HP System Management Homepage

HP Part Number: 466304-004
Published: November 2009
Edition: 19

Table of Contents

List of Tables

1 Product Overview

The *HP System Management Homepage* (HP SMH) is a Web-based interface that consolidates and simplifies single system management for HP servers on HP-UX, Linux (x86, AMD64, and Intel Itanium), and Microsoft® Windows® operating systems.

By aggregating the data from HP Web-based agents and management utilities, HP SMH provides a common, easy-to-use interface for displaying the following information:

- Hardware fault and status monitoring
- Performance data
- System thresholds
- Diagnostics
- Software version control for an individual server

On an HP-UX system, HP SMH has a bundle tag of `SysMgmtWeb` and is installed by default on all HP-UX versions, including HP-UX 11i v1 (B.11.11), HP-UX 11i v2 (B.11.23), and HP-UX 11i v3 (B.11.31) Operating Environments.

HP SIM

HP SMH is tightly integrated with *HP Systems Insight Manager* (HP SIM). You can easily navigate to HP SMH from the **System Lists** and **System Pages** in HP SIM.

NOTE: Accepting the HP SIM certificate is the default behavior. For more information see "Trusted Management Servers".

There are also several HP SIM tools (under the **Configure→HP-UX Configuration** category) that access HP SMH-based plugins directly.

Integrated Management Tools

HP SMH provides the management server for Web-based system administration.

For HP-UX, key functional areas of the *HP-UX System Administration Manager* (SAM) have been enhanced to provide Web-based management capabilities and are now integrated into HP SMH. These include such areas as Partition Management, Peripheral Devices, Disks & File Systems, Users and Groups, and Kernel Configuration.

HP-UX System Administration Manager (SAM) Deprecation

The HP-UX System Administration Manager (SAM) was an HP-UX System Administration tool that provided tools for performing system administration tasks. In the HP-UX 11i v3 (B.11.31) release of HP-UX, SAM is deprecated. HP SMH, an enhanced version of SAM, is the recommended tool for managing HP-UX.

HP SMH provides Graphical User Interface (GUI), Terminal User Interface (TUI) and Command Line Interface (CLI) for managing HP-UX. You can access these interfaces using the `smh` command (`/usr/sbin/smh`). You can also use the *sam*(1M) command, which behaves the same as the *smh*(1M) command, but the deprecation message is displayed in the beginning.

Most applications for performing administration tasks are now available through the web-based GUI interface and the enhanced TUI. However, a few applications continue to open in ObAM based X-windows or ObAM based TUI.

Some functional areas previously available for system administration are obsolete. These areas are listed in the *HP-UX 11i Release Notes*, available on the HP Technical documentation Web site at **http://docs.hp.com**.

Additional Resources

- HP SMH at Software Depot Home at **http://www.hp.com/go/softwaredepot**.
  - **For HP-UX**

    Select **Security and manageability** and then **HP System Management Homepage HP-UX**.
  - **For Linux**

    Select **Linux** and then **HP Integrity Essentials Foundation Pack for Linux**.
- HP Insight Essentials software page at **http://www.hp.com/servers/manage**.
- ***HP System Management Homepage Release Notes*** The release notes provide documentation for what's new with the release, features and change notifications, system requirements, and known issues. The release notes are available on the HP Technical Documentation Web site at **http://docs.hp.com**.
- **HP System Management Homepage Help System** The help system provides documentation for using, maintaining, and troubleshooting HP SMH. In the HP SMH application, go to the **Help** menu.
- ***HP System Management Homepage Installation Guide*** The installation guide provides information about installing and getting started using HP SMH. It includes an introduction to basic concepts, definitions, and functionality associated with HP SMH. The installation guide is available on the HP Technical Documentation Web site at **http://docs.hp.com**. Also, for Linux and Windows releases, the installation guide is available on the Management CD and at the HP SMH Web page at **http://h18013.www1.hp.com/products/servers/management/agents/documentation.html**.
- ***HP System Management Homepage User Guide*** The user guide provides documentation for using, maintaining, and troubleshooting HP SMH. For Linux and Windows, this guide is available on the HP Technical Documentation Web site at **http://docs.hp.com**. For HP-UX, HP no longer provides a printed user guide. For more information on how to use, maintain, and troubleshoot HP SMH see HP SMH online help content.
- **Next generation single-system management on HP-UX 11i v2 (B.11.23)** A white paper that introduces HP SMH and its various plugins. The use cases involving HP SMH plug-ins described in this document highlight the features provided by HP SMH. The white paper is available on the HP Technical documentation Web site at **http://docs.hp.com/en/4AA0-4052ENW/4AA0-4052ENW.pdf**.
- ***hpsmh*** **(1m) manpage** For HP-UX releases, the manpage is available from the command line using the `man hpsmh` command. This information is not available for Linux and Windows.
- ***smhstartconfig*** **(1M) manpage** For HP-UX releases, the manpage is available from the command line using the `man smhstartconfig` command. This information is not available for Linux and Windows.

  smhassist **(1m) manpage** You can use the `smhassist` command to verify the configurations of SMH and see if there are any dependent software, patches or configuration errors. For HP-UX 11i v3 (B.11.31) and HP-UX 11i v2 (B.11.23) operating system releases, the manpage is available from the CLI using the `man smhassist` command. This information is not available for HP-UX 11i v1 (B.11.11), Linux, and Windows operating systems.
- ***sam*** **(1M) manpage** For HP-UX releases, the manpage is available from the command line using the `man sam` command. This information is not available for Linux and Windows. Please note the SAM functionality changes are explained in a previous section of this document.

Related Topics

- Getting Started
- HP SMH Pages

2 Getting Started

To get started with *HP System Management Homepage* (HP SMH), use the following information when configuring HP SMH and setting up users and security properly.

To configure HP SMH:

- On HP-UX operating environments, HP SMH is installed with default settings. You can change the configuration by modifying the environment variables and tag values set in the following files:
  - `/opt/hpsmh/lbin/envvars`
  - `/opt/hpsmh/conf.common/smhpd.xml`
  - `/opt/hpsmh/conf/timeout.conf`
- On Linux operating systems, HP SMH is installed with default settings. The settings are configurable by using the perl script (hpSMHSetup.pl) located in `/usr/local/hp` (for Linux x86 and x64 systems) or, in `/opt/hp/hpsmh/smhconfig/hpSMHSetup.sh` for Itanium systems.
- On Windows operating systems, the installation enables you to configure HP SMH settings during installation.

NOTE: To change the configurations for the HP-UX, Linux, and Windows operating systems, see the *HP System Management Homepage Installation Guide* on the HP Technical Documentation Web site at **http://docs.hp.com**.

To set up user access and security properly:

1. Add user groups to effectively manage user rights.
   See "User Groups".
2. Configure the trust mode.
   See "Trust Mode".
3. Configure local or anonymous access.
   See "Anonymous/Local Access".

Related Topics

- Signing In
- Configuring Firewall Settings
- Automatically Importing Certificates
- Signing Out

Signing In

The **Sign In** page enables you to access the **Home** page, which contains the available *HP Insight Management Agents*.

The **Sign In page** components include:

- Two fields to input your user name and password from an account that is part of a valid group configured in the SMH **users groups** configuration article.
- Two buttons under the input fields:
  - **Sign In** Validates the values in the user name and password. If both values are valid, the HP SMH main page appears.
  - **Clear** Erases the input values.
- The question mark icon, **?**, displays or hides a floating tooltip box with information about the authentication mechanism and sign in process.

Table 2-1 Tooltip box

Name	Description
User Name	User must be part of a user group accepted by SMH
Password	User name and password must match a valid user
Sign In	Validates user name sign-in to SMH
Clear	Erases user name and password input fields
?	Show/hide tooltip box
Checkbox	Automatically imports the management server certificate when selected. This is applicable when using SSO from HP SIM and the trust mode is set to **TrustByCert**.

NOTE: If an error occurs on a sign-in attempt, you are returned to the **Sign In** page.

A configuration mechanism enables the administrator to customize the image and the message in the **Sign In** page. The administrator can use a custom logo and warning message. As the pages load, HP SMH verifies if the personalized content is enabled and available. If the content is not available, HP SMH uses the standard image and warning message.

Starting HP System Management Homepage (HP SMH) from Internet Explorer

To sign in to HP SMH with Internet Explorer:

1. Navigate to **`https://`***`hostname`***`:2381/`**.

   The first time you browse to this URI, the **Security Alert** dialog box appears, prompting you to indicate whether to trust the server. If you do not import the *certificate*, the **Security Alert** appears every time you browse to HP SMH.

   If you are browsing to an HP-UX server, by default you must use **`http://`***`hostname`***`:2301/`**.

   By default, HP-UX is installed with the `autostart` feature enabled. A daemon listens on port 2301, and starts HP SMH on port 2381 when requested, then stops it after a timeout period. You can also configure HP SMH to always run on port 2381. For more information, see the *smhstartconfig*(1M) command.

   If the `Start on Boot` feature is enabled (instead of `autostart`), a message window appears, which explains the security features. Wait a few seconds to be redirected to port 2381 or click the link at the bottom of the message. The System Management Homepage sign in page appears.

   For more information about procedures on changing the configuration variables, see the *HP System Management Homepage Installation Guide* on the HP Technical Documentation Web site at **http://docs.hp.com**.

   NOTE: To implement your own *Public Key Infrastructure* (PKI) or install your own generated certificates into each managed system, you can install a *certificate authority* Root Certificate into each browser to be used for management. If a Root Certificate is implemented, the **Security Alert** dialog box does not appear. If the alert appears, you might have browsed to the wrong system. For more information about installing the **certificate authority Root Certificate**, see the online help in your browser.

2. Click **Yes**.

   The **Sign In** page appears. If you enabled **Anonymous** access during installation, then System Management Homepage appears.

3. Enter your user name that is recognized by the operating system.
   - **HP-UX** HP SMH initially only allows access to the root user.
   - **Linux** HP SMH initially allows access to users belonging to the root operating system group.
   - **Windows** HP SMH allows access to users belonging to the Administrators operating system group.

If the user credentials cannot be authenticated, the user is denied access.

After logging into HP SMH as an initially allowed user, use the Security Settings to grant access to users in other operating system groups.

Administrator on Windows and *root* on HP-UX or Linux have administrator access on HP SMH.

4. Enter the password that is recognized by the operating system.
5. Click **Sign In**.

   The System Management Homepage appears.

Starting HP SMH from Mozilla or Firefox

To sign in to HP SMH with Mozilla or Firefox:

1. Navigate to **`https://`***`hostname`***`:2381/`**.

   If you are browsing to an HP-UX server, by default you must use **`http://`***`hostname`***`:2301/`**.

   By default, HP-UX is installed with the `autostart` feature enabled. A daemon listens on port 2301, and starts HP SMH on port 2381 when requested, then stops it after a timeout period. You can also configure HP SMH to always run on port 2381. For more information, see the *smhstartconfig*(1M) command.

   If the `Start on Boot` feature is enabled (instead of `autostart`), a message window appears, which explains the security features. Wait a few seconds to be redirected to port 2381 or click the link at the bottom of the message. The System Management Homepage sign in page appears.

   For more information about procedures on changing the configuration variables, see the *HP System Management Homepage Installation Guide* on the HP Technical Documentation Web site at **http://docs.hp.com**.

2. Click **OK**.

   The **Sign In** page appears. If you enabled **Anonymous** access during installation, then System Management Homepage appears.

3. Enter your user name that is recognized by the operating system.
   - **HP-UX** HP SMH initially only allows access to the root user.
   - **Linux** HP SMH initially allows access to users belonging to the root operating system group.
   - **Windows** HP SMH allows access to users belonging to the Administrators operating system group.

   Administrator on Windows and *root* on HP-UX or Linux have administrator access on HP SMH.

4. Enter the password that is recognized by the operating system.
5. Click **Sign In**.

   The System Management Homepage appears.

Starting HP SMH from HP SIM

To start HP SMH by signing in to HP SIM with a Web browser:

1. Navigate to **`https://`***`hostname`***`:50000/`**.

   The first time you browse to this link, the **Security Alert** dialog box appears, asking if you want to trust the server. If you do not import the *certificate*, the **Security Alert** appears each time you browse to Systems Insight Manager (HP SIM).

NOTE: To implement a custom *Public Key Infrastructure* (PKI) or install your own generated certificates into each managed system, you can install a certificate authority Root Certificate into each browser to be used for management. If a Root Certificate is implemented, the **Security Alert** dialog box does not

appear. If the alert appears, you might have browsed to the wrong system. For more information about installing the **certificate authority Root Certificate**, see the online help in your browser.

2. Click **Yes**.

   The **Sign In** page appears.
3. Enter your user name that is recognized by the operating system.
4. Enter the password that is recognized by the operating system.
5. Click **Sign In**.
6. Select **Tools→System Information→System Management Homepage**.
7. Select a target system from the list.
8. Select a check box next to a target system, and then click **Apply**.
9. Verify the target system by selecting a check box next to the system, and then click **Run Now**.

   The **Security Alert** dialog box appears, prompting you to trust the server. If you do not import the *certificate*, the **Security Alert** appears each time you browse to HP SMH.

   The System Management Homepage appears.

Starting from the HP-UX Command Line

When you run the `sam` or `smh` command and the DISPLAY environment variable is set, HP SMH opens in the default Web browser. If the DISPLAY environment variable is not set, HP SMH opens in the TUI. Most applications for performing administration tasks are available through the Web-based GUI interface and an enhanced TUI. However, some applications continue to open in ObAM based X-windows or ObAM based TUI.

HP recommends using the *smh*(1M) command. However, the *sam*(1M) command continues to be available and behave just as the *smh*(1M) command. Some functional areas previously available for system administration are obsolete. These areas are listed in the *HP-UX 11i Release Notes*, available on the HP Technical documentation web site at **http://docs.hp.com**.

HP SMH Management Server

By default, the HP SMH management server for HP-UX starts only on demand. It does not run continually. A daemon listens on port 2301 to start an instance of the management server. On Linux, HP SMH is started on boot.

Related Topics

- Getting Started
- Configuring Firewall Settings
- Automatically Importing Certificates
- Signing Out
- HP SMH Pages

Configuring Firewall Settings

Windows

Some operating systems including Windows XP with Service Pack 2 and Windows Server 2003 SBS implement a firewall that prevents browsers from accessing the ports required for the Version Control Repository Manager access. To resolve this issue, configure the firewall with exceptions to enable browsers to access the ports used by HP SIM and Version Control Repository Manager.

NOTE: For Windows XP with Service Pack 2, the firewall configuration leaves the default SP2 security enhancements intact, but enables traffic over the ports. These ports are required for the Version Control

Repository Manager to run. The secure and insecure ports must be added to enable proper communication with your browser.

To configure the firewall:

1. Select **Start→Settings Control Panel**.
2. To configure the firewall settings, double-click **Windows Firewall**.
3. Select **Exceptions**.
4. Click **Add Port**.
5. Enter the following product name and the port number information.

   Add the exceptions listed in the following table to the firewall protection:

   Table 2-2 Firewall exceptions

Product	Port Number
HP SMH Insecure Port:	2301
HP SMH Secure Port:	2381

6. Click **OK** to save your settings and close the **Add a Port** dialog box.
7. Click **OK** to save your settings and close the **Windows Firewall** dialog box.

Linux

Configuring firewalls varies, depending on the version of Linux installed.

Red Hat Enterprise Linux 4 and 5

The following displays an example of iptables firewall rules for Red Hat Enterprise Linux 4 and 5 in the `/etc/sysconfig/iptables` file:

```
# Firewall configuration written by redhat-config-securitylevel
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -p 50 -j ACCEPT
-A RH-Firewall-1-INPUT -p 51 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 21 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

The following displays the new value in the iptables firewall rules for Red Hat Enterprise Linux 4 and 5 that allows access to HP SMH in the `/etc/sysconfig/iptables` file:

```
# Firewall configuration written by redhat-config-securitylevel
# Manual customization of this file is not recommended.
```

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -p 50 -j ACCEPT
-A RH-Firewall-1-INPUT -p 51 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 21 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 2301 -j
ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 2381 -j
ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

SUSE Linux Enterprise Server

SUSE Linux Enterprise Server 9 and 10 firewalls are configured using the YAST2 utility.

To configure the firewall:

1. Using the YAST2 utility, select **Security & Users→Firewall**.
   The **Firewall Configuration (Step 1 of 4): Basic Settings** window appears.
2. Click **Next**.
   The **Firewall Configuration (Step 2 of 4): Services** window appears.
3. In the **Additional Services** field, enter `2301:2381`, and then click **Next**.
   The **Firewall Configuration (Step 3 of 4): Features** window appears.
4. Click **Next**.
   The **Firewall Configuration (Step 4 of 4): Logging Options** window appears.
5. Click **Next**.
   A dialog box appears asking you to confirm your intention to save settings and active firewall.
6. Click **Continue**.
   The firewall is configured and your settings are saved.

Related Topics

- Getting Started
- Signing In
- Automatically Importing Certificates
- Signing Out
- HP SMH Pages

Automatically Importing Certificates

The **Automatically Import Management Server Certificate** feature enables you to automatically import the HP SIM *certificate* when accessing the HP SMH from an HP SIM system.

NOTE: Your login must have administrative access to HP SMH to automatically import the HP SIM certificate.

To automatically import the HP SIM certificate:

1. From an **HP Systems Insight Manager** or **HP Insight Manager 7** system, select a link to a system.

   If the **Trust By Certificate** option is selected in HP SMH **Settings**, click the **Security** link, and then click the **Trust Mode** , and a certificate for the HP SIM system you are accessing has not been imported into the **Trusted Certificates List**, the **Sign In** page displays the **Automatically Import Management Server Certificate** option. The Certificate Information retrieved from *SERVER NAME* displays the HP SIM certificate details.

2. If you do not want to add the HP SIM certificate to the **Trusted Certificates List**; deselect **Automatically Import Management Server Certificate**. Deselecting this option still requires you to enter login credentials. However, administrator credentials are not required to login.

   If you enable HP SMH to automatically import the HP SIM certificate, future access to the system is seamless. You are not prompted for your login credentials.

3. Leave **Automatically Import Management Server Certificate** selected, enter your HP SMH credentials, and then click **Sign In** to automatically import the certificate.

   The certificate is added to the **Trusted Certificates List**.

Related Topics

- Getting Started
- Signing In
- Configuring Firewall Settings
- Signing Out
- Security

Signing Out

You can sign out of HP SMH, using either of the following options:

- In the HP SMH banner, click **Sign Out**.

  The HP System Management Homepage **Sign in** page appears.

- Close every instance of the Web browser used to sign in to HP SMH.

Related Topics

- Getting Started
- Signing In
- Configuring Firewall Settings
- Automatically Importing Certificates
- HP SMH Pages

3 Navigating the Software

The *HP System Management Homepage* (HP SMH) displays all *HP Web-enabled System Management Software* that provides information. In addition, HP SMH displays various categories (in boxes) that have icons defining the status of the items. For more information, see "The Home Page".

The HP SMH main page is divided into two major areas: the header and the standard container.

- **Header Frame** The header frame is constantly visible regardless of the page you are viewing and contains the following four subareas:
  - **Master header.** In Windows and Linux, the links show the path you are viewing, the user, and a **Sign Out** link.

    Master header. In HP-UX, the header displays the path you are viewing, user information (the user who has logged in), the **Sign Out** link, and the **Session never expires** check box.
  - **Menu.** Each item is a direct link to a page or section including:
    - Home
    - Settings
    - Tasks
    - Tools
    - Logs
    - Webapps (Windows and Linux only)
    - Support
    - Help
  - **Main title area.** The area under the master header and menu contains the following items.
    - **Title.** The title of the section of page you are viewing.
    - **Host Name.** The name of the system.
    - **System Model.** The model appears as **Unknown** if the HP Insight Management Agent for servers is not installed on the system.
    - **Management Processor.** The name of the management processor.
    - **Data Source** Indicates which source is populating management data. For instance, WBEM for HP Insight Management WBEM Providers or SNMP for HP Insight Management Agents. If no source is installed, no data string will appear.
    - **Icons.** An option that enables you to switch between icon and list view modes when clicked.
    - **Bread crumbs.** The area under the main title that is divided into four parts.
      - First level menu item
      - **Legend.** A link that, when clicked, displays a floating box listing all possible statuses of webapps.
      - **Refresh.** A link that reloads the header and information areas.
      - **Time.** Displays the time the page was loaded. When you mouse over the time area, you can see the date the page was loaded.
- **Data Frame.** The standard container contains the sections or pages as:
  - Boxes
  - Icons
  - Pages as configurations

- Support
- Help
- Webapps

The data frame shows the status for all HP Web-enabled System Management Software and utilities on the system.

Information Areas

Depending on your operating system (HP-UX, Linux, or Windows), the following information areas appear in the header or data frames:

- **HP SMH Pages**
  - "Signing In"
  - "The Home Page"
  - "The Settings Page"
  - "The Tasks Page"
  - "The Logs Page"
  - "The Installed Webapps Page"
  - "The Support Page"
  - "The Help Page"
- **Current User.** The Current User displays the identity of the user that is signed in.
  - If the user is a operating system-based user, a **Sign Out** link appears.
  - If anonymous access is enabled, the **Current User** displays **hpsmh_anonymous** and the **Sign In** link appears.
  - If **Local Access** is enabled, the **Current User** displays **hpsmh_local_anonymous** or **hpsmh_local_administrator**, depending on what level of access has been enabled, and local access appears below user type.
  - If user type is **local_access_administrator**, no signin or signout link appears.
- **Boxes.** Boxes display webapps results in a list of items with their result status.
  - An overall status icon represents the worst status of items inside the box and appears in the title bar along with the title.
  - Under the title bar, is a list of items in the box. Each item can have a status icon to the left of its name.
  - In the footer of the box, is an expansion line with a link that, when clicked, expands the height of the box to include the total number of items if the items exceed the five-line limit.
- **Loading screen.** When an item is selected, a status indicator appears as the **Loading screen** during the load process of the page. This prevents users from selecting other items after the initial selection.
- **Number of columns.** The number of boxes or columns presented in each line in the list view mode is defined by the display resolution setting. For example, if your resolution is set at 800x600, only three boxes are presented in a line, while in greater resolutions, the number of boxes visible is four.
- **Notes.** Notes are sections placed on the right side and used in most pages. These notes inform you how to use the controls and what kind of values is expected.
- **Icon view.** Icons appear for items and sections. When an icon is clicked, another page appears with its items as icons. You can view the status of the items inside the box by hovering your mouse over the icon to view a tooltip containing the total of **Critical**, **Major**, **Minor** and **Warning** statuses of installed applications.

- **Timeout Warnings.** Timeout warnings appear as a floating box in the page footer on the right side when you do not load a page in SMH within the time limit set for timeouts.
- **Dynamic Lists in Pages.** A dynamically created list of elements appears for each item you want to add or remove to a page and are available for the following pages:
  - IP Binding
  - IP Restricted Login
  - Trust Mode
  - *Kerberos Authentication*
  - User Groups
- **Legend:** This is a link that displays a floating box listing all possible statuses of installed webapps.

Table 3-1 Status icons

Icon	Status
	Critical
	Major
	Minor
	Warning
	Normal
	Disabled
	Unknown
	Informational
	Tools and utilities

- **Management Processor.** This displays a link to the **Remote Insight Lights-Out Edition** (**RILOE**) board or the **Integrated Lights-Out** (**iLO**) board. This information is provided by the HP Insight Management Agent. If no HP Web-enabled System Management Software is installed that provides this information, **none** appears.

Related Topics

- Getting Started
- The Home Page
- The Settings Page
- The Tasks Page
- The Logs Page
- The Installed Webapps Page
- The Support Page
- The Help Page

HP SMH Pages

The *HP SMH* displays up to nine pages that enable you to access and configure settings related to participating *HP Web-enabled System Management Software*. The **Tasks** page and the **Tools** page appears if HP Web-enabled System Management Software provides information for them.

HP SMH pages include:

- "Getting Started"
- "The Home Page"
- "The Settings Page"
- "The Tasks Page"
- "The Logs Page"
- "The Installed Webapps Page"
- "The Support Page"
- "The Help Page"

Related Topics

- Product Overview
- Navigating the Software
- Getting Started

4 The Home Page

The **Home** page provides the system, subsystem, and status views of the server. The **Home** page displays groupings of systems and their status. The information on the **Home** page is provided by the integrated agents or management utilities.

For HP-UX operating systems, the **Home** page includes information provided by integrated *Web-Based Enterprise Management* (WBEM) property pages and management utilities.

For Linux and Windows operating systems, the **Home** page includes information provided by integrated version control, server, and storage agents.

Overall Status Summary

The **Overall Status Summary** displays links to all subsystems that have a critical, major, minor, or warning status, which the integrated *HP Web-enabled System Management Software* provides. If there are no agents installed or no critical, major, minor or warning items, the **Overall Status Summary** displays **no items**.

System Status

The **System Status** displays a status icon with a label under it. A specific webapp sets the value of the **System Status** icon by using a predefined heuristic to signal the system status. If no webapp sets the System Status, then the worst of all the statuses in the *Overall Status Summary* box is displayed.

Default HP-UX Property Pages

Specific WBEM property pages are delivered as part of the HP-UX HP SMH installation. These depend on other WBEM providers that are delivered with the HP-UX operating system, such as `WBEMServices` (WBEM Services for HP-UX) and `SFM-CORE` (HP-UX System Fault Management).

System

The **System** category presents the system hardware WBEM information. The first link is a **System Summary** that includes the system's identity information and health status. This health status is also propagated to the HP Systems Insight Manager (HP SIM) HS column for the HP-UX system if using HP SIM. In addition to the summary, links show status and other information about subsystems, such as memory and processors.

Operating System

The **Operating System** category contains links that show basic operating system configuration, usage, state, and other information.

Network

The **Network** category contains links that display basic network system configuration, usage, state, and other information.

Software

The **System Software** category contains links that display information about the Software Distributor bundles and products, including patch products.

NOTE: This category is not available on Linux Itanium.

Storage

The **Storage** category contains links that show basic storage system configuration, usage, state, and other information.

SysMgmtPlus

SysMgmtPlus is an enhancement plus package to HP SMH. SysMgmtPlus enhances the property pages of SMH by displaying additional details and introducing dynamic capability to the web page. SysMgmtPlus displays information about only devices that exist on the system.

HP SMH version 3.0 and later must be installed for SysMgmtPlus to function. If SysMgmtPlus is installed manually, after installing HP SMH, HP SMH must be restarted.

Related Topics

- Getting Started
- The Home Page
- The Settings Page
- The Tasks Page
- The Logs Page
- The Installed Webapps Page
- The Support Page
- The Help Page

5 The Settings Page

The **Settings** page contains links to the settings and configuration pages of the *HP System Management Homepage* (HP SMH) and other integrated management tools found on the **Tools** page.

Table 5-1 Settings page links

Name	Description	Access
SNMP Webagent Box (Windows and Linux only)	Provides links that enable you to configure HP Web-enabled System Management Software agents. • **"SMH Data Source Management"** Sets options for HP SMH Data Source. • **"SNMP Configuration"** Sets options for HP Web-enabled System Management Software agents. • **"UI Options"** Sets options for HP Web-enabled System Management Software agents help.	Select **Settings** from the menu.
HP SMH Data Source Category (Windows and Linux only)	Enables you to change the HP SMH management data source. For more information, see "SMH Data Source Management".	Select **Settings** from the menu, and then click the **Data Source** link in the **SNMP Webagent** box.
SNMP Configuration Category (Windows and Linux Only)	Provides web serving and abstracts security and HP Systems Insight Manager (HP SIM) interaction for webapps. For more information, see "SNMP Configuration".	Select **Settings** from the menu, and then click the **SNMP Configuration** link in the **SNMP Webagent** box.
UI Options Category (Windows and Linux Only)	Allows you to display the inline help icons or to not display them. For more information, see "UI Options".	Select **Settings** from the menu, and then click the **UI Options** link in the **SNMP Webagent** box.
System Management Homepage Box	Provides links that enable you to configure HP SMH settings. It provides links to the following: • **"UI Properties"** Sets options for the appearance of HP SMH. • **"User Preferences"** Sets how HP SMH appears. • **"Security"** Displays links for security options.	Select **Settings** from the menu.
UI Properties Category	Controls options for the appearance of HP SMH. It has controls for choosing between list and icon view, if you want to use custom text and images relating to your company, and box and item ordering type by name or by status. These options serve as the default options for all users unless users set specific options in **User Preferences**. For more information, see "UI Properties".	Select **Settings** from the menu, and then click the **UI Properties** link in the **System Management Homepage** box.
User Preferences Category	Enables you to set how HP SMH appears. It has controls for choosing between list and icon view, and box and item ordering type by name or status. These settings are valid for the user who sets them. These values are stored for 30 days. For more information, see "User Preferences".	Select **Settings** from the menu, and then click the **User Preferences** link in the **System Management Homepage** box.

Name	Description	Access
Security	Provides links that enable you to configure HP SMH settings. It provides links to the following: • Anonymous/Local Access • IP Binding • IP Restricted Login • Local Server Certificate • Port 2301 (Windows and Linux only) • Timeouts • Trust Mode • Trusted Management Servers • Kerberos Authentication (Windows Only) • User Groups	Select **Settings** from the menu, and then click the **Security** link in the **System Management Homepage** box.

Table 5-2 Security options

Name	Description	Access
"Anonymous/Local Access"	Enables the administrator to set options that allow anonymous users to access SMH pages or to allow automatic login to SMH when running in a local console as administrator or anonymous user. For more information, see "Anonymous/Local Access".	Select **Settings** from the menu, click the **Security** link in the **System Management Homepage** box, and then click the **Anonymous/Local Access** link.
"IP Binding"	Enables you to control the addresses that SMH is bound to. For more information, see "IP Binding".	Select **Settings** from the menu, click the **Security** link in the **System Management Homepage** box, and then click the **IP Binding** link.
"IP Restricted Login"	Enables you to add addresses from where SMH is accessible or blocked. For more information, see "IP Restricted Login".	Select **Settings** from the menu, click the **Security** link in the **System Management Homepage** box, and then click the **IP Restricted Login** link.
"Local Server Certificate"	This category has two blocks and is used for generation of certificate requests that can be sent to a Certificate Authority (CA) to sign and later import the signed certificate that was received. For more information, see "Local Server Certificate".	Select **Settings** from the menu, click the **Security** link in the **System Management Homepage** box, and then click the **Local Server Certificate** link.
"Port 2301"	Enables you to configure access to Port 2301. For more information, see "Port 2301".	Select **Settings** from the menu, click the **Security** link in the **System Management Homepage** box, and then click the **Port 2301** link.
"Timeouts"	Configures the values of timeout for SMH. Two timeouts can be configured: Session timeout and UI timeout. For more information, see "Timeouts".	Select **Settings** from the menu, click the **Security** link in the **System Management Homepage** box, and then click the **Timeouts** link.
"Trust Mode"	Configures the trust mode used by SMH. Three trust modes that can be configured; Trust by Certificate, Trust by Name, and Trust All. For more information, see "Trust Mode".	Select **Settings** from the menu, click the **Security** link in the **System Management Homepage** box, and then click the **Trust Mode** link.
"Trusted Management Servers"	Configures the certificates that are stored in the server and allows you to add or remove certificates. For more information, see "Trusted Management Servers".	Select **Settings** from the menu, click the **Security** link in the **System Management Homepage** box, and then click the **Trusted Management Servers** link.

Name	Description	Access
"Kerberos Authorization Procedure (Windows Only)"	Allows an authorized user to configure which users have **Kerberos** authenticated access to HP SMH and their respective access level. For more information, see "Kerberos Authorization Procedure (Windows Only)".	Select **Settings** from the menu, click the **Security** link in the **System Management Homepage** box, and then click the **Kerberos Authentication** link.
"User Groups"	Allows an authorized user to configure which group of users has access to HP SMH and their respective access level. For more information, see "User Groups".	Select **Settings** from the menu, click the **Security** link in the **System Management Homepage** box, and then click the **User Groups** link.

Related Topics

- The Home Page
- The Tasks Page
- The Logs Page
- The Installed Webapps Page

SMH Data Source Management

The **Data Source** page enables you to change the HP SMH management data source.

The **Data Source** setting is only available if the HP Insight Management WBEM providers are installed.

NOTE: If no source is installed, SMH Data Source is shown with no data string.

- **SMH Data source: WBEM** Indicates that HP Insight Management WBEM Providers are currently providing management data to the SMH pages for this server.
- **SMH Data source: SNMP** Indicates that HP Insight Management Agents (SNMP) are currently providing management data to the SMH pages for this server.

To configure the **Data Source**, complete the following steps:

1. Select **Settings** from the menu.
2. In the **SNMP Webagent** box, click the **Data Source** link.
3. Select **SNMP** or **WBEM** .
4. Click **Save and Apply Changes**.

Related Topic

▲ The Settings Page

SNMP Configuration

The **SNMP Configuration** page provides web serving and abstracts security and HP SIM interaction for webapps. For more information, see the *HP Systems Insight Manager 5.2 Technical Reference Guide*, available on the HP Technical Documentation Web site at **http://docs.hp.com**.

To configure the **SNMP Configuration**, complete the following steps:

1. Select **Settings** from the menu.
2. In the **SNMP Webagent** box, click the **SNMP Configuration** link .

Related Topic

▲ The Settings Page

UI Options

The **UI Options** page enables you to display inline help icons.

To configure the **UI Options**, complete the following steps:

1. Select **Settings** from the menu.
2. In the **SNMP Webagent** box, click the **UI Options** link.
3. Remove the check in the check box beside **Show Help Icons** to no longer display inline help icons.

   Select the check box beside **Show Help Icons** to display the inline help icons.
4. Click **Save and Apply Changes**.

Related Topic

▲ The Settings Page

UI Properties

The **UI Properties** category controls options for the appearance of HP SMH. **UI Properties** has controls for choosing:

- List view
- Icon view
- Box and item ordering type
  - By name
  - By status
- The last option is used by administrators to set custom images for the master header and **Sign In Page** and custom warning text for the **Sign In Page**.

Table 5-3 UI Properties options

Option	Description
Presentation Mode	Enables you to set the default presentation mode by selecting from a list. The **Presentation Mode** has two options: **List View** and **Icon View**.
Box Ordering	Determines the order that the boxes are shown. If you order by name, the items appear alphabetically. If you order by status, items appear from worst (critical) to best (normal).
Box Item Ordering	Determines the order that items in boxes are shown. If you order by name, the items appear alphabetically. If you order by status, items appear from worst (critical), to best (normal).
Use Custom text and images	Enables the administrator to set custom warning messages in the **Sign In** page and imagery in the **Sign In** page and master header.

To set **UI Properties**, complete the following steps:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **UI Properties** link.
3. From the **Presentation Mode** list, Select **List** or **Icon**.
4. From the **Box ordering** list, select **By status** or **By name**.
5. From the **Box item ordering** dropdown list, select either **By status** or **By name**.
6. To use a custom image and custom warning, complete the following steps:
   a. Place the image and text files in the following directories:
      - *SMHBaseDir*`/data/htdocs/custom_ui/logo0.jpg` (for the loading screen image)
      - *SMHBaseDir*`/data/htdocs/custom_ui/logo1.jpg` (for the master header image)
      - *SMHBaseDir*`/data/htdocs/custom_ui/warning1.txt` (for the warning text)

      All three files must be present to view custom images and warning text.
   b. Click the check box beside **Use custom text and images**.
7. Click **Apply**.

Related Procedure

▲ User Preferences

Related Topic

▲ The Settings Page

User Preferences

The **User Preferences** category controls options for the appearance of HP SMH.

- List view
- Icon view
- Box and item ordering type
  - By name
  - By status

Table 5-4 User Preferences options

Option	Description
Presentation Mode	Enables you to set the default presentation mode by selecting from a list. The **Presentation Mode** has two options: **List View** and **Icon View**.
Box Ordering	Determines the order that the boxes are shown. If you order by name, the items appear alphabetically. If you order by status, items appear from worst (critical) to best (normal).
Box Item Ordering	Determines the order that items in boxes are shown. If you order by name, the items appear alphabetically. If you order by status, items appear from worst (critical), to best (normal).

To set **User Preferences**, complete the following steps:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **User Preferences** link.
3. From the **Presentation Mode** list, select **List** or **Icon**.
4. From the **Box ordering** list, select **By status** or **By name**.
5. From the **Box item ordering** list, select **By status** or **By name**.
6. If you do not want the session to expire (in the case of HP-UX only), click the check box beside **Session Never Expires**.

NOTE: HP SMH service timeouts is only applicable to HP-UX systems.

7. Click **Apply**.

NOTE: Each user is able to set their preferences for a session. Individual user preferences take precendence over settings in UI properties.

Related Procedure

▲ UI Properties

Related Topic

▲ The Settings Page

Security

The **Security** link provides options for you to manage the security of HP SMH:

Table 5-5 Security options

Name	Description	Access
"Anonymous/Local Access"	Enables the administrator to set options that allow anonymous users to access SMH pages or to allow automatic login to SMH when running in a local console as administrator or anonymous user. For more information, see "Anonymous/Local Access".	Select **Settings** from the menu, click the **Security** link in the **System Management Homepage** box, and then click the **Anonymous/Local Access** link.
"IP Binding"	Enables you to control the addresses that SMH is bound to. For more information, see "IP Binding".	Select **Settings** from the menu, click the **Security** link in the **System Management Homepage** box, and then click the **IP Binding** link.
"IP Restricted Login"	Enables you to add addresses from where SMH is accessible or blocked. For more information, see "IP Restricted Login".	Select **Settings** from the menu, click the **Security** link in the **System Management Homepage** box, and then click the **IP Restricted Login** link.
"Local Server Certificate"	This category has two blocks and is used for generation of certificate requests that can be sent to a Certificate Authority (CA) to sign and later import the signed certificate that was received. For more information, see "Local Server Certificate".	Select **Settings** from the menu, click the **Security** link in the **System Management Homepage** box, and then click the **Local Server Certificate** link.
"Port 2301"	Enables you to configure access to Port 2301. For more information, see "Port 2301".	Select **Settings** from the menu, click the **Security** link in the **System Management Homepage** box, and then click the **Port 2301** link.
"Timeouts"	Configures the values of timeout for SMH. Two timeouts can be configured: Session timeout and UI timeout. For more information, see "Timeouts".	Select **Settings** from the menu, click the **Security** link in the **System Management Homepage** box, and then click the **Timeouts** link.
"Trust Mode"	Configures the trust mode used by SMH. Three trust modes that can be configured; Trust by Certificate, Trust by Name, and Trust All. For more information, see "Trust Mode".	Select **Settings** from the menu, click the **Security** link in the **System Management Homepage** box, and then click the **Trust Mode** link.
"Trusted Management Servers"	Configures the certificates that are stored in the server and allows you to add or remove certificates. For more information, see "Trusted Management Servers".	Select **Settings** from the menu, click the **Security** link in the **System Management Homepage** box, and then click the **Trusted Management Servers** link.
"Kerberos Authorization Procedure (Windows Only)"	Allows an authorized user to configure which users have **Kerberos** authenticated access to HP SMH and their respective access level. For more information, see "Kerberos Authorization Procedure (Windows Only)".	Select **Settings** from the menu, click the **Security** link in the **System Management Homepage** box, and then click the **Kerberos Authentication** link.
"User Groups"	Allows an authorized user to configure which group of users has access to HP SMH and their respective access level. For more information, see "User Groups".	Select **Settings** from the menu, click the **Security** link in the **System Management Homepage** box, and then click the **User Groups** link.

Related Topics

- The Settings Page
- Command Line Interface Configuration

Anonymous/Local Access

Anonymous/Local access enables you to select the following settings to include:

- **Anonymous Access** (Disabled by default). Enabling **Anonymous Access** enables a user to access the HP SMH without logging in. If **Anonymous** is selected, any user, local or remote, has access to unsecured pages without being challenged for a username and password.

  Caution: HP does not recommend the use of anonymous access.

- **Local Access** (Disabled by default). Enabling **Local Access** means you can gain local access to HP SMH without being challenged for authentication. This means that any user with access to the local console is granted full access if **Administrator** is selected.

  Caution: HP does not recommend the use of local access unless your management server software enables it.

To enable anonymous access:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **Anonymous/Local Access** link.
4. Under **Anonymous Access**, select the box beside **Allow Anonymous users access to unsecured pages**.
5. Click **Apply** to apply your settings.

To disable anonymous access:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **Anonymous/Local Access** link.
4. Under **Anonymous Access**, remove the check from the box beside **Allow Anonymous users access to unsecured pages**.
5. Click **Apply** to apply your settings.

To enable local access:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **Anonymous/Local Access** link.
4. Under **Local Access**, select the box beside **Turn on automatic logon in System Management Homepage**.
5. Select **Anonymous** or **Administrator**.
6. Click **Apply** to apply your settings.

To disable local access:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **Anonymous/Local Access** link.
4. Under **Local Access**, deselect the box beside **Turn on automatic logon in System Management Homepage**.
5. Click **Apply** to apply your settings.

Related Procedures

- IP Binding
- IP Restricted Login
- Local Server Certificate
- Alternative Names Certificates
- Port 2301
- Timeouts
- Trust Mode
- Trusted Management Servers

- Kerberos Authorization Procedure (Windows Only)
- User Groups

Related Topic

▲ The Settings Page

IP Binding

IP Binding specifies the *IP addresses* that HP SMH accepts requests from and controls the nets and subnets that requests are processed.

Administrators can configure HP SMH to only bind to addresses specified in the **IP Binding** window. Five subnet IP addresses and netmasks can be defined.

An IP address on the server is bound if it matches one of the entered IP Binding addresses after the mask is applied.

HP SMH on Windows and Linux supports both IPv4 and IPv6 addresses.

HP SMH on HP-UX currently supports only IPv4 addresses.

NOTE: HP SMH always binds to 127.0.0.1. If IP Binding is enabled and no subnet/mask pairs are configured, HP SMH is only available to 127.0.0.1. If IP Binding is not enabled, you bind to all addresses.

To configure IP Binding:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **IP Binding** link.
4. Enter the **Subnet IP Address**.
5. Enter the **Netmask**.
6. Click **Add** to add the **Subnet IP Address** and **Netmask** that were entered in the preceding steps.

   You can add up to five subnet IP addresses and netmasks by repeating steps 4 through 7.
7. Click **Apply** to apply the configurations.

NOTE: The netmask is applicable only for IPv4 addresses.

To remove IP addresses from the list:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **IP Binding** link.
4. Select the check box beside the IP address you want to remove.
5. Click **Remove**.
6. Click **Apply** to apply the configurations.

Each IP address and netmask must consist of four octets with values between 0 and 255 (the same for each netmask).

Netmasks must start with the number 1 in the highest bit and continue with all number 1s until they switch to all number 0s (for example, 255.255.0.0, 192.0.0.0, 255.192.0.0).

Related Procedures

- Anonymous/Local Access
- IP Restricted Login
- Local Server Certificate
- Alternative Names Certificates
- Port 2301
- Timeouts

- Trust Mode
- Trusted Management Servers
- Kerberos Authorization Procedure (Windows Only)
- User Groups

Related Topic

▲ The Settings Page

IP Restricted Login

IP Restricted login enables HP SMH to restrict login access based on the *IP address* of a system from which the signin is attempted.

For Linux and Windows, you can set a restricted address at installation. From all operating systems, administrators can set a restricted address from the **IP Restricted login** page. Note the following:

- If an IP address is restricted, it is restricted even if it is also listed in the permitted box.
- If IP addresses are in the permitted list, only those IP addresses can sign in, except for *localhost*.
- If no IP addresses are in the permitted list, sign in access is allowed to any IP addresses not in the restricted list.

HP SMH on Windows and Linux supports IPv4 and IPv6 addresses.

NOTE: On systems operating on Windows operating system, the range of IPv6 addresses is valid with and without brackets.

For example: Both [2001:db8:c18:1:250:8bff:fee2:5175]-[2001:db8:c18:1:250:8bff:fee2:5180] and 2001:db8:c18:1:250:8bff:fee2:5175-2001:db8:c18:1:250:8bff:fee2:5180 are valid conditions on systems running on Windows operating system.

HP SMH on HP-UX currently supports only IPv4 addresses.

To restrict IP addresses:

1. Select **Settings** from the menu
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **IP Restricted Login** link.
4. Enter the **IP address** or **IP address range**.

   List IP address ranges beginning with the lower end of the range, followed by a hyphen, followed by the upper end of the range. The upper and lower bounds are considered part of the range.

   IP address ranges and single addresses are separated by semicolons. IP address ranges for IPv4 should be entered in the format: 192.168.0.1-192.168.0.255. IP address ranges for IPv6 should be entered in the format: 2001:db8:c18:1:4c7d:fa25:ccf8:d30c-2001:db8:c18:1:4c7d:fa25:ccf8:d30f
5. Select the **Restrict** or **Permit** radio button.
6. Click **Add** to add the configurations.
7. Click **Apply** to apply the configurations.

To remove IP addresses from the list:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **IP Restricted Login** link.
4. Select the check box beside the IP addresses you want to remove.
5. Click **Remove**.
6. Click **Apply** to apply the configurations.

Related Procedures

- Anonymous/Local Access
- IP Binding
- Local Server Certificate
- Alternative Names Certificates
- Port 2301
- Timeouts
- Trust Mode
- Trusted Management Servers
- Kerberos Authorization Procedure (Windows Only)
- User Groups

Related Topic

▲ The Settings Page

Local Server Certificate

The **Local Server Certificate** link enables you to use *certificates* that are not generated by HP.

If you use the following process, the *self-signed certificate* that was generated by the HP SMH is replaced with one issued by a *certificate authority* (CA).

- The first step of the process is to cause the HP SMH to create a **Certificate Request (PKCS #10)**. This request uses the original private key associated with the self-signed certificate and generates data for the certificate request. The private key never leaves the server during this process.
- After the Public Key Infrastructure **PKCS #10** data is created, the next step is to send it to a certificate authority. Follow your company policies for sending secure requests for and receiving secure certificates.
- After the certificate authority returns the **PKCS #7** data, the final step is to import this into HP SMH.
- After the **PKCS #7** data is imported, the original `\hp\sslshare\cert.pem` certificate file for Windows, `/opt/hpsmh/sslshare/cert.pem` file for HP-UX, and `/opt/hp/sslshare/cert.pem` (`/etc/opt/hp/sslshare/cert.pem` in HP SMH 2.1.3 and later on Linux x86 and x86-64) is overwritten with the system certificate from the **PKCS #7** data envelope. The same private key is used for the new imported certificate that was used with the previous self-signed certificate. This private key is randomly generated at startup when no key file exists.

To create a certificate:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **Local Server Certificate** link.
4. Replace the default values in the **Organization** or **Organizational Unit** fields in the **Create PKCS #10 Data** box with your values, up to 64 characters.

   If not specified, they are filled in with *`Hewlett-Packard Company`* for the **Organization** and *`Hewlett-Packard Network Management Software (SMH)`* for the **Organizational Unit**.
5. Click **Create** in the **Create PKCS #10 Data** box.

   A screen appears indicating that the **PKCS #10 Certificate Request** data has been generated and stored in `/opt/hpsmh/sslshare/req_cr.pem` for HP-UX, `/etc/opt/hp/sslshare/req_cr.pem` on Linux x86 and x64, and *`systemdrive:`* `\hp\sslshare\req_cr.pem` for Windows.
6. Copy the certificate data.

7. Use a secure method to send **PKCS #10** certificate request data to a certificate authority, request the certificate request reply data in **PKCS #7** format, and request that the reply data is in Base64-encoded format.

   If your organization has its own Public Key Infrastructure (PKI) or Certificate Server implemented, send the **PKCS #10** data to the CA manager and request the **PKCS #7** reply data.

NOTE: A third-party certificate signer generally charges a fee.

8. When the certificate signer sends the **PKCS #7** encoded certificate request reply data to you, copy this data from the **PKCS #7** certificate request reply and paste it into the **PKCS #7 information** field in the **Import PKCS #7 Data** box.
9. Click **Import**.

   A message appears indicating whether the customer-generated certificate was imported.
10. Restart HP SMH.
11. Browse to the managed system that contains the imported certificate.
12. When prompted by the browser, select to view the certificate and verify that signer is listed as the signer you used, and not HP, before importing the certificate into your browser.

    If the certificate signer you choose sends you a certificate file in Base64-encoded form instead of **PKCS #7** data, copy the Base64-encoded certificate file to `/opt/hpsmh/sslshare/cert.pem` for HP-UX, `/etc/opt/hp/sslshare/cert.pem` on Linux x86 and x64, and *`systemdrive`*`:\hp\sslshare\cert.pem` for Windows; then restart HP SMH.

Related Procedures

- Anonymous/Local Access
- IP Binding
- IP Restricted Login
- Alternative Names Certificates
- Port 2301
- Timeouts
- Trust Mode
- Trusted Management Servers
- Kerberos Authorization Procedure (Windows Only)
- User Groups

Related Topic

▲ The Settings Page

Alternative Names Certificates

HP SMH allows the setting of multihomed or multiple names to *certificates* that are not generated by HP. Through this functionality, SMHs certificate can contain additional information for the machine, such as other names in the network and IPs that are available. In the same way, it is possible to create a request certified to be signed by a *Certificate Authority (CA)*.

Two kinds of values are acceptable as alternative names:

- DNS name (for example, Linux;Linux.localdomain)
- IP Address (for example, 10.16.165.1;192.168.1.189)

Only users in the Administrator User Group and System Administrators (*root* on Linux and *Administrator* on Windows) can edit the **Alternative Names** fields through the browser.

The *multihomed* configuration is available by completing the following steps:

Changes made here to **Alternative Names** affect only the current certificate.

1. Select **Settings** from the menu
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **Local Server Certificate** link.
4. In the **Current Certificate** box, enter a value in the **Alternative Names** field.
5. Click **Create**.
6. Click **Yes** and the previous page appears with the message: `Success: Value successfully changed`.

When this happens, the new certificate with the alternative names set are negotiated with the browser.

Related Procedures

- Anonymous/Local Access
- IP Binding
- IP Restricted Login
- Local Server Certificate
- Port 2301
- Timeouts
- Trust Mode
- Trusted Management Servers
- Kerberos Authorization Procedure (Windows Only)
- User Groups

Related Topic

▲ The Settings Page

Port 2301

The **Port 2301** link provides options to enable or disable **Port 2301**. The default value, enabled, preserves the compatibility with *HP Web-enabled System Management Software*.

To enable or disable Port 2301, complete the following steps:

1. Select **Settings** from the menu
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **Port 2301** link.
4. In the **Configuration box**, check **Enable Port 2301** to enable Port 2301 or remove the check to **Disable** Port 2301.
5. Click **Apply**.

Related Procedures

- Anonymous/Local Access
- IP Binding
- IP Restricted Login
- Local Server Certificate
- Alternative Names Certificates
- Timeouts
- Trust Mode
- Trusted Management Servers
- Kerberos Authorization Procedure (Windows Only)
- User Groups

Related Topic

▲ The Settings Page

Timeouts

The **Timeouts** link provides options to configure the values of the **Session timeout** and **UI timeout**.

- The **session timeout** value represents the amount of time in minutes that a user can remain inactive in an SMH session. If a user logs in and remains inactive for an amount of time greater than that specified by **session timeout**, the user is redirected to the **Sign In** page in their next interaction with the user interface.
- The **UI timeout** value represents the maximum amount of time in seconds that the SMH user interface (UI) waits for data requested from webapps. Users with Administrator access can set the **session timeout** to between 1 and 60 minutes. The default value is 15 minutes. Users with Administrator access can set the **UI timeout** to between 10 and 3600 seconds. The default value is 20 seconds.

Selecting the **Session never expires** check box in the **User Preferences Category** avoids HP SMH session timeouts by sending a background request every three minutes. This option, when selected, also avoids HP SMH service timeouts. For more information, see "User Preferences"

NOTE: The session never expires option is available in HP-UX systems only.

The following table presents the range of values available for timeouts, with their respective units:

Table 5-6 Timeout settings

Timeout	Range
Session timeout	1 – 60 minutes (Windows and Linux) 6 – 120 minutes (HP-UX)
UI timeout	10 – 3600 seconds

Session Timeout

To change the value for Session timeout, complete the following steps:

1. Select **Settings** from the menu
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **Timeouts** link.
4. In the **Session timeout (minutes)** textbox, enter a value between 1 and 60 minutes in the case of Windows and Linux.

   In the case of HP-UX, enter a value between 6 and 120 minutes.
5. Click **Apply**.

UI Timeout

To change the value for UI timeout, complete the following steps:

1. Select **Settings** from the menu
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **Timeouts** link.
4. In the **UI timeout (seconds)** textbox, enter a value between 10 and 3600 seconds.
5. Click **Apply**.

Related Procedures

- Anonymous/Local Access
- IP Binding
- IP Restricted Login
- Local Server Certificate

- Alternative Names Certificates
- Port 2301
- Trust Mode
- Trusted Management Servers
- Kerberos Authorization Procedure (Windows Only)
- User Groups

Related Topic

▲ The Settings Page

Trust Mode

The **Trust Mode** link provides options to enable you to select the security required by your system. Some situations require a higher level of security than others. Therefore, you have the following security options:

- **Trust by Certificate** Sets HP SMH to accept configuration changes only from HP SIM servers with trusted *certificates*. This mode requires the submitted server to provide authentication by means of certificates. This mode is the strongest method of security because it requires certificate data and verifies the digital signature before allowing access. If you do not want to enable remote configuration changes, leave **Trust by Certificate** selected, and leave the list of trusted systems empty by not importing certificates.

  This is the default behavior on Linux Itanium.

  HP strongly recommends using this option because it is more secure.

- **Trust by Name** Sets HP SMH to accept configuration changes only from servers with HP SIM names designated in the **Trust By Name** field. For example, you might use this option if you have a secure network with two groups of administrators in two divisions. It prevents one group from installing software to the wrong system. This option verifies only the HP SIM server that you designate.

  HP strongly recommends using the **Trust by Certificate** option because the other options are less secure.

- **Trust All** Sets HP SMH to accept specific configuration changes from systems. For example, you could use the Trust All option if you have a secure network, and everyone in the network is trusted.

  HP strongly recommends using the **Trust by Certificate** option because the other options are less secure.

Configuring Trust Mode

For HP-UX, the imported HP SMH certificates are stored in the `/opt/hpsmh/certs` directory.

For Linux, the imported HP SMH certificates are stored in the `/opt/hp/hpsmh/certs` directory.

For Windows, the imported HP SIM certificates are stored in the *`systemdrive:`* `\hp\hpsmh\certs` directory.

You must have administrative authority to access this directory.

To trust by certificate:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link .
3. Click the **Trust Mode** link.
4. In the **Secure Trust Modes** box, click the **Trust by Certificate** radio button.

   Choosing this option sets up the HP SMH to accept **Secure Task Executions** and **Single Sign On** requests that are signed by a HP SIM with a **Trusted Certificate**.

5. Click **Apply**.

To trust by name:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **Trust Mode** link.
4. In the **Other Trust Modes** box, click the **Trust by Name** radio button.

5. In the **Server Certificate Name** textbox, enter the Server Certificate Name.
6. Click **Add**.

   When you click **Add**, the **Server Certificate Name** is validated to see if it meets the following criteria:

   - Each HP SIM server's certificate name must be less than 64 characters
   - The following invalid characters are not included: ~ ' ! @ # $ % ^ & * ( ) + = / " : ' < > ? , |
   - The Server Certificate Name is not already in the list

   If the validation test accepts the value, **Server Certificate Name** is added as a new line in the list table. You can add as many as five **Server Certificate Names** by following steps 5 and 6. If you enter more than five certificate names, you receive the alert `No more names can be added`.
7. Click **Apply** to save the configurations.

   Choosing this option sets up HP SMH to only accept **Secure Task Executions** and ***Single Sign On*** requests from HP SIM on servers with names listed.

To remove a Server Certificate Name from the list, complete the following steps:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **Trust Mode** link.
4. In the **Other Trust Modes** box, find the **Server Certificate Name** to remove and click the check box beside that name.
5. Click **Remove**.
6. Click **Apply**.

To trust all servers:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **Trust Mode** link.
4. In the **Other Trust Modes** box, click the **Trust All** button.
5. Click **Apply**.

   Choosing the **trust all** option sets HP SMH to accept **Secure Task Execution** and **Single Sign On** requests from any HP SIM server.

Related Procedures

- Anonymous/Local Access
- IP Binding
- IP Restricted Login
- Local Server Certificate
- Alternative Names Certificates
- Port 2301
- Timeouts
- Trusted Management Servers
- Kerberos Authorization Procedure (Windows Only)
- User Groups

Related Topic

▲ The Settings Page

Trusted Management Servers

Certificates establish the trust relationship between HP SIM or Insight Manager 7 and HP SMH. The **Trusted Management Servers** link enables you to manage your *certificates* in the **Trusted Certificates List**. Note the following:

- **Import Certificate Data** Certificates establish the trust relationship between HP SIM and HP SMH.
- **Add Certificate From Server** You can add a trusted certificate from an HP SIM server.

To import a certificate to the trusted certificates list:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **Trusted Management Servers** link.
4. In the **Add Certificate** area, click the **Import Certificate Data** radio button.
5. Copy and paste the Base64-encoded certificate into the textbox.
6. Click **Import**.

To add a certificate from a server:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **Trusted Management Servers** link.
4. In the **Add Certificate From Server** area, click the **Add Certificate From Server** radio button.
5. In the **Server Name** textbox, enter the IP address or server name of the HP SIM server.
6. Click **Add**.

Related Procedures

- Anonymous/Local Access
- IP Binding
- IP Restricted Login
- Local Server Certificate
- Alternative Names Certificates
- Port 2301
- Timeouts
- Trust Mode
- Kerberos Authorization Procedure (Windows Only)
- User Groups

Related Topic

▲ The Settings Page

Kerberos Authorization Procedure (Windows Only)

When a user wants to authenticate to a service in a **Kerberos** realm, a series of steps must be taken to perform the authentication. The client (the user's machine) must obtain credentials from the Kerberos servers, which are the *Authentication Server (AS)* and the *Ticket Granting Server (TGS)*.

The AS and the TGS reside on the same machine and are referred to as the *Key Distribution Center (KDC)*.

Kerberos Authentication Procedure

The following outlines the process when a user accesses secure services in a **Kerberos** realm.

The process only occurs when the user initially logs in to a **Kerberos** realm and tries to perform the first access to a Kerberos-secured service.

1. The user logs in to the system (client) using his or her domain username and password.
2. The user's password is hashed, and this hash becomes the user's secret key.
3. When the user tries to access a service, a message informs the AS that the user wants to access that service.
4. If the user is in the AS database, two messages are sent back to the client:
   a. A Client/TGS session key is encrypted with the user's secret key, which is used in the communication with the TGS.
   b. A Ticket-Granting Ticket (TGT) is encrypted with the secret key of the TGS. A **ticket** is used in **Kerberos** to prove one's identity. The TGT allows the client to obtain other tickets for communication with network services.
5. Upon receiving these two messages, the client decrypts the message containing the Client/TGS session key.

The following process occurs every time a user wants to authenticate to a service:

1. When the user requests a service, the client sends two messages to the TGS:
   - A message composed of the TGT and the requested service
   - An authenticator, is made up of the client's ID and the current timestamp encrypted with the Client/TGS session key received before

   Timestamps are used in **Kerberos** to avoid replication attacks. The clock skew among machines cannot exceed a specific limit.
2. The TGS decrypts the authenticator and sends two new messages back to the client:
   - The client-to-server ticket received from the TGS
   - Another authenticator, made up of the client's ID and the current timestamp, encrypted with the client/server session key
3. The service decrypts the client-to-server ticket with its own secret key and sends the client a message with the received timestamp plus one, confirming its true identity. This message is encrypted with the client/server session key.
4. The client decrypts the message and checks the timestamp. If it is correct, requests may be issued to the service and it sends responses back as expected.

HP SMH Kerberos Authentication

HP SMH provides **Kerberos** *Single Sign-On (SSO)*, allowing *users* in a **Kerberos** realm to log in without entering a user name and password in the **Sign In** page. If an allowed user accesses HP SMH and has valid **Kerberos** credentials, the **Home** page appears inside HP SMH.

Kerberos authentication is done using the special `URL /proxy/Kerberos` in HP SMH. By accessing the URL, SMH looks for **Kerberos** credentials in the request and perform user authentication.

If the user does not have valid **Kerberos** credentials or if an error occurs during the authentication process, the **Sign In** page appears, showing an error message. For example, if the clock skew among the machines involved in authentication is too large, you receive an error message and are taken to the **Sign In** page.

Kerberos authentication does not work on the following local access situations:

- Accessing HP SMH from the machine where the KDC (AD) is installed
- Accessing HP SMH from the machine where HP SMH is installed

When an authentication error occurs, the system administrator should check the SMH HTTP server error log to obtain more information about the error.

For example, when the clock skew among the machines is too large, the following log message is written:

```
Thu Jun 25 16:55:09 2009] [error] client 2001:db8:c18:1:b8ca:fcdf:d49d:b5c6]
mod_spnego: Kerberos SSO (QueryContextAttributes) failed; SSPI: The function
requested is not supported\r\n(-2146893054).
```

The following levels of user authorizations are available:

- **Administrator** Users with **Administrator** access can view all information provided through HP SMH. The appropriate default user group, *Administrators* for Windows operating systems and *root* for HP-UX and Linux, always has administrative access.
- **Operator** Users with **Operator** access can view and set most information provided through HP SMH. Some web applications limit access to the most critical information to administrators only.
- **User** Users with **User** access can view most information provided through HP SMH. Some web applications restrict viewing of critical information from individuals with **User** access.

To enable or disable **Kerberos** and add groups to the allowed **Kerberos** group list, complete the following steps for each level of access.

Kerberos support is provided on a per-user basis.

Kerberos Administrator

To add a **Kerberos** Administrator:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **Kerberos Authorization** link.
4. In the **Kerberos Configuration** area, select the box beside **Enable Kerberos Support**.
5. In the **Group Name** textbox, enter a name in the *group@REALM* format or *REALM\group*

   Only alphanumeric and underline values are permitted. The use of special characters such as ~ ' ! # $ % ^ & * ( ) + = / " : ' < > ? , | ; are not permitted.
6. Click the **Administrator** radio button beside **Type**.
7. Click **Add**. The values entered are added as a new line in the list table.

   You can continue to add groups with administrative access by following steps 5 through 7.
8. Click **Apply**.

To remove a **Kerberos** Administrator:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **Kerberos Authorization** link.
4. Click the check box beside the **Group Name** in the dynamic list that you want to remove from HP SMH.
5. Click **Remove**.
6. Click **Apply**.

Kerberos Operator

To add a **Kerberos** Operator:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **Kerberos Authorization** link.
4. In the **Kerberos Configuration** area, select the box beside **Enable Kerberos Support**.
5. In the **Group Name** textbox, enter a name in the *group@REALM* format or *REALM\groupname*.

   Only alphanumeric and underline values are permitted. The use of special characters such as ~ ' ! # $ % ^ & * ( ) + = / " : ' < > ? , | ; are not permitted.
6. Click the **Operator** radio button beside **Type**.
7. Click **Add**. The values entered are added as a new line in the list table.

   You can continue to add groups with operator access by following steps 5 through 7.
8. Click **Apply**.

To remove a **Kerberos** Operator:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **Kerberos Authorization** link.
4. Select the check box beside the **Group Name** in the dynamic list that you want to remove from HP SMH.
5. Click **Remove**.
6. Click **Apply**.

Kerberos User

To add a **Kerberos** User:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **Kerberos Authorization** link.
4. In the **Kerberos Configuration** area, select the box beside **Enable Kerberos Support**.
5. In the **Group Name** textbox, enter a name in the *group@REALM* format or *REALM\groupname*.

   Only alphanumeric and underline values are permitted. The use of special characters such as ~ ' ! # $ % ^ & * ( ) + = / " : ' < > ? , | ; are not permitted.
6. Click the **User** radio button beside **Type**.
7. Click **Add**. The values entered are added as a new line in the list table.

   You may continue to add groups with user access by following steps 5 through 7.
8. Click **Apply**.

To remove a **Kerberos** User:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **Kerberos Authorization** link.
4. Select the check box beside the **Group Name** in the dynamic list that you want to remove from HP SMH.
5. Click **Remove**.
6. Click **Apply**.

Related Procedures

- Anonymous/Local Access
- IP Binding
- IP Restricted Login
- Local Server Certificate
- Alternative Names Certificates
- Port 2301
- Timeouts
- Trust Mode
- Trusted Management Servers
- User Groups

Related Topic

▲ The Settings Page

User Groups

HP SMH uses operating system accounts for authentication and enables you to manage the level of access of operating system accounts at an operating system account group level.

The *users* in the operating system group **Administrators** for Windows, or the operating system group **root** (which in turn contains the user root by default) for HP-UX and Linux, can define operating system groups

that correspond to HP SMH access levels of **Administrator**, **Operator**, or **User**. After operating system groups are added, the operating system administrator can add operating system users into these operating system groups.

Each HP SMH access level can be assigned up to five operating system groups. The HP SMH installation enables you to assign the operating system groups to HP SMH. HP SMH will not allow adding an operating system group if the specified operating system group is not defined in the operating system.

The accounts used for HP SMH do not need to have elevated access on the host operating system. Any administrative HP SMH user can specify operating system user groups to each access level of HP SMH. As a result, all accounts in each operating system user group have the access to HP SMH specified in the **User Groups** window.

NOTE: All user groups must exist in the HP System Management Homepage host system.

The Windows administrators group, the Linux root group, and the HP-UX root group have administrative access to the HP SMH. For HP-UX, only the root user is assigned to the Administrators class. Not every user in the root group is assigned.

For example, the HP SMH Administrator access level could be assigned the user-created operating system groups Admin1, Admin2, and Admin3. Any user that is a member of the operating system user groups (Admin1, Admin2, or Admin3) is given administrative rights on HP SMH whether the accounts have elevated access on the host operating system.

The **User Groups** page enables you to add user groups to HP SMH. The following levels of user group authorizations are available:

- **Administrator** Users with **Administrator** access can view all information provided through HP SMH. The default user group, **Administrators** for Windows operating systems and **root** for HP-UX and Linux, always has administrative access.
- **Operator** Users with **Operator** access can view and set most information provided through HP SMH. Some web applications limit access to the most critical information to administrators only.
- **User** Users with **User** access can view most information provided through HP SMH. Some web applications restrict viewing of critical information from individuals with **User** access.

Administrator Group

To add an Administrator Group:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **User Groups** link.
4. In the **Groups** area, enter a group name in the **Group Name** textbox.

   All user groups must exist in the HP System Management Homepage host system.

   Only alphanumeric and underline values are permitted. The use of special characters such as ~ ' ! @ # $ % ^ & * ( ) + = / " : ' < > ? , | ; are not permitted.
5. Click the **Administrator** radio button beside **Type**.
6. Click **Add**. The values entered are added as a new line in the list table.

   You can continue to add up to five **Administrator groups** by following steps 4 through 6.
7. Select the check box beside the **Group Names** in the dynamic list you want to add to SMH.
8. Click **Apply**.

To remove an Administrator Group:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **User Groups** link.
4. Select the check box beside the **Group Names** in the dynamic list that you want to remove from SMH.
5. Click **Apply**.

Operator Group

To add an Operator Group:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **User Groups** link.
4. In the **Groups** area, enter a group name in the **Group Name** textbox.

   All user groups must exist in the HP System Management Homepage host system.

   Only alphanumeric and underline values are permitted. The use of special characters such as ~ ' ! @ # $ % ^ & * ( ) + = / " : ' < > ? , | ; are not permitted.
5. Click the **Operator** radio button beside **Type**.
6. Click **Add**. The values entered are added as a new line in the list table.

   You can continue to add up to five **Operator groups** by following steps 4 through 6.
7. Select the check box beside the **Group Names** in the dynamic list you want to add to SMH.
8. Click **Apply**.

To remove an Operator Group:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **User Groups** link.
4. Select the check box beside the **Group Names** in the dynamic list that you want to remove from SMH.
5. Click **Apply**.

User Group

To add a User Group:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **User Groups** link.
4. In the **Groups** area, enter a group name in the **Group Name** textbox.

   All user groups must exist in the HP System Management Homepage host system.

   Only alphanumeric and underline values are permitted. The use of special characters such as ~ ' ! @ # $ % ^ & * ( ) + = / " : ' < > ? , | ; are not permitted.
5. Select the **User** radio button beside **Type**.
6. Click **Add**. The values entered are added as a new line in the list table.

   You can continue to add up to five **User groups** by following steps 4 through 6.
7. Select the check box beside the **Group Names** in the dynamic list you want to add to SMH.
8. Click **Apply**.

To remove a User Group:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **User Groups** link.
4. Select the check box beside the **Group Names** in the dynamic list that you want to remove from SMH.
5. Click **Apply**.

Related Procedures

- Anonymous/Local Access
- IP Binding
- IP Restricted Login
- Local Server Certificate

- Alternative Names Certificates
- Port 2301
- Timeouts
- Trust Mode
- Trusted Management Servers
- Kerberos Authorization Procedure (Windows Only)

Related Topic

- ▲ The Settings Page

6 The Tasks Page

The **Tasks** page displays links to routine tasks provided by participating *HP Web-enabled System Management Software*.

If no tasks are provided by HP Web-enabled System Management Software, the **Tasks** page is not visible.

Related Topics

- Getting Started
- The Home Page
- The Settings Page
- The Tasks Page
- The Logs Page
- The Installed Webapps Page
- The Support Page
- The Help Page

7 The Logs Page

At a minimum, the **Logs** page provides the following log categories:

- System Management Homepage Log
- Httpd Error Log (Windows and Linux)
- System Management Homepage Error Log (HP-UX)

Logs contained in the installed *HP Web-enabled System Management Software* can appear on this page. For example, if the *HP Version Control Agent* is installed, a link to the Version Control Agent log appears on the **Logs** page. As another example, if the Distributed Systems Administration Utilities (DSAU) is installed, a link to the System Log Viewer appears on the **Logs** page. Each log file is divided into pages that display a total of 40 log entries to a page.

NOTE: With this installation, in the case of Windows and Linux, the old smh.log file is held in reserve as a human-readable, English-only log. It is not available through the user interface. Access the file directly to read the old log. New log messages are not written to this file.

The `smh_enc.log (in Windows and Linux)`, and `smh.log (HP-UX)` contains encoded entries in the following format:

Table 7-1 Log encoded entries

Type	Description
Severity	The severity of the event logged. The following are the severity levels: • Informational (5) • Warning (6) • Minor (3) • Major (4) • Critical (8)
Timestamp	The time the event happened, represented in seconds since 00:00:00 UTC, January 1, 1970.
ID	The log message ID, used to locate the translated log message.
Arguments	Arguments to be consumed by printf() in log messages that use argument conversion specifiers such as %s and %d.

Default log locations

Table 7-2 Default log locations

Location	Description
`C:\hp\hpsmh\logs`	Default log location (all logs) in Windows systems.
`/var/spool/opt/hp/hpsmh/logs/`	Default log location (error log and access log) in Linux systems.
`/opt/hp/hpsmh/logs`	Default log location (SMH log) in Linux systems.

Changing the log location

NOTE: Changing the log location is supported for access log and error logs only.

1. Enter the command: `smhconfig -O "new log location".`
   The new log directory is created.
2. Enter the following command: `smhconfig -r`
   The SMH application is restarted.

Related Procedures

- System Management Homepage Log
- Httpd Error Log

Related Topics

- The Home Page
- The Settings Page
- The Tasks Page
- The Installed Webapps Page

System Management Homepage Log

The **System Management Homepage Log** contains *HP System Management Homepage* (HP SMH) configuration changes as well as successful and failed signin attempts. It is helpful when troubleshooting signin or access issues when signing in directly to HP SMH, or from the *HP Systems Insight Manager* (HP SIM).

You must have administrative access to HP SMH to access the **System Management Homepage Log**.

To access the HP SMH Log, select **Logs** from the menu and click the **System Management Homepage Log** link in the **System Management Homepage** box.

Related Topics

- The Logs Page
- Httpd Error Log

Httpd Error Log

The **Httpd Error Log** contains error information generated by HP SMH modules, Kerberos misconfiguration errors, and CGI execution errors (`httpd`). It is the first place to look when a problem occurs with starting the server or with server operation because the log often contains details of what went wrong and how to fix the problem.

The **Httpd Error Log** is available on HP-UX directly but is visible in Windows and Linux by adding the *`httpd-error-log`* tag in the `smhpd.xml` file.

You must have administrative access to HP SMH to access the **Httpd Error Log**.

For HP SMH 3.x and later, it is possible to display the `httpd` error log in the HP SMH user interface using the `smhconfig` tool as follows:

To enable displaying the error log:

```
smhconfig -p or --httpd-error-log True
```

To disable displaying the error log:

```
smhconfig -p or --httpd-error-log False
```

HP SMH must be restarted to apply the new configuration.

To restart the HP SMH service:

```
smhconfig -r
```

To access the **Httpd Error Log**:

Select **Logs** from the menu and click the **Httpd Error Log** link in the **System Management Homepage** box.

Related Topics

- The Logs Page
- System Management Homepage Log

Supported Languages

HP SMH maintains PHP files that contain translated strings for supported languages. For each supported language, there is a file named `log_messages.php` in the `data/htocs/lang/` directory, where *`lang`* is the two-letter suffix for a language. The `log_messages.php` files contain an array of translated message strings and arrays for translated severity levels.

The following table contains the locale names for the languages that SMH supports:

Table 7-3 Locale names of supported languages

Language	Linux locale name	Windows locale name
English	en_US.UTF-8	english
Japanese	ja_JP.UTF-8	japanese
German	de_DE.UTF-8	german
Spanish	es_ES.UTF-8	spanish
French	fr_FR.UTF-8	french
Italian	it_IT.UTF-8	italian
Korean	ko_KR.UTF-8	korean
Simplified Chinese	zh_CN.UTF-8	chinese-simplified
Traditional Chinese	zh_TW.UTF-8	chinese-traditional

The following table contains the suffixes of the `log_messages.php` pages according to each supported language:

Table 7-4 Suffixes of supported languages

Language	Suffix
English	en
Japanese	ja
German	de
Spanish	es
French	fr
Italian	it
Korean	ko
Simplified Chinese	zh
Traditional Chinese	zh

Related Procedures

- System Management Homepage Log
- Httpd Error Log

Related Topics

- The Home Page
- The Settings Page
- The Tasks Page
- The Installed Webapps Page

8 The Installed Webapps Page

The **Installed Webapps** page contains a list of installed Webapps in the HP System Management Homepage (HP SMH). It contains links to the following HP Web-enabled System Management Software:

Integrated Agents Lists Webapps names. Participants are agents that contribute information contained in HP SMH. If no HP Web-enabled System Management Software is installed that provides this information, an informative message appears.

Other Agents Lists the visible HP Web-enabled System Management Software. The name of the HP Web-enabled System Management Software provides a link so you can access the agents if they provide a user interface. When you click the link, the webapp is opened in a new browser window. If no HP Web-enabled System Management Software is installed that provides this information, an informative message appears.

Disabling a webapp plug-in

1. Locate the webapp directory available at the following locations: `/opt/hp/hpsmh/webapp` (in Linux systems) and `C:\hp\hpsmh\webapp` (in Windows systems).
2. Create a new directory "disabled" in the webapp directory.
3. Copy the xml files corresponding to the webapp you want to disable from the webapp directory to the "disabled" directory.
4. Execute the command `smhconfig -r` to restart the SMH application.

Related Topics

- Getting Started
- The Settings Page
- The Tasks Page
- The Logs Page
- The Support Page
- The Help Page

9 The Support Page

The **Support page** provides information about HP Essentials Software and instructions on how to obtain guidance from HP Support and official forums. This page also provides the following links for help outside the HP System Management Homepage server domain.

- Insight Essentials Software Information
- Integrity Essentials Software Information
- Support Links

  In the case of HP-UX, the support link opens the IT Resource Center (ITRC) home page.
- Forum Links

  In the case of HP-UX, the forum link opens the IT Resource Center (ITRC) Forums page.

Related Topics

- Getting Started
- The Home Page
- The Settings Page
- The Tasks Page
- The Logs Page
- The Installed Webapps Page
- The Help Page

10 The Help Page

The **Help page** provides help for the HP System Management Homepage (HP SMH) and its webapps.

The **Help page** provides links for the following:

- **System Management Homepage Help** Contains information about the HP SMH infrastructure and its configuration and log pages. The remaining entries link to help systems associated with the webapps installed on the system (those that provide a help system).
- **Credits** Displays information regarding open source licensing and credits.

To access HP SMH help, complete the following steps:

1. Click **Help**.
2. Click the **System Management Homepage Help** link.

To access **Credits**, complete the following steps:

1. Click **Help**.
2. Click the **Credits** link.

Search Form

The **Search Form** section provides a field for you to input a *search term* to search the HP SMH help.

To execute a search, complete the following steps:

1. In the **search terms** textbox in the **Search Form** section, enter a search term.
2. Click **Search**.

   If the search criteria is valid, a list of all documents matching the query appears.

Related Procedures

▲ Credits

Related Topics

- Getting Started
- The Home Page
- The Settings Page
- The Tasks Page
- The Logs Page
- The Installed Webapps Page
- The Support Page

Credits

The **Credits** link displays information regarding open source licensing and credits.

To access Credits, select **Help** and click the **Credits** link.

Related Topic

▲ The Settings Page

11 Command Line Interface Configuration

The Command Line Interface (CLI) provides users with administrative rights access to set these values through the command line. You can use the CLI to modify configuration options, including the required security checks that allow the configuration options to be changed.

NOTE: --kerberos, --user-kerberos, --operator-kerberos, --admin-kerberos, --max-threads and –win32-disable-acceptex options are only available on Windows operating systems.

NOTE: Long options, starting with "--", have an optional symbol "=" before the argument.

Some CLI options require special arguments listed as words in capital letters in the option summary of the command. Descriptions of the format of these arguments are in the following table:

Table 11-1 CLI arguments

Argument type	Description
DIR	A path to a directory where the HP SMH service has write access.
FILE	A path to a file.
GROUPLIST	A list of group names separated by semicolons.
IPBINDLIST	A list of IPv6 addresses and/or IPv4 address/netmask pairs separated by semicolons.
IPLIST	A list of IP addresses separated by semicolons.
NUM	A numeric value with a range that depends on the option being set.
NAMELIST	A list of host names and IP addresses separated by semicolons.
XENAMELIST	A list of trusted server host names.

Anonymous Access

Anonymous access allows anonymous users to access unsecured pages, including local anonymous access. The following command enables or disables the anonymous access setting:

```
smhconfig -a|--anonymous-access [=] True | False
```

Local Access

The local access command sets the local access privilege to anonymous or administrator, applying the specified access to the local system. If local access is selected, a user with access to the local console is granted anonymous or administrator access without being challenged for a username and password.

The following command enables or disables local access:

```
smhconfig -L|--localaccess-enabled [=] True | False
```

The following command configures the local user privileges:

```
smhconfig -l|--local-access [=] administrator | anonymous
```

IP Restricted Logins

IP addresses can be explicitly permitted or restricted based on user type. If an IP address is explicitly restricted, it is restricted even if it is explicitly permitted. If there are IP addresses in the permitted list, only those IP addresses are allowed login access. If there are no IP addresses in the permitted list, login access is granted to any IP address not in the restricted list.

The following command enables or disables IP restricted login:

```
smhconfig -P|--ip-restricted-login [=] True | False
```

IP Address Inclusion Perform the IP address permitted command as follows:

```
smhconfig -i|--ip-restricted-include [=] IPLIST
```

The following is an example of how *IPLIST* is formatted:

122.23.44.1-122.23.44.255;172.84.100.35;172.168.10.5;168.172.10.1-168.172.10.128

IP Address Exclusion Perform the IP address restricted command as follows:

`smhconfig -e|--ip-restricted-exclude [=] IPLIST`

The following is an example of how *IPLIST* is formatted:

122.23.44.1-122.23.44.255;172.84.100.35;172.168.10.5;168.172.10.1-168.172.10.128

NOTE: IPv4 and IPv6 address ranges are supported.

IP Binding

IP binding provides HP SMH the ability to listen only to the addresses configured in the IP binding list. If IP binding is enabled and the IP binding list is empty, HP SMH will only be accessible locally.

Perform the IP binding command as follows:

`smhconfig -g|--ip-binding [=] True | False`

IP binding list Use the following command to configure the IP binding list to be used when IP binding is enabled.

`smhconfig -I|--ip-binding-list [=] IPBINDLIST`

IPBINDLIST must be a list of semicolon-separated IP addresses and/or IP address/netmask pairs.

The following is an example of how *IPBINDLIST* is formatted:

122.23.44.1-122.23.44.255;172.84.100.35;172.168.10.5;168.172.10.1-168.172.10.128

Trust Modes

The HP SMH trusts Systems Insight Manager (HP SIM) or Insight Manager 7 (IM 7) secure task execution requests and single sign on requests with various levels of security, ranging from trust all to only trust HP SIM or Insight Manager 7 with trusted certificates:

- **Trust All** This command sets up the http server to accept all secure task execution requests and single sign on requests from any HP SIM or Insight Manager 7 server:

  `smhconfig -t|--trust-mode [=] TrustByAll`

- **Trust By Name** This command sets up the HP SMH to only accept secure task execution requests and single sign on requests from the listed HP SIM or Insight Manager 7 servers:

  `smhconfig -t|--trust-mode [=] TrustByName`

  To configure the trusted servers name list for the TrustByName trust mode, use the following command:

  `smhconfig -X|--xe-name-list [=] XENAMELIST`

  XENAMELIST is a list of the Systems Insight Manager or Insight Manager 7 servers that trust, using a comma or semicolon as a delimiter. The following is an example of the name list format:

  server1,server2.domain1;server3,server4.domain2

- **Trusted Certificates** This command establishes the trust relationship between HP SIM or Insight Manager 7 and the HP SMH using the certificate. The trust mode is set to TrustByCert using the following command:

  `smhconfig -t|--trust-mode [=] TrustByCert`

  A trusted certificate is added to the trusted certificate list using the following command:

  `smhconfig -C|--trust-certificate [=] FILE`

  FILE is the name of the file containing the base 64 encoded certificate to be added to the trusted certificate list.

Restart service

Restart the HP SMH on completion of applying the new configuration settings.

```
smhconfig -r|--restart
```

Reject Program Admin Login

Reject or accept and HP Web-enabled System Management Software or VCA login request.

```
smhconfig -j|--reject-prog-admin-login [=] true|false
```

Win32DisableAcceptEX

AcceptEX() is a Microsoft WinSock v2 API that provides performance improvements over the use of the BSD style accept() API in specific circumstances. Some popular Windows products, typically virus scanning or virtual private network packages, have bugs that interfere with the operation of AcceptEx(). If you encounter an error condition like:

```
[error] (730038) An operation was attempted on something that is not a socket::
winnt_accept: AcceptEx failed. Attempting to recover.
```

Use the following directive to disable the use of AcceptEx():

```
smhconfig -w|--win32-disable-acceptex [=] True | False
```

NOTE: Win32DisableAcceptEX is only available on Windows operating systems.

Disable SSL v2

By default the HP SMH has SSL v2 disabled. Use the following switch to re-enable SSL v2:

```
smhconfig -s|--disable-sslv2 [=] True | False
```

Log Rotations

Log files can become large and unmanageable. The following switch enables log files to rotate automatically when they reach 5M (default size). Either the log file is over-written on the next rotation when the option is off or a new file is created and the previous file is marked as old when the option is on.

```
smhconfig -A|--rotate-logs [=] 0 | 1 | 2
```

Where: 0= off, 1 or 2= on.

Rotate Log Size

Log files can become large and unmanageable. The following switch allows the user to set the size of the log files.

```
smhconfig -z|--rotate-log-size [=] size
```

Where size is a value in the range of 1-9MB.

Maximum Number of Threads Allowed

The **Maximum Number of Threads Allowed** value allows the user to increase or reduce the maximum number of threads HP SMH creates to handle page requests. The default is 64 for Windows.

NOTE: Maximum Number of Threads Allowed is only available on Windows operating systems.

```
smhconfig -M|--max-threads [=] max-number-of-threads
```

Where *max-number-of-threads* is a number in the range of 64-512.

Maximum Number of Threads Allowed is only available on Windows.

Maximum Number of Sessions

By default, HP SMH supports 128 user sessions. This number can be lowered to 32 or raised to 500 using the `session-maximum` setting.

```
smhconfig -S|--session-maximum [=] maximum-number-of-sessions
```

Session Timeout

The default session timer is set to 15 minutes. The session timeout can be set as low as 1 minute or as high as 60 minutes.

`smhconfig -U|--session-timeout [=] session-timeout-in-minutes`

Log Level

By default, the logging level of HP SMH error messages is set to `error`. When a log level is set, all events that are the same or superior to the configured log level are written to the log file. The log level option only affects the `error_log` file located under *SystemDrive:*`\hp\hpsmh\logs` in Windows and under `/var/spool/opt/hp/hpsmh/logs` in Linux.

The following values are available, in order of decreasing significance:

Table 11-2 Log level

Value	Description
emerg	Emergencies - system is unusable
alert	Action must be taken immediately
crit	Critical conditions
error	Error conditions
warn	Warning conditions
notice	Normal but significant condition
info	Informational
debug	Debug-level messages

`smhconfig -v|--log-level [=] logging-level`

NOTE: Log level only affects new messages written in the HTTP error log. You must perform a soft restart of the system.

Port 2301

Port 2301 determines whether HP SMH listens on port 2301. If the value is set to **True**, HP SMH listens on port 2301. If the value is set to **False**, HP SMH does not listen on port 2301.

The default is to listen on port 2301.

`smhconfig -T|--port2301 [=] True | False`

Multihomed certificate alternative names list

You can set the **name** for the certificate through the multihomed option.

It is important to restart the hpsmhd service when running smhconfig with multihomed values using a single command on the console (`--restart` option).

`smhconfig -u|--multihomed [=] NAMELIST`

`smhconfig -u|--multihomed [=] NAMELIST --restart`

NAMELIST must be a semicolon-separated list of IP addresses and hostnames.

Custom UI

Enabling custom UI enables you to customize the signin and header images as well as adding a small text in the signin page. See the HP SMH `README.txt` in the `hpsmh/data/htdocs/custom_ui` directory in the HP SMH install path.

`smhconfig -c|--custom-ui [=] True | False`

Httpd Error Log

The **httpd error log** option enables you to determine if it is possible to view the httpd `error_log` log file through the user interface.

```
smhconfig -p|--httpd-error-log [=] True | False
```

Icon View

Icon view allows you to set the default view mode to show icons (True) like a desktop File Manager appearance or to show the traditional list (False) that displays items in boxes.

```
smhconfig -n|--iconview [=] True | False
```

Box Order

Box order defines the ordering method used to display the boxes. You can choose **name**, which places the boxes in alphabetical order, or you can choose **status**, which displays the boxes from the worst status (critical) to the best status (normal).

```
smhconfig -x|--box-order [=] Name | Status
```

Box Item Order

Box item order defines the ordering method used to display the items inside boxes. You can choose **name**, which places, boxes in alphabetical order, or you can choose **status**, which displays boxes from the worst status (critical) to the best status (normal).

```
smhconfig -b|--box-item-order [=] Name | Status
```

Kerberos Authentication

To enable or disable Kerberos authentication support, use the following command:

```
smhconfig -k|--Kerberos [=] True | False
```

Administrator Kerberos users To configure Kerberos groups of users from a Kerberos domain with administrator privileges, use the following command:

```
smhconfig –m|--admin-kerberos [=] GROUPLIST
```

Note: `GROUPLIST` is a single Kerberos group or a list of Kerberos group names separated by semicolons.

NOTE: --admin-kerberos is only available on Windows operating systems.

Operator Kerberos users To configure Kerberos groups of users from a Kerberos domain with operator privileges, use the following command:

```
smhconfig –R|--operator-kerberos [=] GROUPLIST
```

Note: `GROUPLIST` is a single Kerberos group or a list of Kerberos group names separated by semicolons.

NOTE: --operator-kerberos is only available on Windows operating systems.

User Kerberos users To configure Kerberos groups of users from a Kerberos domain with user privileges, use the following command:

```
smhconfig –K|--user-kerberos [=] GROUPLIST
```

Note: `GROUPLIST` is a single Kerberos group or a list of Kerberos group names separated by semicolons.

NOTE: --user-kerberos is only available on Windows operating systems.

User Groups

User Groups are a set of policies to access and modify HP SMH functionalities. Only valid existing operating system groups can be added to the group list.

To add groups into HP SMH user types, complete the following:

Administrators Users with Administrator access can view and set all information provided throughout the HP SMH.

The default user group (*Administrators* for Microsoft operating systems and *root* for Linux) always has administrative access.

Windows systems that are part of a domain can specify domain groups and local groups for any level of access.

```
smhconfig -d|--admin-group [=] [ groupList ]
```

Operators Users with Operator access can view and set most information provided through the HP SMH. Some web applications limits access to the most critical information to administrators only.

```
smhconfig -E|--operator-group [=] [ groupList ]
```

Users Users with User access can view most information provided through the HP SMH. Some web applications restricts viewing of critical information from individuals with User access.

```
smhconfig -G|--user-group [=] [ GROUPLIST ]
```

Where *groupList* is a single operating system group or a list of operating system group names separated by semicolons.

Help message

To display a help message on the screen, use the following command:

```
smhconfig –h|--help
```

File Based Command Line Interface

The Command Line Interface (CLI) option enables a file with configuration parameters to be passed on the command line. The CLI parses the file and processs the arguments. The command to use a file for the input to the CLI is:

```
smhconfig -f configFile
```

Command Line Interface File Structure The CLI file structure format includes the # character for comments, a bracketed key word indicating the parameter to be set, and the parameter value. An example of the CLI file structure format is as follows:

Characters placed after the # on a given line are not parsed.

An example of a configuration file for smhconfig is as follows:

```
# SMH configruation file for smhconfig
[anonymous-access]
false
[localaccess-enabled]
true
[localaccess-type]
administrator
[user-group]
users
```

Command Line Log Reader

The command line log reading tool provides the users with a command line tool for reading the SMH log messages without using the UI. The command is:

```
smhlogreader [options]
```

where, the [options] are:

`-h|--help`, displays the help message.

`-f|--file FILE`, FILE represents a path to a file.

`--from FROM`, FROM: to display a range of messages, this option describes the ID of the first message.

`--to TO`, TO: to display a range of messages, this option describes the ID of the last message.

`--lang LANG`, LANG: the language used to display the log messages.

IMPORTANT: smhlogreader CLI also allows the combined use of these options in a single command. For example, `smhlogreader --lang LANG --from FROM --to TO --file FILE`

The different options provided by the smhlogreader CLI are:

- Help

  It allows the user run the command to display the help message for this tool.

  The following command displays the help message for the smhlogreader CLI.

  ```
  smhlogreader -h|--help
  ```

- Version

  It allows the user run the command to display the version of SMH.

  The following command displays the SMH version number.

  ```
  smhlogreader --version
  ```

- Language

  It allows the user to select language of choice for the messages to be displayed

  The following command allows the user to select the language of choice for the messages to be displayed.

  ```
  smhlogreader --lang en|ja
  ```

  By default the SMH Logs and UI supports “en” for English and “ja” for Japanese.

NOTE: To display the messages properly, the necessary fonts to display the messages must be installed on the system. For example, on a non-Japanese version of Windows the user needs to install Japanese fonts to read the log in that language.

- Reading Logs

  It displays a list with the most recent messages.

  The following command displays a list with the most recent messages.

  ```
  smhlogreader
  ```

- Range

  It allows the user to set the range of messages that smhlogreader CLI should display.

  The following command displays a list of messages in the range selected by the user.

  ```
  smhlogreader --from VALUE --to VALUE
  ```

  For example, to display messages the recent five messages, the user should use the following command:
  `smhlogreader --from 1 --to 5`

- File-based command line log reading

  The smhlogreader CLI allows the user to use a properly-formatted log file as an input.

  The following command allows the user to use a properly-formatted log file as an input and also backs up the log files.

  ```
  smhlogreader –f|--file FILE
  ```

Related Topic

▲ The Settings Page

12 File locations

Table 12-1 HP SMH file locations

Description	Windows	Linux	HP-UX
HP SMH Root The root of the HP SMH installation.	*SystemDrive*\hp\hpsmh	/opt/hp/hpsmh	/opt/hpsmh
HP SMH Executable The HP SMH binary. A webapp can use detection of this file's pressence to verify that HP SMH is installed on the system.	*SystemDrive*\hp\hpsmh\bin\hpsmhd.exe	/opt/hp/hpsmh/sbin/hpsmhd	/opt/hpsmh/lbin
Certificate and Key files The certificate and private key files used by HP SMH. This is a shared location used by a number of management applications. The keys may be either 1024 or 2048 bits.	*SystemDrive*\hp\sslshare\cert.pem *SystemDrive*\hp\sslshare\file.pem	/etc/opt/hp/sslshare/cert.pem /etc/opt/hp/sslshare/file.pem	/opt/hpsmh/sslshare
HP SMH XML configuration This file should only be modified by HP SMH itself.	*SystemDrive*\hp\hpsmh\conf\smhpd.xml	/opt/hp/hpsmh/conf/smhpd.xml	/opt/hpsmh/conf.common/smhpd.xml
HP SMH conf file The conf file is regenerated at every startup and modification of the version on disk.	*SystemDrive*\hp\hpsmh\conf\smhpd.conf	/opt/hp/hpsmh/conf/smhpd.conf	/opt/hpsmh/conf
2381 Document Root The root for documents served on port 2381 (HTTPS).	*SystemDrive*\hp\hpsmh\data\htdocs	/opt/hp/hpsmh/data/htdocs	/opt/hpsmh/data/htdocs
2301 Document Root The root for documents served on port 2301. Security restrictions allow only particular HP SMH documents to be served out of this directory (HTTP).	*SystemDrive*\hp\hpsmh\data\isdocs	/opt/hp/hpsmh/data/isdocs	/opt/hpsmh/data/isdocs
cgi-bin Root The root of executable content.	*SystemDrive*\hp\hpsmh\data\cgi-bin	/opt/hp/hpsmh/data/cgi-bin	/opt/hpsmh/data/cgi-bin
Help Root The root where help files are placed.	*SystemDrive*\hp\hpsmh\data\help	/opt/hp/hpsmh/data/help	/opt/hpsmh/data/help
Webapp XML files The root where webapp XML configuration files are placed.	*SystemDrive*\hp\hpsmh\webapp	/opt/hp/hpsmh/webapp	/opt/hpsmh/webapp

Related Topic

▲ The Installed Webapps Page

13 Troubleshooting

NOTE: If noted, a topic might only apply to the HP-UX, Linux, or Windows operating system.

13.1 Access Problems

13.13.1.1 SMH Documentation Unclear on Treatment of securetty.

The HP System Management Homepage (HP SMH) does not use `/etc/securetty`. See *login*(1) for details on `/etc/securetty`.

13.13.1.2 After entering a hostname on Linux, HP SMH does not start.

Hostnames that are 64 characters or longer in length are not supported on Linux.

13.2 Browser Problems

13.13.2.1 When I sign into HP SMH and close the browser, the HP SMH session is not ended. If I reopen Internet Explorer, after closing it I can sign into HP SMH without credentials. How can I fix this problem?

There are two possible solutions in order to be sure the HP SMH shortcut asks for credentials.

Solution 1

1. Select **Tools Internet Options**
2. Choose the **Advanced** tab.
3. Under **Settings Browsing**, deselect **Reuse windows for launching shortcuts (when tabbed browsing is off).**
4. Click **OK**.

Solution 2

1. Select **Tools Internet Options**
2. Under the **General** tab, look for **Tabs: Change how webpages are displayed in tabs**. Click **Settings**.
3. Under **Open links from other programs in:**, select the third option **The current tab or window**.
4. In the **Tabbed Browsing Settings** pop-up window, click **OK**.
5. Click **OK** to close **Internet Options**.

13.13.2.2 When I use Internet Explorer 6.0 in Windows, why do I see warnings in the **Security Alert** dialog box when I sign in to the HP System Management Homepage (HP SMH)?

There are two possible warnings:

- Warning 1: `The name on the security certificate is invalid or does not match the name of the site.`

  This warning occurs when you browse to HP SMH using an IP address. This warning also occurs if you browse locally using localhost for the machine name.

- Warning 2: `The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the CA.`

  The *certificate* is issued by HP SMH. You can add the certificate to your **Trusted Certificate List** and the warning goes away.

13.13.2.3 Opening a second Mozilla browser can appear as an unauthorized signin into HP SMH.

Mozilla browsers share sessions when launched separately.

Separate sessions are shared in Mozilla when launched from the desktop. However they are not shared in Internet Explorer.

13.13.2.4 I get security messages or partially displayed pages when browsing into HP SMH from Internet Explorer running on Windows 2003.

Internet Explorer 6.0 on Windows 2003 Server has different default security settings. To prevent the problem, add each managed system to the local intranet zone twice, once as **`http://`***`hostname`***`:2301`** and once more as **`https://`***`hostname`***`:2381`**. The alternatives to this solution are to decrease the level of security settings in the browser (not recommended) or alter the browser security settings to allow cookies (both stored and per-session) and allow active scripting.

13.13.2.5 My browser page does not display all contents. What is wrong?

Frame sizes are optimized for medium fonts. If you switch your browser to use larger or smaller fonts, manually adjust the frame layout using the mouse.

13.13.2.6 Why does the browser prompt me to accept cookies when accessing a system?

Browser cookies are required to track user state and security. Cookies must be enabled in the browser and prompting for acceptance of cookies should be disabled.

13.13.2.7 I can sign in to HP-UX with **`http://`***`hostname`***`:2301/`**, but not **`https://`***`hostname`***`:2381/`**.

By default, HP-UX is installed with the `autostart` feature enabled. A daemon listens on port 2301 and only starts HP SMH on port 2381 when requested, then stops it again after a timeout period. For more information, see the *smhstartconfig*(1M) command.

13.13.2.8 When I browse to **`https://`***`ipaddress`***`:2381`** on a local machine or a remote machine running Windows 2003, I don't see the **Sign in** screen.

Internet Explorer 6.0 on Windows 2003 sometimes causes only the **Account Sign in** text in a blue bar to appear, instead of the entire **Sign in** page. This issue occurs when browsing on a local system or a remote system.

To resolve the issue, enable Javascript support and add this site to the Trusted sites list.

13.3 Installation Problems

13.13.3.1 After running `setup.exe /r` on a Windows system to import certificates, the installation fails.

Do not use `setup.exe /r` to import or copy certificates. Instead, use the **Configure or Repair Agents** tool in HP SIM.

13.13.3.2 When installing HP SMH, I receive the following error: `another instance is running.`

The HP SMH installation attempted to install on a system that had files that are corrupted, or the installation was aborted.

To resolve this issue, navigate to the `\temp` directory on the HP SMH system and delete the `smhlock.tmp` file.

13.13.3.3 When installing HP SMH, I receive the following errors: `error: cannot get exclusive lock on /var/lib/rpm/Packages error: cannot open Packages index using db3 - Operation not permitted (1) error: cannot open Packages database in /var/lib/rpm.`

This error appears when more than one instance of the install action is initiated on a Linux system. Only one HP SMH installation can run at a time.

13.4 IP Address Problems

13.13.4.1 Why do I get a security warning when I browse to HP SMH with an IPv6 address?

To use IPv6 addresses, you need the following browsers:

- **Windows OS** Internet Explorer 7
- **Linux OS** Mozilla Firefox

Note: Internet Explorer 6 cannot handle IPv6 addresses. For more information, see **http://blogs.msdn.com/ie/archive/2007/02/20/ipv6-uris-in-ie7.aspx** and the Microsoft support page at **http://support.microsoft.com/kb/325414**.

When browsing secure pages, Internet Explorer 7 might ask you to add the page to its Trusted Site Zone. Even clicking **Add**, the message returns. In this case, Internet Explorer 7 fails to handle IPv6 URLs since the Internet Explorer parser uses a colon as the separator of the IP address and the Port number. For example,

- On IPv4, the HP SMH IP address might be **`https://127.0.0.1:2381`**. The IP address is 127.0.0.1 and the port number is 2381.
- On IPv6, the HP SMH IP address might be **`https://[2001:db8:c18:1:21a:4bff:fe4c:c8e0]:2381`**. The IP address is 2001:db8:c18:1:21a:4bff:fe4c:c8e0 and the port number is 2381 in this case, Internet Explorer looks for a colon as a separator and uses [2001 as the IP address.

Choose one of two ways to avoid security warnings when browsing with IPv6 addresses:

- Use a DNS name backed by IPv6 addresses.
- Add the literal IPv6 address to the Local intranet site or Trusted sites of Internet Explorer 7 without the port number. For example, add **`http://[2001:db8:c18:1:250:8bff:fee2:4ed8]`** and **`https://[2001:db8:c18:1:250:8bff:fee2:4ed8]`** without adding the port number.

13.13.4.2 Is there an easier way to access the local system with my browser without finding out its IP address?

Yes. You can access the local system at **`https://`***`hostname`***`:2381`** or **`https://127.0.0.1:2381`**. For HP-UX, you can access the local system at **`http://hostname:2301`** if you keep the default setting of `autostart` enabled.

NOTE: The word *localhost* does not work in all languages. In addition, if you have a proxy server configured in your browser, you might need to add 127.0.0.1 to the browser list of addresses that should not be proxied.

13.13.4.3 When I use the **IP Restricted Login** feature, entering my server IP address does not have the desired effect. How can I be sure that the local machine IP addresses are recognized by this feature?

Enter 127.0.0.1 in addition to the IP addresses of the server if you intend to restrict the local machine. The address 127.0.0.1 is always permitted in the **Include** section, so it is only restricted if it is explicitly placed in the **Exclude** section.

13.13.4.4 Although an IP restriction is configured, localhost access is not being denied. Why is this happening?

If you do not include the IP address for the local host in the Include field, the local host is still granted access because most users do not intend to block local host access. If you **do** need to block localhost access, enter **`127.0.0.1`** into the **Exclude** field under **IP Restriction**.

13.13.4.5 Under **IP Restriction**, I did not include the system's local IP address or 127.0.0.1 to the **Include** list, but I can still browse to it locally.

As a precaution against users unintentionally locking themselves out of HP SMH access, localhost requests are not denied when the local IP addresses are not mentioned in the **Include** list. If necessary, the local system's IP address and 127.0.0.1 can be added to the **Exclude** list, and this setting denies access to any user trying to gain access from the local system.

13.5 Sign In Problems

13.13.5.1 After signing onto the Windows operating system on a ProLiant or Integrity server running HP SMH Version 2.1.3 (or later), the ROTATELOGS.EXE command prompt appears on the screen if SMH is configured to allow interaction with the desktop. When this occurs, one or two smaller command prompt windows appear with messages similar to the following:

```
(drive) :\hp\hpsmh\bin\rotatelogs.exe
```

The command prompt window messages do not affect the performance or functionality of the server or of SMH and can be ignored.

Any ProLiant or Integrity server configured with Windows 2000 Server or Windows Server 2003 (any edition) and HP SMH Version 2.1.3 (or later) when SMH is allowed to interact with the desktop can be affected.

To prevent HP SMH from interacting with the server desktop, perform the following:

1. Click **Start→Programs→Administrative Tools→Services**
2. Click HP System Management Homepage **Properties**.
3. Click the **Log On** tab.
4. Deselect **Allow service to interact with desktop**.
5. Click **Apply** and then click **OK**.
6. Restart the HP System Management Homepage service.

13.13.5.2 I gave a user group defined by Windows, such as **Backup Operators**, **Administrator**, **Operator** and **User** , privileges through the HP SMH **User Groups** settings page. However, users in that group cannot sign in or do not have the correct privileges in HP SMH.

HP SMH only recognizes four user groups defined by Windows: **Administrators**, **Users**, **Guests** and **Power Users**. Other groups defined by Windows, such as **Backup Operators**, are not recognized.

NOTE: On Linux, the group must be previously created using system tools as groupadd.

13.13.5.3 When trying to sign in to HP SMH on a Windows system using an administrative account defined in the **Backup Operators** group, the sign in fails.

On Windows systems in the defined user groups, only **Administrators**, **Users**, **Guests** and **Power Users** are recognized. Other groups defined by Windows, such as **Backup Operators**, are not recognized. Create a new group and use it for providing access to HP SMH.

13.13.5.4 I cannot sign in to HP SMH on my server running the Windows operating system.

Complete the following:

1. Verify that a valid Windows operating system account is set up and that the signin is included in the **Administrators** group or in an HP SMH operating system group.
2. Sign in to the operating system, and change the password if prompted.

   If this password prompt appears, the operating system Administrator has set up the user account with the **user must change the password at next sign in option** selected.

   Any signin created in the future can be added by the operating system group Administrator without selecting the **user must change the password at next sign on** option. In addition, if this option is selected, you can change the password through the operating system before signing in to HP SMH.

13.13.5.5 I cannot sign in to HP SMH on my Windows XP operating system.

Go to **Programs→Administrative Tools→Local Security Settings** and change the policy to **Network Access: Sharing and security model for local accounts** from **Guest Only** to **Classic Only**.

13.13.5.6 Why doesn't my password work after I upgrade my web-managed Products?

HP SMH v2.0 and later use operating system accounts, but previous versions use static accounts (**administrator**, **operator**, and **user**). Any operating system account belonging to the administrators group (root group in Linux) has administrative access to HP SMH. With this access, you can assign accounts in other operating system account groups to different levels of access for HP SMH. The HP SMH online help describes this process in detail. See "User Groups".

NOTE: This does not apply to HP-UX.

13.13.5.7 I created new Windows accounts, using default settings, for use with HP SMH but I cannot use them to sign in.

By default, new accounts created in Windows operating systems are set to **user must change the password at next sign in**. Deselect this option so the account can be used to sign in to HP SMH.

13.13.5.8 When I use Internet Explorer 6.0 in Windows and browse through the management server to a system that was discovered by IP address, I cannot sign in to HP SMH. If anonymous access is enabled, I get through anonymously but the user name is incorrect.

or

When I use Internet Explorer 6.0 in Windows and browse through the management server to a device that was discovered by IP address, the detailed certificate information does not appear in the text box of the **Automatic Import Certificate** screen.

These issues can be resolved in the following ways by adjusting the Internet Explorer settings:

- Configure the **Internet Explorer Privacy** settings from **Medium** to **Low**. (HP does not recommend using this option.)

  To change the settings:

  1. In Internet Explorer, click **Tools** → **Internet Options**.
  2. Click **Privacy**.
  3. Click and drag the slide bar to **Low**.
  4. Click **Apply**.
  5. Click **OK**.

     The changes are saved.

- Add the IP address of the target HP SMH to the Local Intranet's zone.

  To change the settings:

  1. In Internet Explorer, click **Tools** → **Internet Options**.
  2. Click **Security**.
  3. Select **Local Intranet**.
  4. Click **Sites** → **Advanced**.
  5. In **Add this website to the zone**, enter the IP address of the HP SMH system for example, enter **`https://`***`ipaddress`* .
  6. Click **Add**.
  7. Click **OK**.
  8. Click **OK** again.
  9. Click **OK**.

     The changes are saved.

13.13.5.9 When I browse to my system using the server name **`http://`***`my-server-name`***`:2301`** with Internet Explorer, I cannot sign in using my valid Windows administrator account username and password. However, I can sign in if I browse to my system using my IP address, **`http://`***`my-ip-address`***`:2301`**.

Verify whether there is an underscore "_" defined in your server's computer name. If there is, remove it or use "-" (dash) instead of "_" (underscore).You should be able to log in using the system name.

NOTE: You might need to change the Microsoft Internet Information Server (IIS) configuration after you rename a system.

This is a security feature added by Microsoft security patch MS01-055 for Internet Explorer 5.5 or 6.0 that prevents systems with improper name syntax from setting cookie names. Domains that use cookies must use only alphanumeric characters (- or .) in the domain name and the system name. Internet Explorer blocks cookies from a system if the system name contains other characters, such as an underscore character (_).

13.6 Security Problems

13.13.6.1 After updating my Windows XP system with Service Pack 2, I cannot access HP SIM or HP Version Control Repository Manager. What happened?

Windows XP Service Pack 2 implements a software firewall that prevents browsers from accessing the ports required for HP SIM and Version Control Repository Manager access. To resolve this issue, configure the firewall with exceptions to allow browsers to access the ports used by HP SIM and Version Control Repository Manager.

HP recommends the following actions:

1. Select **Start→Settings Control Panel.**
2. Double-click **Windows Firewall** to configure the firewall settings.
3. Select **Exceptions**.
4. Click **Add Port**.
5. Enter the product name and the port number.

   Add the following exceptions to the firewall protection:

   Table 13-1 Firewall protection exceptions

Product	Port Number
HP SMH Insecure Port:	2301
HP SMH Secure Port:	2381
HP SIM Insecure Port:	280
HP SIM Secure Port:	50000

6. Click **OK** to save your settings and close the **Add a Port** dialog box.
7. Click **OK** to save your settings and close the **Windows Firewall** dialog box.

This configuration leaves the default SP2 security enhancements intact, but allows traffic over the ports previously indicated. These ports are required for HP SIM and Version Control Repository Manager to run. Ports 2301 and 2381 are required for the Version Control Repository Manager and ports 280 and 50000 are required by HP SIM. The secure and insecure ports must be added for each product to enable communication with the applications.

13.13.6.2 Why can't I import X.509 certificates directly into HP SMH?

HP SMH generates Certificate Request in Base64-encoded PKCS #10 format. This certificate request should be supplied to the certificate authority. Most CAs return Base64-encoded PKCS #7 certificate data that you can import directly into HP SMH by selecting **Settings→HP System Management Homepage→Security→Local Server Certificate**.

If the CA returns the certificate data in X.509 format, rename the X.509 certificate file as `cert.pem` and place it into the `\hp\sslshare` directory. When HP SMH is restarted, this certificate is used.

13.13.6.3 Why is my PKCS #7 cert data not accepted?

When using a Mozilla browser, there can be problems when cutting and pasting cert request and reply data using Notepad or other editors. To avoid these problems, use Mozilla to open certificate reply files from your CA. Use the Select All, Cut, and Paste operations supplied by Mozilla when working with certificates.

13.13.6.4 Why is my private key file not protected by the file system?

If you are using Windows operating systems, you must have the system drive in NTFS format for the private key file to be protected by the file system.

13.13.6.5 Why do I get errors when I paste my customer-generated certificate PKCS #7 data into the HP SIM Certificate Data field in **Settings→SMH→Security→Trusted Management Servers**?

The customer-generated certificate PKCS #7 data is not relevant to the date given in the **Trusted Management Servers** field. The **PKCS #7** data should be imported into the **Customer Generated Certificates Import PKCS #7 Data** field under **Settings→SMH→Security→Local Server Certificate**. The **HP Systems Insight Manager Certificate Data** field is used to trust HP SIM servers with HP SMH. For more information, see "Trusted Management Servers".

13.13.6.6 Why can't I use a Windows 2003 CA to grant my third-party certificate into HP SMH?

To use a Windows 2003 CA to create a certificate for HP SMH:

1. Create the PKCS #10 data packet by clicking **Settings→SMH→Security→Local Server Certificate** page.
2. Press the **Ctrl**+ **C** keys to copy the data into a buffer.
3. Navigate to **`http://`***`W2003CA`***`/certsrv`** where *`W2003CA`* is the name of your Windows 2003 certificate authority system and complete the following:
   a. Select **Request a certificate**.
   b. Select **Advanced certificate request**.
   c. Select **Submit a certificate request by using a base**.
   d. Press the **Ctrl**+ **V** keys to paste the **PKCS #10** data into the field.
4. From your Windows 2003 certificate authority system complete the following:
   a. Click **Start→All Programs→Administrative Tools→Certification Authority**.
   b. Click **CA (Local)** ⇒ **W2003CA/certsrv** ⇒ where *`W2003CA`* is the name of your Windows 2003 certificate authority system.
   c. Issue the pending request certificate.
5. Navigate to **`http://`***`W2003CA`***`/certsrv`**, where *`W2003CA`* is the name of your Windows 2003 certificate authority system and complete the following:
   a. Select **View the status of a pending certificate request**.
   b. Select **Base64-encoded** and **Download certificate** (not **certificate chain**).
   c. The file download is `certnew.cer`.
   d. Rename `certnew.cer` to `cert.pem`.

13.13.6.7 What are the security options when using Bastille?

Bastille is a system hardening program that enhances the security of an HP-UX host. It configures daemons, system settings and firewalls to be more secure. It can shut off unneeded services and tools such as rcp(1) and rlogin(1), and can help limit the vulnerability of common Internet services such as Web servers and DNS.

NOTE: At this time, HP System Management Homepage does not support Partition Manager.

One facility that Bastille uses to lock down a system is IP filtering. Refer to the Partition Manager Online Help for requirements when using IP filtering with Partition Manager. If Bastille's interactive user interface is used, be aware of these issues when answering the questions asked by Bastille. Bastille also has three install-time security options that are represented by the following files in `/etc/opt/sec-mgmt/bastille`.

- **HOST.config** Host-based lockdown, without IPFilter configuration. Using this configuration has no impact on Partition Manager.
- **MANDMZ.config** A fairly tight lockdown, but leaves select network ports open that are used by common management protocols and tools. For example, WBEM still functions when this configuration is used. Launching Partition Manager under this configuration requires the use of SSH or changes to enable ports 2301 and 2381. To enable launching Partition Manager on a system where ports 2301 and 2381 are disabled, adjust the IP filtering by adding entries such as:

  pass in quick proto tcp from any to any port = 2301 flags S/0xff keep state keep frags

  pass in quick proto tcp from any to any port = 2381 flags S/0xff keep state keep frags

  to `/etc/opt/sec-mgmt/bastille/ipf.customrules` prior to running Bastille.

  For more information, see *ipf*(5).
- **DMZ.config** A tight lockdown. Launching Partition Manager under this configuration requires the use of SSH.

  Bastille also impacts Partition Manager when remotely managing a system where Bastille is enabled. After the normal transfer of certificates, Partition Manager works as described above if the HOST.config or MANDMZ.config configurations are used. However, the DMZ.config configuration blocks WBEM traffic and prevents Partition Manager from remotely managing the system.

For more information about Bastille, see *bastille*(1M) and the *Bastille User Guide*, installed at `/opt/sec-mgmt-bastille/docs/user-guide.txt`.

13.7 Other Problems

13.13.7.1 I am having problems downgrading HP SMH from 3.x to 2.x.

To successfully downgrade HP SMH from 3.x to 2.x, stop the HP SMH service and then execute the downgrade by completing the following steps:

1. `$/etc/init.d/hpsmhd stop`
2. `$rpm --oldpackage --U hpsmh-`*`old version`*`.rpm`

13.13.7.2 Why can't I install HP SMH on my system?

The HP SMH install action requires a Java version that requires at least 256 colors to load.

NOTE: This applies to Windows only.

13.13.7.3 Why do I get an error indicating the page cannot be displayed when I click the **Management Processor** link?

The administrator for the management processor has configured the Web server on the management processor to use a port other than port 80. HP SMH does not have access to that parameter and assumes the management processor is on port 80.

13.13.7.4 Why can't I install HP SMH on HP-UX or Linux when I am not root?

You must be logged in as root for HP SMH to have the proper access rights.

13.13.7.5 In the ServiceGuard Manager plugin, selecting **Display Consolidated Syslog** might require you to reauthenticate or cause a page not found error.

If the page not found error appears, press the **Refresh** button in the browser to allow the page to be shown. Subsequently, you need to reauthenticate.

13.13.7.6 The value presented in the **Total Swap Space Size** field of the Memory Utilization property page includes the swap space that exists in the system as a device or file system and the size of the pseudo-swap, which does not exist as a memory resource. The actual device and file system swap space is not presented in the page.

Currently, it is not possible to obtain the actual size of the device and file system swap space through HP SMH property pages. You can obtain this information from the HP-UX command line, using the `swapinfo` command.

Service and Support

Support for HP SMH is provided as an adjunct to support of the underlying hardware. The HP Support pages provide you with a variety of product, service, and support-related resources for HP SMH.

- Access HP SMH on the Software Depot home. Go to **http://www.hp.com/go/softwaredepot** and select **Security and manageability**. Look for the **HP System Management Homepage** link. The support for Linux Integrity is found by selecting the Linux link on Software Depot home. Look for the **HP Integrity Essentials Pack for Linux** link.
- Access the *HP ProLiant Essentials software* page at **http://www.hp.com/servers/manage**. You find a wealth of Systems Management Products and service-related information.
- Access the HP IT Resource Center for maintenance and support, forums, and training and education of HP products at **http://itrc.hp.com**.
- Contact the HP Support Forum to get answers to your HP product questions at **http://forums.itrc.hp.com**.

Keeping good records of your configuration can significantly speed up the troubleshooting process. Keep current and consult the following list when you obtain assistance from your HP service provider:

- Management system make, model, and serial number information
- Operating system information, operating environment information (HP-UX), including version number, a list of service packs applied, patches, the Compaq SSD version, and Insight Agents' names and versions that have been applied
- Hardware configuration information for Linux and Windows:
  - Survey Utility output or Inspect printout
  - System Configuration Utility printout
  - Description of non-HP or non-Compaq equipment that is not shown on the Inspect or System Configuration printout

14 Legal Notices

Warranty

The information in this document is subject to change without notice. Hewlett-Packard makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental, or consequential damages in connection with the furnishing, performance, or use of this material.

A copy of the specific warranty terms applicable to your Hewlett-Packard product and replacement parts can be obtained from your local Sales and Service Office.

U.S. Government License

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

Copyright Notice

Trademark Notices

HP-UX Release 10.20 and later and HP-UX Release 11.00 and later (in both 32- and 64-bit configurations) on all HP 9000 computers are Open Group UNIX 95-branded products.

Intel® and Itanium® are registered trademarks of Intel Corporation in the US and other countries and are used under license.

Java is a U.S. trademark of Sun Microsystems, Inc.

Linux is a U.S. registered trademark of Linus Torvalds.

MS-DOS®, Microsoft®, and Windows® are registered trademarks of Microsoft Corporation in the United States of America and in other countries.

UNIX is a registered trademark of The Open Group.

Publication History

The publication date and part number indicate the current edition. The publication date will change when a new edition is released. The manual part number will change when extensive changes are made. To ensure that you receive the latest edition, you should subscribe to the appropriate product support service. See your HP sales representative for details.

Please direct comments regarding this guide to:

Hewlett-Packard Company HP-UX
Learning Products 3404 East Harmony Road Fort Collins, Colorado 80528-9599

Or, use this Web form to send us feedback: **http://docs.hp.com/en/feedback.html**

Revision History

Revision History
Revision Edition 19 November 2009
MPN: 466304-004. This edition of HP System Management Homepage help contains updates for product changes and defect fixes for the Windows and Linux HP SMH 6.0.0 release.
Revision Edition 18 March 2009

MPN: 466304-003. This edition of HP System Management Homepage help contains Integrity updates for the Windows and Linux HP SMH 3.0.0 release.

Revision Edition 17 March 2009

MPN: 466304-002. This edition of HP System Management Homepage help contains updates for product changes and defect fixes for the HP-UX HP SMH 3.0.0 release. The product changes include the following:

- New look and feel for HP SMH
- User configurable user interface (UI) properties
- User control of session and user interface (UI) timeouts
- The `smhassist` command to help debug problems related to HP SMH configuration

Revision Edition 16 November 2008

MPN: 466304-001. The first edition of HP System Management Homepage 3.0 contains Linux and Windows information and tasks including the following:

- New user interface
- Support for Kerberos on Windows
- Support for Command Line Interface
- The ability to disable port 2301
- User configurable user interface properties
- User control of session and user interface timeouts
- Log localization
- IPv6 support

Revision Edition 15 February 2008

MPN: 436304-007. The fifteenth edition added new hardware support for Windows and Linux as well as adding new functionality for controlling the size of log files and support for Alternative Named Certificates for the HP SMH v2.1.11 release, and the online help was produced in two languages.

Revision Edition 14 December 2007

MPN: 436304-008. The fourteenth edition added new functionality and defect fixes for the HP-UX HP SMH v.2.2.7 release, and the online help was produced in nine languages for the HP-UX release.

Revision Edition 13 August 2007

MPN: 436304-006. The thirteenth edition added new functionality for IPF Linux and Windows for the HP SMH v2.1.10-00 release, and the online help was produced in two languages.

Revision Edition 12 June 2007

MPN: 436304-005. The twelfth edition added new security fixes for the HP SMH v2.1.10 release, and the online help was produced in two languages.

Revision Edition 11 June 2007

MPN: 436304-004. The eleventh edition added new functionality and defect fixes for the HP-UX HP SMH v2.2.6 release, and the online help was produced in nine languages for the HP-UX release.

Revision Edition 10 April 2007

MPN: 436304-003. The tenth edition added new security fixes for the HP SMH v2.1.8 release, and the online help was produced in two languages.

Revision Edition 9 February 2007

MPN: 436304-001. The ninth edition added new functionality and defect fixes for the HP-UX HP SMH v2.2.5 release, and the online help was produced in nine languages for the HP-UX release.

Revision Edition 8 January 2007

MPN: 436304-002. The eighth edition added new operating system and browser support for the HP SMH v2.1.7 release, and the online help was produced in two languages.

Revision Edition 7 December 2006

MPN: 365395-009. The seventh edition added defect fixes for the HP-UX HP SMH v2.2.5 release, and the online help was produced in nine languages for the HP-UX release.

Revision Edition 6 November 2006

There was an error in the edition sequence for this online help system. There was no Edition 6 shipped for HP System Management Homepage.

Revision Edition 5 September 2006

MPN: 365395-008. The fifth edition added functionality changes for the HP-UX HP SMH v2.2.4 release, and the online help was produced in nine languages for the HP-UX release.

Revision Edition 4 June 2006
MPN: 365395-007. The fourth edition added functionality changes for the HP-UX HP SMH v2.2.3 release, and the online help was produced in nine languages.
Revision Edition 3 December 2005
MPN: 365395-005. The third edition added functionality changes for the HP-UX HP SMH v2.2.1 release, and the online help was produced in nine languages.
Revision Edition 2 February 2005
MPN: 365395-004. The second edition added information and tasks for the HP-UX HP SMH v2.2 release.

Glossary

Accounts for Users & Groups tool (ugweb) The HP-UX Accounts for Users and Groups (ugweb) tool is used to manage user accounts and group accounts on the local system. This tool can also be used to manage user accounts on a NIS system. The ugweb tool can be launched from the HP-UX System Administration Manager (SAM) tool or from HP SMH.

AS *See* Kerberos Authentication Server.

CA *See* certificate authority.

caution A note to indicate that failure to follow directions could result in damage to equipment or loss of information.

certificate An electronic document that contains a subject's public key and identifying information about the subject. The certificate is signed by a certificate authority (CA) to bind the key and subject identification together.

certificate authority (CA) A trusted third-party organization or company that issues digital certificates used to create digital signatures and public-private key pairs. The role of the CA in this process is to guarantee that the individual who has been granted the unique certificate is the individual he or she claims to be.

CLI *See* command line interface.

command line interface (CLI) The set of commands that you can execute directly from the command shell of an operating system.

Disks and File Systems tool (fsweb) The HP-UX Disks and File Systems (fsweb) tool is used to manage file systems, logical volumes, and disks. The Disks and File Systems tool can be launched from the HP-UX System Administration Manager (SAM) tool or from HP SMH.

DNS *See* Domain Name Service.

Domain Name Service (DNS) A service that translates domain names into IP addresses.

evweb *See* System Fault Management tool .

external sites Third-party application URLs.

fsweb *See* Disks and File Systems tool.

graphical user interface (GUI) A program interface that uses the graphics capabilities of a computer to make the program easier to use. The HP SMH GUI is Web-enabled and displays in a Web browser.

GUI *See* graphical user interface.

HP Insight Management Agent A program that regularly gathers information or performs some other service without the user's immediate presence.

HP SIM *See* HP Systems Insight Manager.

HP SMH *See* HP System Management Homepage.

HP System Management Homepage (HP SMH) The HP System Management Homepage (HP SMH) is a Web-based interface that consolidates and simplifies single system management for HP servers on HP-UX, Linux, and Microsoft Windows operating systems. By aggregating the data from HP Web-based agents and management utilities, HP SMH provides a common, easy-to-use interface for displaying hardware fault and status monitoring, performance data, system thresholds, diagnostics, and software version control for an individual server. HP SMH is an integrated piece of software used by the suite of HP Web-enabled System Management Software to communicate over HTTP and HTTPS. It provides a uniform set of functionality and security to HP Web-enabled System Management Software.

HP Systems Insight Manager (HP SIM) System management software that is capable of managing a wide variety of systems, including HP systems, clusters, desktops, workstations, and portables. HP SIM combines the strengths of HP Insight Manager 7, HP Toptools, and HP Servicecontrol Manager to deliver a single tool for managing HP ProLiant, HP Integrity, and HP 9000 systems running HP-UX, Linux, and Windows. The core HP SIM software delivers the essential capabilities required to manage all HP server platforms. HP SIM can also be extended to deliver unparalleled breadth of system management with plugins for HP storage, power, client, and printer products. Plugins for rapid deployment,

	performance management, and workload management enable systems administrators to pick the value added software required to deliver complete lifecycle management of their hardware assets. To obtain more information about HP SIM, go to **http://www.hp.com/go/hpsim**.
HP Version Control Agent (VCA)	An Insight Management Agent that is installed on a system to enable the customer to see the HP software installed on that server. The HP Version Control Agent can be configured to point to a HP Version Control Repository Manager, allowing easy version comparison and software update from the repository.
HP Version Control Repository Manager (VCRM)	An Insight Management Agent that allows a customer to manage HP-provided software stored in a user-defined directory/repository.
HP Web-enabled System Management Software	Software that manages HP Web-enabled products.
HP-UX System Administration Manager (SAM)	Is the primary interface for HP-UX 11i v1 (B.11.11) and HP-UX 11i v2 (B.11.23) system management. For HP-UX 11i v3 (B.11.31), HP SMH provides the primary interface for HP-UX system administration tasks. The legacy SAM functionality is still available.
HTTPS	*See* Secure HTTP.
in-place	Locally. For example to install in-place means to install locally.
Integrated Agents and Other Agents	The Integrated Agents area on the Tools page contains participants and links to their entry points if applicable. You can click an agent link to access that particular agent. Participants are agents that are contributing information contained in the HP System Management Homepage (HP SMH). If no HP Web-enabled System Management Software is installed that provides this information, then **none** is displayed. The Other Agents area on the Tools page lists the visible HP Web-enabled System Management Software that does not participate in HP SMH. The name of the HP Web-enabled System Management Software provides a link so that you can still access the agents if they provide a user interface. If no HP Web-enabled System Management Software is installed that provides this information, then **none** is displayed.
Integrity Support Pack	A set of HP software components that have been bundled together by HP, and verified to work with a particular operating system. An Integrity Support Pack contains driver components, agent components, and application and utility components. All of these are verified to install together.
Internet Protocol (IP) range	Systems with an IP address that falls in the specified range.
IP	*See* Internet Protocol (IP) range.
kcweb	*See* Kernel Configuration tool.
KDC	*See* Kerberos Key Distribution Center.
Kerberos	A trusted third-party authentication protocol developed at MIT which allows different hosts and users to authenticate and confirm the identity of each other.
Kerberos Authentication Server	A service whose sole purpose is to authenticate user account records. The AS serves as an introducer for the user and the service through the use of a shared secret key registered with the AS.
Kerberos Key Distribution Center	Kerberos Key Distribution Center, composed of the Authentication Server and the Ticket Granting Server.
Kerberos Ticket Granting Server	Adds an extra layer of indirection so that the user only needs to enter in a password once; the ticket and session key obtained from that password is used for all further tickets. Before accessing any regular service, the user requests a ticket from the Authentication Server (AS) to talk to the TGS. This ticket is called the *ticket granting ticket* or TGT; it is also sometimes called the *initial ticket*. The session key for the TGT is encrypted using the user's long-term key, so the password is needed to decrypt it from the AS's reponse to the user.

Kernel Configuration tool (kcweb) The HP-UX Kernel Configuration (kcweb) tool is used to manage kernel tunables, modules and alarms. The Kernel Configuration tool can be launched from the HP-UX System Administration Manager (SAM) tool or from HP SMH

MIT Massachusetts Institute of Technology.

multihomed Multiple names set to a certificate.

parMgr *See* Partition Manager.

Partition Manager (parMgr) Provides system administrators with a convenient GUI to configure and manage nPartitions on HP server systems. Perform complex configuration tasks without having to remember commands and parameters. Select nPartitions, cells, I/O chassis, or other components from the graphical display, then select an action from a menu. You can use Partition Manager to perform the following tasks: create, modify, and delete nPartitions; examine the nPartition configuration of a complex, check the complex for potential configuration and hardware problems, and manage hardware resources on the complex.

NOTE: At this time, HP System Management Homepage does not support Partition Manager.

pdweb *See* Peripheral Device tool.

Peripheral Device tool (pdweb) The HP-UX Peripheral Device (pdweb) tool can be used to easily and quickly view I/O devices and OLRAD cards. It helps manage hot pluggable PCI slots on systems that support adding and replacing cards without rebooting. On all HP-UX systems, pdweb displays the I/O devices and can be used to (re)create device files for a selected device. The Peripheral Device tool can be launched the HP-UX System Administration Manager (SAM) tool or from HP SMH.

PKI *See* Public Key Infrastructure.

Principal Users or service / host which are present in a Kerberos realm and are allowed to authenticate to each other.

ProLiant or Integrity Support Pack A set of HP software components that have been bundled together by HP, and verified to work with a particular operating system. A ProLiant or Integrity Support Pack contains driver components, agent components, and application and utility components. All of these are verified to install together.

Public Key Infrastructure (PKI) Public Key Infrastructure is the combination of software, encryption technologies, and services that enables enterprises to protect the security of their communications and business transactions on the Internet.

Realm Kerberos domain. Usually, it is the network's domain name in capital letters. For example, the Kerberos realm for the smhkerberos.com would conventionally be called `SMHKERBEROS.COM`.

Red Hat Package Manager (RPM) The Red Hat Package Manager is a powerful package manager that can be used to build, install, query, verify, update, and uninstall individual software packages. A package consists of an archive of files and package information, including name, version, and description.

repository The database that stores vital information about the managed cluster, including users, nodes, node groups, roles, tools, and authorizations.

RPM *See* Red Hat Package Manager.

SAM *See* HP-UX System Administration Manager.

search criteria A set of variables (information) used to define a requested subset of information from the set of all information. The information set that can be filtered includes action information, some of the system's information, and so on. A filter is composed of an permitted filter followed by a restricted filter. The result of these two filtering operations is called a group. An example of a filter is a SQL statement that creates viewable information or causes management operations to be performed.

Secure HTTP (HTTPS) An extension to the HTTP protocol that supports sending data securely over the Web.

Secure Shell (SSH) A program that enables you to sign in to another system over a network and execute commands on that system. It also enables you to move files from one system to another, and it provides authentication and secure communications over insecure channels.

Secure Sockets Layer (SSL) A standard protocol layer that lies between HTTP and TCP and provides privacy and message integrity between a client and server. A common use of SSL is to provide authentication of the

	server, so the client can be assured it is communicating with the system that the system claims to be. It is application protocol independent.
Secure Task Execution (STE)	Secure execution of a task from a managed system. This feature of HP SMH ensures that the user requesting the task has the appropriate rights to perform the task and encrypts the request to protect data from snooping.
Security Attributes Configuration tool (secweb)	The HP-UX Security Attributes Configuration (secweb) tool is used to view and configure system-wide and per-user (local users and NIS users) values of security attributes. It also gives information about account locks. The Security Attributes Configuration tool can be launched from the HP-UX System Administration Manager (SAM) tool, or from HP SMH.
secweb	*See* Security Attributes Configuration tool .
self-signed certificate	A certificate that is its own certificate authority (CA), so that the subject and the CA are the same. *See also* certificate, certificate authority.
single sign on	Permission granted to an authenticated user browsing to HP Systems Insight Manager (HP SIM) to browse to any of the managed systems from within HP SIM without re-authenticating to the managed system. HP SIM is the initial point of authentication and browsing to another managed system must be from within HP SIM.
software update	A task to remotely update software and firmware.
SSH	*See* Secure Shell.
SSL	*See* Secure Sockets Layer.
status type	Systems of specified status type (Critical, Failed/Major, Degraded/Minor, Normal, and Unknown) as defined by HP SMH.
STE	*See* Secure Task Execution.
survey utility	An agent (or online service tool) that gathers and delivers hardware and operating system configuration information. This information is gathered while the server is online.
System Fault Management tool (evweb)	The System Fault Management (evweb) tool is used to view and administer WBEM indications. The evweb tool can be launched from HP SMH.
TGS	*See* Kerberos Ticket Granting Server.
ugweb	*See* Accounts for Users & Groups tool.
URI	Provides methods to access a resource on the Internet. A Uniform Resource Locator (URL) is a type of Uniform Resource Indicator (URI).
URL	A global address of resources on the World Wide Web. A Uniform Resource Locator (URL) is a type of Uniform Resource Indicator (URI).
user	A network user with a valid sign in on the HP System Management Homepage.
user accounts	Accounts used to sign in to HP System Management Homepage (HP SMH). These accounts associate a local Windows user, domain account, or an HP-UX or Linux user group with privilege levels and paging attributes inside HP SMH.
VCA	*See* HP Version Control Agent.
VCRM	*See* HP Version Control Repository Manager.
version control	Referred to as the Version Control Repository Manager installed on a Windows system for Windows and Linux Proliant or Integrity systems, and Software Distributor on HP-UX operating systems. Provides an overview of the software status for all managed ProLiant or Integrity systems and can update system software and firmware on those systems programmatically using predetermined criteria. Version control identifies systems that are running out-of-date system software, indicates if an upgrade is available, and provides reasons for upgrading. For HP-UX systems, Software Distributor can be launched from an HP Systems Insight Manager CMS against one or more installed HP-UX systems.
WBEM	*See* Web-Based Enterprise Management.
Web-Based Enterprise Management (WBEM)	Is a platform and resource independent DMTF (Distributed Management Task Force) standard that defines both a common model (for example, description) and protocol (for example, interface) for monitoring and controlling a diverse set of resources. The HP WBEM Services for HP-UX

products is the HP-UX implementation of the DMTF (Distributed Management Task Force) WBEM standard.

Index

T

U

W