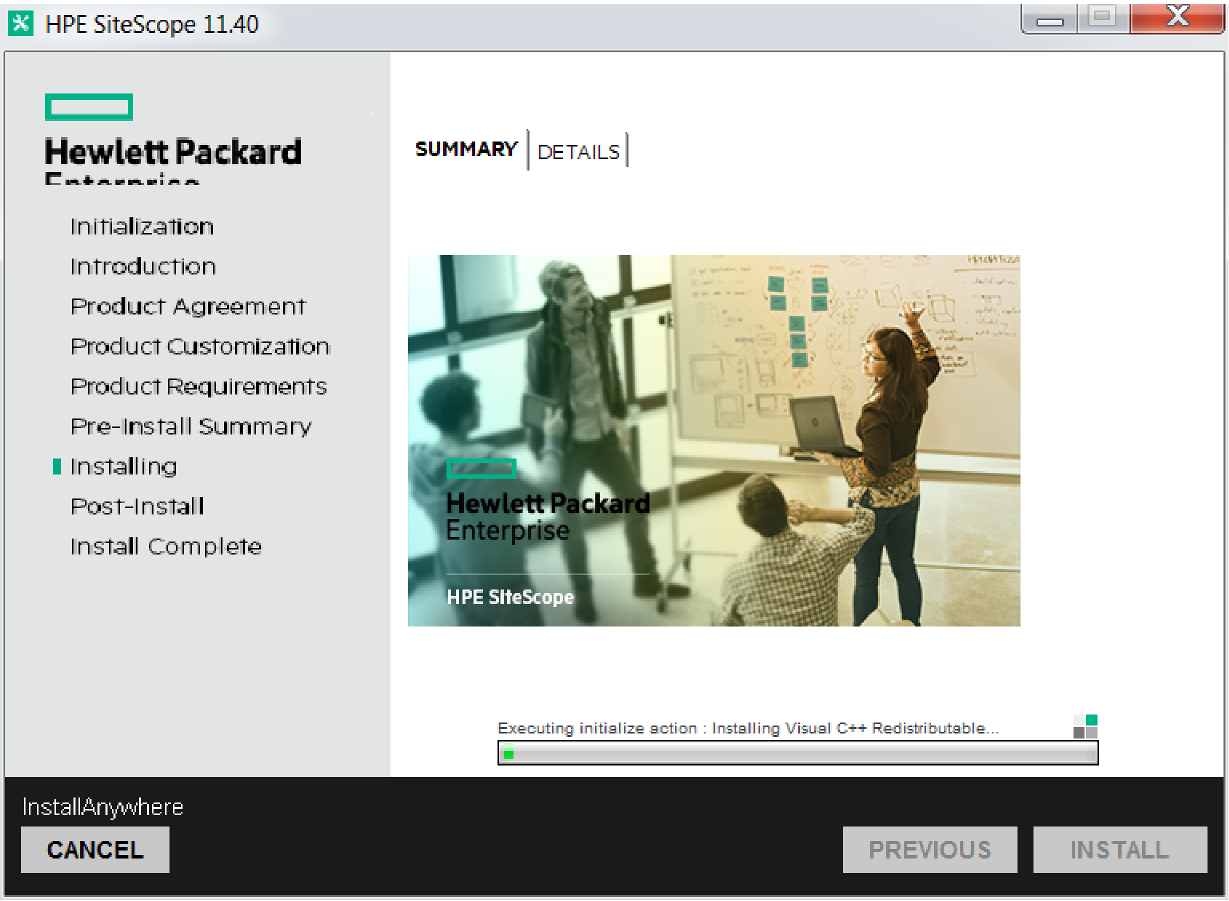


Hewlett Packard Enterprise installer

HPE SiteScope 11.40
HPE SiteScope(install)

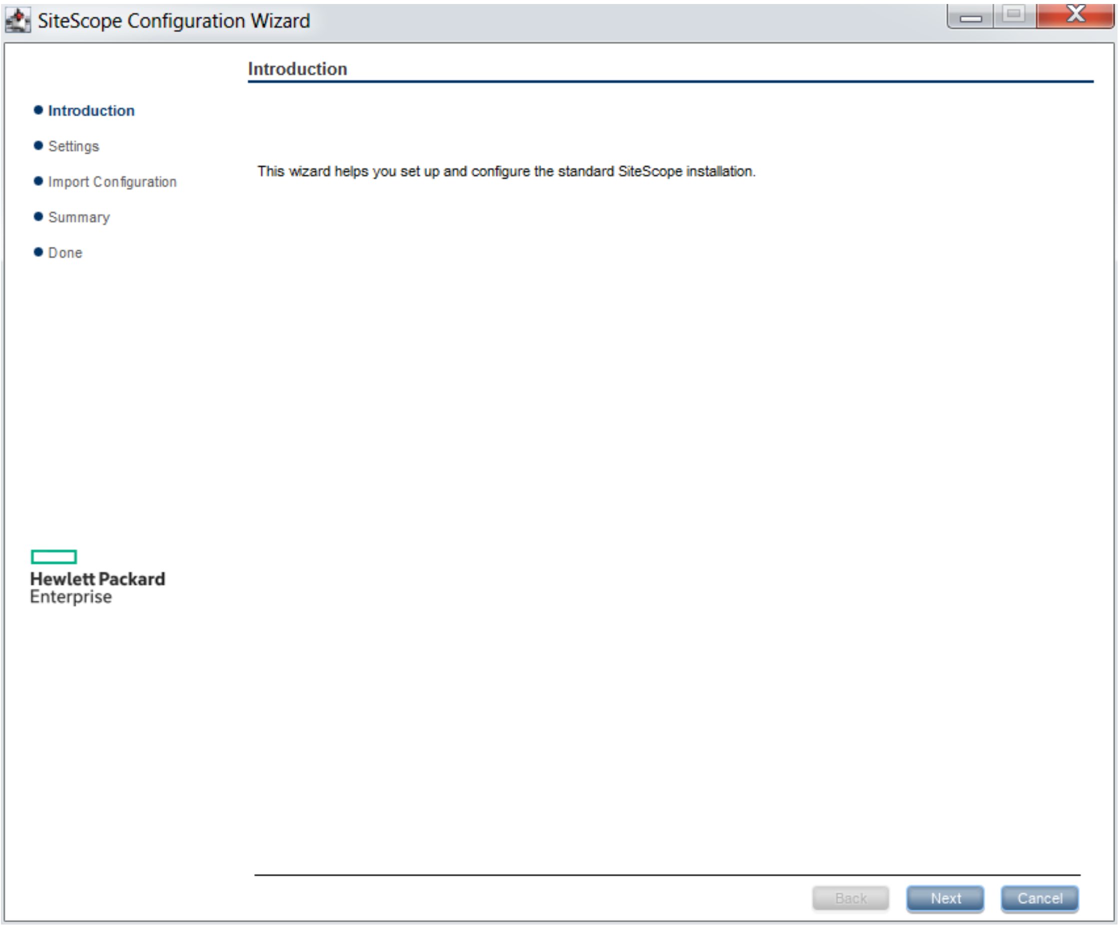
HPE SiteScope 11.40
Application folder : C:\SiteScope\
Please click on INSTALL button to continue.

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.



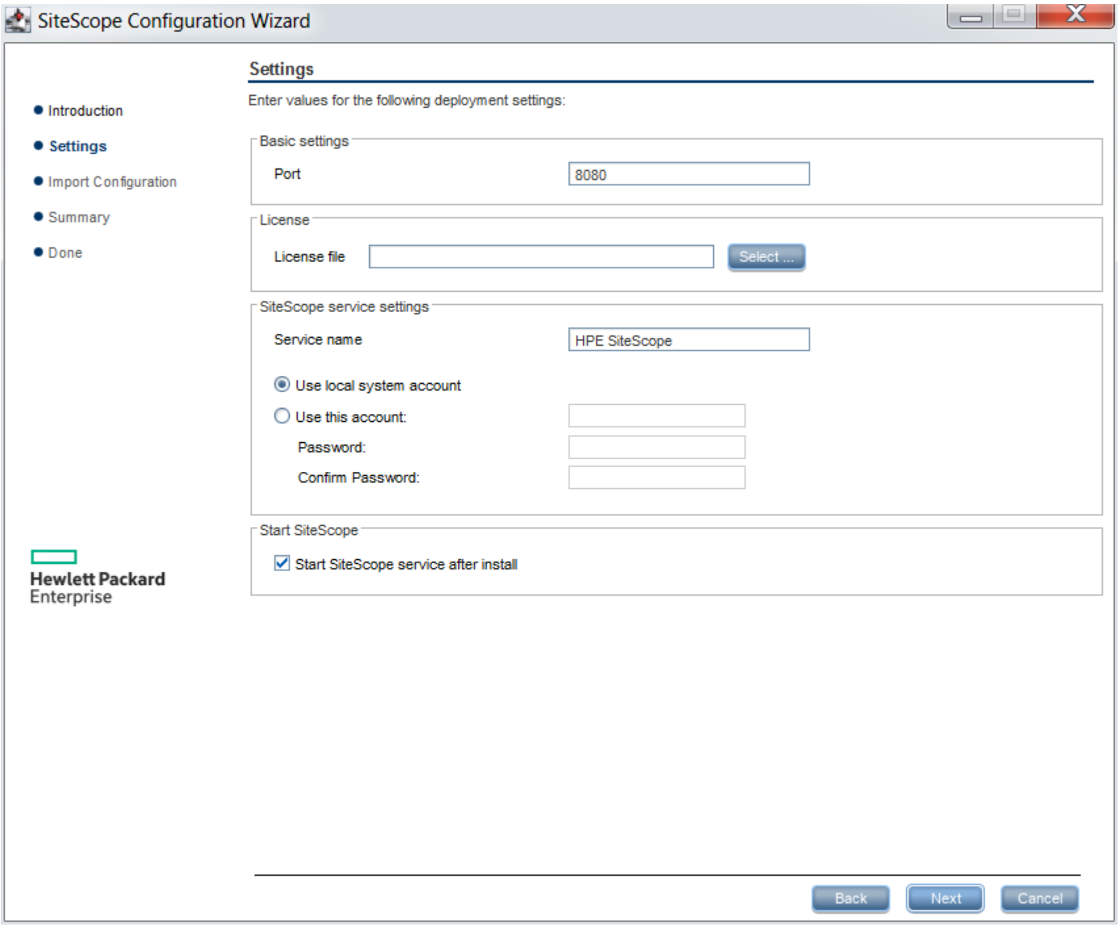
Executing initialize action : Installing Visual C++ Redistributable...

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



This wizard helps you set up and configure the standard SiteScope installation.

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



Settings

Enter values for the following deployment settings:

Basic settings

Port: 8080

License

License file:

SiteScope service settings

Service name: HPE SiteScope

● Use local system account

○ Use this account:

Password:

Confirm Password:

Start SiteScope

☑ Start SiteScope service after install

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`.
- **License file.** Enter the path to the license file, or click **Select** and select the SiteScope license key file. It is not necessary to enter license information at this point, since the SiteScope Community edition license is activated automatically after a regular SiteScope installation. To extend SiteScope functionality beyond the limited features included in Community edition, you need to purchase a commercial edition license (see "Upgrading the SiteScope Edition License" on page 1).

- **Use local system account** (not applicable for 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 system account, it attempts to connect to remote servers using credentials of the server as configured in SiteScope.

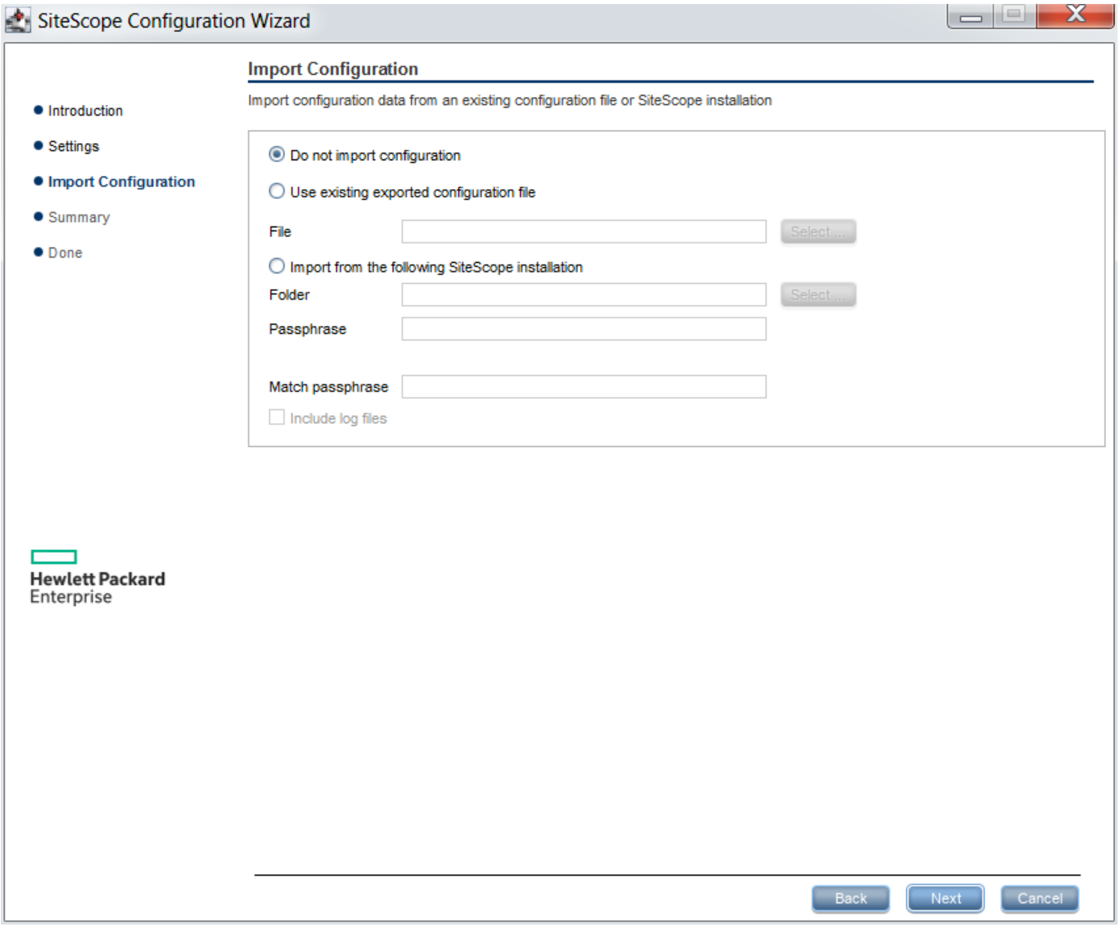
  > **Note:** We recommend setting the SiteScope service to log on as a user with domain administration privileges since the local system account may not have sufficient privileges (the local system account has domain administrator user privileges in a domain environment, and build-in administrator user privileges in a non-Domain environment).

- **Use this account** (not applicable for 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 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 Linux installations). Automatically starts the SiteScope service after the installation is complete.

14. The Import Configuration screen opens, enabling you to import existing SiteScope configuration data to the new SiteScope installation.



Import Configuration

Import configuration data from an existing configuration file or SiteScope installation

● Do not import configuration

○ Use existing exported configuration file

File

○ Import from the following SiteScope installation

Folder

Passphrase

Match passphrase

□ Include log files

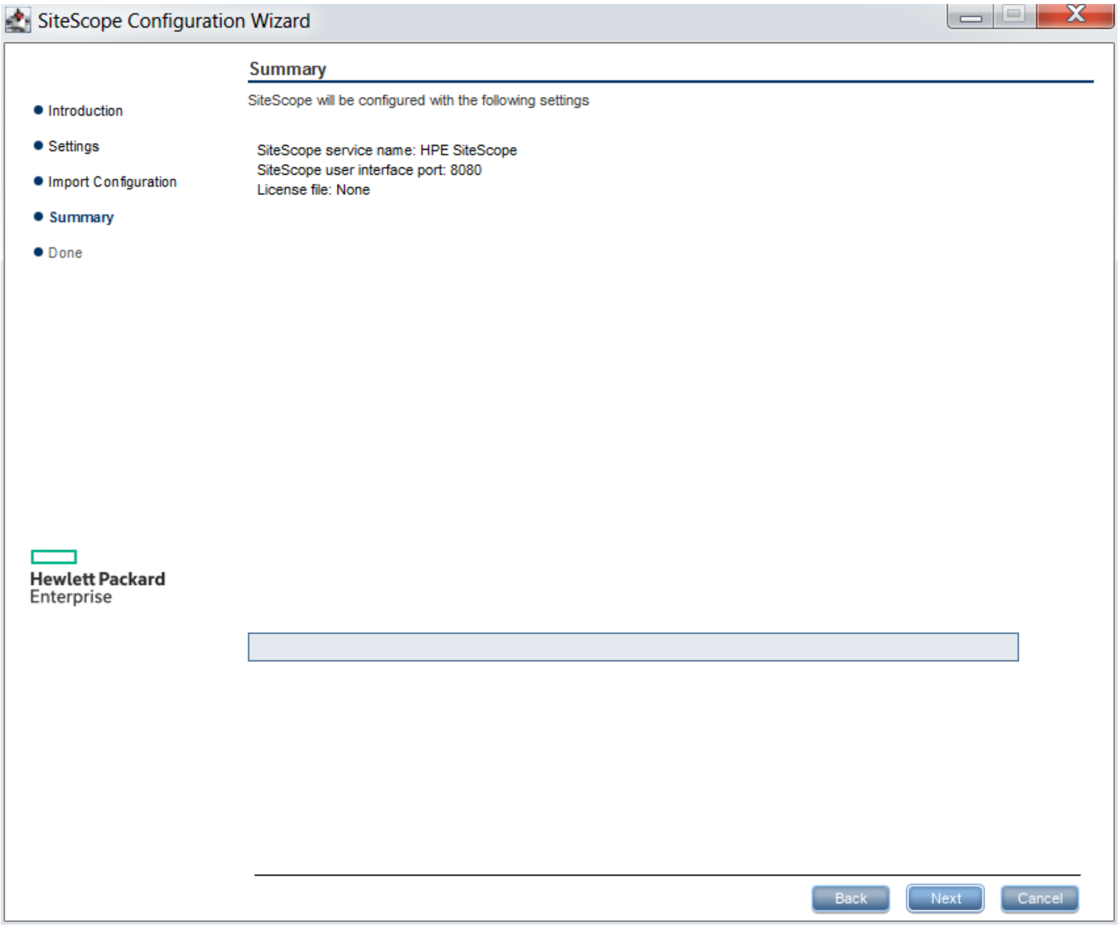
Select one of the following options and click **Next**:

- **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.

- If SiteScope was configured to run using key managed encryption, enter the passphrase for the SiteScope server KeyStore in the **Passphrase** box. Confirm the passphrase in the **Match passphrase** box. For details, see "Configure SiteScope to Use a Custom Key for Data Encryption" on page 153. These boxes are disabled when the default SiteScope encryption is used.

> **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.
> - If the imported configuration contains expired certificates, they will be merged inside the default SiteScope KeyStore on configuration import. This can result in the SSL Certificate monitor being in error state. To avoid this, you should delete any expired certificates before exporting configuration data.

15. 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.

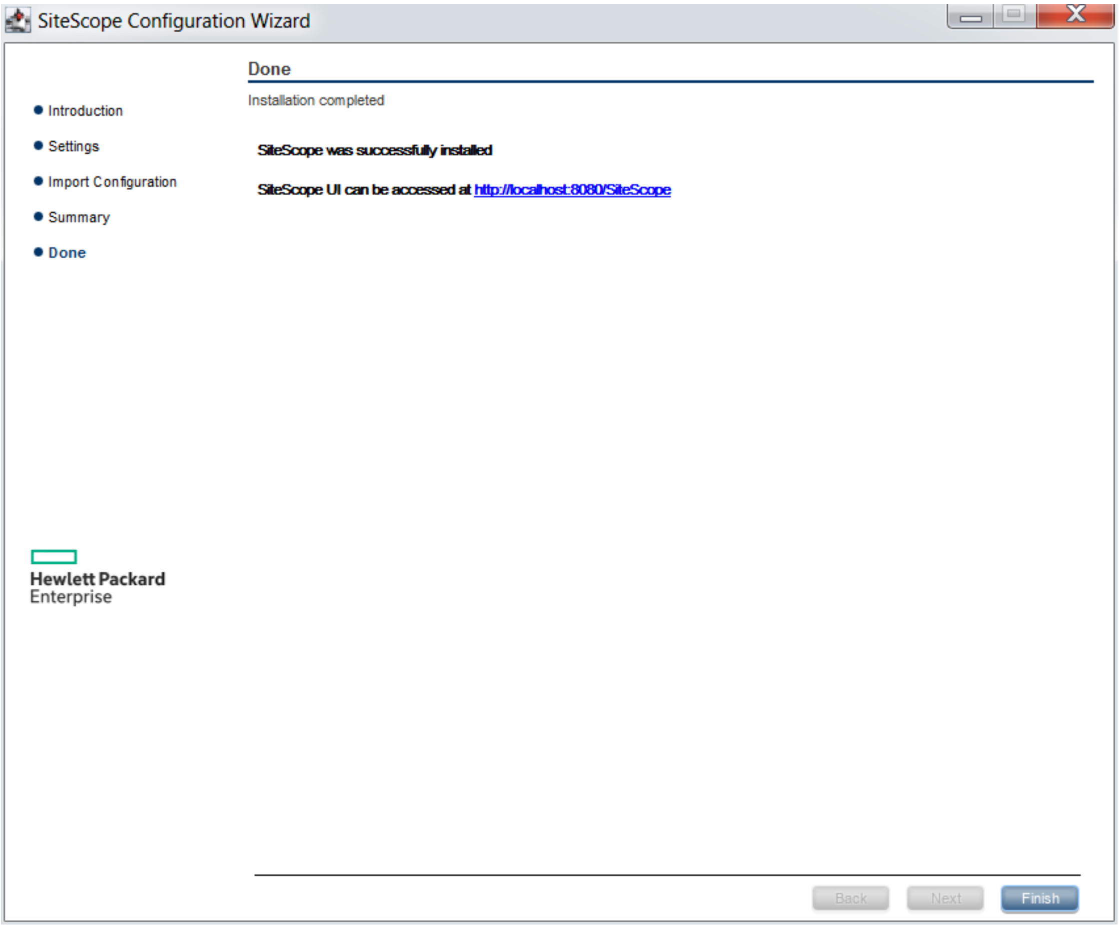


Summary

SiteScope will be configured with the following settings

SiteScope service name: HPE SiteScope
SiteScope user interface port: 8080
License file: None

16. The Done screen opens.



Done

Installation completed

SiteScope was successfully installed

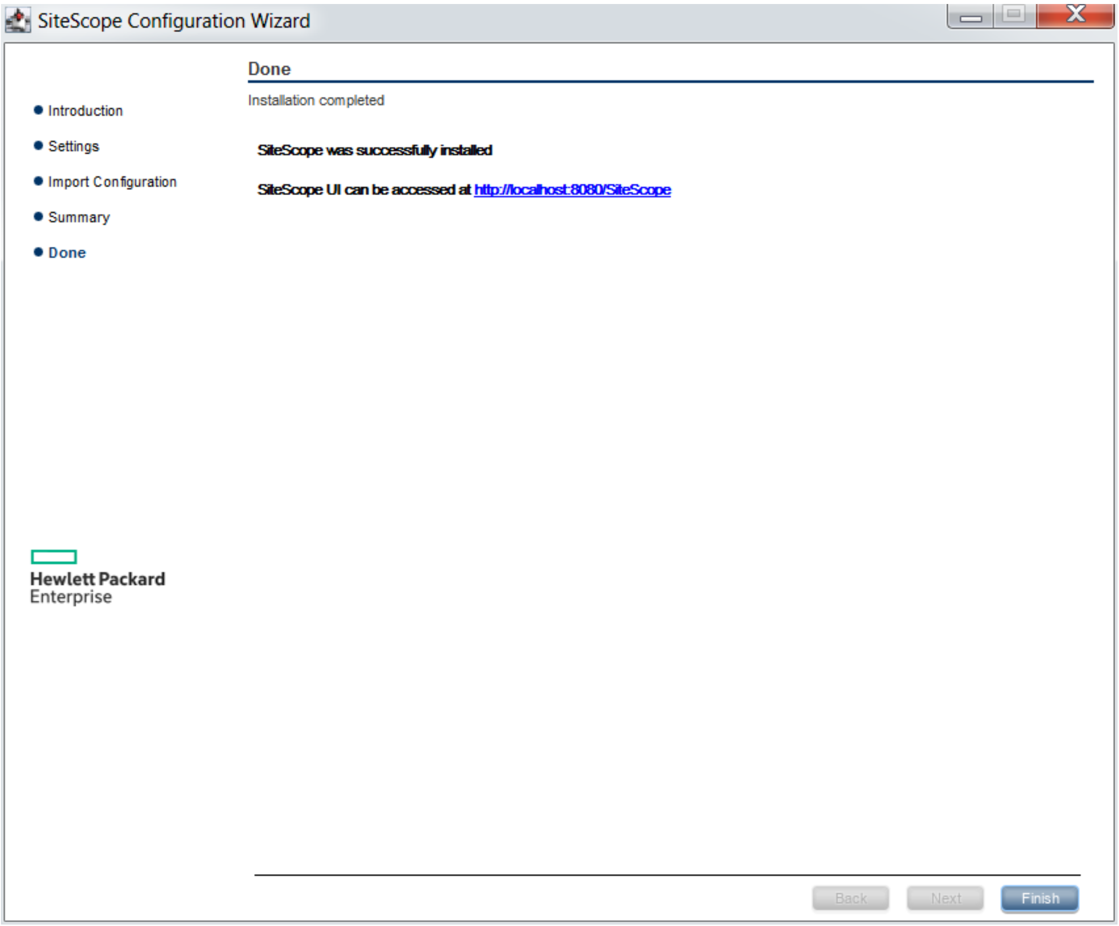
SiteScope UI can be accessed at http://localhost:8080/SiteScope

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 207.

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

17. When the installation finishes, the Installation Complete window opens displaying a summary of the installation paths used and the installation status.



Done

Installation completed

SiteScope was successfully installed

SiteScope UI can be accessed at http://localhost:8080/SiteScope

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.

18. For the latest available functionality, download and install the latest SiteScope patch (if available) from the same location from which you installed SiteScope. For information on accessing the SiteScope interface, see "Connecting to SiteScope" on page 209.

19. After installing SiteScope on a Linux 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.

Install 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 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 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 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 9: Install on Linux Using Console Mode

You can install SiteScope on Linux 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:** The option to install the Operations Agent was removed from SiteScope console mode. Instead, you must manually install and configure the agent. The agent is required for sending events and storing metrics data if SiteScope is integrated with OM or APM (except when graphing metrics data to Performance Graphing using the profile database in APM). For details on installing and configuring the agent, see the Integrating SiteScope with Operations Manager Products Guide available in the SiteScope Help or on the HPE Software Integrations site.

To install SiteScope on Linux using the console mode:

1. Download the installer package (**SiteScope_11.40_Linux.zip**) 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.

   SiteScope is available via HPE Systems as follows:

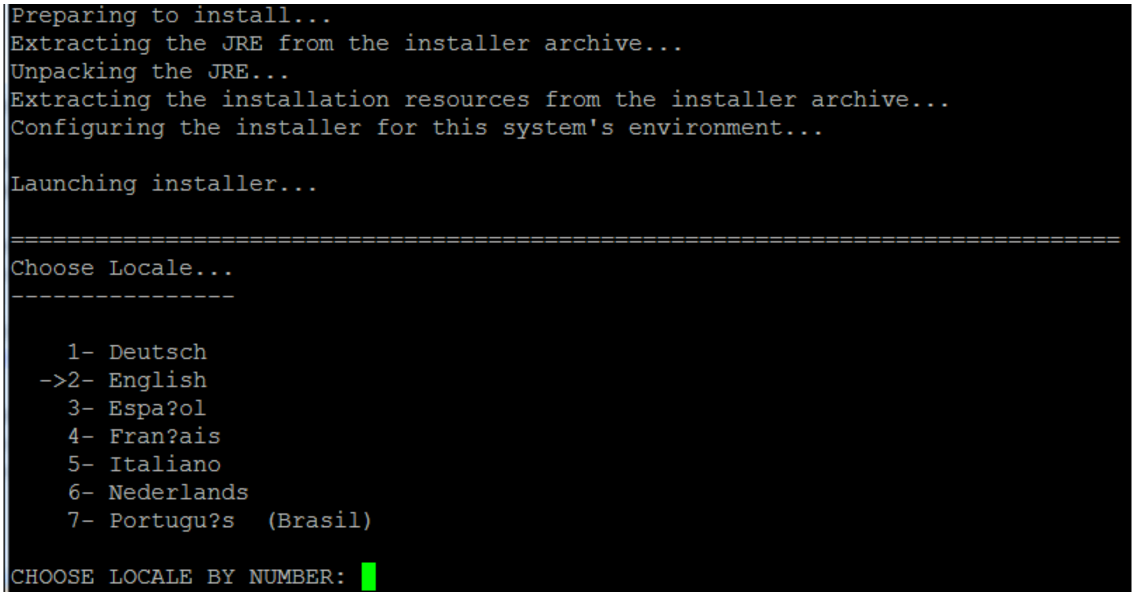
Customer	Download Options
For Evaluating Customers	Link for electronic download evaluation HPE Software Partner Central for HPE Authorized Software Partners (The above links require HPE Passport accounts. Register for an HPE Passport at http://h20229.www2.hpe.com/passport-registration.html.)
For New Customers	Electronic Software Download. Customer receives a link via email where the software can be downloaded; this link is specific to the order.

Customer	Download Options
For Existing Customer Updates	https://h20575.www2.hpe.com/usbportal/softwareupdate.do **Prerequisites:** a. You need an HPE Passport account to access the above link, and a Support Agreement ID (SAID) to receive updates through the SSO Portal. To register for an HPE Passport, see http://h20229.www2.hpe.com/passport-registration.html. For details on activating your SAID, see the FAQ on the Software Support Online site. b. A new license key is required for the software upgrade. Contact your HPE support renewal rep to request product contract migration first. Once contract migration is completed, go to the My Software Updates portal (https://h20575.www2.hpe.com/usbportal/softwareupdate.do) and click the **Get Licensing** tab to get the new license key(s). **To download software updates:** a. Select **My software updates**. b. Expand **Application Performance Management**, select the HPE SiteScope 11.40 Software E-Media you require, and click **Get software updates**. c. In the Selected Products tab, click **Get Software** for the product update (s) you want, and follow the instructions on the site to download the software.

2. Run the following command:

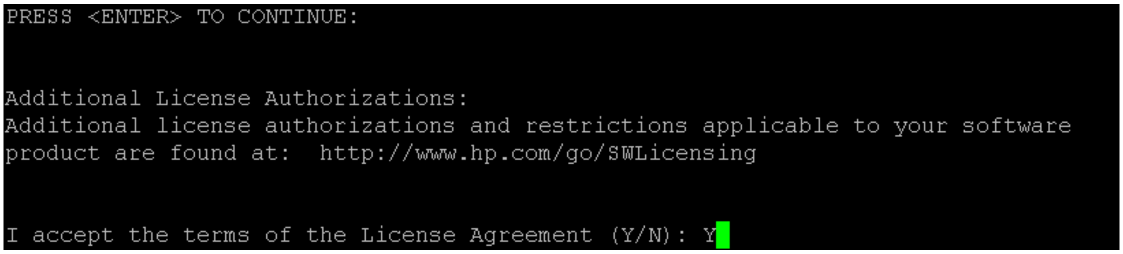
Example:
```
HPSiteScope_11.40_setup.bin -i console
```

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

Launching installer...

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

    1- Deutsch
  ->2- English
    3- Espa?ol
    4- Fran?ais
    5- Italiano
    6- Nederlands
    7- Portugu?s  (Brasil)

CHOOSE LOCALE BY NUMBER: 
```

3. Enter the number to select the desired locale, and press ENTER to continue. A confirmation screen is displayed. Press ENTER to continue. The Introduction screen is displayed.
4. Press ENTER to continue with the installation. 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.
5. When you have viewed all the pages of the license agreement, you have the option to accept or not accept the license agreement.

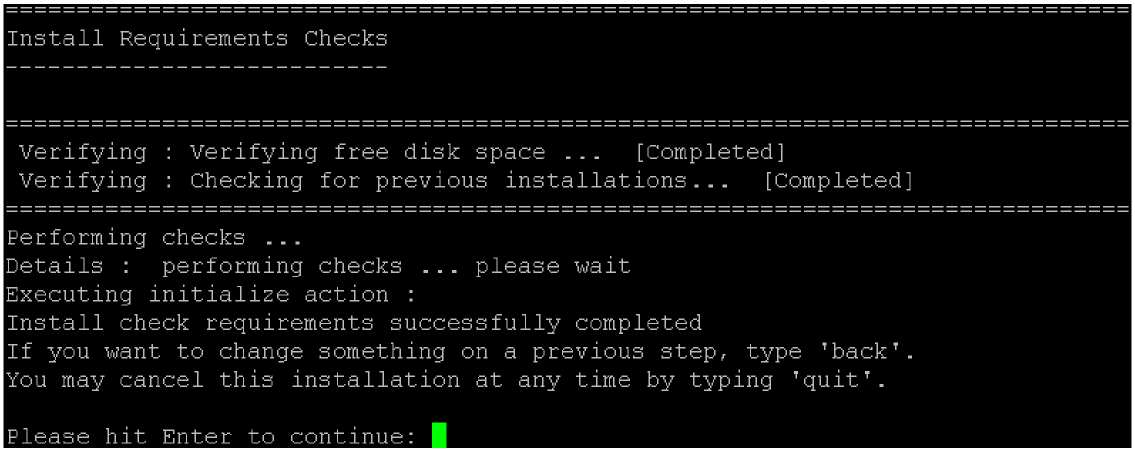
   ```
   PRESS <ENTER> TO CONTINUE:


   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.

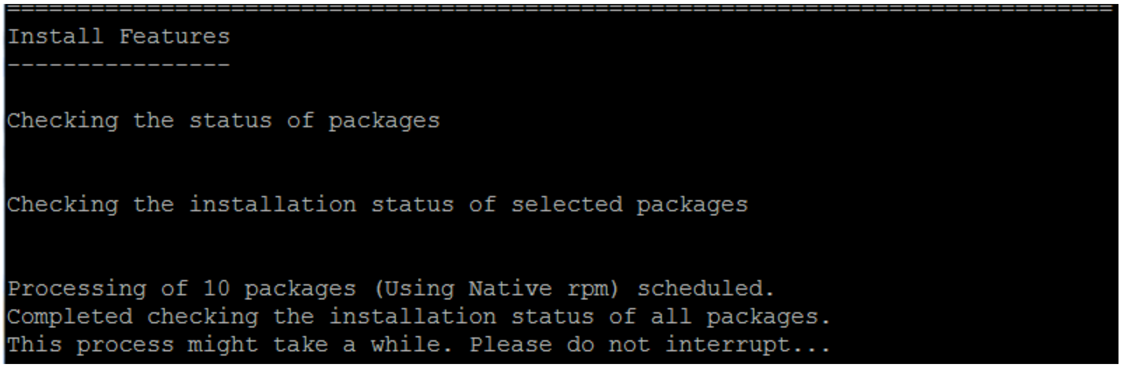
   The setup type screen opens.
6. Choose the type that is suitable for your site. Enter the number of the setup type, and then press ENTER to continue. The Select Features screen opens.

7. Enter the number `1` (required) to install SiteScope.
   Press `ENTER` to continue with the installation. 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:
```

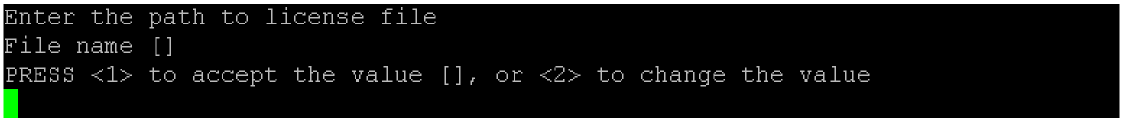
8. Press `ENTER` to continue with the installation. The Pre-Installation Summary screen opens.
9. Press `ENTER` to continue with the installation. The Install Features screen opens and the installation process starts.



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

Checking the status of packages


Checking the installation status of selected packages


Processing of 10 packages (Using Native rpm) scheduled.
Completed checking the installation status of all packages.
This process might take a while. Please do not interrupt...
```

10. When the installation process is complete, the post-installation configuration screen opens. The port prompt is displayed.
11. 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.

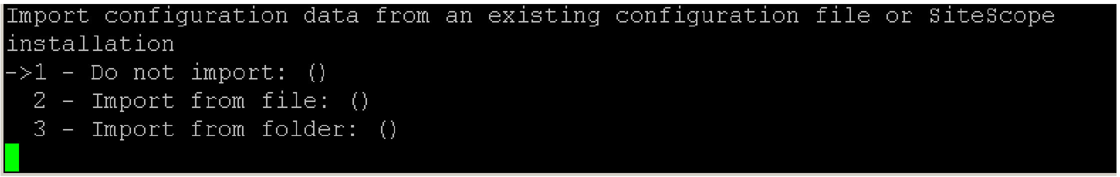
    Press `ENTER` to continue with the installation. The license file path prompt is displayed.



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

12. 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 since the SiteScope Community edition license is activated automatically after a regular SiteScope installation), or enter the number `2`, and then enter the license file path in the next text box.

    Press `ENTER` to continue with the installation. 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: ()
```

13. 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.

    If SiteScope was configured to run using key management data encryption, when prompted, enter the passphrase for the SiteScope server KeyStore, and confirm the passphrase by entering it again. For details, see "Configure SiteScope to Use a Custom Key for Data Encryption" on page 153.

    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.
    > - If the imported configuration contains expired certificates, they will be merged inside the default SiteScope KeyStore on configuration import. This can result in the SSL Certificate monitor being in error state. To avoid this, you should delete any expired certificates before exporting configuration data.

14. 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.

15. 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 15.

16. To connect to SiteScope, follow the steps in the section "Starting and Stopping the SiteScope Process on Linux Platforms" on page 208.

Chapter 10: Install SiteScope in Silent Mode

This chapter includes:

- "Silent Installation Overview" below
- "Run a Silent Installation" below
- "Uninstall SiteScope in Silent Mode" on page 129

Silent Installation Overview

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_11.40** on Windows platforms
  - **/tmp/HPOvInstaller/HPSiteScope_11.40** on 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).
- The option to install the Operations Agent directly from within SiteScope was removed. Instead, you must manually install and configure the agent. The agent is required for sending events and storing metrics data if SiteScope is integrated with OM or APM(except when graphing metrics data to Performance Graphing using the profile database in BSM). For details on installing and configuring the agent, see the Integrating SiteScope with Operations Manager Products Guide available in the SiteScope Help or on the HPE Software Integrations site.

Run a Silent Installation

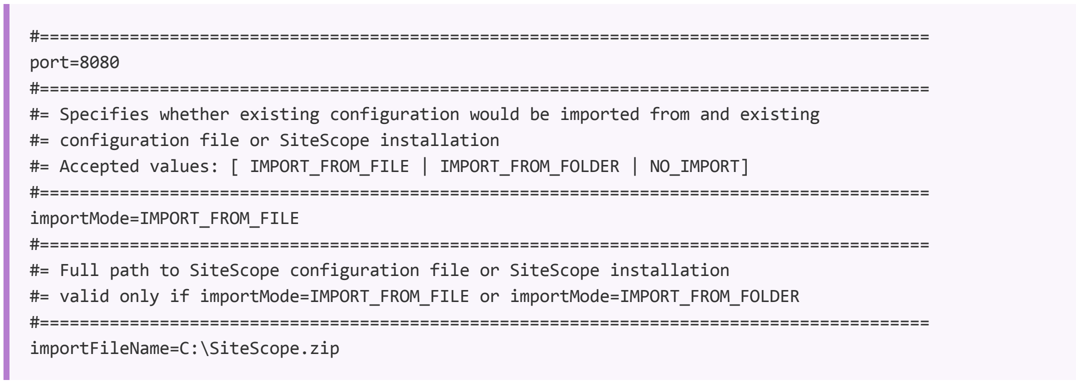
You can run a silent installation using the **ovinstallparams.ini** file. If you have already installed SiteScope, a sample **ovinstallparams.ini** file is available from the **<SiteScope installation directory>\examples\silent_installation** folder.

How to create the ovinstallparams.ini file manually:

1. Create a text file, and save it with an ini suffix.
2. Copy the following text to the file, and customize it as necessary:

Example:

```
#=========================================================================================
#= Sample ovinstallparams.ini file
#= To install SiteScope in non-interactive (silent) mode, edit this file according
#= to your needs and place it in the same folder where HPESiteScope_11.40_setup.exe file and
#= "packages" folder are.
#=
#= For silent installation, run the installer with "-i silent" flag
#= Example: HPESiteScope_11.40_setup.exe -i silent (Windows)
#=          HPESiteScope_11.40_setup.bin -i silent (Unix)
#=
#= Note: We do not recommend changing the installer properties parameters that follow.
========================================================================================
[installer.properties]
setup=HPESiteScope
licenseAgreement=true
#=========================================================================================
#= The following 2 keys specify the installation flavor:
#=
#= 1) For Standard (standalone) HPE SiteScope installation:
#= group=Standalone
#= customFeatureSelected=StandaloneFeature
#= 2) For HPE SiteScope Failover installation:
#= group=Failover
#= customFeatureSelected=HAFeature
#= 3) For HPE System Health Installation:
#= group=SystemHealth
#= customFeatureSelected=SystemHealthFeature
#= 4) For HPE SiteScope for LoadRunner installation (on Windows only)
#= group=LoadRunner
#= customFeatureSelected=LoadRunnerFeature
#=========================================================================================
group=Standalone
customFeatureSelected=StandaloneFeature
#=========================================================================================
#= [Windows only] Installation folder. The path cannot contain spaces and must end with
#=                "SiteScope". Note: On Unix systems, SiteScope installation folder is set
#=                to "/opt/HP/SiteScope" and cannot be changed
#=========================================================================================
prodInstallDir=C:\SILENT\SiteScope\
#=========================================================================================
#= [Windows only] The name of SiteScope service
#=========================================================================================
serviceName=SiteScopeService
#=========================================================================================
#= [Windows only]. Specifies whether SiteScope service would be started automatically
#=                 after installation ends
#= Accepted values: [ yes | no ]
#=========================================================================================
startService=yes
#=========================================================================================
#= Specifies the path to license file
#=========================================================================================
licenseFile=c:\SiteScopeLicenses.txt
#=========================================================================================
#=SiteScope user interface port
```



```
#========================================================================================
port=8080
#========================================================================================
#= Specifies whether existing configuration would be imported from and existing
#= configuration file or SiteScope installation
#= Accepted values: [ IMPORT_FROM_FILE | IMPORT_FROM_FOLDER | NO_IMPORT]
#========================================================================================
importMode=IMPORT_FROM_FILE
#========================================================================================
#= Full path to SiteScope configuration file or SiteScope installation
#= valid only if importMode=IMPORT_FROM_FILE or importMode=IMPORT_FROM_FOLDER
#========================================================================================
importFileName=C:\SiteScope.zip
```

How to run a silent installation for SiteScope 11.40:

1. Navigate to the **ovinstallparams.ini** file.
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_11.40_setup.exe** or **HPSiteScope_11.40_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_11.40_setup.exe -i silent` (Windows)

   `./HPSiteScope_11.40_setup.bin -i silent` (Linux)

Uninstall SiteScope in Silent Mode

How to uninstall SiteScope 11.40 (and all minor-minor or patch versions, if any) in silent mode:

1. Stop the SiteScope service.
2. Run the command:
   - For Windows:

     `%SiteScopeHome%/installation/bin/uninstall.bat -i silent`
   - For Linux:

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

Part 3: Configure Security

Chapter 11: Hardening the SiteScope Platform

This chapter includes:

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.

Set 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.

Use 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 "Configure SiteScope to Communicate Over a Secure Connection" on page 138.

> **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.

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. There are different types of smart cards that can be used with SiteScope, which include:

- **CAC.** The Common Access Card (often called CAC card), is a smart card that it is used by the US Department of Defense. This smart card is required to do any work on government systems in the military.
- **PIV.** Like their military counterparts, Federal employees and contractors within civilian agencies also need smart cards. They use a similar standard known as a PIV card (Personal Identification Verification). The cards are slightly different from CACs, and have varying information printed on them, depending on the issuing agency. They use a different set of CA (Certificate Authority) servers than the ones that CACs use. The PIV card is personalized with data needed by the PIV system to grant access to the subscriber to Federal facilities and information systems; assure appropriate levels of security for all applicable Federal applications; and provide interoperability among Federal organizations using the standards.

For details on configuring smart card authentication, see "Configure Smart Card Authentication" on page 138.

Note: There are many different smart card vendors that exist in the market. To support all the different permutations for using client certificates, you can use the following parameters in the **<SiteScope root>\groups\master.config** file:

- _clientCertificateAuthJITCComplianceEnforcementEnabled
- _clientCertificateAuthSmartCardEnforcementEnabled
- _clientCertificateAuthIsGetUidFromSubject
- _clientCertificateAuthAllowLocalUsers
- _clientCertificateSubjectAlternativeNamesGeneralName
- _clientCertificateAuthEnabled

Joint Interoperability Test Command (JITC) Certification

JITC is a United States military organization that tests technology that pertains to multiple branches of the armed services and government. JITC provides test, evaluation, and certification services for acquiring and deploying of global “net-centric” military capabilities.

SiteScope is currently undergoing JITC testing and evaluation. JITC certification is one of the Common Criteria certifications required for supporting CAC and smart card authentication login.

Note: This section will be updated when the evaluation process has been completed.

Common Criteria Certification

HPE SiteScope is committed to providing industry-leading monitoring software that meets global industry standards and government certification programs.

HPE SiteScope has been evaluated under the terms and conditions of the Canadian Common Criteria Scheme and complies with the requirements for Common Criteria Recognition Agreement (CCRA). SiteScope has achieved the Common Criteria certification with Evaluation Assurance Level (EAL) 2+. Certifications like Common Criteria are fundamentally important to federal government security measures. In addition to protecting government customers from today’s advanced attacks and data theft, these security certifications also supports the needs of HPE's global business customers as well.

The Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria) is an international standard for computer security certification. Common Criteria is validation that the product does what is promised, and is built in a manner that is both secure and stable. Results are verified by and evaluated by independent testing laboratories. It is also a requirement by the U.S. government for federal purchases of security products.

FIPS 140-2 Compliancy

As part of Common Criteria certification, SiteScope can be configured to operate in FIPS 140-2 compliant mode. FIPS 140-2, or Federal Information Processing Standard 140-2 is a set of security requirements for cryptographic modules. FIPS 140-2 is overseen by CMVP (Cryptographic Module Validation Program) which is a joint effort mandated by both the United States and Canadian governments.

SiteScope 11.40 is the only version of SiteScope at this time that can be configured to work in FIPS 140-2 compliant mode.

For details on FIPS 140-2 and configuring SiteScope to operate in FIPS 140-2 compliant mode, see "Configure SiteScope to Operate in FIPS 140-2 Compliant Mode" on page 145.

Encrypt Data Using a Custom Key

By default, SiteScope uses a standard encryption algorithm to encrypt the persistency data (this includes configuration data of all defined monitors, groups, alerts, templates, and many other SiteScope entities). You can use Key Management in the Hardening Tool to change the cryptographic keys that are used for encrypting the persistency data.

For details, see "Configure SiteScope to Use a Custom Key for Data Encryption" on page 153.

Recommendations for Securing User Accounts

The following table lists the various accounts available in SiteScope and the steps that can be taken to secure these accounts.

User Account	Description	Hardening Steps
Default (Administrator)	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.	To restrict access to this account and its privileges, we recommend editing the Administrator account profile to include a user login name and login password after installing and accessing the product. SiteScope then displays a login page before SiteScope can be accessed. You should create other user account profiles to control how other users may access the product and what actions they can perform. For more information, see the User Management Preferences section in Using SiteScope in the SiteScope Help. **Note:** To create other accounts, you must first edit the Administrator account profile to include a user login name and password.
Integration Viewer	By default, SiteScope provides an Integration Viewer user that is used for drilling down from OM events. This is a regular user that has been granted view permissions, and permissions to refresh groups and monitors. For more details, see Integrating SiteScope with Operations Manager Products.	If you have an OM or APM integration, we recommend changing the predefined login password for the Integration Viewer account profile. If you do not have an OM/APM integration, you can disable or delete this user.

User Account	Description	Hardening Steps
SiteScope Service User	**For Windows:** By default, SiteScope is installed to run as a local system account (not applicable for Linux installations). This account has extensive privileges on the local computer, and has access to most system objects. When SiteScope is running under a local system account, it attempts to connect to remote servers using credentials of the server as configured in SiteScope. **For Linux:** SiteScope must be installed on a Linux environment by the root user.	**For Windows:** We recommend setting 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. In a domain environment, use the domain administrator user; in a non-domain environment use the built-in administrator user. You can change this setting during installation time (see"Install Using the Installation Wizard" on page 103), or after SiteScope is installed (see the Configure SiteScope to Monitor Remote Windows Servers section in Using SiteScope in the SiteScope Help). **For Linux:** 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 "Recommendations for Securing User Accounts" on page 134.

User Account	Description	Hardening Steps
JMX User	JMX has remote access to the SiteScope server by default (the connection using the JMX protocol can be configured using the Hardening Tool).	To fully secure SiteScope, it is recommended that you disable JMX remote access by using the Hardening Tool. For details, see "How to Use the Hardening Tool to Configure JMX Remote Access" on page 167.
API User	Generally there is no such a user (SiteScope has a number of APIs that do not require authentication).	If you need to disable old unused API users, you can do so by setting **Disable old APIs** to `true` in **Preferences > Infrastructure Preferences > Custom Settings**.

Configure a Warning Banner to be Displayed on Login

You can enable SiteScope to display a warning message to users when they log on to SiteScope that they are about to log in to a secure system. The property `_isAllowedHTMLTagsInBannerMessage` is added to support HTML tags.

To configure a message to be displayed on login:

1. Open the **<SiteScope root directory>\templates.fips\banner.template** file in a text editor, and enter the text that you want to be displayed in the login screen.
2. Open the **<SiteScope root directory>\groups\master.config** file in a text editor, and set `_isLogonWarningBannerDisplayed= true`.
3. (optional) Set the parameter `isAllowedHTMLTagsInBannerMessage = true` if you want to support HTML tags. When set to "true", the message is formatted as per the HTML tags.

   By default, the parameter `isAllowedHTMLTagsInBannerMessage = false`. The HTML tags are not supported and if any markup character sequences are used in the banner.template file, the whole message string is escaped and displayed as markup code instead of formatted text, and no code is executed. An error message is logged to the error.log file. The only exception is <br> tag which can be used to separate message lines along with regular line breaks.
4. Restart SiteScope (required after making any changes to the **master.config** file).

   Whenever a user logs on to SiteScope, the notification message is displayed. The user must confirm the message before being able to use SiteScope.

Chapter 12: Configure SiteScope to Communicate Over a Secure Connection

This chapter includes:

- "Configure SiteScope to Require a Secure Connection" below
- "Configure Smart Card Authentication" below
- "Configure SiteScope to Verify Certificate Revocation" on page 141

Configure 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 161.
- Manually configuring SiteScope to use TLS. For details, see "Manually Configuring SiteScope for Using a Secure Connection" on page 231.

Configure 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 APM and you want to integrate SiteScope with APM, you must configure SiteScope smart card authentication to authenticate the APM client certificate. For details, see "Configure SiteScope to Connect to an APM Server That Requires a Secure Connection" on page 157.

Similarly, if SiteScope is configured for smart card authentication and you want to allow APM to communicate with SiteScope, you must first configure APM to authenticate with the client certificate in SiteScope. For details, see "Configure SiteScope to Connect to an APM Server That Requires a Secure Connection" on page 157.

> **Example: 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 141.

> **Tip:** For more information about smart cards, see the Smart Card Authentication Configuration Guide (https://softwaresupport.hpe.com/group/softwaresupport/search-result/-/facetsearch/document/KM01134341).

Configure SiteScope to Require Client Certificate Authentication

If you have configured SiteScope to work over TLS (see "Configure 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 166.

Configure SiteScope to be accessible using the Reverse Proxy Server

SiteScope can be configured to be accessible by a reverse proxy server. The configuration is supported for environments where

- A single instance of SiteScope resides behind the secured reverse proxy server
- Multiple instances of SiteScope resides behind the secured reverse proxy server. The number of SiteScope instances that can reside behind the proxy server depend on the number of available ports.

Prerequisites

Ensure the following are met to configure reverse proxy server for SiteScope:

- Configure SiteScope to work over SSL (https)
- Map the SSL-enabled SiteScope default port 8443 to the reverse proxy server's port 8443. This enables to access SiteScope UI using the reverse proxy server using

https://<reverseproxy>:8443/SiteScope.

- Map the SiteScope port 8899 to the reverse proxy server’s port 8899. This enables to generate quick reports when accessing SiteScope UI using the reverse proxy server.

  For environments where multiple SiteScope instances reside behind the reverse proxy server:

- All SiteScope instances must be configured for SSL
- Map any one instance of SiteScope default port 8443 to reverse proxy server's port 8443. Also map the same instance's port 8899 to the reverse proxy server's port 8899 to generate quick reports using the reverse proxy.
- Map any other instance of SiteScope port 8444 to the reverse proxy port 8444. Also map the same instance's port 8898 to the reverse proxy port 8898 to generate quick reports using the reverse proxy.
- You can use the remaining available ports for other configurations in your environment as required.

Chapter 13: Advanced Hardening Configuration

This chapter includes:

Configure 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 162.

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** > **Certificates** > **View Certificates**. The Certificate Manager dialog box opens.
   b. Click **Import...** and open your personal certificate in **.p12** (or **.pfx**) 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.

Import 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 163.

Enable JMX Remote Access

By default, JMX remote access to the SiteScope server is disabled. You can enable the 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 167.

Restore 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 168.

Configuring Framing Filters in SiteScope

A frame is a part of a web page or browser window which displays content independent of its container, with the ability to load content independently. Framing of SiteScope is enabled by default.

If you do not want other sites to be able to frame SiteScope, or you want to allow partial framing only, you must perform the following:

1. Open the **master.config** file in **<SiteScope root directory>\groups**, and configure the **_disableFramingFiltering** property as required:
   - **True.** Filter is disabled which allows SiteScope to be framed from every web page. (This is the default setting.)

- **False.** Filter is enabled which prevents SiteScope being framed from web pages, including HPE products such as APM, OM, and Performance Center. For example, APM's hosted user interface will not work.
- **Smart.** Enables partial framing of SiteScope according to the plugs listed in the **_framingFilteringPlugsClasses** property.

2. When using partial framing, create plugs that you want applied by the filter, and add them to the **_framingFilteringPlugsClasses** property.

   a. Navigate to the **_framingFilteringPlugsClasses** property in the **master.config** file. By default, this property includes the following out-of-the-box plugs:

      - `com.mercury.sitescope.web.request.framing.plugs.LWSSOPlug`. Allows requests sent with a Lightweight Single Sign-On (LW-SSO) token.
      - `com.mercury.sitescope.web.request.framing.plugs.BSMPlug`. Allows requests sent from APM's SAM Administration.
      - `com.mercury.sitescope.web.request.framing.plugs.PerformanceCenterPlug`. Allows requests from Performance Center.

      You can disable any of the out-of-the-box plugs by removing them from the property.

   b. To add your own plugs:

      i. Write the plug which must implement the interface: `com.mercury.sitescope.web.request.framing.IFramingPlug`.

         This interface exists in **<SiteScope root directory>\WEB-INF\lib\ss_webaccess.jar**. This jar must be in the classpath to compile the plug.

         Below is an example of a plug that allows framing for a parameter with the request name *exampleParameter* when this parameter is set to true:

Example:

```
package com.company.sitescope.examples.plug
import javax.servlet.ServletRequest;
import com.mercury.sitescope.web.request.framing.IFramingPlug;
public class ExamplePlug implements IFramingPlug{
    @Override
       public boolean isAuthorized(ServletRequest request) {
          //Add the code that will determine whether this request comes from an
authorized product.
          if (request == null){
               return false;
           }
           HttpServletRequest httpServletRequest = (HttpServletRequest)request;
           if (httpServletRequest.getParameter("exampleParameter") == null){
           return false;
           }

           return "true".equalsIgnoreCase((String)httpServletRequest.getParameter
("exampleParameter"));
           }
}
```

      ii. Add the class fully qualified name to the **_framingFilteringPlugsClasses** property in the **master.config** file (separated by a comma).

For example, `com.company.sitescope.examples.plug.ExamplePlug` should be appended to the list.

iii. Create a jar that contains all your own plugs, and add it to the **<SiteScope root directory>\WEB-INF\lib** folder.

3. Restart SiteScope (required after making any changes to the **master.config** file).

Automatically Terminating Sessions

After you have logged in to SiteScope, you can set a time period for terminating session identifiers.

1. Open the **<SiteScope root directory>\groups\master.config** file, and change the value of the **_maxSessionTimeMinutes** property. For example, if you enter `2`, after two minutes, the session will expire and automatically redirect you to the SiteScope login page.

   > **Note:** The default value is -1, which indicates the session will not expire.

2. Restart the SiteScope server.

Chapter 14: Configure SiteScope to Operate in FIPS 140-2 Compliant Mode

This chapter includes:

FIPS 140-2 Compliancy Overview

FIPS 140-2, or Federal Information Processing Standard, is a U.S. and Canadian government certification standard for encryption and cryptographic modules where each individual encryption component in the overall solution requires an independent certification. It was developed to define procedures, architecture, algorithms, and other techniques used in computer systems. The full FIPS text is available online from the National Institute of Standards and Technology (NIST).

To operate in FIPS 140-2 complaint mode, the SiteScope administrator must enable FIPS 140-2 mode using the SiteScope Hardening Tool. SiteScope runs self-tests at startup, performs the cryptographic modules integrity check, and then regenerates the keying materials. At this point, SiteScope is operating in FIPS 140-2 mode.

Reasons to Enable FIPS Mode:

Your organization might need to use SiteScope in FIPS mode if:

- You are a Federal Government department or contractor.
- You want to increase your security to protect your business from advanced attacks and data theft.

Software Requirements

FIPS compliance requires that your operating system and browser meet specific requirements for versions and settings.

While all browsers supported in SiteScope are supported in FIPS mode, not all versions of operating systems can handle the cryptographic demands FIPS requires. As a result, some operating systems SiteScope normally supports are not supported in FIPS mode.

To run in FIPS mode, SiteScope must be installed on one of the following operating systems:

- Windows Server 2008 R2 (64-bit)

- Windows Server 2012 R2 (64-bit)

JDBC Drivers

When running SiteScope in FIPS mode, you should consider using your JDBC driver instead of the default drivers that are provided with SiteScope.

SiteScope Connected With Non-FIPS Compliant Applications

When SiteScope is connected to an application that uses an algorithm that is not FIPS approved, the connection between SiteScope and that application will not be FIPS compliant (even if FIPS-140-2 mode was enabled on SiteScope).

Enable FIPS 140-2 Compliant Mode

To enable SiteScope to run in FIPS 140-2 compliant mode when using a secure connection, you must perform the following steps:

- "Step 1: Configure LDAP integration" below
- "Step 2: Configure Your Windows operating system for FIPS 140-2 compliant mode" on the next page
- "Step 3: Run SiteScopeHardeningToolRuntime " on page 148
- "Step 4: Disable JMX remote access to the SiteScope server " on page 148
- "Step 5: Configure SSL" on page 149
- "Step 6: Configure Client Authentication" on page 150

> **Note:** If you plan on enabling key management data encryption (provides stronger encryption than the standard encryption), you must do this after enabling or disabling FIPS 140-2 mode. If key management data encryption has already been configured, you must follow the steps in "How to Enable or Disable FIPS Compliant Mode After Changing the Encryption Key" on page 155.

Step 1: Configure LDAP integration

You need to enable LDAP user authentication to log in to SiteScope using client certificates.

1. 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.
2. Create a new role in SiteScope user management for LDAP users.
3. Change the SiteScope administrator login name to the email address of the user located in LDAP. This should be the same as the user in the client certificate (that is entered in step 3 of "Step 6: Configure Client Authentication" on page 150). Do not enter a password.

Step 2: Configure Your Windows operating system for FIPS 140-2 compliant mode

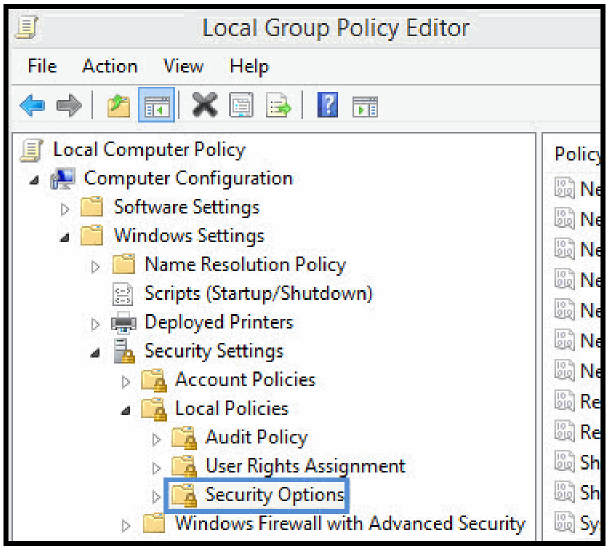
1. Configure your Windows operating system for FIPS 140-2 mode.

   a. Use administrative credentials to log on to the computer.

   b. Click **Start**, click **Run**, type `gpedit.msc`, and then press `ENTER`. The Local Group Policy Editor opens.

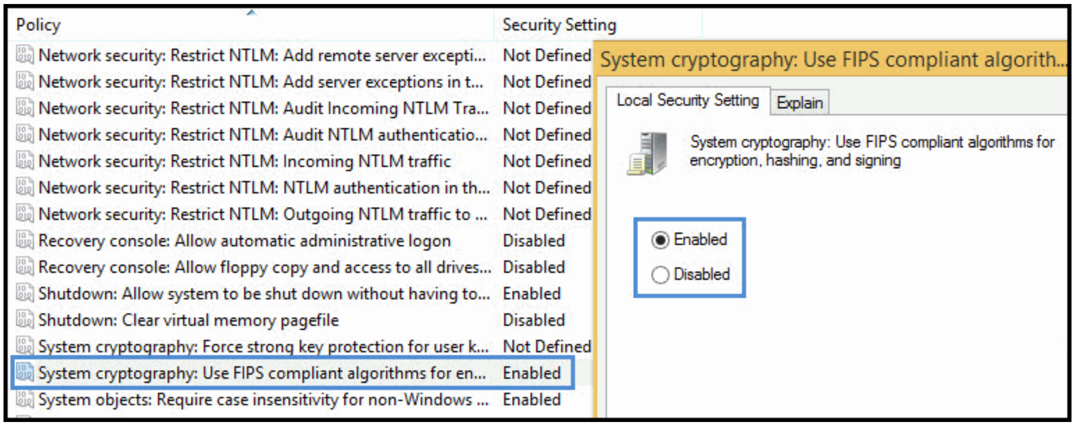
   c. In the Local Group Policy Editor, double-click **Windows Settings** under the **Computer Configuration** node, and then double-click **Security Settings**.

   d. Under the **Security Settings** node, double-click **Local Policies**, and then click **Security Options**.



   e. In the details pane, double-click **System cryptography: Use FIPS-compliant algorithms for encryption, hashing, and signing**.

   f. In the System cryptography: Use FIPS-compliant algorithms for encryption, hashing, and signing dialog box, click **Enabled**, and then click **OK** to close the dialog box.



Policy	Security Setting
Network security: Restrict NTLM: Add remote server excepti...	Not Defined
Network security: Restrict NTLM: Add server exceptions in t...	Not Defined
Network security: Restrict NTLM: Audit Incoming NTLM Tra...	Not Defined
Network security: Restrict NTLM: Audit NTLM authenticatio...	Not Defined
Network security: Restrict NTLM: Incoming NTLM traffic	Not Defined
Network security: Restrict NTLM: NTLM authentication in th...	Not Defined
Network security: Restrict NTLM: Outgoing NTLM traffic to ...	Not Defined
Recovery console: Allow automatic administrative logon	Disabled
Recovery console: Allow floppy copy and access to all drives...	Disabled
Shutdown: Allow system to be shut down without having to...	Enabled
Shutdown: Clear virtual memory pagefile	Disabled
System cryptography: Force strong key protection for user k...	Not Defined
System cryptography: Use FIPS compliant algorithms for en...	Enabled
System objects: Require case insensitivity for non-Windows ...	Enabled

System cryptography: Use FIPS compliant algorith...

System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing

● Enabled
○ Disabled

g. Close the Local Group Policy Editor.

h. Make sure that this security option was enabled.

   i. Open Registry Editor. Click **Start**, click **Run**, type `regedit`, and then press `ENTER`. The Registry Editor opens.

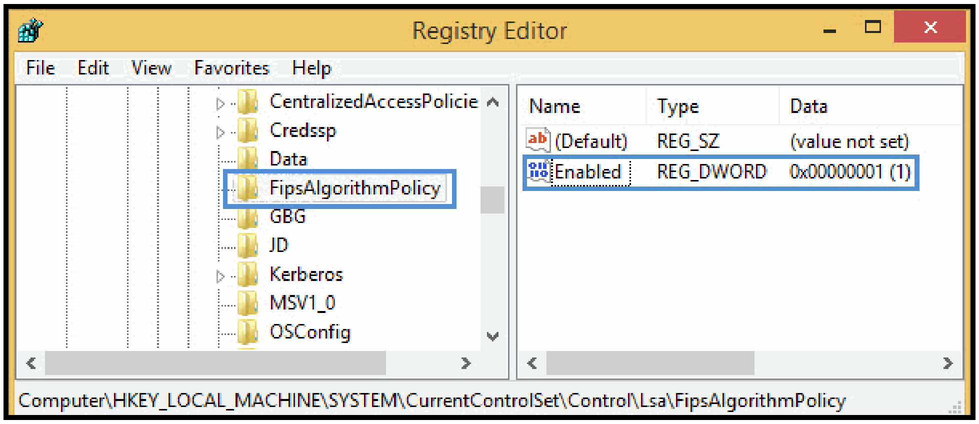
   ii. Find the following key and verify the value.

   - Key: **HKLM\System\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy\Enabled**.

     This registry value reflects the current FIPS setting. If this setting is enabled, the value is 1. If this setting is disabled, the value is 0.

   - Value: **1**.

   iii.



Name	Type	Data
(Default)	REG_SZ	(value not set)
Enabled	REG_DWORD	0x00000001 (1)

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\FipsAlgorithmPolicy

> **Tip:** For additional information, see:
>
> - http://technet.microsoft.com/en-us/library/cc750357.aspx
> - http://support.microsoft.com/kb/811833

Step 3: Run SiteScopeHardeningToolRuntime

1. Copy the **SiteScopeHardeningToolRuntime.zip** file from the **\Tools** folder of the SiteScope installer package to the SiteScope server.
2. Extract the contents of the file to the **<SiteScope root directory>\tools\SiteScopeHardeningTool** folder.
3. Start the Hardening Tool by running the command line:

```
<SiteScope_home_directory>\tools\SiteScopeHardeningTool\runSSLConfiguration.bat
```

Step 4: Disable JMX remote access to the SiteScope server

Use the Hardening Tool to disable JMX remote access to the SiteScope server:

1. Run the Hardening Tool. For details, see "How to Run the Hardening Tool" on page 159.
2. Select the option "Configure JMX remote access".
3. Follow the instructions in the tool for disabling JMX remote access.

> **Tip:** Changes in configuration take effect only after you exit the Hardening Tool.

Step 5: Configure SSL

1. Start the Hardening Tool by running the command line:

   ```
   <SiteScope_home_directory>\tools\SiteScopeHardeningTool\runSSLConfiguration.bat
   ```
2. Enter `1` to select the "SiteScope hardening configuration" option.
3. Enter a name to use for the backup file that is created. This is required if you need to disable FIPS 140-2 mode and restore the previous SiteScope configuration that existed before running the Hardening Tool. For details, see "Disable FIPS 140-2 Compliant Mode" on page 151.
4. Enter `2` to select the "Configure SiteScope Standalone to work over SSL (https)" option.
5. Enter `Y` to confirm that you want to configure SiteScope to work over SSL.
6. Enter `Y` to confirm you want SiteScope to be FIPS 140-2 compliant.
7. When FIPS 140-2 compliant mode is successfully configured, select one of the following methods to create the SiteScope server keystore to hold the SiteScope server certificate:
   - **Import a server keystore in .pkcs12 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 "Configure SiteScope to Require Client Certificate Authentication" on page 139), 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. For the Common Name, you must enter the same URL used on your machine, including FQDN if used (for example, `yourserver.domain.com`), and for the alias name, your machine's name (for example, `yourserver`).

8. Copy the signed SiteScope server certificate to create a signed certificate by your Certificate Authority server.
9. Enter the full path to the signed certificate that you received from the Certificate Authority server.
10. Enter the full path to the root CA certificate that was used to issue the above certificate.
11. Type `yes` to trust the certificate you received from the Certificate Authority server. The certificate is added to the SiteScope server keystore.

Step 6: Configure Client Authentication

1. Enter a password for the SiteScope server TrustStore for client certificate authentication. The password must be at least 6 characters long, and should not contain any special characters. The default password is `changeit`.
2. Enter `Y` to confirm that you want to enable client certification authentication.

   If you enable client authentication, SiteScope performs full client authentication upon the handshake and extracts a client certificate. This client certificate is checked against the SiteScope user management (LDAP) system. For details, see "Step 1: Configure LDAP integration" on page 146.
3. Enter a username property for the client certificate in the client certificate AlternativeSubjectName field. The default username is `Other Name`.
4. Enter `Y` to confirm you want to enable smart card enforcement.

   If you enable smart card enforcement, SiteScope verifies that the client certificate originates from a hardware device, and adds the certificate to the SiteScope TrustStore.

   For more details about smart card enforcement, see "Configure Smart Card Authentication" on page 138.
5. Enter `Y` to confirm you want to add CA certificates to the SiteScope TrustStore.

   > **Note:** 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 imported into the SiteScope server TrustStore.

6. Enter the full path to the root CA certificate file in CER format.
7. The CA certificate is added to the SiteScope TrustStore.

   If the certificate already exists in the keystore a message is displayed. Type `yes` to confirm you still want to add the certificate to the SiteScope TrustStore.
8. (Optional) To add additional CA certificates to the SiteScope server TrustStore, enter `Y`, and repeat steps 1-3.

> **Note:** No additional CA certificates are required.

9. Enter `Q` to complete the Hardening Tool process.

Disable FIPS 140-2 Compliant Mode

If FIPS 140-2 compliant mode was enabled and you are using a secure connection, you cannot use the disable FIPS option in the Hardening Tool to disable FIPS 140-2 compliant mode. Instead, you must restore the previous SiteScope configuration that existed before FIPS mode was enabled.

If FIPS 140-2 compliant mode was enabled using a non-secure connection, you use the disable FIPS 140-2 compliant mode option in the Hardening Tool.

Disable FIPS 140-2 Compliant Mode for a Secure Connection

1. Start the Hardening Tool by running the command line:

   ```
   <SiteScope_home_directory>\tools\SiteScopeHardeningTool\runSSLConfiguration.bat
   ```

2. Enter `2` to select the "Restore SiteScope configuration from backup" option.
3. Enter the number of the backup configuration you want to restore from the list of available backups.
4. Enter `y` to confirm you want to restore the selected backup configuration.
5. Enter `Q` to complete the Hardening Tool process.

Disable FIPS 140-2 Compliant Mode for a Non-Secure Connection

1. Start the Hardening Tool by running the command line:

   ```
   <SiteScope_home_directory>\tools\SiteScopeHardeningTool\runSSLConfiguration.bat
   ```

2. Enter `1` to select the "SiteScope hardening configuration" option.
3. When prompted in the tool, select the "Configure FIPS 140-2 compliancy for a non-secure connection" option.
4. Enter `2` to disable FIPS 140-2 compliant mode.
5. Enter `y` to confirm that you want to disable FIPS 140-2 compliant mode.
6. Enter `Q` to complete the Hardening Tool process.

Troubleshooting and Limitations

Limitations:

- Only SSH2 is supported for SSH connections when SiteScope is run in FIPS 140-2 mode.
- The **Prefer SSL to TLS** option in URL monitors, URL Tool, and New/Edit HTTP Recipient dialog

box is ignored when SiteScope is run in FIPS 140-2 mode (authentication using TLS is mandatory in FIPS 140-2 mode).

Troubleshooting:

- **Problem:** Unable to import a certificate into SiteScope from a remote host using Certificate Management when FIPS 140-2 mode is enabled.

  Workaround: Import the certificate from a file, either from the Certificate Management page in the SiteScope user interface, or manually by running the following command:

  > **Example:**
  > ```
  > keytool -import -file <trusted cert file> -alias <trust cert name>
  > -keypass <password> -keystore <trust store file
  > (SiteScope\java\lib\security\cacerts)>
  > -storepass <password> -providername JsafeJCE –storetype PKCS12
  > ```

Chapter 15: Configure SiteScope to Use a Custom Key for Data Encryption

This chapter includes:

Key Management Overview

By default, SiteScope encrypts the persistency data using a standard encryption algorithm (persistency data includes configuration data of all the defined monitors, groups, alerts, templates, and many other SiteScope entities found in the **<SiteScope root>\persistency** directory).

You can use the Key Management for data encryption option in the Hardening Tool to change the cryptographic key used for encrypting SiteScope persistency data. Changing cryptographic keys provides stronger encryption than the standard SiteScope encryption.

Using Key Management for data encryption is supported on the following SiteScope tools: Hardening Tool, Persistency Viewer, and Persistency Logger. Key Management for data encryption can also be configured to operate when SiteScope is in FIPS 140-2 compliant mode.

When Key Management is enabled, you configure SiteScope to use a custom key for data encryption. You do this by entering a passphrase which SiteScope uses to generate a new key and encrypt the persistency data. You must enter this passphrase when exporting SiteScope persistency data from your current SiteScope for later import into SiteScope. When importing the persistency data (either during installation, or after installation using the SiteScope Configuration Tool), you must enter the same passphrase for the SiteScope server key. Note that the key is not saved to the persistency.

> **Note:**
>
> - If you plan on enabling or disabling FIPS 140-2 compliant mode (see "Configure SiteScope to Operate in FIPS 140-2 Compliant Mode" on page 145), you must do this before you enable key management data encryption, to avoid having to disable and then re-enable key management data encryption.
> - If you need to enable or disable FIPS 140-2 compliancy mode after changing the cryptographic keys for encrypting SiteScope data, follow the steps described in "How to Enable or Disable FIPS Compliant Mode After Changing the Encryption Key" on page

> 155.

Troubleshooting and Limitations

- Key Management for data encryption is not supported in SiteScopes installed on Linux platforms.
- Key Management for data encryption is not supported when using SiteScope Failover to provide backup infrastructure monitoring for the primary SiteScope (neither on the primary SiteScope, or on the SiteScope Failover server). If you are using SiteScope Failover with a SiteScope that uses the default key encryption and you then switch SiteScope to Key Management data encryption using the Hardening Tool, you will get an UNEXPECTED_SHUTDOWN error in the **high_availability.log** when mirroring the configuration.

How to Configure SiteScope to Use a Custom Key for Data Encryption

Using Key Management, you can manage and change the cryptographic keys that are used for encrypting the SiteScope configuration data (persistency).

> **Note:** If you plan to use SiteScope in FIPS 140-2 compliant mode (see "FIPS 140-2 Compliancy Overview" on page 145), you must configure FIPS compliant mode before changing the cryptographic key, to avoid having to disable and then re-enable Key Management for data encryption. If you need to make changes to FIPS mode after customizing the encryption key, follow the steps described in "How to Enable or Disable FIPS Compliant Mode After Changing the Encryption Key" on the next page.

1. Install SiteScope.

   For details, see "Installation Workflow" on page 92.
2. Start SiteScope (in order to generate SiteScope persistency data).
3. Stop SiteScope.
4. Run the Hardening Tool.
   a. When prompted in the tool, select the option "Enable or re-encrypt key management data encryption".
   b. Enter 1 to encrypt or re-encrypt persistency data using a custom key. Changing cryptographic keys for encrypting the configuration provides stronger encryption than the standard SiteScope encryption.

      To restore persistency data to the standard key encryption, enter 2.
   c. Confirm you want to encrypt or re-encrypt persistency data using a custom key.
   d. Enter a new passphrase to use for the custom key (this passphrase is not the one that is

already in use; it is for the new iteration of the encryption). The passphrase cannot contain empty spaces or escaped characters.

SiteScope generates a new key, and uses it to encrypt the persistency data.

> **Note:** You must enter this passphrase when using the SiteScope Configuration Wizard or the SiteScope Configuration Tool to export or import SiteScope configuration data that was encrypted using this custom key. Note that the passphrase is not stored with the zip file in the exported configuration.

5. Start SiteScope.

How to Enable or Disable FIPS Compliant Mode After Changing the Encryption Key

If you want to enable or disable FIPS 140-2 compliant mode after you have changed the SiteScope server key used for encrypting data, you must perform the following:

> **Note:** Failure to perform the steps in the order listed below can result in SiteScope data loss.

1. Disable Key Management for data encryption (see step 4 of "How to Configure SiteScope to Use a Custom Key for Data Encryption" on the previous page, and enter 2 to restore the standard encryption).
2. Enable/disable FIPS 140-2 compliant mode. For details, see "Enable FIPS 140-2 Compliant Mode" on page 146.
3. Enable Key Management for data encryption (continue from step 4 of "How to Configure SiteScope to Use a Custom Key for Data Encryption" on the previous page and enter 1 to encrypt persistency data using a custom key).

How to Export and Import Configuration Data When Using a Custom Key for Data Encryption

When SiteScope is configured to use Key Management for data encryption, you enter a passphrase that SiteScope uses to generate a new key. SiteScope uses this key to encrypt the persistency data. When you later export or import this encrypted data into SiteScope, you must enter the same passphrase for the SiteScope server key.

1. Export SiteScope configuration data from your current SiteScope for later import into SiteScope.

- When using the SiteScope Configuration Tool:
    i. In the Export Configuration screen, enter the passphrase used for the SiteScope server KeyStore in the **Passphrase** box. This box is disabled when the default SiteScope encryption is used.

    ii. Click **Next** to complete the export operation. The configuration data is encrypted and exported using the custom key.

    > **Note:** These input fields are disabled when the default SiteScope encryption is used.

- When running the Configuration Tool in console mode using the Configuration Tool: In the Export Configuration screen, enter the passphrase used for the SiteScope server KeyStore when prompted, and then press ENTER to complete the export operation.
- When using silent mode: Enter the key management data encryption passphrase in the relevant section of the **ovinstallparams.ini** file.

2. Import SiteScope configuration data.
    - User interface (during installation in the SiteScope Configuration Wizard, or post-installation in the SiteScope Configuration Tool):
        i. In the Import Configuration screen, enter the name of the user data (zip) file to import, or enter the SiteScope installation directory from which to import the user data file.

        ii. In the **Passphrase** box, enter the passphrase used for the SiteScope server KeyStore. Confirm the passphrase by entering the same passphrase in the **Match passphrase** box.

        > **Note:** These boxes are disabled when the default SiteScope encryption is used.

        iii. Click **Next** to complete the import operation.
    - Console mode (during installation, or post-installation using the Configuration Tool): In the Import Configuration screen, enter the passphrase used for the SiteScope server key when prompted, and then press ENTER to complete the import operation.
    - Silent installation: Enter the passphrase for the custom key used for data encryption in the relevant section of the **ovinstallparams.ini** file.

    The imported configuration data is encrypted using the custom key.

Chapter 16: Configure SiteScope to Communicate With APM Over a Secure Connection

This chapter includes:

- "Configure SiteScope to Connect to an APM Server That Requires a Secure Connection" below
- "Configure SiteScope to Connect to an APM Server That Requires a Client Certificate" below
- "Configure APM to Connect to SiteScope When SiteScope Requires a Client Certificate" below

Configure SiteScope to Connect to an APM Server That Requires a Secure Connection

To configure SiteScope to connect to an APM server that requires a secure connection, you must establish trust to enable secure communication between SiteScope and APM. This means that SiteScope must trust the Certificate Authority that issued the APM 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 "Import Certificate Authority Certificates into SiteScope TrustStores" on page 142.

Configure SiteScope to Connect to an APM Server That Requires a Client Certificate

You can configure SiteScope to connect to an APM server that requires a client certificate. This involves importing the APM 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 an APM Server That Requires a Client Certificate" on page 164.

It is also possible use the manual procedures in "Manually Configuring SiteScope to Connect to an APM Server That Requires a Client Certificate" on page 239.

Configure APM to Connect to SiteScope When SiteScope Requires a Client Certificate

In APM, 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 APM machine.
2. Stop APM.
3. Edit **<HPE APM root directory>\EjbContainer\bin\product_run.bat** and add the following:

Example:

```
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 APM.
5. Configure APM 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 17: 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 168.

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 161
- "How to Use the Hardening Tool to Configure SiteScope to Verify Certificate Revocation" on page 162
- "How to Use the Hardening Tool to Import Certificate Authority Certificates into SiteScope TrustStores" on page 163
- "How to Use the Hardening Tool to Configure SiteScope to Connect to an APM Server That Requires a Client Certificate" on page 164
- "How to Use the Hardening Tool to Enable FIPS 140-2 Compliant Mode" on page 166
- "How to Use the Hardening Tool to Enable Key Management for Data Encryption" on page 166
- "How to Use the Hardening Tool to Configure SiteScope and SiteScope Public API Client Certificate Authentication" on page 166
- "How to Use the Hardening Tool to Configure JMX Remote Access" on page 167
- "How to Use the Hardening Tool to Restore a Backed Up Configuration" on page 168

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. If you want to enable LDAP user authentication (required if you intend to log in to SiteScope by using client certificates only), 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_home_directory>\tools\SiteScopeHardeningTool\runSSLConfiguration.bat
   ```

   Linux:

   ```
   ./opt/HP/SiteScope/tools/SiteScopeHardeningTool/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 168.

   > **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

> **Note:** If you plan to enable SiteScope to run in FIPS 140-2 compliant mode, follow the procedures in "Enable FIPS 140-2 Compliant Mode" on page 146.

You can use the Hardening Tool to configure SiteScope to require a secure connection (https).

1. Run the Hardening Tool. For details, see "How to Run the Hardening Tool" on page 159.
2. When prompted in the tool, select the option "Configure 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. Confirm whether you want to configure SiteScope to be FIPS 140-2 compliant. For details, see "Enable FIPS 140-2 Compliant Mode" on page 146.
5. 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 "Configure SiteScope to Require Client Certificate Authentication" on page 139), 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.

  > **Note:** When you are creating the server certificate in .pfx format, you must create it with a password.

6. 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.

7. 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.

8. 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 "Configure Smart Card Authentication" on page 138.

9. 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 the next page.

10. Enter `Q` to complete the Hardening Tool process.

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 159.
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.

   You can also configure SiteScope to comply with the Federal Information Processing Standard (FIPS) Publication 140-2 if required. For details, see "Configure SiteScope to Operate in FIPS 140-2 Compliant Mode" on page 145.

   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 "Import Certificate Authority Certificates into SiteScope TrustStores" on page 142.

To import Certificate Authority certificates into SiteScope TrustStores:

1. Prerequisites (if configuring SiteScope to require a secure connection)

   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 161.

2. Run the Hardening Tool. For details, see "How to Run the Hardening Tool" on page 159.
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.

- 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 an APM Server That Requires a Client Certificate

You use the Hardening Tool to configure client TLS authentication for APM integration. The tool enables you to configure SiteScope to allow APM 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 APM 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 161.
>
> 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 APM integration:

1. Run the Hardening Tool. For details, see "Using the Hardening Tool" on page 159.
2. Select the option "Configure SiteScope client certificate authentication for APM 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 APM server certificate. The APM server certificate is imported into the SiteScope TrustStore.

b. When prompted, confirm that you trust the APM server certificate. The APM 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 "Configure SiteScope to Require Client Certificate Authentication" on page 139), 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.

     > **Note: Note**: When you are creating the server certificate in .pfx format, you must create it with a password.

d. When prompted, enter the password for the client keystore that will be used to authenticate APM. SiteScope creates the APM 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 APM server certificate into SiteScope TrustStore.

f. When prompted, confirm that you trust the APM server certificate.The APM server certificate is imported into the SiteScope keystore.

- 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 Enable FIPS 140-2 Compliant Mode

You can use the Hardening Tool to configure SiteScope to be FIPS 140-2 compliant. FIPS 140-2 is a cryptographic module validation program, administered by the National Institute of Standards and Technology (NIST), that specifies the security requirements for cryptographic modules.

For details, see "Enable FIPS 140-2 Compliant Mode" on page 146.

How to Use the Hardening Tool to Enable Key Management for Data Encryption

You can use Key Management in the Hardening Tool to change the cryptographic key used for encrypting the persistency data in SiteScope. This is a stronger encryption method than the standard method used in SiteScope.

For details, see "How to Configure SiteScope to Use a Custom Key for Data Encryption" on page 154.

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 "How to Run the Hardening Tool" on page 159.
2. Select the option "Configure SiteScope and SiteScope public API client for client certificate authentication".
3. Follow the instructions in the tool.
   - 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 159.
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.

Enable JMX Remote Access with Authentication

By default JMX port is disabled in SiteScope without authentication. You can enable or disable JMX remote access with authentication using the SiteScope Hardening Tool.

Note: The Hardening tool user and SiteScope log on user must be the same. For example, if

SiteScope log on user is 'Admin' then you must be logged in as 'Admin' to the server.

Enable JMX remote access

1. Stop the SiteScope service.
2. Go to `<SiteScope_Directory>\tools\SiteScopeHardeningTool.`
3. Run `runSSLConfiguration.bat` (for Windows) or `runSSLConfiguration.sh` (for Linux).
4. Select **Option 1 - SiteScope hardening configuration.**
5. Enter a description for the backup.
6. Select **Option 7 - Configure JMX remote access.**
7. Type 'y' to "Would you like to configure JMX remote access ([y]/n)?"
8. Type 'y' to "Would you like to allow JMX remote access (y/[n])?"
9. Enter Username and Password for JMX remote access.
10. Start the SiteScope service.

Disable JMX remote access

1. Stop the SiteScope service.
2. Go to `<SiteScope_Directory>\tools\SiteScopeHardeningTool.`
3. Run `runSSLConfiguration.bat` (for Windows) or `runSSLConfiguration.sh` (for Linux).
4. Select **Option 1 - SiteScope hardening configuration**.
5. Enter a description for the backup.
6. Select **Option 7 - Configure JMX remote access.**
7. Type 'y' to "Would you like to configure JMX remote access ([y]/n)?"
8. Type 'n' to "Would you like to allow JMX remote access (y/[n])?"
9. Start the SiteScope service.

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 159.
2. Select the option "Restore SiteScope configuration from backup".
3. Follow the instructions in the tool.
   - 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 HPE 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 159.

- **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 "Import Certificate Authority Certificates into SiteScope TrustStores" on page 142.

- **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.

  > **Note:** If you intend to log in to SiteScope by using client certificates only, you must first configure the LDAP server in SiteScope before performing the hardening procedures. After hardening SiteScope, the user name used for logging in is extracted from the Client Certificate and is checked against the LDAP server, and the following properties are added to the **<SiteScope root>\groups\master.config** file (you should not modify these properties):
  >
  > ◦ **_clientCertificateAuthIdentityPropertyName**. Indicates to SiteScope where the user name used for the connection is found in Client Certificate properties.
  >
  > ◦ **_clientCertificateAuthIsAPIRealLDAPUserRequired**. Indicates to SiteScope that user name authentication should be done through LDAP when calling SiteScope APIs.
  >
  > ◦ **_clientCertificateAuthUsernamePropertyNameInSubjectField**. The property under which the user name can be found in Client certificate that was used for API call.

  b. Restore the SiteScope configuration that was backed up before running the tool (for details, see "Restore a Backed Up Configuration" on page 142).

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 18: 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 88.

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
3	Internet zone	Sites that are on the Internet

Value	Zone Type	Description
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 4: Upgrade SiteScope

Chapter 19: Upgrade an Existing SiteScope Installation

This chapter includes:

Before Performing the Upgrade

This section describes how to upgrade existing SiteScope installations with minimum disruption 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.

Before upgrading SiteScope, you should consider the following:

- Before importing the configuration from SiteScope 11.3x version, back up the `Kubernetes.config` file (<SiteScopeDir>\templates.docker\api). After importing the configuration, copy the `Kubernetes.config`file back in the same location as it gets overwritten after the import.
- If you are already using ODBC driver, then you must switch to JDBC or any other drivers. Change the connection URLs and drivers using GSAR.
- SiteScope must be installed on a supported Windows or Linux environments as listed in "System Requirements" on page 84.
- If you plan to enable SiteScope to send events and to act as a data storage for metrics data when SiteScope is integrated with Operations Manager or APM, you must install the Operations Agent on the SiteScope server. For details on installing the agent, see the Integrating SiteScope with Operations Manager Products Guide available in the SiteScope Help or on the HPE Software Integrations site.
- You can upgrade from 11.24 or 11.3x to SiteScope 11.40 by using the Configuration Tool to make a backup of your current SiteScope configuration data, uninstalling your current SiteScope version, installing SiteScope 11.40 followed by the latest minor-minor version on top of it (if one exists), and then importing the configuration data back into SiteScope. For upgrade instructions, see "Upgrade SiteScope 11.24 or 11.3x to SiteScope 11.40" on page 178.
- You can upgrade from SiteScope 10.x by first upgrading to SiteScope 11.24 or 11.3x, and then upgrading to SiteScope 11.40.

Notes and Limitations

- Cross-platform upgrade is not supported.
- You may face issues when importing SiteScope Windows configurations into Linux deployments (for example, when adding Windows remotes with NetBIOS or WMI connection type). Check that you do not have platform specific monitor settings, such as URL monitors with WinInet options, File monitors on Windows remotes, or Script monitors.
- If deprecated monitors were configured in a previous version of SiteScope, they are still displayed in SiteScope after performing an upgrade (although the 32-bit only monitors will not work).

Migrate from 32-Bit to 64-Bit SiteScope

SiteScope 11.40 supports only 64-bit operating systems and 64-bit Java versions. As a result, the SiteScope 32-bit and SiteScope 32-bit on 64-bit installers no longer exist in SiteScope 11.40.

From SiteScope 11.40, the Web Script monitor is supported in 64-bit. To use the monitor, you must install HPE Load Generator 12.02 on the SiteScope server, and specify the path to the Load Generator. For details, see the Web Script Monitor section in SiteScope Monitor Reference guide.

The other 32-bit monitors are deprecated and will not work after upgrading from SiteScope 11.24 or 11.3x to SiteScope 11.40.

To upgrade from SiteScope 11.24 (32-bit version) to SiteScope 11.40 (64-bit version), follow the steps in "Upgrade SiteScope 11.24 or 11.3x to SiteScope 11.40" on the next page (in step 5, make sure that you install SiteScope on a 64-bit machine).

Back Up the 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 the required 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 "Backing up and recovering a SiteScope installation if unable to start SiteScope" on page 212.

> **Note:**
>
> - You should make a backup of the **<SiteScope>\htdocs** directory and copy it to the SiteScope 11.40 directory after an upgrade so that you can see old reports, since this directory is not copied when you export SiteScope data.
> - When importing configurations with monitors deployed from Monitor Deployment Wizard Templates or Template Examples, you must rename the templates on the source SiteScope before exporting the configuration, or rename or delete the templates on the destination SiteScope.

For details on exporting SiteScope data using the Configuration Tool, see "Run the SiteScope Configuration Tool" on page 186.

Alternatively, you can export SiteScope data as part of the installation process. For details, see "Installation Workflow" on page 92.

Import the SiteScope Configuration Data

After upgrading SiteScope, monitor configuration data can be copied from earlier versions of SiteScope using the Configuration Tool. For details, see "Run the SiteScope Configuration Tool" on page 186.

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 212.

Upgrade SiteScope 11.24 or 11.3x to SiteScope 11.40

Perform the following steps to upgrade from SiteScope 11.24 or 11.3x to SiteScope 11.40.

Steps to upgrade

1. Stop the SiteScope service.
2. Backup the SiteScope 11.24/11.3x folder (copy it to a temp folder on your system).
3. Export the SiteScope configuration from SiteScope 11.24/11.3x:
   a. Launch the SiteScope Configuration Tool (**Start > Programs > HPE SiteScope > Configuration Tool**) and click **Next**.
   b. Select **Export configuration** and click **Next**.
   c. In the Export Configuration screen, select the location of the SiteScope 11.24/11.3x installation directory, and a target directory where you want to save exported data. Enter a backup file name. If you want to generate reports for old data, select **Include log files**.
   d. After the export is completed, click **Next/Finish**.
   e. 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 11.24/11.3x (**Start > Settings > Control panel > Add or Remove Programs**):
   a. Uninstall Window launches. Click **Next** twice and uninstall begins.
   b. After uninstall is complete, click **Finish**.
   c. Delete any remaining files under the SiteScope directory.

   > **Note:** If you are upgrading from SiteScope 11.33 on Linux, the JRE component `HPESiteScopeJRE-1.08.092-1.x86_64` still resides in the directory after uninstall. See the section "Upgrade to SiteScope 11.40 from 11.33 on Linux - JRE component still resides in the directory after uninstall. " on page 181 to

> remove the JRE component.

   d. 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.
   e. Reboot the server.

5. Install SiteScope 11.40:
   a. Run the SiteScope 11.40 installer and click **Next**.
   b. Accept the license agreement and click **Next**.
   c. Select a directory for SiteScope 11.40, and click **Next**.
   d. Select **HPE SiteScope** installation type and click **Next**.
   e. Leave the default port, and then click **Next**. If the default port is not available, enter 8088 instead.
   f. Leave license blank and click **Next**.
   g. In the summary screen click **Next**.
   h. After installation is complete, click **Next** (the installer windows closes).
   i. Restore the third-party libraries and jars that were copied to the temp folder (in step 3).
   j. Stop the SiteScope service.
6. Set the SiteScope service to run under a monitoring account.
7. Import data into SiteScope:
   a. Run the Configuration Tool (**Start > Programs > HPE SiteScope > Configuration Tool**) and click **Next**.
   b. Select **Import configuration** and click **Next**.
   c. In the Import Configuration screen, select the zip file previously exported from the 11.24/11.3x installation, verify the target directory is correct, and then click **Next**.
   d. After the import is completed, click **Finish** (the configuration tool closes).

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

   e. If you want to use previously generated reports, replace the existing **<SiteScope>\htdoc** folder with the **\htdocs** folder that you backed up from the previous SiteScope in step 2.
8. Change the following parameters in the **master.config** file:
   a. Open the **<SiteScope root>\groups\master.config** file.
   b. Change the line **_suspendMonitors=** to **_suspendMonitors=true**.

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

   c. If SiteScope is connected to APM:
      - Change the line **_topazEnforceUseDataReduction=** to **_topazEnforceUseDataReduction=false**.
      - Add the parameter **_disableHostDNSResolution=true**.

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

9. Start the SiteScope service. SiteScope upgrades the configuration and then restarts itself. Log in using the user interface and verify the integration to APM is correct under **Preferences > Integration Settings**.
10. Contact your HPE support renewal rep to request product contract migration. Once contract migration is completed, go to the My Software Updates portal (https://h20575.www2.hp.com/usbportal/softwareupdate.do) and click the **Get Licensing** tab to get the new license key(s).

    When you receive the license key, open SiteScope, select **Preferences > General Preferences**, expand the **Licenses** panel, and import the new license file.

    > **Note:** For license purchase inquiries (or if you require additional capacity), contact your HPE sales representative or use the Software Licenses and Downloads Portal http://www.hpe.com/software/entitlements.

11. Stop SiteScope.
12. Open the **master.config** file and perform the following:

   a. Unsuspend monitors by changing **_suspendMonitors=true** to **_suspendMonitors=**.

   b. If SiteScope is connected to APM:
      - Enable data reduction by changing **_topazEnforceUseDataReduction= false** to **_topazEnforceUseDataReduction=**.
      - Change the value of parameter **_disableHostDNSResolution=false**.

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

Troubleshooting and Limitations

This section describes troubleshooting and limitations for SiteScope upgrades.

- "Upgrade to SiteScope 11.40 from 11.33 on Linux - JRE component still resides in the directory after uninstall. " on the next page
- "First SiteScope Restart After Upgrade Can Take a Long Time" on the next page
- "SiteScope Fails to Get the Customer ID" on the next page
- "Default Alert Action Is Named According to Action Type" on page 182
- "APM/ServiceCenter or Service Manager Integration" on page 182

- "SiteScope Fails to Upgrade" on the next page
- "Moving SiteScope to a Different Server When Integrated with APM" on the next page

> **Note:** You can also check for other information relating to upgrading SiteScope in the Self-Solve Knowledge Search. To enter the knowledge base, you must log on with your HPE Passport ID.

Upgrade to SiteScope 11.40 from 11.33 on Linux - JRE component still resides in the directory after uninstall.

If you are upgrading to SiteScope 11.40 from SiteScope 11.33 on Linux, the JRE component `HPESiteScopeJRE-1.08.092-1.x86_64` still resides after uninstall. Perform the following steps to remove the JRE component.

1. Verify if the following JRE component is still residing in the directory:
   `HPESiteScopeJRE-1.08.092-1.x86_64`
2. Use the following command to remove the JRE file:
   ```
    [root@iwfvm08067 ~]# rpm -e HPESiteScopeJRE-1.08.092-1.x86_64
   ```
3. Verify that the JRE component is removed using the command:
   ```
   [root@iwfvm08067 ~]# rpm -qa | grep SiteScope
   ```
   If the JRE component is removed, the output should be as follows:

   [root@iwfvm08067 ~]#

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 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 APM, 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 APM 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 APM. If APM is down during the restart, SiteScope is unable to retrieve the customer ID, and SiteScope restarts itself again.

Possible Solution: Make sure that any APM 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.

APM/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 APM/ServiceCenter or Service Manager integration. When setting up the ServiceCenter monitor in SiteScope, a file called **peregrine.jar** is created and placed in the **WEB-INF\lib** directory on the SiteScope machine. This file must be backed up before upgrading SiteScope or it will be deleted during the upgrade. After the upgrade is complete, copy the backed up **peregrine.jar** file back to the **WEB-INF\lib** directory.

SiteScope Fails to Upgrade

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

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

Possible Solution: Perform the SiteScope installation again.

Moving SiteScope to a Different Server When Integrated with APM

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 APM integration. Perform the following steps to minimize the impact on the integration:

1. Make a backup of your current SiteScope installation. For details, see "Back Up the SiteScope Configuration Data" on page 177.

2. Install SiteScope on the new hardware, and import the SiteScope configuration data to the SiteScope installation directory. For details, see "Import the SiteScope Configuration Data" on page 178.
3. Configure the SiteScope server with the same port number that was used on the old hardware.
4. Perform the following on the APM Gateway Server:

   > **Note:** This must be done before starting the new SiteScope server.

   a. Open the Topaz Browser under **<HPBSM_Dir>\tools\bsmbrowser\bsmbrowser.bat** (on Windows) or **bsmbrowser.sh** (on Linux), click **File > Topaz Connect**, and select the APM **management** database.
   b. In the **HOSTS** table, identify the record that contains information from the old SiteScope server:
      i. Run the command:
      ```
      "select * from hosts"
      ```
      ii. Write down the **H_ID** and **H_LocID** record that corresponds with the old SiteScope server.
      iii. Run the command:
      ```
      "update hosts set h_name ='<NewHostName>', h_ip='<NewHostIP>' where h_
      id=<H_ID PreviouslyFound>";
      ```
   c. In the **LOCATIONS** table, change the location to match the new value:
      i. Run the command:
      ```
      "select * from locations where l_locid=<H_LocID
      PreviouslyFoundFromHOSTS>"
      ```
      ii. Run the command:
      ```
      "update locations set L_LOCNAME='<NewHostName>' where l_locid=<H_LocID
      PreviouslyFoundFromHOSTS>";
      ```
   d. In the **SESSIONLOCATIONS** table, find the correct **SESSION_ID**:
      i. Run the command:
      ```
      "select * from sessionlocations where sl_locid=<H_LocID
      PreviouslyFoundFromHOSTS>"
      ```
      ii. Write down the **SL_SESSIONID** from the record found.
   e. In the **SESSION_SITESCOPE_PROPS** table, modify the SiteScope properties to match the new host:
      i. Run the command:
      ```
      "select * from session_sitescope_props where session_id=<SL_SESSIONID
      PreviouslyFound>"
      ```

and verify this is the correct record.

ii. Run the command:

```
"update session_sitescope_props set SITESCOPE_HOST='<NewHostName>',
SITESCOPE_LOCATION='<NewHostName>' where session_id=<SL_SESSIONID
PreviouslyFound>";
```

f. Start the new SiteScope server (make sure you do not start the old SiteScope server).

Part 5: Post-Installation: Getting Started

Chapter 20: Run the SiteScope Configuration Tool

This chapter includes:

- "Run the Configuration Tool on Windows Platforms" below
- "Run the Configuration Tool on Linux Platforms" on page 193
- "Run the Configuration Tool Using Console Mode" on page 198
- "Run the Configuration Tool in Silent Mode" on page 201

Run 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 complete the installation of the 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.

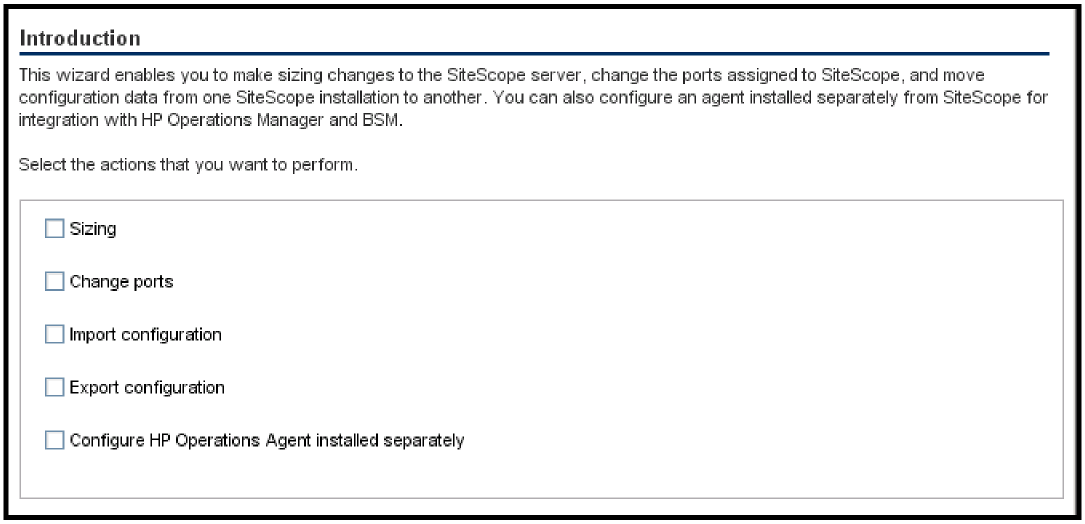
Note:

- You can also run the configuration Tool on Windows platforms in console mode. For details, see "Run the Configuration Tool Using Console Mode" on page 198.
- The option to install and uninstall the Operations Agent directly from within SiteScope was removed from the Configuration Tool. Instead, you must manually install and configure the agent. The agent is required for sending events and storing metrics data if SiteScope is integrated with OM or APM (except when graphing metrics data to Performance Graphing using the profile database in APM). For details on installing and configuring the agent, see the Integrating SiteScope with Operations Manager Products Guide available in the SiteScope Help or on the HPE Software Integrations site.
- 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 207.

- 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.
- 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 with monitors deployed from Monitor Deployment Wizard Templates or Template Examples, you must rename the templates on the source SiteScope before exporting the configuration, or rename or delete the templates on the destination SiteScope.
- If the imported configuration contains expired certificates, they will be merged inside the default SiteScope KeyStore on configuration import. This can result in the SSL Certificate monitor being in error state. To avoid this, you should delete any expired certificates before exporting configuration data.
- Files from the following folders cannot be overridden when importing configuration data: **templates.os**, **templates.post**, **templates.health**, **templates.applications**, and **conf\ems**.
- 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 "Upgrade an Existing SiteScope Installation" on page 175.

To run the SiteScope Configuration Tool:

1. On the SiteScope server, select **Start > All Programs > HPE 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, and move configuration data from one SiteScope installation to another. You can also configure an agent installed separately from SiteScope for integration with HP Operations Manager and BSM.

Select the actions that you want to perform.

☐ Sizing

☐ Change ports

☐ Import configuration

☐ Export configuration

☐ Configure HP Operations Agent installed separately

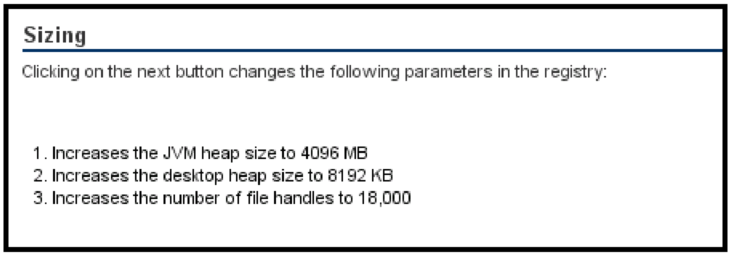
- **Sizing.** Enables optimizing SiteScope's performance by increasing JVM heap size, desktop heap size, and the number of file handles in the Windows Registry keys. For details, see step 3.

> **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 **–Xmx1024m** parameter, as required, up to a maximum of **–Xmx8192m** (for 8GB).

- **Change ports.** 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.
- **Configure Operations Agent installed separately.** Required to complete the installation of the 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 Operations Manager or APM Gateway server. For details, see step 7.

> **Note:** This option is disabled if Operations Agent 11.14 has not been installed on the SiteScope server. For details on installing and configuring the agent, see the Integrating SiteScope with Operations Manager Products Guide available in the SiteScope Help or on the HPE Software Integrations site.

3. If you selected the **Sizing** option, the Sizing screen opens listing the parameters in the Windows Registry.



Sizing

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

1. Increases the JVM heap size to 4096 MB
2. Increases the desktop heap size to 8192 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 4096 MB. For more details on JVM heap size, refer to http://docs.oracle.com/javase/1.5.0/docs/guide/vm/gc-ergonomics.html.
- **Desktop heap size.** The value is changed from 512 KB to 8192 KB. For more details on

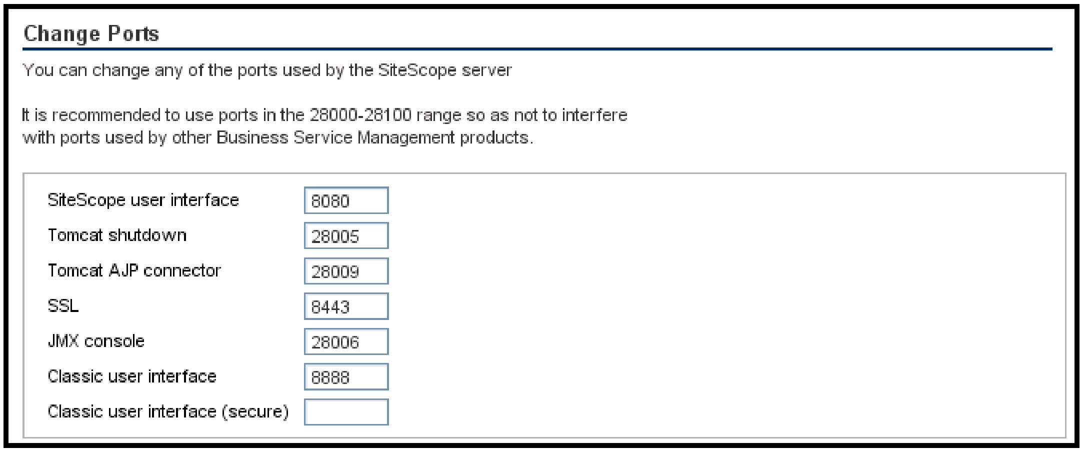
Desktop heap size, refer to http://support.microsoft.com/kb/126962.

> **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 (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.



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)	

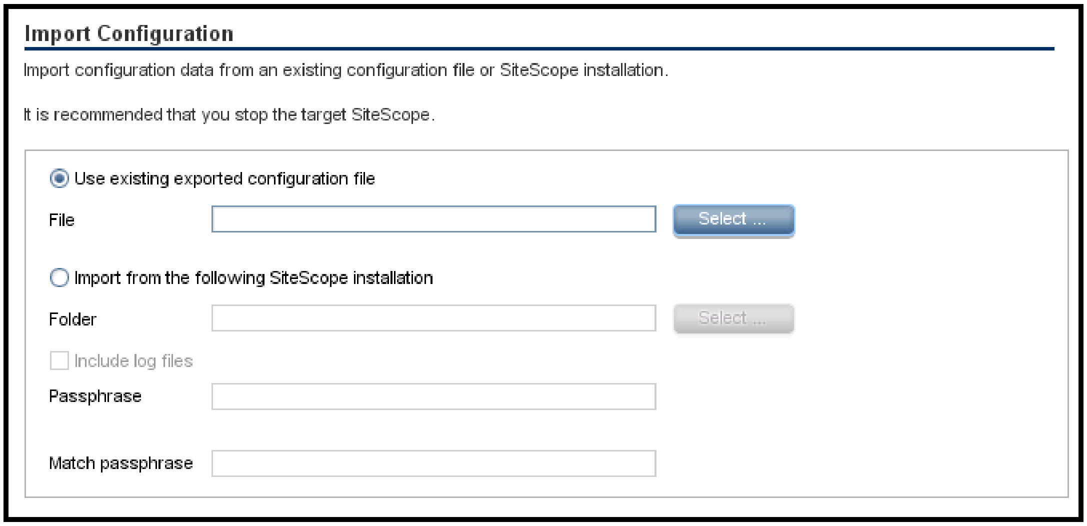
Modify the ports used by the SiteScope server as required. Port numbers must be numeric and should be in the 1-65534 range. A port is mandatory for all components except Classic user interface.

> **Note:** It is recommended to use ports in the 28000-28100 range so as not to interfere with ports used by other Application Performance 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 > HPE SiteScope > Open HPE SiteScope** link.

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



Import Configuration

Import configuration data from an existing configuration file or SiteScope installation.

It is recommended that you stop the target SiteScope.

● Use existing exported configuration file

File: ______ Select ...

○ Import from the following SiteScope installation

Folder: ______ Select ...

□ Include log files

Passphrase: ______

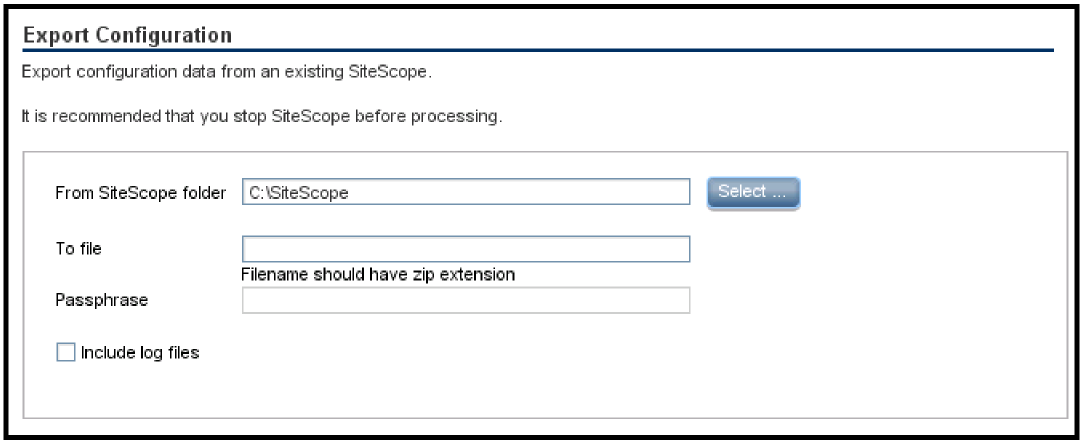
Match passphrase: ______

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 207.

- 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**.
- If SiteScope was configured to run using key management data encryption, enter the passphrase for the SiteScope server KeyStore in the **Passphrase** box. Confirm the passphrase by entering the same passphrase in the **Match passphrase** box. For details, see "Configure SiteScope to Use a Custom Key for Data Encryption" on page 153. These boxes are disabled when the default SiteScope encryption is used.

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

To file:
Filename should have zip extension

Passphrase:

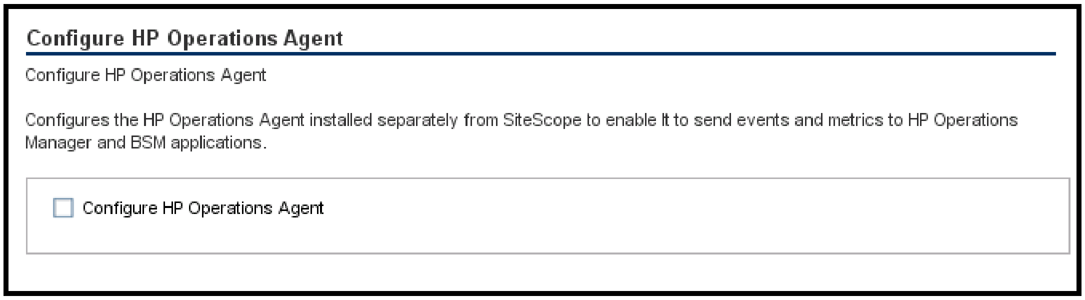
□ Include log files

- 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**.
- If SiteScope was configured to run using key managed encryption, enter the passphrase used for the SiteScope server KeyStore in the **Passphrase** box. For details, see "Configure SiteScope to Use a Custom Key for Data Encryption" on page 153. This box is disabled when the default SiteScope encryption is used.

> **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 207.
> - 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 11.40 directory after an upgrade, so that you can see old reports.

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

7. If you selected the **Configure Operations Agent installed separately** option, the Configure Operations Agent screen opens.

   Configure HP Operations Agent

   Configure HP Operations Agent

   Configures the HP Operations Agent installed separately from SiteScope to enable it to send events and metrics to HP Operations Manager and BSM applications.

   ☐ Configure HP Operations Agent

   Select **Configure Operations Agent**. This is required to complete the installation of the Operations agent. The agent enables SiteScope to send events and act as a data storage for metrics data when SiteScope is integrated with an Operations Manager or APM Gateway server.

   For details on sending events and reporting metrics data, see the Integrating SiteScope with Operations Manager Products Guide available in the SiteScope Help or on the HPE Software Integrations site.

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

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.

Run the Configuration Tool on 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 complete the installation of the 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 Linux platforms in console mode. For details, see "Run the Configuration Tool Using Console Mode" on page 198.
- The option to install and uninstall the Operations Agent directly from within SiteScope was removed from the Configuration Tool. Instead, you must manually install and configure the agent. The agent is required for sending events and storing metrics data if SiteScope is integrated with OM or APM (except when graphing metrics data to Performance Graphing using the profile database in APM). For details on installing and configuring the agent, see the Integrating SiteScope with Operations Manager Products Guide available in the SiteScope Help or on the HPE Software Integrations site.
- 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.
- When importing configurations with monitors deployed from Monitor Deployment Wizard Templates or Template Examples, you must rename the templates on the source SiteScope before exporting the configuration, or rename or delete the templates on the destination SiteScope.
- If the imported configuration contains expired certificates, they will be merged inside the default SiteScope KeyStore on configuration import. This can result in the SSL Certificate monitor being in error state. To avoid this, you should delete any expired certificates before exporting configuration data.
- Files from the following folders cannot be overridden when importing configuration data: **templates.os**, **templates.post**, **templates.health**, **templates.applications**, and

conf\ems.

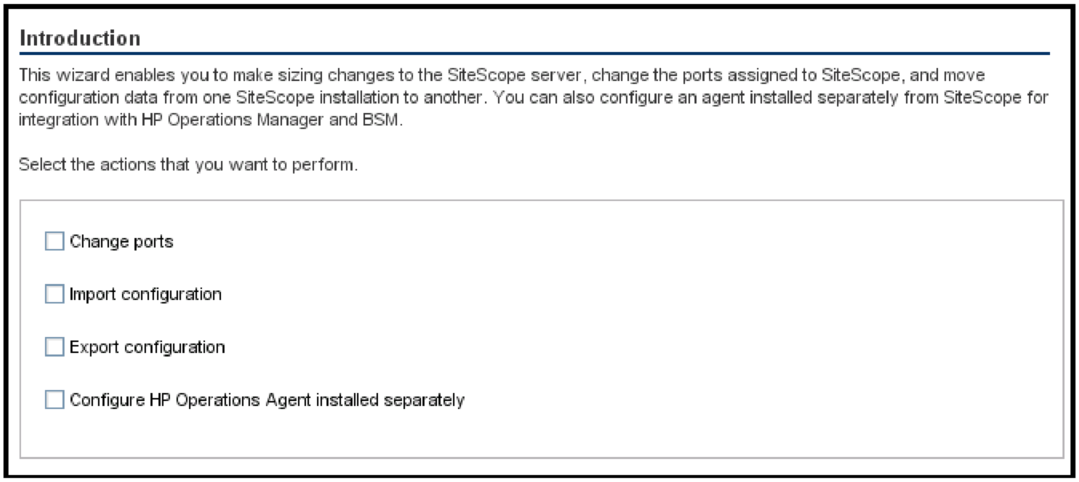
- The inclusion of server certificates and scripts when exporting data is supported by the SiteScope Configuration Tool. For details on how to include server certificates and scripts when exporting data from earlier versions of SiteScope, see "Upgrade an Existing SiteScope Installation" on page 175.
- When using SiteScope on a loaded environment that requires more than 4GB of memory, 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 the **-Xmx4096m** parameter 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 make sizing changes to the SiteScope server, change the ports assigned to SiteScope, and move configuration data from one SiteScope installation to another. You can also configure an agent installed separately from SiteScope for integration with HP Operations Manager and BSM.

Select the actions that you want to perform.

☐ Change ports

☐ Import configuration

☐ Export configuration

☐ Configure HP Operations Agent installed separately

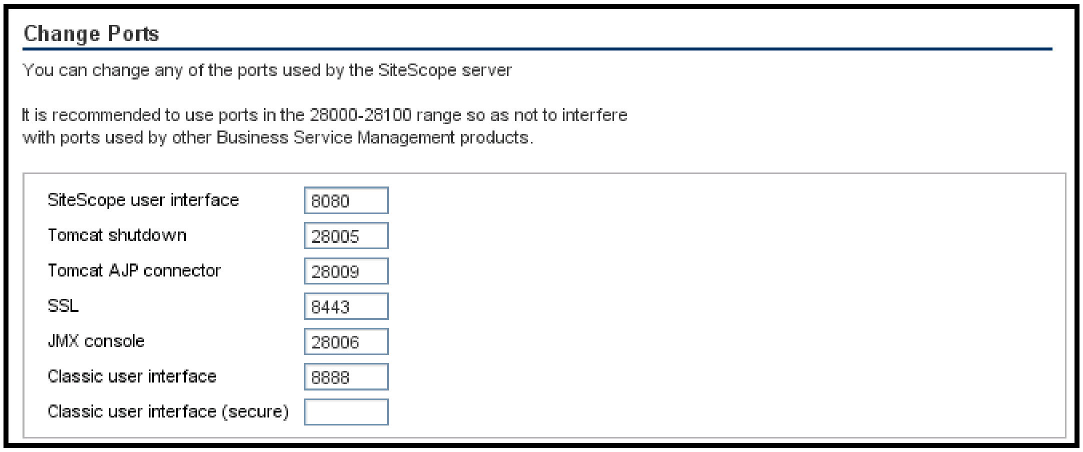
- **Change port.** Enables changing any of the ports used by the SiteScope server. For details, see step 3.
- **Import Configuration.** Enables importing configuration data from an exported configuration data (**.zip**) file, or from an existing SiteScope installation. For details, see step 5.
- **Export 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.

- **Configure Operations Agent installed separately.** Required to complete the installation of the Operations Agent. The agent enables SiteScope to send events and act as a data storage for metrics data when SiteScope is integrated with an perations Manager or APM Gateway server. For details, see step 6.

> **Note:** This option is disabled if Operations Agent 11.14 has not been installed on the SiteScope server. For details on installing and configuring the agent, see the Integrating SiteScope with Operations Manager Products Guide available in the SiteScope Help or on the HPE Software Integrations site.

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.

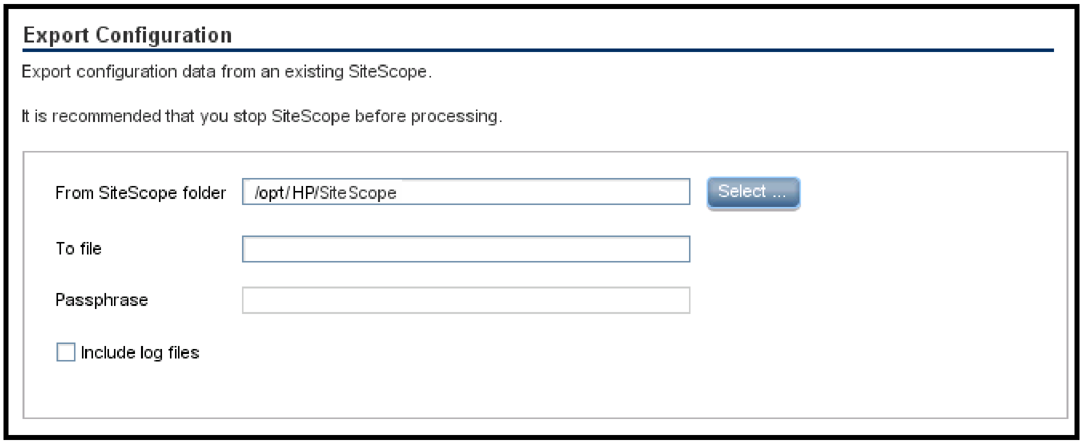
SiteScope user interface	8080
Tomcat shutdown	28005
Tomcat AJP connector	28009
SSL	8443
JMX console	28006
Classic user interface	8888
Classic user interface (secure)	

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.



Export Configuration

Export configuration data from an existing SiteScope.

It is recommended that you stop SiteScope before processing.

From SiteScope folder /opt/HP/SiteScope

To file

Passphrase

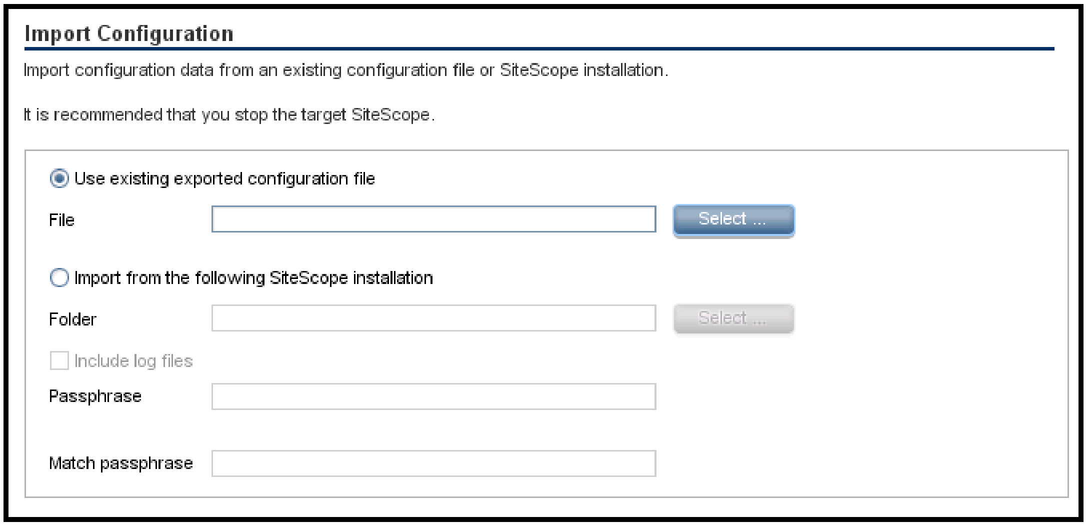
□ Include log files

> **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 Process on Linux Platforms" on page 208.

- 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 SiteScope was configured to run using key management data encryption, enter the passphrase used for the SiteScope server KeyStore in the **Passphrase** box. For details, see "Configure SiteScope to Use a Custom Key for Data Encryption" on page 153. This box is disabled when the default SiteScope encryption is used.
- 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.



Import Configuration

Import configuration data from an existing configuration file or SiteScope installation.

It is recommended that you stop the target SiteScope.

● Use existing exported configuration file

File

○ Import from the following SiteScope installation

Folder

□ Include log files

Passphrase

Match passphrase

> **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 Linux Platforms" on page 208.

- 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**.
- If SiteScope was configured to run using key management data encryption, enter the passphrase for the SiteScope server KeyStore in the **Passphrase** box. Confirm the passphrase by entering the same passphrase in the **Match passphrase** box. For details, see "Configure SiteScope to Use a Custom Key for Data Encryption" on page 153. These boxes are disabled when the default SiteScope encryption is used.

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

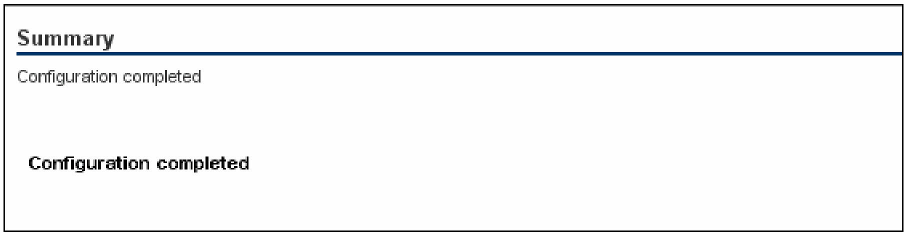
6. If you selected the **Configure Operations Agent installed separately** option, the Configure Operations Agent screen opens.

Select **Configure Operations Agent**. This configures the Operations Agent. The agent enables SiteScope to send events and act as a data storage for metrics data when SiteScope is integrated with an Operations Manager or APM Gateway server.

For details on sending events and reporting metrics data, see the Integrating SiteScope with Operations Manager Products Guide available in the SiteScope Help or on the HPE Software Integrations site.

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

7. The Summary screen opens.



Summary

Configuration completed

Configuration completed

Click **Finish** to close the wizard.

Run the Configuration Tool 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.

Note:

- The option to install and uninstall the Operations Agent directly from within SiteScope was removed from the Configuration Tool. Instead, you must manually install and configure the agent. The agent is required for sending events and storing metrics data if SiteScope is integrated with OM or APM (except when graphing metrics data to Performance Graphing using the profile database in APM). For details on installing and configuring the agent, see the Integrating SiteScope with Operations Manager Products Guide available in the SiteScope Help or on the HPE Software Integrations site.
- When importing configurations with monitors deployed from Monitor Deployment Wizard Templates or Template Examples, you must rename the templates on the source SiteScope before exporting the configuration, or rename or delete the templates on the destination SiteScope.
- Files from the following folders cannot be overridden when importing configuration data: **templates.os**, **templates.post**, **templates.health**, **templates.applications**, and **conf\ems**.
- When using SiteScope on a loaded environment that requires more than 4GB of memory, 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 the **-Xmx4096m** parameter to a higher value, as required, up to a maximum of **-Xmx8192m** (for 8GB).

To run the Configuration Tool using the console mode:

> **Note:** The procedure below shows screen captures of how to run the Configuration Tool on a Linux environment.

1. Run the following command:

   `/opt/HP/SiteScope/bin/config_tool.sh -i console` on Linux, or `<SiteScope root>\bin\config_tool.bat -i console` on Windows.

2. The configuration selection screen is displayed.

   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 complete the installation of the Operations Agent (the agent enables SiteScope to send metrics and events to Operations Manager and APM applications).

   Press `ENTER` to continue.

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

   - 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 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.

  > **Note:** If the imported configuration contains expired certificates, they will be merged inside the default SiteScope KeyStore on configuration import. This can result in the SSL Certificate monitor being in error state. To avoid this, you should delete any expired certificates before exporting configuration data.

5. 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 APM products.

   Press ENTER to complete the change port operation.

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

   The agent is required for sending events and storing metrics data if SiteScope is integrated with OM or APM, The Operations Agent is not required when graphing metrics data to Performance Graphing using the profile database in APM. The profile database is the recommended option, because it is a more robust and scalable data source, and does not require configuration of the Operations Integration.

   Enter Y to complete the installation of the Operations Agent.

   After the agent installation is complete, we recommend restarting the SiteScope server.

   For details on configuring the agent, see the Integrating SiteScope with Operations Manager Products Guide available in the SiteScope Help or on the HPE Software Integrations site.

Run 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.

Consideration Before Running a Silent Configuration

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 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 with monitors deployed from Monitor Deployment Wizard Templates or Template Examples, you must rename the templates on the source SiteScope before exporting the configuration, or rename or delete the templates on the destination SiteScope.
- If the imported configuration contains expired certificates, they will be merged inside the default SiteScope KeyStore on configuration import. This can result in the SSL Certificate monitor being in error state. To avoid this, you should delete any expired certificates before exporting configuration data.
- 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 207 and "Starting and Stopping the SiteScope Process on Linux Platforms" on page 208.
- Files from the following folders cannot be overridden when importing configuration data: **templates.os**, **templates.post**, **templates.health**, **templates.applications**, and **conf\ems**.
- 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 "Upgrade an Existing SiteScope Installation" on page 175.

- 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 (4GB).
  - If you start SiteScope by running the **go.bat** file in the **<SiteScope installation>\bin directory**, open the **go.bat** file and increase the **–Xmx4096m** parameter, 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 Application Performance Management products.
- When using SiteScope on a loaded environment that requires more than 4GB of memory, 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 the **-Xmx4096m** parameter to a higher value, as required, up to a maximum of **-Xmx8192m** (for 8GB).
- The option to install and uninstall the Operations Agent directly from within SiteScope was removed from the Configuration Tool. Instead, you must manually install and configure the agent. The agent is required for sending events and storing metrics data if SiteScope is integrated with OM or APM (except when graphing metrics data to Performance Graphing using the profile database in APM). For details on installing and configuring the agent, see the Integrating SiteScope with Operations Manager Products Guide available in the SiteScope Help or on the HPE Software Integrations site.

Run Silent Configuration

You can 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_tool** folder.

To run a silent configuration for SiteScope:

1. Navigate to the **configtoolparams.txt** file located in the **<SiteScope installation directory>\examples\silent_config_tool** 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)

Chapter 21: 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 1.
	To improve SiteScope scalability and performance, we recommend installing Microsoft hotfixes. For more information, see "Install Microsoft Hotfixes" on page 206.
	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 "Run the SiteScope Configuration Tool" on page 186.
	Log on to the SiteScope Web interface using a Web browser. For more information, see "Connecting to SiteScope" on page 209.
	New installations are automatically activated with the Community license which enables using SiteScope with limited functionality for an unlimited period of time. If you are upgrading your SiteScope edition to one that provides full SiteScope functionality, you can enter your SiteScope license information during installation, or post-installation in the General Preferences page, as described in the General Preferences section of Using SiteScope in the SiteScope Help. For license details, see "SiteScope Licenses" on page 1.
	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.

✓	Step
	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.
	Install middleware drivers for connectivity with remote databases and applications for those monitors that require drivers.
	When using SiteScope as a data collector for Application Performance Management (APM), configure the APM integration. For details, see the Working with APM section in Using SiteScope in the SiteScope Help.
	When using SiteScope to send events or report metrics for use in Operations Manager (OM) or Operations Management in APM, configure the Operations Manager integration. For details, see "Integrating SiteScope with Operations Manager Products" available from the HPE Software Integrations site.
	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 22: Install Microsoft Hotfixes

To improve SiteScope scalability and performance, we recommend installing the following Microsoft hotfixes after installing SiteScope:

Hotfix Download	Description
https://support.microsoft.com/en-us/kb/2847018 https://support.microsoft.com/en-us/kb/2775511	Install the latest Microsoft mrxsmb.sys and mrxsmb10.sys or mrxsmb20.sys patch files on the SiteScope server to prevent performance issues and monitor skips when running multiple perfex-based monitors against the same host.
https://support.microsoft.com/en-us/kb/942589	Install the Microsoft hotfix to use the Microsoft Exchange monitor on 64-bit version of Windows 2003, Windows 2008, or Windows XP (since a 32-bit application cannot access the system32 folder on a computer that is running a 64-bit version of Windows Server 2003 or 2008).
https://support.microsoft.com/en-us/kb/961435	Install the Microsoft hotfix on the target Windows system to enable monitoring Microsoft Windows Server 2008 using WMI.

In addition, we recommend you perform the steps in the Microsoft Knowledge Base articles below to avoid issues with permissions and missing or corrupted counter values:

Microsoft Knowledge Base Article	Issue / Description
https://support.microsoft.com/en-us/kb/300702 https://support.microsoft.com/en-us/kb/164018	**Unable to connect to machine**: Monitoring performance objects on Windows remote server requires that a user have specific access permissions as described in the Microsoft Knowledge Base for article 300702 and article 164018.
https://support.microsoft.com/en-us/kb/295292	**WMI Permissions**: To configure the WMI Service for Remote Monitoring, the user entered on the WMI remote server must have permissions to read statistics remotely from WMI namespace root\CIMV2.
https://support.microsoft.com/en-us/kb/300956	**Missing/corrupted Performance Counter Library values**: If the required Performance Counter Library values are missing or are corrupted, follow the instructions in Microsoft knowledge base article KB300956 to manually rebuild them.

Chapter 23: Getting Started with SiteScope

This chapter includes:

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 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 Linux Platforms

SiteScope has an autostart process that automatically starts SiteScope when the system starts, and stops SiteScope when the system is stopped. Note that if you change the permissions on SiteScope executables (start, stop), you must also change the permissions in the **/etc/init.d/sitescope** file as described in "To enable the service to start as a non-root user of SiteScope:" below.

You can also 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 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 15.

To enable the service to start as a non-root user of SiteScope:

1. Stop SiteScope (if it is running) by running the command:

   ```
   /etc/init.d/sitescope stop
   ```
2. Update the **/etc/init.d/sitescope** file as follows:
   a. Add `su sitecope -c` in front of the start command as follows:

      ```
      su sitescope -c $sis_dir/start
      ```
   b. Add `su sitecope -c` in front of the stop command as follows:

      ```
      su sitescope -c $sis_dir/stop
      ```
3. If SiteScope was previously running as root, change ownership of files to the right non-root user:

   ```
   % chown sitescope /opt/HP/SiteScope/ -R
   ```
4. Start SiteScope by running the command:

   ```
   /etc/init.d/sitescope start
   ```

To manually start the SiteScope process on 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 manually stop the SiteScope process on 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.

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 > HPE SiteScope > Open HPE SiteScope**. If the SiteScope port is changed after installing SiteScope, the port is updated in the **Open HPE SiteScope** link.

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

Note:

- To restrict access to this account and its privileges, you need to edit the administrator account profile to include a user login name and 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 the latest supported Java Runtime Environment 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:

Specific Startup Issues:

- "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
- "SiteScope hangs when opening the same SiteScope server on more than one tab in a browser window" on the next page
- "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 212
- "Backing up and recovering a SiteScope installation if unable to start SiteScope" on page 212
- "SiteScope does not open in Firefox" on page 214

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)
32-bit JRE	Internet Explorer (32-bit)

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 "Run the SiteScope Configuration Tool" on page 186.
   - 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 Application Performance Management if Application Performance 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 Application Performance Management application.
\conf\integration	Contains topology files used for integrations with Application Performance 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.
\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.

Directory	Description
\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 HPE Service Manager integration.

To recover the SiteScope installation:

1. Perform a new installation of SiteScope. For details, see "Installation Workflow" on page 92.
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 "Run the SiteScope Configuration Tool" on page 186.
   - 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 141.

Part 6: Uninstall SiteScope

This chapter includes:

- "Uninstall SiteScope on a Windows Platform" below
- "Uninstall SiteScope on a Linux Platform" on the next page

Uninstall SiteScope on a Windows Platform

This section includes:

- "How to Uninstall SiteScope " below

How to Uninstall SiteScope

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**.

      Each software component and its uninstallation progress are displayed on your screen during the uninstallation operation.

      After the uninstallation process is complete, the Uninstall Complete window opens showing you a summary of the uninstallation process.

      Note: Note: The Modify and Repair options are not available for selection.
   e. 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. Unconfigure and uninstall the Operations Agent.

   If the Operations Agent was installed on the SiteScope server and you want to remove it, you need to unconfigure and then uninstall the agent.

   a. To manually unconfigure the Operations Agent, run the following command:

      i. `msiexec /x <SiteScope root directory>\installation\components\oa_policy_signing_tool\win64\HPOprIAPA-09.00.111-Win5.2_64-release.msi /quiet`

      ii. `<SiteScope root directory>\installation\components\oa_template_management\all\install.bat -remove windows64`

   b. To uninstall the agent installed on the SiteScope server, see the instructions in the HPE Operations Agent Installation Guide.

4. When the uninstall process is complete, restart the machine if requested.

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 > Uninstall a Program > View installed updates**.Right-click the patch, for example, **HP SiteScope patch**, select **Uninstall**, and follow the uninstall wizard instructions listed in step 2 above ("Uninstall SiteScope" on the previous page).

3. When the uninstall process is complete, restart the machine if requested.

Uninstall SiteScope on a Linux Platform

This section includes:

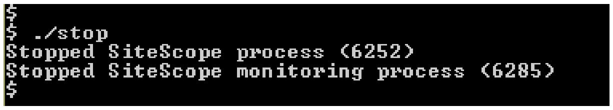
- "How to Uninstall SiteScope " below

How to Uninstall SiteScope

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.

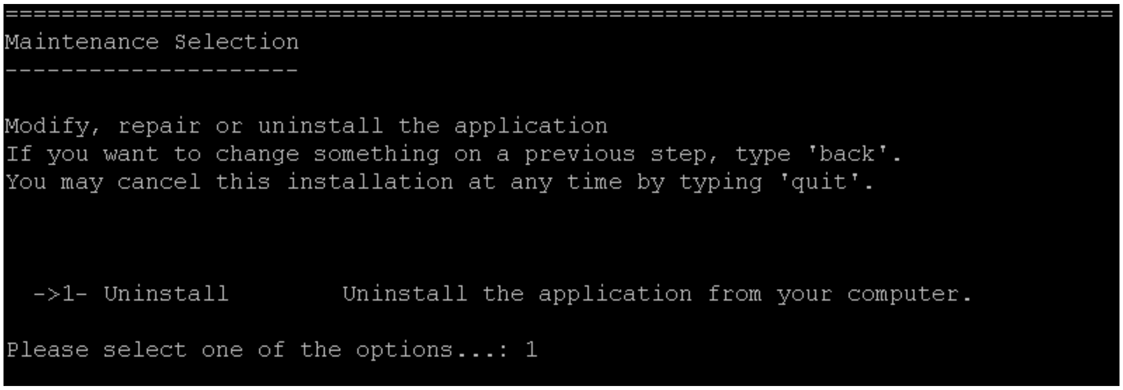
```
$
$ ./stop
Stopped SiteScope process (6252)
Stopped SiteScope monitoring process (6285)
$
```

3. If you work in X Windows mode, you should:

   - Uninstall SiteScope 11.40 by running the command (for example, for SiteScope 11.40):
     `/opt/HP/SiteScope/installation/HPSiS1140/bin/uninstall.sh`

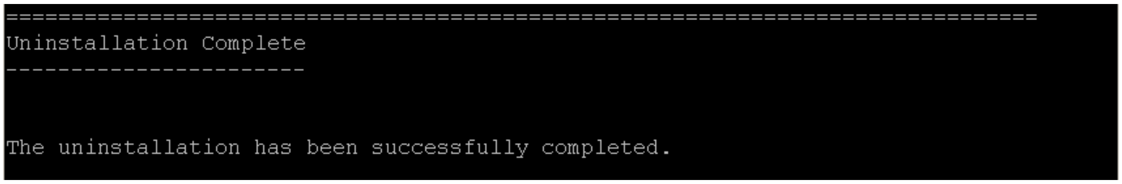
- Uninstall SiteScope 11.40 by running the command:
  `/opt/HP/SiteScope/installation/bin/uninstall.sh`

4. If you work in console mode, you should:
   - Uninstall SiteScope 11.40 by running the command (for example, for SiteScope 11.40):
     `/opt/HP/SiteScope/installation/HPSiS1140/bin/uninstall.sh -i console`
   - Uninstall SiteScope 11.40 by running the command:
     `/opt/HP/SiteScope/installation/bin/uninstall.sh -i console`
5. The HPE Software Installer starts. Specify the Locale and press `ENTER`.
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 package uninstall status messages are displayed and then the uninstall completes:



```
===============================================================================
Uninstallation Complete
-----------------------


The uninstallation has been successfully completed.
```

8. Unconfigure and uninstall the HPE Operations Agent

   If the HPE Operations Agent was installed on the SiteScope server and you want to remove it, you need to unconfigure and then uninstall the agent.

   a. To manually unconfigure the HPE Operations Agent, run the following on the Linux terminal:

      i. `rpm -e HPOprIAPA`

      ii. `<SiteScope root directory>\installation\components\oa_template_management\all\install.sh -remove linux64`

   b. To uninstall the agent installed on the SiteScope server, see the instructions in the HPE Operations Agent Installation Guide .

Appendixes

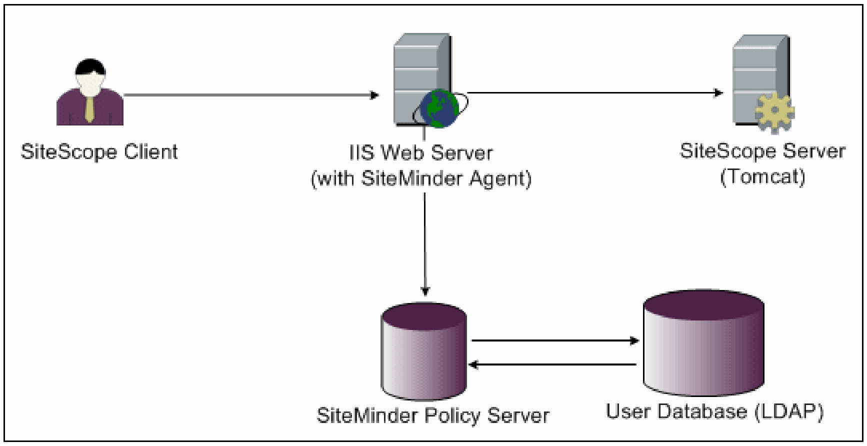
Appendix A: Integrating SiteScope with SiteMinder

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 2008 or higher
Web Server	IIS 7.0, IIS 8.0

The Integration Process

This section describes the SiteMinder integration process.

To integrate SiteScope with SiteMinder:

1. **Configure IIS as Reverse Proxy Using Application Request Routing (ARR) Module.**

   Download and install the ARR module and "Configure IIS as Reverse Proxy Using Application Request Routing (ARR) Module" below

2. "SiteMinder Agent Installation and Configuration " on page 223

3. **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 229.

Configure IIS as Reverse Proxy Using Application Request Routing (ARR) Module

Prerequisites

- Download and install the Web Platform and URL rewrite package from the location: http://www.microsoft.com/web/gallery/install.aspx?appid=urlrewrite2
- Add IIS role using default settings.
- Enable ISAPI filters and ISAPI extensions.

Steps to Install the ARR module

You can install the ARR module using either one of the options:

Option 1

You can install the ARR module directly from the location: http://www.microsoft.com/web/gallery/install.aspx?appid=ARRv3_0.

Note: Note: You might have to disable the options **IE ESC** and **Run as Administrator**.

Option 2

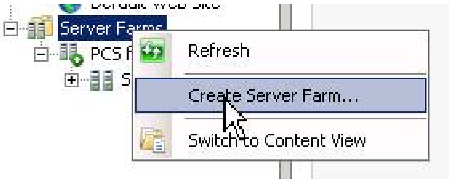
Install the ARR module from the Web Platform and URL rewrite package installer with the following steps:

1. Click the installer to open the Web Platform Installer dialog box.
2. On the top right corner, search for the ARR module using the string "ARR" in the Search bar.
3. Select **Application Request Routing 3.0** and click **Add**.

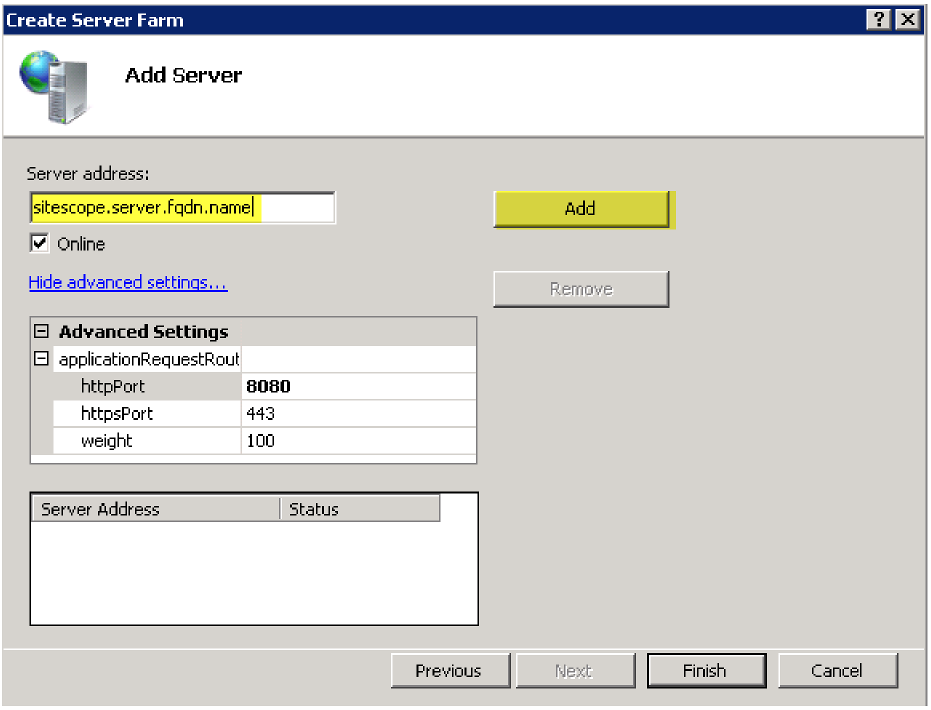
Steps to Configure IIS as Reverse Proxy

To configure IIS as Reverse Proxy using the ARR Module, follow the steps:

1. From the Windows Start menu, click Settings > Control Panel > Administrative Tools > Internet Information Services (IIS) Manager.
2. On the left pane, right-click and select **Create Server Farm**. The Add Server window opens.



3. Enter SiteScope server details:
   - Type the SiteScope FQDN name in the Server address box.
   - Expand **Advanced Settings** and **applicationRequestRoute**.
   - Change the http/https port to match your SiteScope port (default port is 8080).
   - Click **Add** and then **Finish**. The Rewrite Rules dialog box opens.



Server address: sitescope.server.fqdn.name

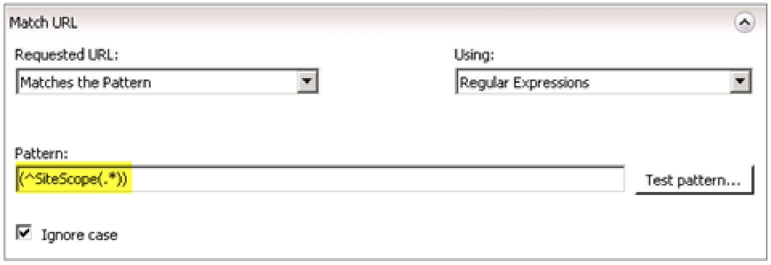
☑ Online

Advanced Settings	
applicationRequestRout	
httpPort	8080
httpsPort	443
weight	100

Server Address	Status

4. You are prompted to create rewrite rule. Click **Yes** if this is the first time you are creating the rule else click **No** and edit the existing URL rewrite rule to use the new Server Farm.
5. Enable Proxy with the following steps:
   a. Select the **main tree node** (server name) > **Application Request Routing Cache** (double-click) > **Server Proxy Settings**.
   b. Check the option **Enable proxy**.
   c. Verify that **HTTP Version** = **Pass Through.**
   d. Verify the option **Reverse rewrite host in response headers** is enabled.
   e. Click **Apply**.
   f. Select **Server Farms** and then select the server farm you created.
   g. Click **Proxy**.
   h. Change **time-out** to '60'.
   i. Enable the option **Reverse rewrite host in response headers**.
   j. Click **Apply**.
6. Select main tree node (server name) Edit URL rewrite rule to set pattern:
   a. Select your server from the drop-down and select URL rewrite.
   b. Select the rule and click **Edit**.
   c. In the Match URL box, select the following:
      - Requested URL=Matches the Pattern
      - Using = Regular Expressions

- Set pattern = (^SiteScope(.*))



Match URL

Requested URL: Matches the Pattern

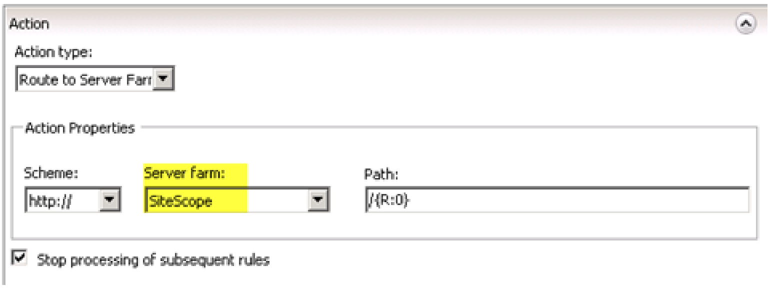
Using: Regular Expressions

Pattern: (^SiteScope(.*))

☑ Ignore case

d. Verify that you are using the correct Server Farm.

e. Click **Apply**.



Action

Action type: Route to Server Farr

Action Properties

Scheme: http://

Server farm: SiteScope

Path: /{R:0}

☑ Stop processing of subsequent rules

7. Close the IIS Management Console and restart it.
8. Test if the URL opens to SiteScope home page: http://<IISmachine>/SiteScope/

SiteMinder Agent Installation and Configuration

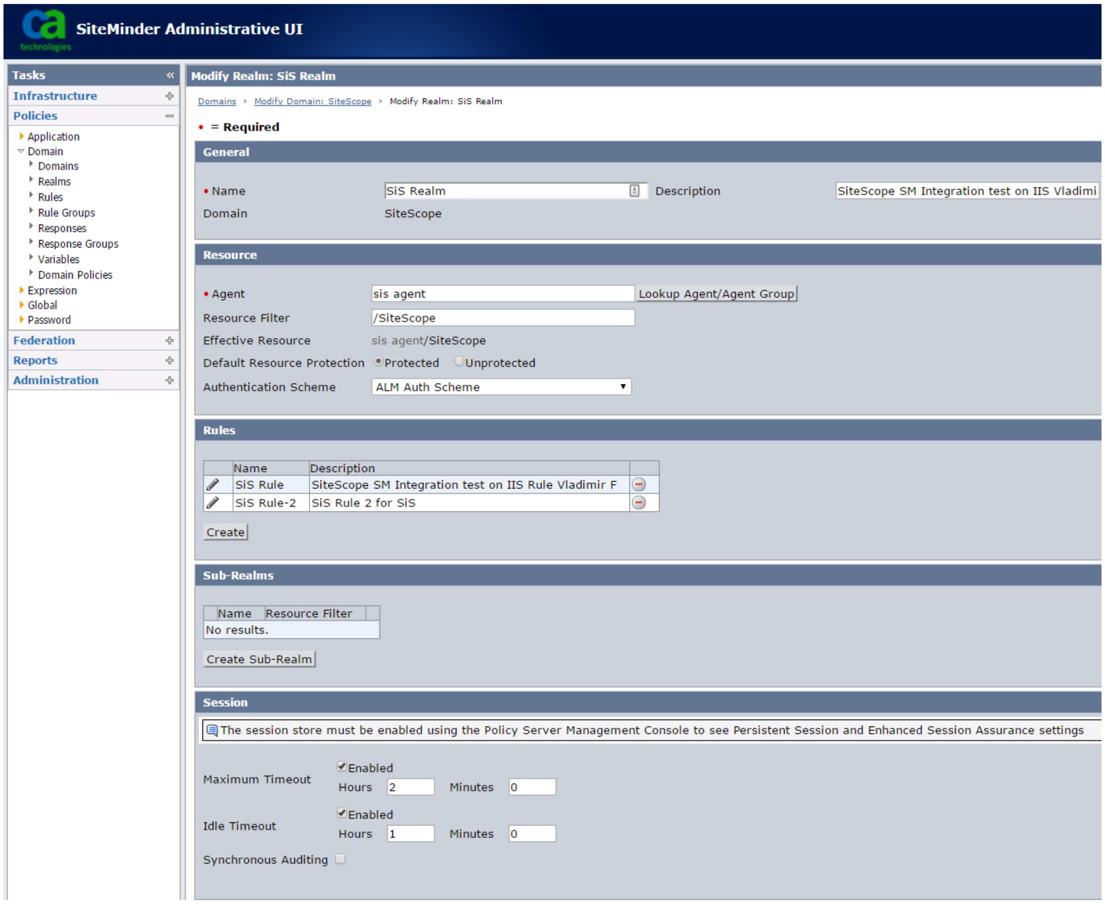
Prerequisites

- 64-bit SiteMinder web agent is required since IIS is a 64-bit process.
- Refer to the SiteMinder documentation for detailed instructions for creating domain and configuring SiteScope.

Steps to configure SiteMinder

Perform the following steps from the SiteMinder Administrative UI:

1. From the SiteMinder Administrative UI, select **Policies** > **Domain** > **Domains**.
2. Create a domain for SiteScope or use an existing domain based on your organization policy.
3. Add a **User Directory**.
4. Create a new **Realm**.



Modify Realm: SiS Realm

Domains › Modify Domain: SiteScope › Modify Realm: SiS Realm

• = Required

General

• Name: SiS Realm

Description: SiteScope SM Integration test on IIS Vladimi

Domain: SiteScope

Resource

• Agent: sis agent [Lookup Agent/Agent Group]

Resource Filter: /SiteScope

Effective Resource: sis agent/SiteScope

Default Resource Protection: ● Protected ○ Unprotected

Authentication Scheme: ALM Auth Scheme

Rules

	Name	Description	
✎	SiS Rule	SiteScope SM Integration test on IIS Rule Vladimir F	⊖
✎	SiS Rule-2	SiS Rule 2 for SiS	⊖

[Create]

Sub-Realms

Name	Resource Filter
No results.	

[Create Sub-Realm]

Session

The session store must be enabled using the Policy Server Management Console to see Persistent Session and Enhanced Session Assurance settings

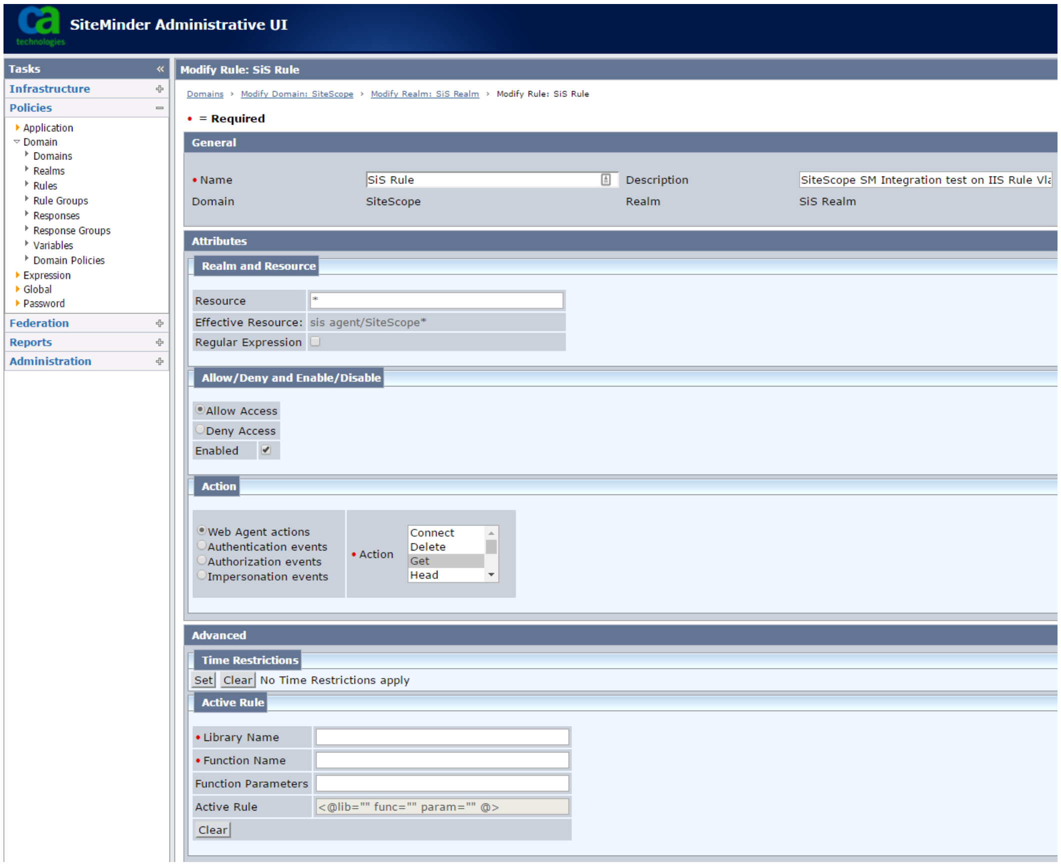
Maximum Timeout: ☑ Enabled; Hours 2; Minutes 0

Idle Timeout: ☑ Enabled; Hours 1; Minutes 0

Synchronous Auditing □

5. Create the following rules:
   - Regular rule that allows GET, POST, PUT traffic to SiteScope protected by Form Login page space.

- Rule that sends “Authentication events” > Action “OnAuthAccept”.



SiteMinder Administrative UI

Tasks

- Infrastructure
- Policies
  - Application
  - Domain
    - Domains
    - Realms
    - Rules
    - Rule Groups
    - Responses
    - Response Groups
    - Variables
    - Domain Policies
  - Expression
  - Global
  - Password
- Federation
- Reports
- Administration

Modify Rule: SiS Rule

Domains › Modify Domain: SiteScope › Modify Realm: SiS Realm › Modify Rule: SiS Rule

• = Required

General

• Name	SiS Rule	Description	SiteScope SM Integration test on IIS Rule Vi
Domain	SiteScope	Realm	SiS Realm

Attributes

Realm and Resource

Resource	*
Effective Resource:	sis agent/SiteScope*
Regular Expression	☐

Allow/Deny and Enable/Disable

● Allow Access
○ Deny Access
Enabled ☑

Action

● Web Agent actions
○ Authentication events
○ Authorization events
○ Impersonation events

• Action: Connect, Delete, Get, Head

Advanced

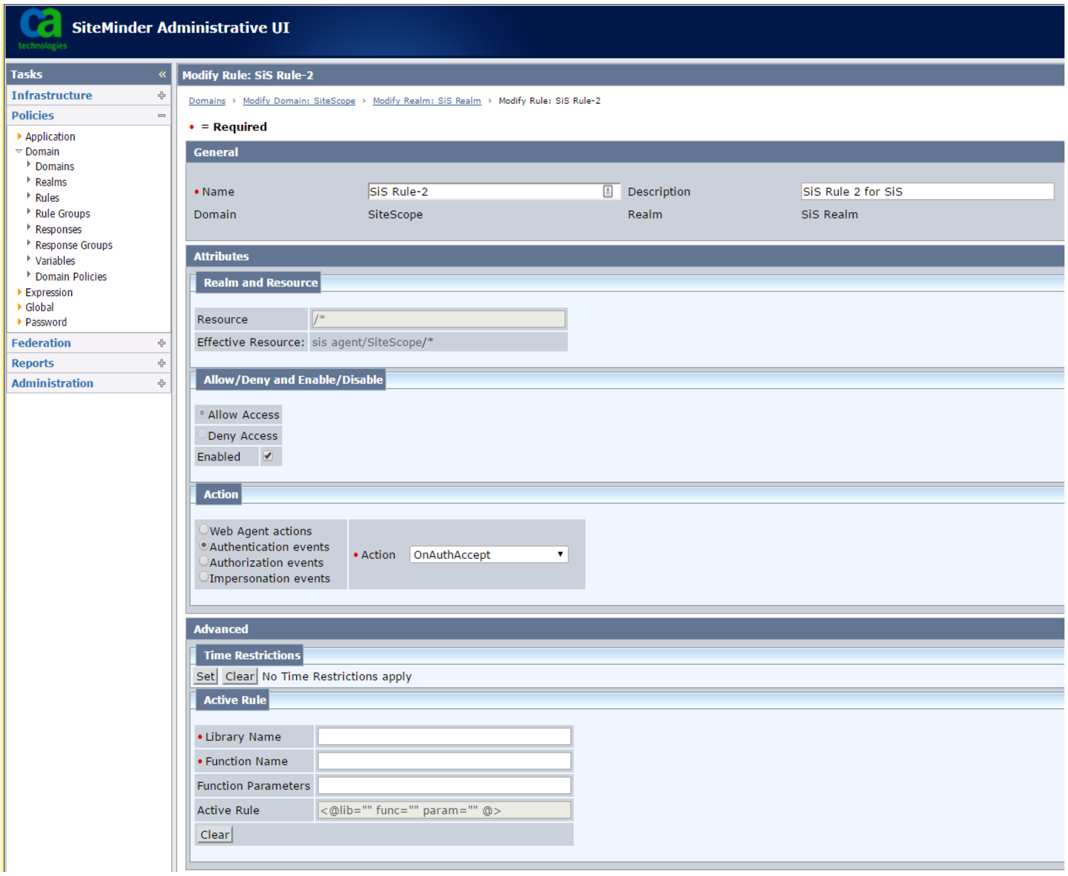
Time Restrictions

Set | Clear | No Time Restrictions apply

Active Rule

• Library Name	
• Function Name	
Function Parameters	
Active Rule	<@lib="" func="" param="" @>

Clear



Modify Rule: SiS Rule-2

Domains › Modify Domain: SiteScope › Modify Realm: SiS Realm › Modify Rule: SiS Rule-2

• = Required

General

• Name	SiS Rule-2	Description	SiS Rule 2 for SiS
Domain	SiteScope	Realm	SiS Realm

Attributes

Realm and Resource

Resource	/*
Effective Resource:	sis agent/SiteScope/*

Allow/Deny and Enable/Disable

● Allow Access
○ Deny Access
Enabled ☑

Action

○ Web Agent actions
● Authentication events
○ Authorization events
○ Impersonation events

• Action: OnAuthAccept

Advanced

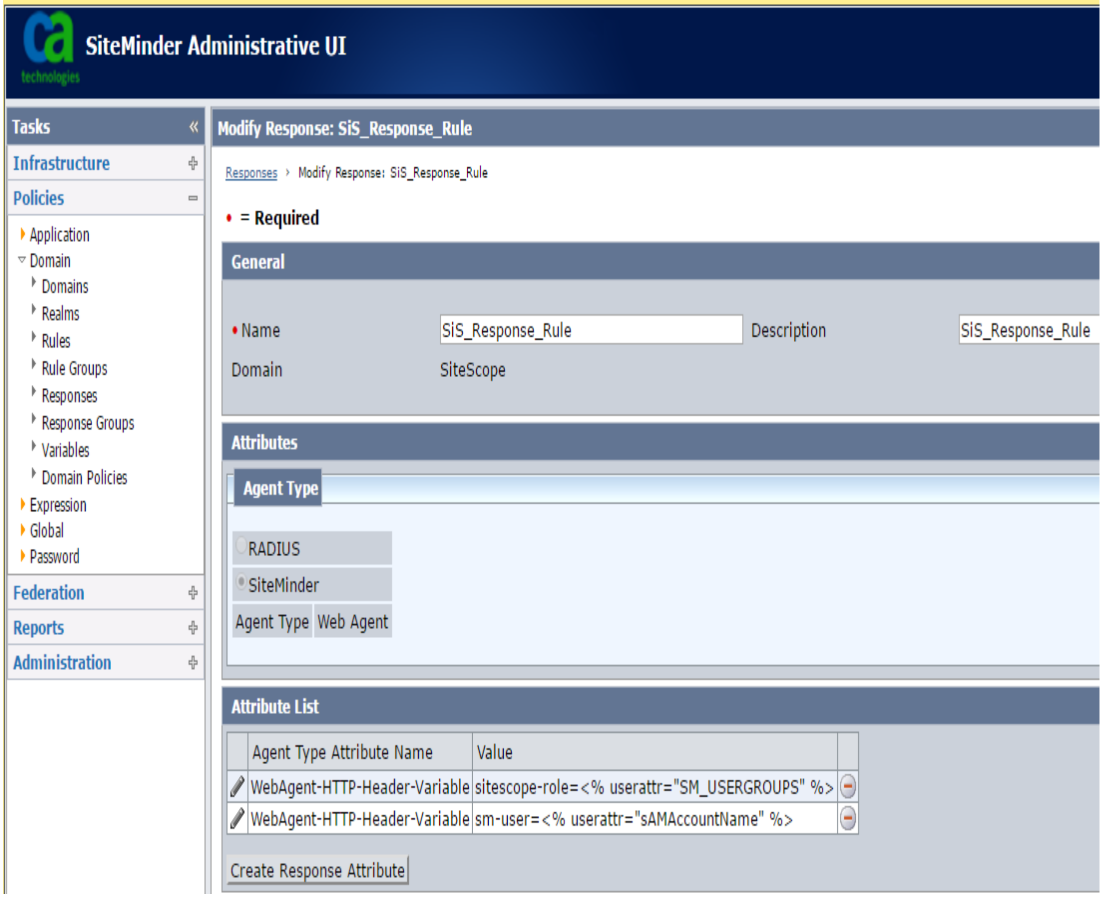
Time Restrictions

No Time Restrictions apply

Active Rule

• Library Name	
• Function Name	
Function Parameters	
Active Rule	<@lib="" func="" param="" @>

6. Create a **Response Rule**.



Modify Response: SiS_Response_Rule

Responses › Modify Response: SiS_Response_Rule

• = Required

General

• Name	SiS_Response_Rule	Description	SiS_Response_Rule
Domain	SiteScope		

Attributes

Agent Type

○ RADIUS

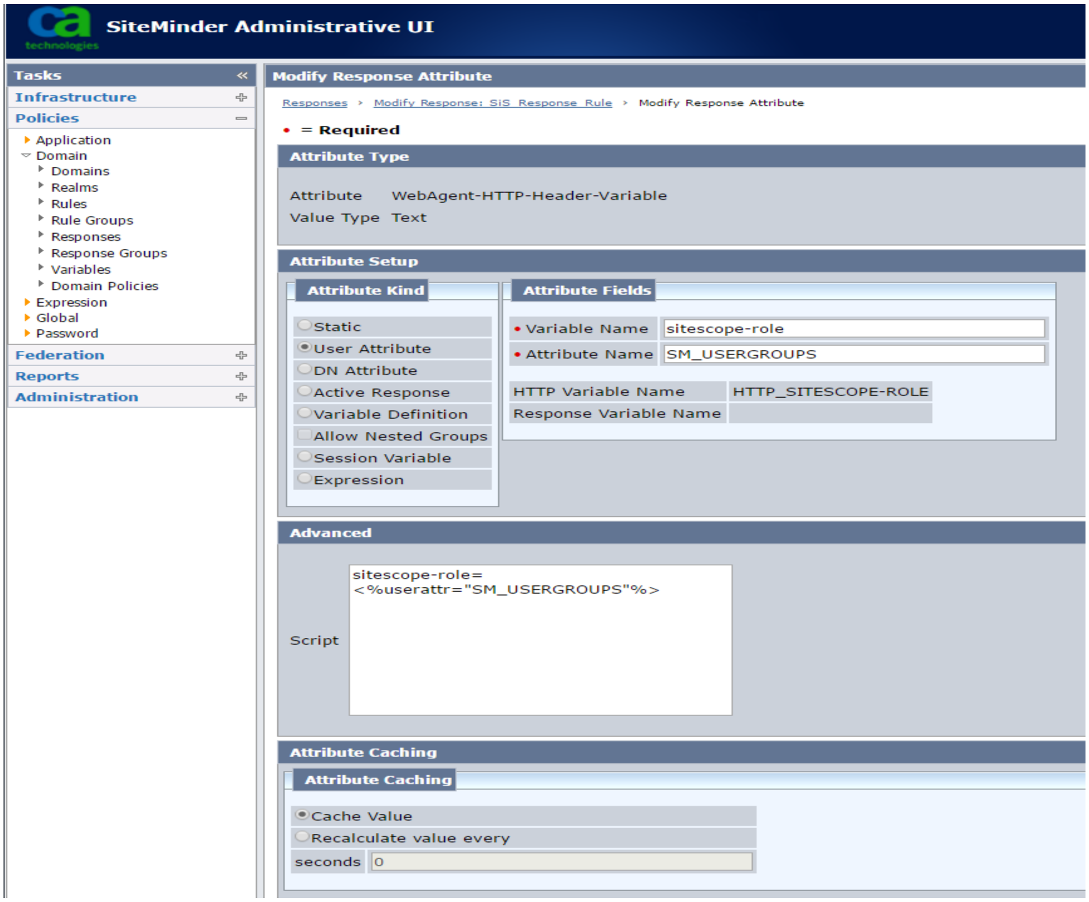
● SiteMinder

Agent Type Web Agent

Attribute List

Agent Type Attribute Name	Value
WebAgent-HTTP-Header-Variable	sitescope-role=<% userattr="SM_USERGROUPS" %>
WebAgent-HTTP-Header-Variable	sm-user=<% userattr="sAMAccountName" %>

7. Set up User Attribute that you want to use as a logon unique identifier (UID).



Modify Response Attribute

Responses › Modify Response: SiS_Response_Rule › Modify Response Attribute

• = Required

Attribute Type

Attribute	WebAgent-HTTP-Header-Variable
Value Type	Text

Attribute Setup

Attribute Kind

- ○ Static
- ● User Attribute
- ○ DN Attribute
- ○ Active Response
- ○ Variable Definition
- □ Allow Nested Groups
- ○ Session Variable
- ○ Expression

Attribute Fields

• Variable Name	sitescope-role
• Attribute Name	SM_USERGROUPS
HTTP Variable Name	HTTP_SITESCOPE-ROLE
Response Variable Name	

Advanced

Script

```
sitescope-role=
<%userattr="SM_USERGROUPS"%>
```

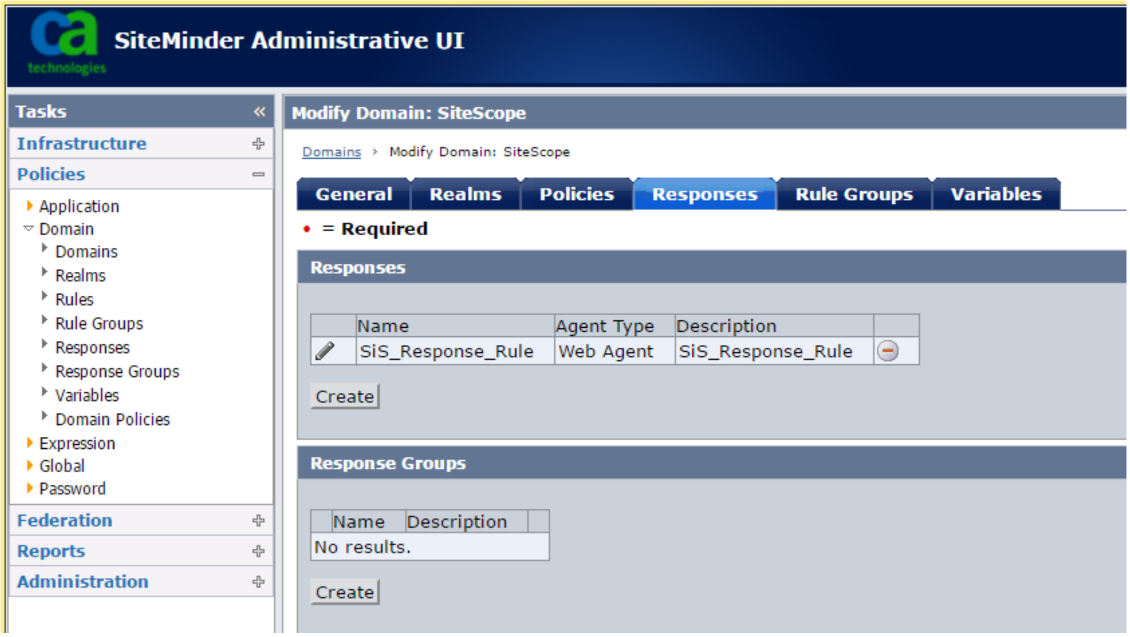
Attribute Caching

Attribute Caching

- ● Cache Value
- ○ Recalculate value every

seconds 0

8. Assign the rule to the SiteScope domain.



Modify Domain: SiteScope

Domains › Modify Domain: SiteScope

• = Required

Responses

	Name	Agent Type	Description	
✎	SiS_Response_Rule	Web Agent	SiS_Response_Rule	⊖

Response Groups

Name	Description
No results.	

You can run the Web Agent Configuration wizard on SiteScope server. For detailed instructions, see the SiteMinder Installation Guide.

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 B: 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 159.

This section includes:

- "Preparing SiteScope for Using TLS" below
- "Manually Configuring SiteScope for TLS on Tomcat" on page 235
- "Manually Configuring SiteScope for Mutual TLS Configuration" on page 237
- "Manually Configuring SiteScope to Connect to APM Server With TLS Deployment" on page 238
- "Manually Configuring SiteScope to Connect to an APM Server That Requires a Client Certificate" on page 239
- "Manually Configuring the Topology Discovery Agent in SiteScope When APM Server Requires a Client Certificate" on page 242

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 "Manually Configuring SiteScope for TLS on Tomcat" on page 235) and the classic interface engine (refer to the instructions in "Accessing SiteScope Reports and Classic User Interface Using HTTPS" on page 246).

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" below
- "Using a Self-Signed Certificate" on page 234

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.

   When you receive your certificate from a certificate authority, the reply message should include a file called **cert.cer**. The **cert.cer** file can be in any of the formats - P12, JKS, or PEM. Then 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 "Manually 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 "Manually Configuring SiteScope for TLS on Tomcat" below.
5. Optionally, you can export the certificate for use in APM 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.

Manually 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:

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

```
<!--
Connector port="8443" maxHttpHeaderSize="8192"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75" SSLEnabled="true"
enableLookups="false" disableUploadTimeout="true"
acceptCount="100" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS"
compression="on" compressionMinSize="2048" noCompressionUserAgents="gozilla,
traviata"
compressableMimeType="text/html,text/xml,text/javascript,text/css,image/x-
icon,application/json" />
->
```

3. Change this section to the following:

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

```
<Connector port="8443"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75" SSLEnabled="true"
enableLookups="false" disableUploadTimeout="true"
acceptCount="100" debug="0" scheme="https" secure="true"
clientAuth="false" sslEnabledProtocols="TLSv1,TLSv1.1,SSLv2Hello"
keystoreFile="<SiteScope_install_path>\SiteScope\groups\serverKeystore"
keystorePass="testing"
/>
```

where `<SiteScope_install_path>` is the path to your SiteScope installation.

If you do not want to use the default 8443 port, you can change the `Connector port`value to any required port. For example, to access SiteScope using port 44 make the following change in the configuration file:

Example: `<!-- Define a SSL Coyote HTTP/1.1 Connector on port 443 -->`

```
<Connector port="443"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75" SSLEnabled="true"
enableLookups="false" disableUploadTimeout="true"
acceptCount="100" debug="0" scheme="https" secure="true"
clientAuth="false" sslEnabledProtocols="TLSv1,TLSv1.1,SSLv2Hello"
keystoreFile="<SiteScope_install_path>\SiteScope\groups\serverKeystore"
keystorePass="testing"
/>
```

Note:

- If there are other HPE 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\lib\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"
  sslEnabledProtocols="TLSv1,TLSv1.1,SSLv2Hello" 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. Restart the SiteScope service. 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)

Manually 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 "Manually Configuring SiteScope for TLS on Tomcat" on page 235.
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:

   Example:
   ```
   <Connector port="8443"
          maxThreads="150" minSpareThreads="25" maxSpareThreads="75" SSLEnabled="true"
          enableLookups="false" disableUploadTimeout="true"
          acceptCount="100" debug="0" scheme="https" secure="true"
          sslEnabledProtocols="TLSv1,TLSv1.1,SSLv2Hello"
          keystoreFile="..\groups\serverKeystore"
          keystorePass="changeit"
   ```

   and adding the following attributes, and changing `clientAuth="true"`:

   Example:
   ```
          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> -keystore ..\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 certificate 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 keystore>
> ```
>
> (Optional) `-Djavax.net.ssl.trustStore=<pathname to truststore in JKS format>`

Manually Configuring SiteScope to Connect to APM Server With TLS Deployment

To connect SiteScope to a APM server with an TLS deployment, perform the following:

1. Connect to the SiteScope server.
2. Import the CA root certificate or APM 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 APM 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 APM, see the Using SSL with SiteScope section in the APM Hardening Guide in the APM Documentation Library.

Manually Configuring SiteScope to Connect to an APM Server That Requires a Client Certificate

To connect SiteScope to a APM server that requires a client certificate, perform the following:

1. Connect to the SiteScope server.
2. Import the CA root certificate or APM 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.certificates\.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\templates.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
   2013
   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 > APM Preferences Available Operations**, click **Reset** to delete all APM related settings from the SiteScope server and all SiteScope configurations from APM.
15. Restart the SiteScope server.
16. In APM, select **Admin > System Availability Management Administration**, and click the **New SiteScope** button to add the SiteScope instance.

> **Note:** If the connection between SiteScope and APM fails, check the **<SiteScope root directory>\log\bac_integration.log** for errors.

Manually Configuring the Topology Discovery Agent in SiteScope When APM Server Requires a Client Certificate

After configuring SiteScope to connect to the APM Gateway server using a client certificate (see "Manually Configuring SiteScope to Connect to an APM Server That Requires a Client Certificate" on page 239), you need to perform the following steps for discovery to report topology to the APM 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 APM 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: 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\classes\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 APM, 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 **APM Front End Use HTTPS** check box.
12. Check the topology appears in **APM > 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:

  > **Example:**
  > ```
  > 2010-12-30 11:03:06,399 [TopologyReporterSender]
  > (TopologyReporterSender.java:364)
  >  ERROR - failed to run main topology agent. topologyCommand=TopologyCommand
  > {commandType=RUN_SCRIPT, …
  > java.lang.IllegalArgumentException: cannot find script with name=create_
  > monitor.py
  > at
  > com.mercury.sitescope.integrations.bac.topology.dependencies.DependenciesC
  > rawler.
  > 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 C: 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 249

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 Oracle Microsystems web site:

http://docs.oracle.com/javase/7/docs/technotes/tools/windows/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=yourCompanyName, L=yourLocation, S=yourState, C=yourCountryCode" -alias
yourAlias -keypass keypass -keystore ..\..\groups\serverKeystore -storepass
passphrase -keyalg "RSA" -validity valdays
```

This command will create a file called **serverKeystore** in the **SiteScope\groups directory**. SiteScope 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")

> **Note:**
>
> - The subcomponents within the **-dname** (distinguished name string) variable are case-insensitive and they are order-sensitive, although you do not have to include all of the subcomponents. The -dname variable should represent your company and the CN is the domain name of the Web server on which SiteScope is installed.
> - 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
keypass -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=yourCompanyName, L=yourLocation, S=yourState, C=yourCountryCode" -alias
   yourAlias -keypass 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 -
   dname "CN=www.yourDomain.com, OU=yourDepartment, O=yourCompanyName,
   L=yourLocation, S=yourState, C=yourCountryCode" -keystore
   ..\..\groups\serverKeystore
   ```

4. To change SiteScope to use a secured connection, you need to add or modify 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
```

Appendix D: Integration with AutoPass License Usage Hub

SiteScope can integrate with the AutoPass License Usage Hub. With this integration, you will be able to view all your HPE product licenses information from the dashboard of the AutoPass License Server Usage Hub reporting server.

To integrate with the AutoPass License server, follow these steps:

1. Stop the SiteScope service.
2. Browse to the `master.config` file located in <SiteScope_directory>SiteScope\groups directory.
3. Open the `master.config` file in edit mode.
4. Enter the IP address of the AutoPass server in the parameter `_usageHubIPAddress=` *<IP address>*, where *`IP address`* is the IP address of the AutoPass server.
5. Start the SiteScope service.

Send Us Feedback

Let us know how we can improve your experience with the Deployment Guide.

Send your email to: docteam@hpe.com