HP System Management Homepage

HP Part Number: 436304-003
Published: April 2007
Edition: 10

Table of Contents

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, 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 can be installed on HP-UX, Linux (x86, AMD64, and Intel Itanium), and Windows operating systems.

On an HP-UX system, HP SMH has a bundle tag of `SysMgmtWeb` and is default installed with the HP-UX 11i v1 (B.11.11) and HP-UX 11i v2 (B.11.23) Operating Environments, and recommended to install with the 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.

You can also configure HP SMH to trust HP SIM such that an additional login is not required when traversing from HP SIM to HP SMH. This is done by accepting the HP SIM certificate from the HP SMH **Login** page when first accessing HP SMH from HP SIM.

NOTE: Accepting the HP SIM certificate is the default behavior.

There are also several HP SIM tools (under the **Configure > HP-UX Configuration** category) that access HP SIM-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 various 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`). However, you can also use the *sam*(1M) command which behaves the same as the *smh*(1M) command except that the deprecation message is displayed in the beginning. Most of the applications for performing administration tasks are now available through the web-based GUI interface and the enhanced TUI. However, few applications continue to open in ObAM based X-windows or ObAM based TUI. Some of the functional areas previously available for system administration are obsolete. These areas are listed in the *HP-UX 11i v3 Release Notes* available on the HP Technical documentation web site at http://docs.hp.com.

Additional Resources

For additional resources, go to these links:

- 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.
- HP ProLiant 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 a complete set of 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 install 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 install guide is available on the HP Technical Documentation Web site at http://docs.hp.com. Also, for Linux and Windows releases, the install 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 a complete set of documentation for using, maintaining, and troubleshooting HP SMH. For Linux and Windows, this user guide is available under the HP SMH Help menu, and on the HP Technical Documentation Web site at http://docs.hp.com. For HP-UX, we no longer provide a printed user guide, please refer to the HP SMH online help content for information on how to use, maintain, and troubleshoot HP SMH.
- **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.
- ***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 in a previous section of this help topic.

Related Topics

- Getting Started
- HP SMH Pages

2 Getting Started

To get started with HP System Management Homepage (HP SMH), use the following information as a guideline for configuring HP SMH and then 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 set in the `/opt/hpsmh/lbin/envvars` and `/opt/hpsmh/conf/timeout.conf` scripts.
- On Linux operating systems, HP SMH is installed with default settings. The settings are configurable by using the perl script (hpSMHSetup.pl) located under `/usr/local/hp`.
- On Windows operating systems, the installation enables you to configure the 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: "User Groups"
2. Configure the trust mode: "Trust Mode"
3. Configure local or anonymous access: "Local/Anonymous Access"

Related Topics

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

Logging In

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

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

To log in to the HP SMH with Internet Explorer:

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

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

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. You can also configure HP SMH to always be running on port 2381. See the *smhstartconfig*(1M) command for more information. If the `Start on Boot` feature is enabled (instead of `autostart`) a message window explains the security features. You can wait a few seconds to be redirected to port 2381 or click the link at the bottom of the message. The System Management Homepage Login page will appear.

You can find procedures on how to change the configuration variables in the *HP System Management Homepage Installation Guide* on the HP Technical Documentation Web site at http://docs.hp.com.

2. The first time you browse to this URI, the **Security Alert** dialog box appears, asking 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.

NOTE: If you want 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 this is implemented, the **Security Alert** dialog box does not appear. If the alert appears when you do not expect it, you might have browsed to the wrong system. You can refer to the online help in your browser for more information about installing the **certificate authority Root Certificate**.

3. Click **Yes**.

   The **Login** page appears. If you have enabled **Anonymous** access, then System Management Homepage appears.

4. Enter your user name that is recognized by the operating system.

   On HP-UX, HP SMH initially only allows access to the root user, on Linux access is initially allowed to users belonging to the root operating system group, and on Windows 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 one of the initially allowed users, you can use the Security Settings to grant access to users in different operating system groups.

NOTE: In most cases, the **administrator** on Windows and **root** on HP-UX or Linux have administrator access on HP SMH.

5. Enter the password that is recognized by the operating system.
6. On HP-UX, click **Sign In**. On Linux and Windows, click **Login**. System Management Homepage appears.

Starting HP SMH from Mozilla or Firefox

To log in to HP SMH with Mozilla:

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

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

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. You can also configure HP SMH to always be running on port 2381. See the *smhstartconfig*(1M) command for more information. If the `Start on Boot` feature is enabled (instead of `autostart`) a message window explains the security features. You can wait a few seconds to be redirected to port 2381 or click the link at the bottom of the message. The System Management Homepage Login page will appear.

You can find procedures on how to change the configuration variables in the *HP System Management Homepage Installation Guide* on the HP Technical Documentation Web site at http://docs.hp.com.

The first time you browse to the URI, the **Website Certified by an Unknown Authority** dialog box appears, asking you to indicate whether to trust the server. If you do not select **Accept this certificate permanently**, the **Website Certified by an Unknown Authority** dialog box appears every time you use a browser.

2. Click **OK**.

   The **Login** page appears. If you have enabled **Anonymous** access, then System Management Homepage appears.

3. Enter your user name that is recognized by the operating system.

   On HP-UX, HP SMH initially only allows access to the root user, on Linux access is initially allowed to users belonging to the root operating system group, and on Windows 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 one of the initially allowed users, you can use the Security Settings to grant access to users in different operating system groups.

NOTE: In most cases, the **administrator** on Windows and **root** on HP-UX and Linux have administrator access on HP SMH.

4. Enter the password that is recognized by the operating system.
5. On HP-UX, click **Sign In**. On Linux and Windows, click **Login**.

   System Management Homepage appears.

Starting HP SMH from HP SIM

To start HP SMH by logging 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 is displayed, asking you to indicate whether to trust the server. If you do not import the *certificate*, the **Security Alert** is displayed every time you browse to HP SIM.

NOTE: If you want 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 this is implemented, the **Security Alert** dialog box does not appear. If the alert is displayed when you do not expect it, you might have browsed to the wrong system. You can refer to the online help in your browser for more information about installing the **certificate authority Root Certificate**.

2. Click **Yes**.

   The **Login** page is displayed.
3. Enter a user name that is recognized by the operating system.
4. Enter a 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 checkbox next to a target system. Click **Apply**.
9. Verify the target system by selecting a checkbox next to the system. Click **Run Now**.

   The **Security Alert** dialog box is displayed, asking you to indicate whether to trust the server. If you do not import the *certificate*, the **Security Alert** is displayed every time you browse to HP SMH.

   The System Management Homepage is displayed.

Starting from the HP-UX Command Line

When you run either 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 of the applications for performing administration tasks are now available through the web-based GUI interface and an enhanced TUI. However, few applications continue to open in ObAM based X-windows or ObAM based TUI.

You are recommended to use the *smh*(1M) command. However, the *sam*(1M) command will continue to be available and behave just as the *smh*(1M) command. Some of the functional areas previously available for system administration are obsolete. These areas are listed in the *HP-UX 11i v3 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 under HP-UX only starts on demand. It does not run continually. A daemon listens on port 2301 to start an instance of the management server.

Related Topics

- Getting Started
- Configuring Firewall Settings
- Automatically Importing Certificates
- Logging 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, you must configure the firewall with exceptions to allow browsers to access the ports used by HP Systems Insight Manager and Version Control Repository Manager.

NOTE: For Windows XP with Service Pack 2, this configuration leaves the default SP2 security enhancements intact, but allows 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. Double-click **Windows Firewall** to configure the firewall settings.
3. Select **Exceptions**.
4. Click **Add Port**.

   You must enter the product name and the port number.

   Add the following exceptions to the firewall protection:

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

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

Linux

Firewalls are configurable various ways depending on the version of Linux installed.

Red Hat Enterprise Linux 3 and 4

The following list displays an example for iptables firewall rules for Red Hat Enterprise Linux 3 and 4 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 list displays the new value for iptables firewall rules for Red Hat Enterprise Linux 3 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 8 and 9 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 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 displays 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
- Logging In
- Automatically Importing Certificates
- Logging Out
- HP SMH Pages

Configuring Timeout Settings

HP SMH 2.1.5 and later enables you to configure the HP SMH GUI timeout.

To modify this setting:

1. As a precautionary measure, copy the existing `smhpd.xml` file into a different directory.
2. Manually add the tag:
   a. Open the `smhpd.xml` file in the `\hp\hpsmh\conf` directory on the boot drive and add (/opt/hp/hpsmh/conf for Linux) with a text editor.
   b. Add the following line between the <system-management-homepage> and </system-management-homepage> tags:

      ```
      <ui-timeout>any value between 10 and 3600</ui-timeout>
      ```

   c. Save the file.
3. Restart the HP SMH service.

Related Topics

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

Automatically Importing Certificates

The **Automatically Import Management Server Certificate** feature enables you to automatically import the HP Systems Insight Manager (HP SIM) system *certificate* when accessing the HP System Management Homepage (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**→**Security**→**Trust Mode**), and a certificate for the HP SIM system you are accessing has not been imported into the **Trusted Certificates List**, then the **Login** page displays the **Automatically Import**

Management Server Certificate option. The Certificate Information retrieved from *SERVER NAME* displays the HP SIM certificate details.

2. **Automatically Import Management Server Certificate** is selected by default. Deselect this option if you do not want to add the HP SIM certificate to the **Trusted Certificates List**. However future access to this system requires log-in credentials.

   If you allow HP SMH to automatically import the HP SIM certificate, future access to the system is seamless. You will not be challenged for your log-in credentials.

3. Leave **Automatically Import Management Server Certificate** selected, enter your HP SMH credentials, and click **Login** to automatically import the certificate. The certificate is added to the **Trusted Certificates List**.

NOTE: Deselect **Automatically Import Management Server Certificate** if you do not want to import the certificate. Deselecting this option still requires you to enter log-in credentials. However, administrator credentials are not required to log in.

Related Topics

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

Logging Out

To log out of the HP System Management Homepage (HP SMH), you have several options:

- In the HP SMH banner, for HP-UX click **Sign Out** and for Linux and Windows click **logout**. The HP System Management Homepage **Login** page appears.
- Close every instance of the Web browser that was used to log in to HP SMH.

Related Topics

- Getting Started
- Logging 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 borders defining the status of the items. Refer to the "The Home Page" for more information.

The HP SMH interface is separated into two frames:

- **Header Frame** The header frame is constantly visible regardless of which page you are viewing. A link shows the path you are currently viewing.
- **Data Frame** 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), you will see the following information areas in the header or data frames:

- **HP SMH Pages**
  - "The Home Page"
  - "The Settings Page"
  - "The Tasks Page"
  - "The Tools Page"
  - "The Logs Page"
- **Support** The **Support** link provides you with links to HP support areas.
- **Forums** The **Forums** link provides you with links to HP forums.
- **Help** The **Help** link launches the help files in a separate browser window. The help may contain a combination of help files related to the HP Web-enabled System Management Software and utilities.
- **System Model** The **System Model** shows the model of the system. For Linux and Windows, it is displayed as **Unknown** if the HP Insight Management Agent for servers is not installed on the system. For HP-UX, it is displayed because the operating system can determine the system model independently of the HP Insight Management Agent.
- **Current User** The Current User displays the identity of the user that is currently logged in. If the current user is a real operating system-based user, then a **Logout** or **Sign Out** link is displayed. If anonymous access is enabled and you are accessing the page anonymously, the **Current User** displays **hpsmh_anonymous** and the **Login** or **Sign In** link is displayed. If **Local Access** is enabled and you are accessing the HP Web-enabled System Management Software from a local machine, the **Current User** displays **hpsmh_local_anonymous** or **hpsmh_local_administrator**, depending on what level of access has been enabled, and local access is displayed below it. If it is local_access_administrator, there will not be any login or logout link.

Related Topics

- The Home Page
- The Settings Page
- The Tasks Page
- The Tools Page
- The Logs Page

HP SMH Pages

The *HP System Management Homepage* (HP SMH) displays up to five tabbed 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 are only visible if HP Web-enabled System Management Software provides information for them.

The HP SMH pages that may display are:

- "The Home Page"
- "The Settings Page"
- "The Tasks Page"
- "The Tools Page"
- "The Logs Page"

Related Topics

- Product Overview
- Navigating the Software
- Getting Started

4 The Home Page

The **Home** page provides the system, subsystem, and status view of the server. It 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, these include information provided by integrated *Web-Based Enterprise Management* (WBEM) property pages and management utilities. For Linux and Windows operating systems, these include information provided by integrated version control, server, and storage agents.

Software Status Categories (Boxes)

The status of the HP Web-enabled System Management Software is configured to appear in categories, which are shown in individual boxes. Each category (box) contains links that enable you to drill down into the HP Web-enabled System Management Software that is providing the data.

Additional Status Categories: The status of the integrated WBEM is configured to appear in additional categories (boxes). Each category contains links that enable you to drill down into the WBEM Software that is providing the data.

Status Category Indicators: The border around the category (box) provides a color-coded status for the data in each category. The following table lists the color indicators and the status they define.

Indicator	Description
Blue	Unknown
Green	Normal
Yellow	Minor
Orange	Major
Red	Critical
Gray	Disabled
Aqua	Warning
White	Informational

Overall System Status/System Status Summary

The **Overall System Status** category (**System Status Summary** on HP-UX) displays links to all subsystems which have a failed or degraded status, as provided by the integrated *HP Web-enabled System Management Software*. If there are no agents installed or no failed or degraded items, then the **Overall System Status** category displays **no failed/degraded items**.

Organizational Menu

The organizational menu is displayed in the left side of the **Home** page. It contains links to the HP Web-enabled System Management Software to include:

- **Integrated Agents** 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.

- **Other Agents** 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.
- **Management Processor** 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, then **none** is displayed. The December 2006 release for HP-UX HP SMH 2.2.5 implemented the Management Processor link and property page.
- **Other Software/Other Links** May provide links to ProLiant, Integrity, Support, and Forums.
- **KEY/Legend** Displays a listing of status icons and a brief description of each.

Icon	Status
	Critical
	Major
	Minor
	Warning
	Normal
	Disabled
	Unknown
	Information

Default HP-UX Property Pages

Certain 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, in particular the products `B8465BA` (WBEM Services for HP-UX) and `SysFaultMgmt` (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 the health status. This health status is also propagated to the HP Systems Insight Manager's HS column for the HP-UX system if using HP SIM. In addition to the summary, there are links that 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.

Software

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

Related Topics

- The Settings Page
- The Tasks Page
- The Tools Page
- The Logs 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 (that you would find on the **Tools** page).

Menus Category (HP-UX only)

This category provides links that enable you to add and remove custom menus to any page and category for HP SMH. You can use these menus for running commands, launching X applications, or launching into a separate Web page or Web site. See "Menus".

System Management Homepage Category

This category provides links that enable you to configure your HP SMH settings. It provides links to the following:

- **"Credits"** Displays information regarding licensing and credits.
- **"Security"** Displays links for security options.

Related Procedures

- Menus
- Add Custom Menu
- Remove Custom Menu
- Credits
- Security
- IP Binding
- IP Restricted Login
- Local Server Certificate
- Local/Anonymous Access
- Trust Mode
- Trusted Management Servers
- User Groups

Related Topics

- The Home Page
- The Tasks Page
- The Tools Page
- The Logs Page

Menus

The **Menus** category provides links to add custom menus and remove custom menus:

- Select **Settings→Menus→Add Custom Menu**.
- Select **Settings→Menus→Remove Custom Menu**.

Related Procedures

- Add Custom Menu
- Remove Custom Menu

Related Topics

- The Settings Page

Add Custom Menu

The **Add Custom Menu** link displays options for you to configure and add custom menus.

To add a Custom Menu to HP SMH (HP-UX only):

1. Select **Settings→Menus→Add Custom Menu**.
2. For **Type**, specify whether the menu will be a command execution, an X application launch, or a link to another Web site or Web application.
3. For **Page**, specify which page within the HP SMH pages the menu should be under. For example, you can specify **Home**, **Tasks**, **Settings**, **Tools**, or **Logs**.
4. For **Category**, specify a category (box) for the menu to be placed under. You can provide the name of an existing category or enter a new category, which will be created.
5. For **Tool Name**, enter the name of the menu as you want it to appear under the Page and Category specified.
6. For **Command/URL**, enter the actual command line to the command or X application, or the URL to the Web page that will be the target of the link.
7. For **Run as root**, the check box on the right will determine whether the command should be run as the root user. If checked, then only HP SMH users with Administrator privileges will be allowed to run this menu.

NOTE: Only HP SMH users with Administrator authorization can create menus and can run custom menus that are set to run as the user "root". For HP SMH users with Operator or User authorization, the custom menus they are allowed to run will run as the actual user id of the user logged in.

These custom menus are stored and managed in the `/opt/hpsmh/data/htdocs/xlaunch/custom_menus.js` file, which can be manually copied from one system to other systems.

Related Topics

- The Settings Page
- Menus
- Remove Custom Menu

Remove Custom Menu

The **Remove Custom Menu** link displays options for you to remove custom menus.

To access the Remove a Custom Menu, select **Settings→Menus→Remove Custom Menu**.

Related Topics

- The Settings Page
- Menus
- Add Custom Menu

Credits

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

To access Credits, select **Settings→System Management Homepage→Credits**.

Related Topics

- The Settings Page

Security

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

- **IP Binding** Select **Settings→System Management Homepage→Security→IP Binding**.
- **IP Restricted Login** Select **Settings→System Management Homepage→Security →IP Restricted Login**.
- **Local Server Certificate** Select **Settings→System Management Homepage→Security →Local Server Certificate**.
- **Local/Anonymous Access** Select **Settings→System Management Homepage→Security →Local/Anonymous Access**.
- **Trust Mode** Select **Settings→System Management Homepage→Security →Trust Mode**.
- **Trusted Management Servers** Select **Settings→System Management Homepage→Security →Trusted Management Servers**.
- **User Groups** Select **Settings→System Management Homepage→Security →User Groups**.

NOTE: To configure *user accounts*, use the applicable tools for each type of operating system for managing user and group accounts. For HP-UX 11i v2 (B.11.23) December 2005 and later releases, this includes the *Accounts for Users & Groups* (ugweb) user interface found under the **Tools** page.

Related Procedures

- IP Binding
- IP Restricted Login
- Local Server Certificate
- Local/Anonymous Access
- Trust Mode
- Trusted Management Servers
- User Groups

Related Topics

- The Settings Page

IP Binding

IP Binding specifies from which IP addresses the HP System Management Homepage (HP SMH) accepts requests from and provides control over which nets and subnets requests are processed.

Administrators can configure HP SMH to only bind to addresses specified in the **IP Binding** window. A maximum of 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.

NOTE: HP SMH always binds to 127.0.0.1. If IP Binding is enabled and no subnet/mask pairs are configured, then 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. Click **Settings→System Management Homepage→Security**.
2. Click **IP Binding**.
3. Select **IP Binding** box to enable IP binding.
4. Enter the **Subnet IP Address**.
5. Enter the **Netmask**.
6. Click **Save Configuration** to save the current configurations, or click **Reset Values** to cancel all changes.

   If **Save Configuration** is clicked, the following message appears:

   ```
   Setting this value requires restarting the HP System Management
   Homepage which may require you to log in again.
   ```

7. Click **OK**.
   - 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 Topics

- Security
- IP Restricted Login
- Local Server Certificate
- Local/Anonymous Access
- Trust Mode
- Trusted Management Servers
- User Groups

IP Restricted Login

The IP Restricted Login enables the HP System Management Homepage (HP SMH) to restrict log-in access based on the *IP address* of a system from which the log in is attempted.

For Linux and Windows, you can set a restricted address at installation time or, from HP-UX, Linux, and Windows, administrators can set a restricted address from the **IP Restricted Login** page.

- If an IP address is excluded, it is excluded even if it is also listed in the included box.
- If there are IP addresses in the inclusion list, then only those IP addresses are allowed log-in access with the exception of *localhost*.
- If no IP addresses are in the inclusion list, then log-in access is allowed to any IP addresses not in the exclusion list.

To restrict IP addresses:

1. Click **Settings→System Management Homepage→Security**.
2. Click **IP Restricted Login**.
3. Select the **IP Restricted Login** box to enable restricted login.
4. Enter the IP addresses to exclude.
5. Enter the IP addresses to include.

6. Click **Save Configuration** to save the current configurations, or click **Reset Values** to cancel all changes.

   If **Save Configuration** is clicked, the following message appears:

   ```
   Setting this value requires restarting the HP System Management
   Homepage which may require you to log in again.
   ```

7. Click **OK**.

Related Topics

- Security
- IP Binding
- Local Server Certificate
- Local/Anonymous Access
- Trust Mode
- Trusted Management Servers
- User Groups

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 originally generated by the HP System Management Homepage (HP SMH) is replaced with one that was 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 that was associated with the self-signed certificate and generates the appropriate data for certificate request. The private key never leaves the server during this process.
- After the ***PKCS #10*** data has been created, the next step is to send it to a certificate authority. Follow your company policy with regard to sending secure requests for and receiving secure certificates.
- After the certificate authority has returned **PKCS #7** data, the final step is to import this into HP SMH.
- After the **PKCS #7** data has been successfully 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) for Linux is overwritten with the system certificate from that **PKCS #7** data envelope. The same private key is used for the new imported certificate as 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→System Management Homepage→Security**.
2. Select **Local Server Certificate**.
3. Optionally, you can replace the default values in the **Organization** or **Organizational Unit** fields with your own values up to a maximum of 64 characters.
4. Click **Create PKCS #10 Data**. A screen appears indicating that the **PKCS #10 Certificate Request** data has been successfully generated and stored in `/opt/hpsmh/sslshare/req_cr.pem` for HP-UX, `/opt/hp/sslshare/req_cr.pem` (`/opt/hp/hpsmh/data/req_cr.pem` in HP SMH 2.1.4 and later) for Linux, and `c:\hp\sslshare\req_cr.pem` (`c:\hp\hpsmh\data\req_cr.pem` in HP SMH 2.1.4 and later) for Windows.
5. Copy the certificate data.

6. Use a secure method to send **PKCS #10** certificate request data to a certificate authority and request the certificate request reply data in the form of **PKCS #7** format. Request that the reply data be 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.

7. When the certificate signer sends the **PKCS #7** encoded certificate request reply data to you, copy the data from the **PKCS #7** certificate request reply and paste the copied data in the **PKCS #7 Data** field.
8. Click **Import PKCS #7 Data**. A message appears indicating whether the customer-generated certificate was successfully imported.
9. Restart HP SMH.
10. Browse to the managed system that contains the imported certificate.
11. Select to view the certificate when prompted by the browser. Be sure the signer is listed as the signer you used, and not HP, before importing the certificate into your browser.

NOTE: If the certificate signer of your choice 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, `/opt/hp/sslshare/cert.pem` (`/etc/opt/hp/sslshare/cert.pem` in HP SMH 2.1.3 and later) for Linux, and `c:\hp\sslshare\cert.pem` for Windows; then restart HP SMH.

Related Topics

- Configuring Firewall Settings
- Security
- IP Binding
- IP Restricted Login
- Local/Anonymous Access
- Trust Mode
- Trusted Management Servers
- User Groups

Local/Anonymous Access

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

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

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

- **Local Access** Is disabled by default. Enabling it means you can locally gain 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→System Management Homepage→Security.**
2. Select **Local/Anonymous Access**.

3. Select **Anonymous Access**.
4. Click **Save Configuration** to save your settings.

To enable local access:

1. Select **Settings→System Management Homepage→Security**.
2. Select **Local/Anonymous Access**.
3. Select **Local Access** to enable local access.
4. Select **Anonymous** or **Administrator**.
5. Click **Save Configuration** to save your settings.

Related Topics

- Security
- IP Binding
- IP Restricted Login
- Local Server Certificate
- Trust Mode
- Trusted Management Servers
- User Groups

Trust Mode

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

- **Trust by Certificate** Sets the HP System Management Homepage (HP SMH) to accept configuration changes only from HP Systems Insight Manager (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 since it requires certificate data and verifies the digital signature before allowing access. If you do not want to enable any remote configuration changes, leave **Trust by Certificate** selected, and leave the list of trusted systems empty by avoiding importing any certificates.

NOTE: HP strongly recommends using this option as it is more secure.

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

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

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

NOTE: HP strongly recommends using the **Trust by Certificate** option as 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.

NOTE: You must have administrative authority to access this directory.

To trust by certificate:

1. Select **Settings→System Management Homepage→Security**.
2. Click **Trust Mode**.
3. Select **Trust by Certificate** to require trusted certificates.
4. Click **Save Configuration** to save the current configurations or **Reset Values** to cancel all changes.
5. Click **Trusted Certificate** to access the Trusted Management server certificate.

To trust by name:

1. Select **Settings→System Management Homepage→Security**.
2. Click **Trust Mode**.
3. Select **Trust by Name** to trust HP SIM by names.
4. Enter the HP SIM certificate name.
5. Click **Save Configuration** to save the current configurations or **Reset Values** to cancel all changes.

The server name option must meet the following criteria:

- Each server name must be less than 64 characters
- The overall length of the server name list is 1,024 characters
- Special characters should not be included as part of the *`SIM certificate name`*: ~ ' ! @ # $ % ^ & * ( ) + = \ " : ' < > ? , |
- Semicolons are used to separate *`SIM certificates names`*

To trust all servers:

1. Select **Settings→System Management Homepage→Security**.
2. Click **Trust Mode**.
3. Select **Trust All** to trust all servers.
4. Click **Save Configuration** to save the current configurations or **Reset Values** to cancel all changes.

Related Topics

- Automatically Importing Certificates
- Security
- IP Binding
- IP Restricted Login
- Local Server Certificate
- Local/Anonymous Access

- Trusted Management Servers
- User Groups

Trusted Management Servers

The **Trusted Management Servers** link enables you to manage your *certificates* in the **Trusted Certificates List**.

- **Import Certificate Data** Certificates are used to establish the trust relationship between HP Systems Insight Manager (HP SIM) and HP System Management Homepage (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→System Management Homepage→Security→Trusted Management Servers**.
2. In the **Add Certificate From Server** area, enter the name or IP address of the HP SIM system that contains the certificate to be added.

   This step is optional as the Base64-encoded certificate used in the next step provides the server name.
3. In the **Import Certificate Data** area, cut and paste the Base64-encoded certificate into the text box.
4. Click **Import Certificate Data**.

To add a certificate from a server:

1. Select **Settings→System Management Homepage→Security→Trusted Management Servers**.
2. In the **Add Certificate From Server** area, enter the name or IP address of the HP SIM server that contains the certificate to be added.
3. Click **Add Certificate From Server**. The certificate information is presented for verification/confirmation before it is added to the list.
4. Verify the certificate information in the **Verify Certificate** window, and if you want to add it to the trusted certificate list, click **Add Certificate to Trust List**.

Related Topics

- Security
- IP Binding
- IP Restricted Login
- Local Server Certificate
- Local/Anonymous Access
- Trust Mode
- User Groups

User Groups

The HP System Management Homepage (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 the 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 different operating system groups. The HP SMH installation enables you to assign the operating system groups to the HP SMH. If a specified operating system group is not defined in OS when HP SMH is started, the System Management Homepage Log message indicates which operating system groups are not defined.

The accounts used for HP SMH do not need to have any 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, and then all accounts in each operating system user group have the access to HP SMH that is specified in the **User Groups** window. The Windows administrators group, the Linux root group, and the HP-UX root automatically have administrative access to the HP System Management Homepage. For HP-UX, only the root user is automatically 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 any elevated access on the host operating system.

The **User Groups** window 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 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 add an Administrator Group:

1. Select **Settings→System Management Homepage→Security**.
2. Click **User Groups**.
3. In the **Administrator** section, enter a user group name.
4. Click **Save Configuration** to save the current configurations, click **Clear All Groups** to clear the fields or **Reset Values** to cancel all changes.

To add an Operator Group:

1. Select **Settings→System Management Homepage→Security**.
2. Click **User Groups**.
3. In the **Operator** section, enter a user group name.
4. Click **Save Configuration** to save the current configurations, click **Clear All Groups** to clear the fields or **Reset Values** to cancel all changes.

To add a User Group:

1. Select **Settings→System Management Homepage→Security**.
2. Click **User Groups**.
3. In the **User** section, enter a user group name.
4. Click **Save Configuration** to save the current configurations, click **Clear All Groups** to clear the fields, or click **Reset Values** to cancel all changes.

Related Topics

- Security
- IP Binding

- IP Restricted Login
- Local Server Certificate
- Local/Anonymous Access
- Trust Mode
- Trusted Management Servers

6 The Tasks Page

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

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

System (HP-UX only)

This category provides four built-in tasks to enable easy execution of commands on a system without having to log in.

- The **Launch X Application** link displays options for you to launch an X application. Enter the command line of the X Application to launch. All HP SMH users can use this task as the commands will run with the user id of the user that is logged in.
- The **Launch X Application as Root** link displays options for you to launch an X application with root privilege. Enter the command line of the X Application to launch. Log in as a user with HP SMH Administrator authorization to use this task.
- The **Run Command** link displays options for you to run a command. All HP SMH users can use this task as the commands will run with the user id of the user that is logged in.
- The **Run Command as Root** link displays options for you to run a command with root privilege. Log in as a user with HP SMH Administrator authorization to use this task.

Related Topics

- The Home Page
- The Settings Page
- The Tools Page
- The Logs Page

7 The Tools Page

The **Tools** page displays links to system management tools provided by participating *HP Web-enabled System Management Software*. For HP-UX, the **Tools** page provides an entry point into management tools that are analogous to the *System Administration Manager* (SAM) main page, also known as the SAM Functional Area Launcher (or FAL). For HP-UX this also includes categories and menus for several X-based management applications. Some links that you may see on the **Tools** page follow:

- Accounts for Users and Groups
- Audit Configuration
- Authenticated Commands (PAM)
- Disks and File Systems
- Distributed Systems Administration Utilities (DSAU)
- Evweb
- IPMI Event Viewer
- Kernel Configuration
- Networking and Communications
- nPartition Management
- Peripheral Devices
- Printer Management
- Resource Management
- Resource Monitors
- Serviceguard
- Software Management
- Time

NOTE: Each of these functional areas has its own associated online help.

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

Related Topics

- The Home Page
- The Settings Page
- The Tasks Page
- The Logs Page

8 The Logs Page

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

- System Management Homepage Log
- System Management Homepage Legacy Log (Linux and Windows only)
- SAM Log Viewer (HP-UX only)

Any logs contained in the installed *HP Web-enabled System Management Software* can be displayed on this page. For example, if the *HP Version Control Agent* is installed, a link to the Version Control Agent log is displayed on the **Logs** page. As another example, if the Distributed Systems Administration (DSA) utility is installed, a link to the System Log Viewer is displayed on the **Logs** page.

Related Procedures

- System Management Homepage Log
- System Management Homepage Legacy Log
- SAM Log

Related Topics

- The Home Page
- The Settings Page
- The Tasks Page
- The Tools Page

System Management Homepage Log

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

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

To access the System Management Homepage Log, select **Logs→System Management Homepage→System Management Homepage Log**.

Related Topics

- The Logs Page
- System Management Homepage Legacy Log
- SAM Log

System Management Homepage Legacy Log

If your Linux or Windows system has HP Web-enabled System Management Software installed prior to the installation of the HP System Management Homepage (HP SMH), then its logs are visible by way of the **System Management Homepage Legacy Log** link in the **System Management Homepage** category. This log contains historical information regarding the security-related events that occurred prior to the installation of the new version. HP-UX does not include a Legacy Log.

To access the System Management Homepage Legacy Log, select **Logs→System Management Homepage→System Management Homepage Legacy Log**.

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

Related Topics

- The Logs Page
- System Management Homepage Log
- SAM Log

SAM Log

The **SAM Log** link provides access to the **SAM Log Viewer**. The SAM Log Viewer provides a Web interface into the *HP-UX System Administration Manager* (SAM) logfile. This logfile is used by existing SAM applications as well as the new Web-based management applications.

To access the SAM Log, select **Logs→SAM Log→SAM Log Viewer**.

To filter messages from the SAM Log, select the criteria to filter by then click OK. The messages are displayed at the bottom of the screen.

Related Topics

- The Logs Page
- System Management Homepage Log
- System Management Homepage Legacy Log

9 Troubleshooting

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

Access Problems

*Solution:*In order to avoid the multiple certificate warnings, you can import both the HP SIM and HP SMH certificates into the web browser. For Internet Explorer, this can be done by selecting the **View Certificate** button in the certificate warning boxes, and then selecting the **Install certificate** button. For Mozilla and Firefox, you can select **Accept this certificate permanently** in the certificate warning boxes.

*Solution:*The HP System Management Homepage (HP SMH) does not use `/etc/securetty`. Refer to the *login*(1)for details on `/etc/securetty`.

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

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

After updating my Windows XP system with Service Pack 2 or installing Windows Server 2003 SBS, I am unable to access the HP Version Control Repository Manager. What happened?

Solution: 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, you must configure the firewall with exceptions to allow browsers to access the ports used by HP Systems Insight Manager and Version Control Repository Manager.

To configure the firewall:

1. Select **Start→Settings Control Panel**.
2. Double-click **Windows Firewall** to configure the firewall settings.
3. Select **Exceptions**.
4. Click **Add Port**.

   You must enter the product name and the port number.

   Add the following exceptions to the firewall protection:

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

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

For Windows XP with Service Pack 2, this configuration leaves the default SP2 security enhancements intact, but allows traffic over the ports. These ports are required for the HP Version Control Repository Manager to run. The secure and insecure ports must be added to enable proper communication with your browser.

The breadcrumb links presented in the HP SMH top frame only display the current location within the HP SMH menu structure up to the plugin name, but not including the names of internal plugin pages.

Solution: Use the buttons and links provided inside the plug-in pages to cancel an operation or move to a different plug-in page.

Browser Problems

When I log into HP SMH and then close the browser, the HP SMH process is not killed. If I go back and open Internet Explorer, after closing it, I can log into HP SMH without credentials. How can I fix this problem?

Solution: There are two possible solutions in order to be sure the HP SMH shortcut will ask for credentials.

Solution #1

1. Select **Tools Internet Options**
2. Choose the **Advanced** tab.
3. Under **Settings Browsing**, uncheck **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. Click **OK** in the **Tabbed Browsing Settings** pop-up window.
5. Click **OK** to close **Internet Options**.

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

Solution: There are two possible warnings that might be seen including:

- `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 cert 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.

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

Solution: Mozilla browsers share sessions when launched separately.

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

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

Solution: Internet Explorer 6.0 on Windows 2003 Server has different security settings in the default install. To prevent the problem, add each managed system into 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.

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

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

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

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

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

Solution: 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. See the *smhstartconfig*(1M) command for more information.

When I browse to `https://ipaddress:2381` on a local machine running Windows 2003, I don't see the Login screen.

Solution: Internet Explorer 6.0 on Windows 2003 sometimes causes only the **Account Login** text in a blue bar to appear instead of the entire **Login** page. This issue only occurs when browsing on a local system. Rather than specifying the IP address in the URL, the problem can be resolved by using *hostname*.

HP recommends using the following URL to resolve this issue:

`https://hostname:2381`

When using HP SMH (until version 2.1.5), the Back button in the browser window may not behave as expected. After pressing the Back button, the current page will be refreshed instead of the previous page being displayed.

Solution: The use of the browser's **Back** button is not the supported method of navigating within HP SMH. You can navigate within HP SMH using the breadcrumb links and the navigation buttons and links presented inside the HP SMH pages.

Clustering Problems

I cannot browse to the HP SMH on my cluster IP address after a cluster fail over has occurred.

Solution: Install HP SMH 2.1.4 or later (which is available in SmartStart 7.5 or later) and modify the XML file to accommodate the cluster.

HP recommends the following actions:

1. As a precautionary measure, copy the existing smhpd.xml file into a different directory.
2. Manually add the tag:
   a. Open the smhpd.xml in the \hp\hpsmh\conf directory on the boot drive with a text editor.
   b. Add the following line between the <system-management-homepage> and </system-management-homepage> tags:

      ```
      <monitor-ip-changes>1</monitor-ip-changes>
      ```

   c. Save the file.
3. Repeat these steps on any system that could be a target of a cluster failover.
4. Restart the HP SMH service on both systems.

Installation Problems

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

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

When installing HP SMH, I am getting an error that reads `another instance is running.`

Solution: The HP SMH installation attempted to install on a system that had files that were previously 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.

When installing HP SMH, I am getting an error that reads `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.`

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

IP Address Problems

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

Solution: 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.

When I use the IP Restricted Login feature on Windows 2000 Advanced Server, 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?

Solution: On Microsoft Windows NT 4.0 and Windows 2000 Advanced Server, enter 127.0.0.1 in addition to the actual IP addresses of the server if you intend to include or exclude the local machine. The address 127.0.0.1 is always included in the **Include** section, so it is only excluded if it is explicitly placed in the **Exclude** section.

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

Solution: 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 the local host access. If you **do** need to block localhost access, enter **`127.0.0.1`** into the **Exclude** field under **IP Restriction**.

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.

Solution: 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 this is absolutely 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.

Login Problems

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 but users in that group cannot login or do not have the correct privileges in HP SMH.

Solution: HP SMH only recognizes four of the user groups predefined by Windows which are **Administrators**, **Users**, **Guests** and **Power Users**. Any other groups predefined by Windows, such as **Backup Operators**, are not recognized.

When trying to login to HP SMH on a Windows system using an administrative account defined in the Power Users or Backup Operators group, the login fails.

Solution: On Windows systems within the pre-defined user groups, only **Administrators**, **Users**, **Guests** and **Power Users** are recognized. Any other groups predefined by Windows, such as **Backup Operators**, are not recognized. The work around is to create a new group and use that for providing access to HP SMH.

I cannot log in to HP SMH on my Windows operating system.

Solution:

1. Verify that a valid Windows operating system account has been set up and that the login is included in the **Administrators** group or one of the HP SMH operating system groups.
2. Log in to the operating system. Change the password if prompted.

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

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

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

Solution:

- 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**.

Why doesn't my password work after I upgrade my Web Managed Products?

Solution: HP SMH 2.0 and greater uses operating system accounts whereas previous versions use three 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. Note that this does not apply to HP-UX.

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

Solution: By default, new accounts created in Windows operating systems are set to **user must change the password at next logon**. This option must be deselected before the account can be used to log in to HP SMH.

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 log 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 the IP address, the detailed certificate information does not appear in the text box of the Automatic Import Certificate screen.

Solution: These issues can be resolved two different 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.

or

- 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.

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

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

Security Problems

After updating my Windows XP system with Service Pack 2, I am unable to access HP Systems Insight Manager or the HP Version Control Repository Manager. What happened?

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

   You must enter the product name and the port number.

Add the following exceptions to the firewall protection:

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

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

This configuration leaves the default SP2 security enhancements intact, but will allow traffic over the ports previously indicated. These ports are required for HP Systems Insight Manager 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 Systems Insight Manager. The secure and insecure ports must be added for each product to enable proper communication with the applications.

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

Solution: HP SMH generates Certificate Request in Base64-encoded PKCS #10 format. This certificate request should be supplied to the CA. Most Certificate Authorities 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.

Why is my PKCS #7 cert data not accepted?

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

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

Solution: 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.

Why do I get errors when I paste my customer-generated certificate PKCS #7 data into the HP Systems Insight Manager Certificate Data field in Settings→HP System Management Homepage→Security→Trusted Management Servers ?

Solution: The customer-generated certificate PKCS #7 data does not belong 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→HP System Management Homepage→Security→Local Server Certificate**. The **HP Systems Insight Manager Certificate Data** field is used to configure which HP Systems Insight Manager servers are trusted by HP SMH. For more information, refer to "Trusted Management Servers".

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

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

1. Create the PKCS #10 data packet by clicking **Settings→HP System Management Homepage→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.
   - Select **Request a certificate**.
   - Select **Advanced certificate request**.
   - Select **Submit a certificate request by using a base**.
   - Press the **Ctrl**+ **V** keys to paste the **PKCS #10** data into the field.
4. From your Windows 2003 certificate authority system:
   - Click **Start**→**All Programs**→**Administrative Tools**→**Certification Authority**.
   - Click **CA (Local)** ⇒ **W2003CA/certsrv** ⇒ where *W2003CA* is the name of your Windows 2003 certificate authority system.
   - Issue the pending request certificate.
5. Navigate to **`http://W2003CA/certsrv`** where *W2003CA* is the name of your Windows 2003 certificate authority system.
   - Select **View the status of a pending certificate request**.
   - Select **Base64-encoded** and **Download certificate** (not **certificate chain**).

     The file download is `certnew.cer`.
   - Rename `certnew.cer` to `cert.pem`.

What are the security options when using Bastille?

Solution: Bastille is a system hardening program which 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 to limit the vulnerability of common internet services such as Web servers and DNS.

One of the facilities 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 open select network ports 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 have been 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.

  Refer to *ipf*(5) for more information.
- DMZ.config

  A tight lockdown. Launching Partition Manager under this configuration requires the use of SSH.

  Bastille also impacts using Partition Manager to remotely manage a system where Bastille is enabled. After the normal transfer of certificates, Partition Manager will work as described

above if the HOST.config or MANDMZ.config configurations are used. However, the DMZ.config configuration blocks WBEM traffic and thus prevents Partition Manager from remotely managing the system.

For more information about Bastille, refer to *bastille*(1M) and the *Bastille User Guide*, installed at `/opt/sec_mgmt_bastille/docs/user_guide.txt`.

Other Problems

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

Solution: The HP SMH install requires a Java version that requires at least 256 colors to load. Note this applies to Windows only.

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

Solution: 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 currently have access to that parameter and assumes the management processor is on port 80.

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

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

NOTE: You cannot `su -` to mimic root access to reinstall on United Linux 1.0 or SUSE SLES 8.

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

Solution: If the page not found error is displayed, you can press the **Refresh** button in the browser to allow the page to be properly shown. Subsequently, you will need to reauthenticate.

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

Solution: Currently, it is not possible to obtain the actual size of the device and file system swap space through the 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 System Management Homepage (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.
- Access the *HP ProLiant Essentials software* page at http://www.hp.com/servers/manage. You will 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 all service packs that have been 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 any non-HP or non-Compaq equipment that is not shown on the Inspect or System Configuration printout

10 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 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.
Revision Edition 1 November 2004
MPN: 365395-003. The first edition contained Linux and Windows information and tasks.

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.

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.

certificates 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.

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 will still be available.
HTTPS	*See* Secure HTTP.
in-place	Locally. For example to install in-place means to install locally.
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.
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
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.
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 will display 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.

ProLiant 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 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.
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 inclusion filter followed by an exclusion 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 to log 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 login	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).
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.
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 login on the HP System Management Homepage.
user accounts	Accounts used to log 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 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 (i.e., description) and protocol (i.e., 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

U

W