## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>5</td>
</tr>
<tr>
<td>Minimum System Requirements</td>
<td>5</td>
</tr>
<tr>
<td>Verifying System Requirements</td>
<td>8</td>
</tr>
<tr>
<td>Installing the Software</td>
<td>8</td>
</tr>
<tr>
<td>Console Installation for Linux on IA-32</td>
<td>9</td>
</tr>
<tr>
<td>Linux Uninstall on IA-32</td>
<td>15</td>
</tr>
<tr>
<td>Silent Installation on IA-32</td>
<td>15</td>
</tr>
<tr>
<td>Installation for Linux IPF</td>
<td>16</td>
</tr>
<tr>
<td>Configuration of the System Management Homepage on Linux IPF</td>
<td>16</td>
</tr>
<tr>
<td>Linux Uninstall on IPF</td>
<td>20</td>
</tr>
<tr>
<td>Silent Configuration on Linux IPF</td>
<td>20</td>
</tr>
<tr>
<td>Initializing the Software for the First Time</td>
<td>20</td>
</tr>
<tr>
<td>Logging In</td>
<td>21</td>
</tr>
<tr>
<td>Logging Out</td>
<td>21</td>
</tr>
<tr>
<td>Automatically Importing Certificates</td>
<td>21</td>
</tr>
<tr>
<td>System Management Homepage Overview</td>
<td>22</td>
</tr>
<tr>
<td>Navigating the Software</td>
<td>22</td>
</tr>
<tr>
<td>Header Frame</td>
<td>23</td>
</tr>
<tr>
<td>Data Frame</td>
<td>23</td>
</tr>
<tr>
<td>Tabs</td>
<td>23</td>
</tr>
<tr>
<td>Home Tab</td>
<td>24</td>
</tr>
<tr>
<td>Settings Tab</td>
<td>25</td>
</tr>
<tr>
<td>Tools Tab</td>
<td>34</td>
</tr>
<tr>
<td>Tasks Tab</td>
<td>34</td>
</tr>
<tr>
<td>Log Tab</td>
<td>34</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>35</td>
</tr>
<tr>
<td>Browser Problems</td>
<td>35</td>
</tr>
<tr>
<td>Installation Problems</td>
<td>36</td>
</tr>
<tr>
<td>IP Address Problems</td>
<td>36</td>
</tr>
<tr>
<td>Login Problems</td>
<td>37</td>
</tr>
<tr>
<td>Security Problems</td>
<td>37</td>
</tr>
<tr>
<td>Other Problems</td>
<td>37</td>
</tr>
<tr>
<td>Glossary</td>
<td>38</td>
</tr>
</tbody>
</table>
Overview

The System Management Homepage is a Web server used by much of HP Web-enabled System Management Software. It is the one stop for a centralized simple view of all the management information and configuration data generated by HP Web-enabled System Management Software and utilities. The status of the management software and utilities installed on the system is aggregated on the System Management Homepage.

The System Management Homepage can be installed on Microsoft® Windows® and Linux® operating systems. On IA-32, the Setup Wizard performs the installation of the System Management Homepage and enables you to set the security options used by all of the HP Insight Management Agents on the system. On Linux IPF, the System Management Homepage can be installed with default settings through an RPM package, and configured by the smhconfig tool.

Minimum System Requirements

Table 1: Minimum Requirements

<table>
<thead>
<tr>
<th>Operating Systems</th>
<th>Browsers</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Red Hat Linux Advanced Server 2.1 QU2</td>
<td>- Mozilla 1.5, 1.6</td>
</tr>
<tr>
<td>- Red Hat Linux Advanced Server 3 U1</td>
<td>- Microsoft Internet Explorer 6.0</td>
</tr>
<tr>
<td>- UnitedLinux 1.0</td>
<td></td>
</tr>
<tr>
<td>- SuSE SLES 8</td>
<td></td>
</tr>
<tr>
<td>- SuSE SLES 9</td>
<td></td>
</tr>
</tbody>
</table>

For the Itanium platform:

- Red Hat Linux Advanced Server 2.1 Update 3
- Red Hat Enterprise Linux 3 Update 2
- SuSE SLES 8 SP3

NOTE: The System Management Homepage Installation on a device does not require a browser.

NOTE: The HP Web-enabled System Management software is hardware dependent. For the installation to complete successfully, your system must support at least 256 colors. Refer to the documentation provided with the HP Web-enabled System Management software for information regarding the hardware requirements.

The System Management Homepage requires the following RPMs for each of the Linux operating systems.
Table 2: Required RPMs for Each Linux Operating System on the IA-32 Platform

<table>
<thead>
<tr>
<th>Operating System</th>
<th>RPM</th>
</tr>
</thead>
</table>
| All supported distributions require these packages for base support | openssl v0.9.x  
gdbm v1.8.0  
pam v0.75  
glibc v2.2.4  
db3 v3.3  
expat v1.95  
zlib v1.1.4 |
| All of the packages listed should be included in a standard Red Hat Linux Advanced Server 2.1 installation. |
| Red Hat Linux Advanced Server 3 Extra RPM Packages (Backward compatibility) | openssl096-0.9.6b.i386.rpm (OpenSSL compatibility)  
compat-db-4.0.14-4 (Berkely DBv3)  
compat-libstdc++-7.3-2.96.119 |
| United Linux 1.0 Package Dependencies List | compat-2003.1.10-0 (Berkeley DB v3/GLIBC compatibility) |
| SuSE SLES 8 Package Dependencies List | compat-2002.8.15-29.rpm (Berkeley DB v3/GLIBC compatibility) |
| SuSE Linux Server 9 Dependencies List | compat-2003-5.12-80.i586.rpm (for db3 backward compatibility)  
compat-sles8-1-16.i586.rpm (for OpenSSL backward compatibility) or later |
<table>
<thead>
<tr>
<th>Operating System</th>
<th>RPM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat Linux Advanced Server 2.1</td>
<td>glibc v2.2.4</td>
</tr>
<tr>
<td></td>
<td>perl 5.6.1 or greater</td>
</tr>
<tr>
<td></td>
<td>openssl 0.9.6b-35.7 or greater</td>
</tr>
<tr>
<td></td>
<td>expat 1.95.1-7 or greater</td>
</tr>
<tr>
<td></td>
<td>jrockit-j2se 8.1.1.1-2 or greater</td>
</tr>
<tr>
<td></td>
<td>gdbm 1.8.0-11 or greater</td>
</tr>
<tr>
<td></td>
<td>zlib 1.1.4-8 or greater</td>
</tr>
<tr>
<td></td>
<td>pam 0.75-46.7.3 or greater</td>
</tr>
<tr>
<td></td>
<td>db3 3.3.11-5 or greater</td>
</tr>
<tr>
<td></td>
<td>iproute</td>
</tr>
<tr>
<td></td>
<td>ucd-snmp 4.2.4 or greater</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 3</td>
<td>glibc v2.3.2</td>
</tr>
<tr>
<td></td>
<td>perl 5.8.0-88.4 or greater</td>
</tr>
<tr>
<td></td>
<td>openssl 0.9.7a-22.1 or greater</td>
</tr>
<tr>
<td></td>
<td>expat 1.95.5-6 or greater</td>
</tr>
<tr>
<td></td>
<td>jrockit-j2se 8.1.1.1-2 or greater</td>
</tr>
<tr>
<td></td>
<td>gdbm 1.8.0-20 or greater</td>
</tr>
<tr>
<td></td>
<td>zlib 1.1.4-8.1 or greater</td>
</tr>
<tr>
<td></td>
<td>pam 0.75-51 or greater</td>
</tr>
<tr>
<td></td>
<td>db4 4.1.25-8iproute or greater</td>
</tr>
<tr>
<td></td>
<td>net-snmp 5.0.9 or greater</td>
</tr>
<tr>
<td></td>
<td>net-snmp-perl 5.0.9 or greater</td>
</tr>
</tbody>
</table>

*continued*
Table 3: Required RPMs for Each Linux Operating System on the Itanium Platform

<table>
<thead>
<tr>
<th>Operating System</th>
<th>RPM</th>
</tr>
</thead>
<tbody>
<tr>
<td>SuSE SLES 8</td>
<td>glibc v2.2.5</td>
</tr>
<tr>
<td></td>
<td>perl 5.8.0-124 or greater</td>
</tr>
<tr>
<td></td>
<td>openssl 0.9.6g-73 or greater</td>
</tr>
<tr>
<td></td>
<td>expat 1.95.4-41 or greater</td>
</tr>
<tr>
<td></td>
<td>jrockit-j2se 8.1.1.1-2 or greater</td>
</tr>
<tr>
<td></td>
<td>gdbm 1.8.0-557 or greater</td>
</tr>
<tr>
<td></td>
<td>zlib 1.1.4-53 or greater</td>
</tr>
<tr>
<td></td>
<td>pam 0.76-70 or greater</td>
</tr>
<tr>
<td></td>
<td>db 4.0.14-161 or greater</td>
</tr>
<tr>
<td></td>
<td>iproute2</td>
</tr>
<tr>
<td></td>
<td>ucdsnmp 4.2.5 or greater</td>
</tr>
</tbody>
</table>

Verifying System Requirements

Before installation begins, the installation utility verifies whether:

- The operating system meets the minimum requirements. If the System Management Homepage does not support the operating system, an error message appears, indicating that an invalid operating system is found.
- The user is logged in with administrator/root rights. If the user is not logged in with administrator/root rights, an error message appears, indicating that administrator/root rights were not detected.
- On the IA-32 platform, during a Linux installation, missing dependencies are displayed. If Linux dependencies are not met, the installation will complete, but the System Management Homepage will not be started. During the preinstallation, the RPM will detect any dependencies and display those not met by your system.

If a dependency is not met on an Itanium platform, the installation does not complete.

Installing the Software

The System Management Homepage can be installed on systems running Windows and Linux. On the IA-32 platform, the Setup Wizard installs the System Management Homepage and enables you to set the security options used by all of the Web-based Management Agents on the system. On a Linux system running on the Itanium platform, the System Management Homepage is installed by an RPM package without asking you to configure any settings. After the installation is complete, run the smhconfig utility to set the security options used by all of the HP Insight Management Agents on the system, otherwise default values are used for these settings.
If a previous version of the System Management Homepage is currently installed on the machine, the configuration settings are carried over from the /opt/hp/hpsmh/conf/smhpd.xml file on Linux systems and the wizard initiates.

**Console Installation for Linux on IA-32**

In a console installation for Linux, the Setup Wizard performs the console installation of the System Management Homepage and enables you to set the security options used by all of the Web-based Management Agents on the system. You must be logged in as the root user, and type the following command line:

```
rpm –ivh hpsmh-2.0.0-linux.i386.rpm
```

After the system requirements have been verified, the Setup Wizard initiates and the installation panel appears with a message explaining what product is being installed, the company name, and website.

1. Select 1 for next. The Operating System Group list appears.
2. Select 1 to add.
3. Select 0 to continue.
4. Select the access level:
   - Select 1 for Root.
   - Select 2 for Operator.
   - Select 3 for User.
5. Select 0 to continue.
6. Enter Group name for root, for example, root1. The Group Name appears under the Root Group List.
7. To add more group names, select 1 to add or 3 to finish. A maximum of five group names can be added for root, operator, and user.
8. Select 0 to continue.

   **NOTE:** To delete, press 2. To continue, press 0, and choose the operating system group list. To delete a group name, enter the number next to the group name you want to delete.

9. Select 1 for next. The User Access dialog box appears.

**User Access**

User Access enables you to configure from the following access types:

- Anonymous Access
- Local Access
- Local Administrator Access

- Select **Anonymous Access** to enable anonymous access to unsecured pages, including local Anonymous access.
a. For Anonymous Access, select 1.
b. Select 0 to continue.

- Select **Local Access** to set up the System Management Homepage to automatically configure local IP addresses as part of the selected group.

To set up Local Access:

a. Select 1.
b. Select 0 to continue.
c. Select 1 for Local Anonymous Access
d. Select 0 to continue.

or

To set up Local Administrator Access:

a. Select 2 for Local Administrator Access.
b. Select 0 to continue.

⚠️ **CAUTION:** Selecting Local Access with administrator as the login provides any user with access to the local console full access without prompting them for a user or password.

10. Select 1 for Next. Trust Mode dialog box appears.

**Trust Mode**

Select the level of security you want to provide from one of the following trust modes:

- Trust By Certificate
- Trust By Name
- Trust All

- **Trust By Certificate**
  b. Select 0 to continue.
  c. Select 1 for next.

**NOTE:** If you selected the Trust By Certificate without adding any certificates to the list, a message appears, indicating that if you do not specify any trusted certificates, HP Systems Insight Manager cannot access the HP Web-based agents on this device. Select 1 for OK, if you do not want to access the HP Web-based agents on this device, or select 2 for Cancel, and add the trusted certificates to the list.

**NOTE:** The Trust By Certificates option enables the System Management Homepage server and designated HP Insight Manager servers to establish trust relationships by means of certificates. This mode is the strongest method of security because it requires certificate data and verifies the digital signature before enabling access.
To add files to the Trusted Certificates List:
   a. Select 1 for Add File.
   b. Select 0 to continue.
   c. Specify the file you want to add, for example, /user/local/hp/nila.pem. Press Enter. The file appears in the Trusted Certificates List. You can add as many files as you want.

   NOTE: If an invalid file name is entered in the file name field, an error message appears indicating the file does not exist.

To import certificates to the Trusted Certificates List:
   a. Select 2 for Import.
   b. Select 0 to continue.
   c. Enter the name or IP address of the server whose certificate you would like to import.
   d. Press the Enter key.
   e. Press Enter to view the certificate information.
   a. Select 1 to accept the certificate information. The file appears in the Trusted Certificates List. Select 2 to reject the information.
   b. Select 0 to continue. The certificate appears under the Trusted Certificates List.

To delete certificates from the Trusted Certificates List:
   a. Select 3 to delete.
   b. Select 0 to continue.
   c. Enter the number next to the certificate file you want to delete.
   d. Press the Enter key. This removes the certificate from the Trusted Certificates List.
   e. Select 4 to finish.
   f. Select 0 to continue.

   NOTE: To change a previous selection, press 2; to cancel, press 3; or to redisplay, press 4.
   a. Select 1 to go to IP Binding.

• Trust by Name
   a. Select 2 for Trust By Name.
   b. Select 0 to continue.
NOTE: Although Trust By Name mode is a slightly stronger method of security than the Trust All mode, it still leaves your system vulnerable to security attacks. The Trust By Name mode sets the System Management Homepage to only accept certain requests from servers with the HP Systems Insight Manager names designated in the Trust By Name field. The Trust By Name option is easy to configure and can prevent non-malicious access. For example, you may want to use the Trust By Name option if you have a secure network, but your network has two groups of administrators in two separate divisions. The Trust By Name option would prevent one group from installing software to the wrong system. This option does not verify anything other than the HP Systems Insight Manager server name submitted.

To add a server name to the Trusted Servers List:

a. Select 1 for Add.
b. Select 0 to continue.
c. Specify the server name you want to add.
d. Press the Enter key. The server displays in the Trusted Servers List. Add as many servers as you want.

NOTE: The server name cannot contain the following characters:
~ ` ! @ # $ % ^ & * ( ) + = " : ' < > ? , ;
e. Enter 0 when you selection has been made.

To delete a server name from the Trusted Servers List:

a. Select 2 to delete.
b. Select 0 to continue.
c. Enter the number next to the server name you want to delete.
d. Press the Enter key. The server name will be removed from the Trusted Servers List.
e. Select 3 to finish.
f. Select 0 to continue.
g. Select 1 to go to IP Binding.

NOTE: If you enter 0 without adding any server names to the list, an error message appears, indicating that if you do not specify any trusted server names, HP Systems Insight Manager cannot access the HP Web-based agents on this device. Select 1 to proceed without trusting any servers, or select 3 to Cancel and add server names to the list.

NOTE: To change a previous selection, press 2; to cancel, press 3; or to redisplay, press 4.

- Trust All
  a. Select 3 for Trust All.
  b. Select 0 to continue.
  c. Select 1 to go to IP binding. The IP Binding screen appears.
**NOTE:** The Trust All option leaves your system vulnerable to security attacks and sets the System Management Homepage to accept certain requests from any server. For example, you might want to use Trust All if you have a secure network, and everyone in the network is trusted.

IP Binding allows you to bind to specific IP addresses that match a specific Subnet IP Address or Netmask.

11. Select 1 to enable IP Binding, which enables the Subnet IP Address and Netmask.
12. Select 0 to continue.

To add a Subnet IP Address and Netmask to the IP Binding list:
   a. Select 1. A maximum of five Subnet IP Addresses and Netmask pairs can be added to the list.
   b. Select 0 to continue.
   c. Enter the Subnet IP Address in the designated field.
   d. Enter the Netmask in the designated field. The Subnet IP Address and Netmask are added to the IP Binding List.

To delete a Subnet IP Address and Netmask from the IP Binding List:
   a. Select 2 to delete.
   b. Select 0 to continue.
   c. Enter the number next to the Subnet IP Address/Netmask pair to delete.

13. Select 0 to continue.

14. Select 3 to finish.
15. Select 0 to continue.

16. Select 1 for IP Restricted Login. The IP Restricted Login window appears. IP Restricted Logins enables you to select whether a specific IP address or IP address ranges are included or excluded from gaining login access. Although optional, the System Management Homepage can restrict login access based on the IP addresses of the machine attempting to gain access. These restrictions apply to direct login attempts and not logins attempted as part of the single sign-on or secure task execution features of a trusted HP Systems Insight Manager server.

**NOTE:** A single address or ranges of addresses can be accepted into the IP Restriction Logins list. Enter the single address first.

17. Select 1 to enable the IP Restricted Logins. The IP Address to Include option enables you to specify the IP addresses or IP address ranges to grant login access permission. If any IP addresses are in the Inclusion list, then only those IP addresses will be enabled with login privileges. If no IP addresses are in the Inclusion list, then login privileges are granted to all IP addresses that are not in the Exclusion list.
18. Select 0 to continue.

19. Select 1. The IP Addresses to Include screen appears.

To add an IP address or IP address range to the IP Address Inclusion list:
   a. Select 1 to add an IP address or IP address range to the IP Address Inclusion list.
   b. Select 0 to continue.
   c. Enter an IP address or IP address range to which you want to grant login access. Press the **Enter** key. The IP address will display in the IP Address Inclusion List. Add as many as you want.

To delete an IP address or IP address range from the IP Address Inclusion list:
   a. Select 2 to delete.
   b. Select 0 to continue.
   c. Enter the number next to the IP address or IP address range to delete.
   d. Press the **Enter** key.
   e. Select 3 to finish.
   f. Select 0 to continue.
   g. Select 1. The IP Address to Exclude screen appears.

To add an IP address or IP address range to the IP Address Exclusion list:
   a. Select 1.
   b. Select 0 to continue.
   c. Enter an IP address or IP address range to which you want to deny login access. Press the **Enter** key. The IP address will display in the IP Address Exclusion List. Add as many as you want.

To delete an IP address or IP address range from the IP Address Exclusion list:
   a. Select 2 to delete.
   b. Select 0 to continue.
   c. Enter the number next to the IP address or IP address range to delete.
   d. Press the **Enter** key.
   e. Select 3 to finish.
   f. Select 0 to continue.
   g. Select 1 for next. The Install Preview Panel appears.

**NOTE:** If you do not specify any IP addresses in either the Include or Exclude list, a warning message appears indicating that IP Restricted Logins will be disabled and you can proceed or cancel the operation. Click **OK** to continue the installation. The Install Preview window appears. Text that is set off in this manner presents additional information to emphasize or supplement important points of the main text.
NOTE: If you do not specify any IP addresses to either the Include or Exclude lists, a warning message appears indicating that IP Restricted Logins will be disabled and allows you to proceed or cancel the operation. Click OK to continue the installation. The Install Preview window appears. Text that is set off in this manner presents additional information to emphasize or supplement important points of the main text.

20. Press Enter to read the install text. The Install Preview Panel lists the location where the System Management Homepage is installed, the amount of space the installation requires and a summary of the options that the user specified during the installation.

21. Press 1 for next and the installation begins. Press 3 to cancel or 4 to display install information.

Linux Uninstall on IA-32

To uninstall the System Management Homepage:

Run /opt/hp/hpsmh/_uninst/uninstaller.bin

or

Run rpm -e hpsmh

Silent Installation on IA-32

The silent installation enables you to install the System Management Homepage without having to manually enter information through the console or graphical user interface (GUI).

You can force a silent install using the following environment variable. Otherwise, the install goes into an interactive InstallShield mode.

To force a silent install:

1. In a script or from the command line, enter export HPSMHSLIENT=true | yes.
2. To start the silent install with the default configuration, enter the following command:

   rpm -ivh hpsmh-2.0.0-linux.i386.rpm

The RPM post script generates a random password and creates an default ELM Linux configuration (/var/spool/compaq/wbem/CPQHMMD.ACL) file if one does not exist. It uses hpwebsetup without the force option.

The RPM also looks for the HPLSPINSTALL environment variable, and take actions based on the hpsmh.cfg file stored in /usr/local/hp directory.
Installation for Linux IPF

In a console installation for Linux IPF, you first install an RPM package that sets default values for all security options. After installation is complete, you can change these security options by running the smhconfig utility. The following is an installation for Linux IPF. To install the System Management Homepage run the following command, logged in as root user.

```
# rpm -Uhv hpsmh-<version>.ia64.rpm
```

Configuration of the System Management Homepage on Linux IPF

After installing the RPM package, you can configure the System Management Homepage, by running the following command, logged in as root user:

```
/opt/hp/hpsmh/smhconfig/smhconfig.sh
```

The smhconfig tool displays the following:

1. Welcome screen appears with the company name and website.

2. Select 1 for Next, 3 to cancel or 4 to redisplay the dialog box.

3. Select 1. The OS Groups dialog box appears.

4. To add an Operating System Group Name to one of the OS Group Lists, select 1-Add. A maximum of five entries can be added for each group level.

5. Select the Operating Systems Group level from 1-Root, 2-Operator, and 3-User.

6. Enter the name of an Operating Systems Group that you want to assign to the Root Group List. Press Enter when you are finished.

**NOTE:** To delete, press 2 and choose the OS group list. To delete a group name, enter the number next to the group name you would like to delete.

7. Select 3-Continue when you are finished adding group names.

8. Select 1 for Next, 2 for Previous, 3 to cancel or 4 to redisplay screen.

9. Select 1. User Access screen appears. User Access enables you to configure the following access types:
   - Select **Anonymous Access** to enable anonymous access to unsecured pages, including local Anonymous access.
   - Select **Local Access** to set up the System Management Homepage to automatically configure local IP addresses as part of the selected group.

**CAUTION:** Selecting Local Access with Administrator as the login provides any users, with access to the local console, full access without prompting them for a user or password.
— Select Anonymous Access to enable the Anonymous Access.
— Select Local Access to enable Local Access.
— Press Enter to continue.
— Select 1 for Next, 2 for Previous, 3 to cancel or 4 to redisplay screen.

10. Select 1. Trust Mode screen appears.

11. Select the level of security you want to provide from one of the following trust modes:
   - Trust by Certificate - Select 1 for Next, 2 for Previous, 3 to cancel or 4 to redisplay the screen.
     a. Select 1. The Trusted Certificate dialog box appears. The Trusted Certificate dialog box enables trusted certificate files to be added to the Trusted Certificate list.

   **NOTE:** If you selected Trust by Certificate without adding any certificates to the list, a message appears indicating that if you do not specify any trusted certificate files, HP Systems Insight Manager will not be able to access the HP Web-based agents on this device. You can select 1 for OK, if you do not want to be able access the HP Web-based agents on this system, or you can select 2 for Cancel and add the trusted certificates to the list.

   **NOTE:** The Trust By Certificates option enables the System Management Homepage server and designated management servers to establish trust relationships by means of certificates. This mode is the strongest method of security, because it requires certificate data and verifies the digital signature before enabling access

   b. Select **Add File** to select any certificates to be included in the Trusted Certificates List. Add File is displayed. If an invalid file name is typed in the file name field, an error message displays stating the file does not exist. Please try again.

   c. Select **4-Continue**.

      Select 1 for Next, 2 for Previous, 3 to cancel or 4 to redisplay screen.

   d. Select 1. IP Binding is displayed.

   or

   b. Select **2-Import** and the Import Server Certificate appears.

   c. Enter the name of the server whose certificate you would like to import and press Enter.

   d. Select **Accept** to add the certificate to the Trusted Certificates list, or select **Reject** to cancel the selection.

      Select 1 for Next, 2 for Previous, 3 to cancel or 4 to redisplay screen.

   e. Select 1. IP Binding screen appears.

   **NOTE:** Delete enables you to remove any of the trusted certificate files that appear. To delete a certificate file, select **3-Delete** and select the certificate file.
• Trust by Name
  a. Select Trust By Name. Select 1 for Next, 2 for Previous, 3 to cancel or 4 to redisplay screen.
  b. Select 1. Trusted Server screen appears.

  **NOTE:** Although Trust By Name mode is a slightly stronger method of security than the Trust All mode, it still leaves your system vulnerable to security attacks. The Trust By Name mode will set up the System Management Homepage to only accept certain requests from servers with the HP Systems Insight Manager names designated in the Trust By Name field. The Trust By Name option is easy to configure, and will prevent non-malicious access. For example, you may want to use the Trust By Name option if you have a secure network, but your network has two groups of administrators in two separate divisions. The Trust By Name option would prevent one group from installing software to the wrong system. This option will not verify anything other than the HP Systems Insight Manager server name submitted.
  c. Select 1-Add to add a server name to the Trusted Servers List and enter the name of the server you want to trust.

  **NOTE:** The Server Name must conform to the standard described by RFC 952: it must be a list of names separated by period (.), where each name is composed by letters (upper and lower case), digits or minus sign (-). These names must start with a letter and must finish with a letter or a digit. For more information about RFC 952, refer to http://www.rfc-editor.org/rfc/rfc952.txt.
  d. Select 3-Continue. Select 1 for Next, 2 for Previous, 3 to cancel or 4 to redisplay screen.
  e. Select 1. IP Binding screen appears.

  **NOTE:** If you select Next without adding any server names to the list, an error message appears indicating that if you do not specify any trusted server names, HP Systems Insight Manager will not be able to access the HP Web-based agents on this device. You can select 1 to proceed without trusting any servers, or you can select 2 to Cancel and add server names to the list.

  **NOTE:** Delete enables you to remove any of the trusted certificate files that appear in the Trusted Servers list. To delete a server name, select 2 and select the server name.

• Trust All
  a. Select Trust All. Select 1 for Next, 2 for Previous, 3 to cancel or 4 to redisplay screen.
  b. Select 1. IP Binding screen appears.

  **NOTE:** The Trust All option leaves your system vulnerable to security attacks and sets up the System Management Homepage to accept certain requests from any server. An example of why you may want to use Trust All would be if you have a secure network, and everyone in the network is trusted.

  IP Binding allows you to bind to specific IP Addresses that match a specific Subnet IP Address or Netmask.

  12. Select the IP Binding. This enables the Subnet IP Address and NetMask.

  13. Select 1-Add to add a Subnet and NetMask to the IP Binding List. No more than 5 Subnet IP Addresses and NetMask pairs can be added to the list.
14. Enter the Subnet IP Address and press Enter.

15. Enter the NetMask and press Enter.

16. Select **3-Continue** when you are finished. Select **1** for Next, **2** for Previous, **3** to cancel or **4** to redisplay screen.

17. Select **1**, IP Restricted Logins screen appears.

   IP Restricted Logins enables you to select whether to include and/or exclude a specific IP Address or IP Address Ranges from gaining login access. Although optional, the System Management Homepage can restrict login access based on the IP addresses of the machine attempting to gain access. These restrictions apply to direct login attempts and not logins attempted as part of a trusted HP Systems Insight Manager server’s single login or secure task execution features.

   **NOTE:** A single address as well as ranges can be accepted into the IP Restriction Logins. Enter the single address first.

18. Select the **IP Restricted Logins** to include and/or exclude specific IP Addresses or IP Address ranges. The IP Address to Include enables you to specify the IP Addresses or IP Address Ranges to grant login access permission. If there are any IP addresses in the Inclusion list, then only those IP addresses will be enabled login privileges. If there are no IP addresses in the Inclusion list, then login privileges is permitted to all IP address that is not in the Exclusion list. Select **1** for Next, **2** for Previous, **3** to cancel or **4** to redisplay screen.

19. Select **1**, IP Address Include screen appears.

20. Select **1-Add** to add an IP Address or IP Address range to the IP Address Inclusion List.

21. Enter na IP address or IP address range that you want to grant login access to. All IP address that fall between the beginning and ending IP addresses are granted login access.

22. Select **3-Continue**, The IP address or IP address range are added to the Inclusion list.

   **NOTE:** If you entered an invalid IP address or IP address range, an error message appears indicating the IP address is invalid. Enter a valid IP address or IP address range and select **3-Continue**. To delete or remove an IP address or IP address range, select **2-Delete** to remove it from the Inclusion list.

   Select **1** for Next, **2** for Previous, **3** to cancel or **4** to redisplay screen.

23. Select **1**, IP Address Exclude screen appears.

24. Select **1-Add** to add an IP Address or IP Address Range to the IP Address Exclusion List.

25. Enter a beginning IP address to be denied login access.

26. Enter an ending IP address that you want to deny login access to. All IP address that fall between the beginning and ending IP addresses are denied login access.
27. Select **3-Finished** or **0** when your selection is made. The IP address or IP address range are added to the Inclusion list. You can select an IP address or IP address range.

**NOTE:** If you entered an invalid IP address or IP address range, an error message appears indicating the IP address is invalid. Enter a valid IP address or IP address range and select **3-Continue**. To delete or remove an IP address or IP address range, select **2-Delete** to remove it from the Inclusion list.

**NOTE:** If you do not specify any IP addresses to either the Include or Exclude lists a warning message is displayed, stating that the IP Restricted Logins checkbox will be marked as disabled and asking if you want to proceed without adding any IP Address restrictions. If you select **OK**, the IP Restricted Logins checkbox on the IP Restricted Logins is unselected and the Install Preview appears.

28. Select **Continue**. The Configuration Preview screen appears.

29. Click **Enter** to begin configuration of the System Management Homepage.

30. The Configuration Summary screen displays a message stating configuration was successful.

**Linux Uninstall on IPF**

To Uninstall the System Management Homepage:

Run `rpm -e hpsmh`

**Silent Configuration on Linux IPF**

The silent configuration enables you to configure the System Management Homepage without manually entering information on the Console. On Linux IPF you can run the `smhconfig` utility in a non-interactive way.

There are two silent switches available for the `smhconfig` utility:

- The `-silent` switch is used to define all security settings with default values. The RPM installation already runs the `smhconfig` utility with this switch.

- The `-options <settings.xml>` is used to obtain pre-defined settings stored in the `settings.xml` file. This file is in the same format as the `smhpd.xml` file already used by the System Management Homepage.

**Initializing the Software for the First Time**

After the System Management Homepage has been installed and configured for the first time, a process to create a private key and corresponding self-signed base64 encoded certificate is initiated. This certificate is a base64-encoded PEM file. In Linux, both public and private keys for the System Management Homepage are stored in the `/opt/hp/sslshare` directory. The files are called file.pem and cert.pem.
If you feel that the private key has been compromised, the administrator can delete the \hp\sslshare\cert.pem file and restart the server. This action causes the System Management Homepage to generate a new certificate and private key.

**NOTE:** Certificate and private key generation only occurs the first time the System Management Homepage is started or when no certificate and key pair exists.

**NOTE:** A certificate from a Certificate Authority (CA) such as Verisign or Entrust can be used to replace self-generated certificates. These certificate and key files are shared with other HP Management software such as HP Systems Insight Manager.

### Logging In

To log in to the System Management Homepage with Mozilla:


2. The first time you browse to this link, 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 browse in.

3. Click OK. The Login page appears unless you have enabled Anonymous access, then the System Management Homepage appears.

4. Enter your user name that is recognized by the operating system. If you have not yet added user groups into System Management Homepage security settings, then users must log in with an operating system account in the root group. If the credentials cannot be authenticated, the user is denied access.

**NOTE:** In most cases, the root has administrator access on the System Management Homepage.

5. Enter the correct password in the Password field. The password must be the operating system–based password for the user.

6. Click Login. The System Management Homepage appears.

### Logging Out

Click Logout in the System Management Homepage banner or close every instance of the Web browser that is logged in.

### Automatically Importing Certificates

The Automatically Import Management Server Certificate feature enables you to automatically import the HP Systems Insight Manager system certificate when accessing the System Management Homepage from an HP Systems Insight system.
NOTE: Your login must have administrative access to the System Management Homepage to automatically import the HP Systems Insight Manager certificate.

To automatically import the HP Systems Insight Manager 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 the System Management Homepage and a certificate for the HP Systems Insight Manager system you are accessing has not been imported into the Trusted Certificates List, the Login page displays the Automatically Import Management Server Certificate option. The Certificate Information retrieved from SERVER NAME displays the HP Systems Insight Manager certificate details.

   For more information regarding logging in, refer to the “Logging In” section.

2. Automatically Import Management Server Certificate is selected by default. Deselect this option if you do not want to add the HP Systems Insight Manager certificate to the Trusted Certificates List. However, future access to this system requires login credentials.

3. If you allow the System Management Homepage to automatically import the HP Systems Insight Manager certificate, future access to the system is seamless. You will not be challenged for your login credentials through HP Systems Insight Manager.

4. Leave Automatically Import Management Server Certificate selected, enter your System Management Homepage administrator 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 login credentials. However, administrator credentials are not required to log in.

**System Management Homepage Overview**

The System Management Homepage displays all HP Web-enabled System Management Software that provides information. In addition, the System Management Homepage displays various boxes that have borders defining the status of the items contained in that box. Refer to the “Status Box Indicators” section for more information.

**Navigating the Software**

The System Management Homepage is separated into two frames:

- Header frame
- Data frame
Header Frame

The header frame is constantly visible regardless of which tab you are viewing. A link, located in the top section, displays the path you are currently viewing.

The header displays the following information:

- **Support**—Takes you to the ProLiant Server Management page. The HP Support page provides a variety of product, service, and support-related resources. You can access support at [http://www.hp.com/servers/manage](http://www.hp.com/servers/manage).
- **Forums**—Contact the HP Support Forum to get answers to your questions about HP products. The HP Support Forum can be found at [http://forums.itrc.hp.com](http://forums.itrc.hp.com).
- **Help**—Launches the help files in a separate browser window. The help contains a combination of the help files related to the HP Web-enabled System Management Software and utilities.
- **System Model**—Displays the model of the system. On IA-32, the System Model displays **Unknown** if the HP Insight Management Agents for Servers are not installed on the system. On the Itanium platform, the System Model appears even when the HP Insight Management Agents for Servers are not installed.
- **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 link is displayed. If anonymous access is enabled and you are accessing the page anonymously, the Current User displays `hpsmh_anonymous`, and the Login 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.

Data Frame

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

Tabs

The System Management Homepage displays up to five tabbed pages that enable you to access and configure settings related to participating HP Web-enabled System Management Software. The Tools tab and the Tasks tab are only visible if HP Web-enabled System Management Software provides information for them.

The System Management Homepage tabs that can be displayed are:

- Home
- Settings
- Tools
- Tasks
Home Tab

The Home tab is displayed on the System Management Homepage. The following information appears on the Home tab:

- Overall System Status
- Software Status
- Organizational menu

Overall System Status

The Overall System Status box displays links to all systems, which have a failed or degraded status, provided by the HP Web-enabled System Management Software. If there are no agents installed or no failed or degraded items, then the Overall System Status box displays no failed/degraded items.

Software Status

The status of the HP Web-enabled System Management Software is configured to appear in the Status boxes. Each box contains links that enable you to drill down into the HP Web-enabled System Management Software that is providing the data.

Table 4. Status Box Indicators

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blue</td>
<td>Unknown</td>
</tr>
<tr>
<td>Green</td>
<td>OK</td>
</tr>
<tr>
<td>Yellow</td>
<td>Degraded</td>
</tr>
<tr>
<td>Orange</td>
<td>Failed</td>
</tr>
<tr>
<td>Gray</td>
<td>No status</td>
</tr>
</tbody>
</table>

Organizational Menu

The left organizational menu is displayed on the Home tab. 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.

NOTE: Participants are agents that are contributing information contained in the System Management Homepage.
• Other Agents—Lists the visible HP Web-enabled System Management Software that does not participate in the System Management Homepage. The name of the HP Web-enabled System Management Software provides a link so you can still access the agents if they provide a user interface.

• Management Processor—Displays a link to either the Remote Insight Lights-Out Edition (RILOE) board or the Integrated Lights-Out (iLO) board. This information is provided by HP Insight Management Agents. If no HP Web-enabled System Management Software is installed that provides this information, then None is displayed.

• Other Software—Provides information regarding value-added software as well as links to pages on http://www.hp.com that contain software information, including ProLiant Essentials Value Added Software. Refer to http://www.hp.com/servers/proliantessentials for detailed information regarding ProLiant Essentials Value Added Software.

• KEY—Displays a listing of status icons and a brief description of each.

Table 5: System Status of Icons Legend

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔️</td>
<td>OK</td>
</tr>
<tr>
<td>🚨</td>
<td>Degraded</td>
</tr>
<tr>
<td>⚠️</td>
<td>Failed</td>
</tr>
<tr>
<td>🎧</td>
<td>Unknown</td>
</tr>
</tbody>
</table>

Settings Tab

This section contains links to the settings or configuration pages of various HP Web-enabled System Management Software. After installing System Management Homepage, only the System Management Homepage section is present, enabling you to view or edit the System Management Homepage settings.

System Management Homepage section

This section provides links that enable you to configure your System Management Homepage settings. The System Management Homepage section provides links to the following:

• Credits—Displays information regarding licensing and credits.

• Security—Provides the following security options:
  — IP Binding—Click Settings • System Management Homepage • Security • IP Binding.
  — IP Restricted Login—Click Settings • System Management Homepage • Security • IP Restricted Login.
  — Local Server Certificate—Click Settings • System Management Homepage • Security • Local Server Certificate.
  — Local/Anonymous Access—Click Settings • System Management Homepage • Security • Local/Anonymous Access.
— Trust Mode—Click **Settings** • **System Management Homepage** • **Security** • **Trust Mode**.

— Trusted Management Servers—Click **Settings** • **System Management Homepage** • **Security** • **Trusted Management Servers**.

— User Groups—Click **Settings** • **System Management Homepage** • **Security** • **User Groups**.

**IP Binding**

IP Binding specifies the IP addresses that are permitted to send requests to the System Management Homepage.

Administrators can configure the System Management Homepage to only bind to addresses specified in the IP Binding page. A maximum of five Subnet IP Addresses and Netmasks can be defined.

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

**NOTE:** The System Management Homepage always binds to 127.0.0.1. If IP Binding is enabled and no subnet/mask pairs are configured, then the System Management Homepage 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**. The IP Binding page appears.
3. Select **IP Binding** to enable IP binding.
4. Enter the 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:

   **On IA-32 platforms:**
   
   Setting this value requires restarting the System Management Homepage that may require you to log in again.

   **On Itanium platforms:**
   
   New SMH settings will not take effect until you restart the SMH service.

7. Click **OK**.
Each IP address and Netmask must consist of four octets with values between 0 and 255.

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

**IP Restricted Login**

The IP Restricted Login enables the System Management Homepage to restrict login access based on the IP address of the system from which the login is attempted.

Address restriction can be set at installation time or by administrators 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 IP addresses are in the inclusion list, then only those IP addresses are allowed login access with the exception of the local host. If no IP addresses are in the inclusion list, then login 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**. The IP Restricted Login page appears.
3. Select **IP Restricted Login** to enable IP restricted login.
4. Enter the IP addresses to exclude, for example, 1.1.1.1;2.2.2.2-3.4.5.6.
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:

**On IA-32 platforms:**

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

**On Itanium platforms:**

New SMH settings will not take effect until you restart the SMH service.

7. Click **OK**.
Local Server Certificate

The Local Server Certificate page enables you to use certificates that are not generated by HP. If this process is followed, the self-signed certificate that was originally generated by the System Management Homepage is replaced with one that was issued by a CA. The first step of the process is to cause the System Management Homepage to create a Certificate Request (PKCS #10). This request utilizes 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, send it to a CA. After the CA has returned PKCS #7 data, import this data into the System Management Homepage. After the PKCS #7 data has been successfully imported, the original \hp\sslshare\cert.pem certificate file is overwritten with the system certificate from that PKCS #7 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 PKCS #10:

1. Click **Settings** > **System Management Homepage** > **Security**.
2. Select **Local Server Certificate**.
3. Optionally, you can replace the default values in the Organization and/or Organizational Unit fields with your own (maximum 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/hp/sslshare/req_cr.pem`.
5. Copy the certificate data.
6. Send PKCS #10 certificate request data to a CA 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 PKI/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. In this case, step 7 can be skipped.

8. Click **Import PKCS #7 Data**. A message appears, indicating whether the customer-generated certificate was successfully imported.

9. Stop the System Management Homepage.

10. Restart the System Management Homepage.

11. Browse to the managed system that contains the imported certificate.
12. 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. Alternatively, you can import the root CA certificate into all the browsers on your network to avoid being prompted.

**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 the file name /hp/sslshare/cert.pem and restart the System Management Homepage.

Local/Anonymous Access

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

- **Anonymous Access**—Anonymous access is disabled by default. Enabling Anonymous Access enables a user to access the System Management Homepage without logging in.

  ![CAUTION: HP does not recommend the use anonymous access.]

- **Local Access**—Local access enables you to gain access locally to the System Management Homepage without being challenged for authentication. This means that any user with access to the local console is granted full access if Administrator is selected. If Anonymous is selected, any local user has access limited to unsecured pages without being challenged for a user name and password.

  ![CAUTION: HP does not recommend the use of local access unless your management server software enables it.]

To enable anonymous access:

1. Click **Settings**>**System Management Homepage**>**Security**
2. Select **Local/Anonymous Access**.
3. Select **Anonymous Access** to enable anonymous access.
4. Click **Save Configuration** to save your settings.

**NOTE:** If this System Management Homepage is running on the same machine as HP Systems Insight Manager, local access (anonymous) must be enabled for certain features of HP Systems Insight Manager to work. If local access (administrator) or anonymous access is enabled, this also works but is not necessary.

To enable local access:

1. Click **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.

**Trust Mode**

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

- **Trust by Certificate**—The Trust by Certificate mode sets the System Management Homepage to accept configuration changes only from HP Systems Insight Manager 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 recommends using Trust by Certificate.

- **Trust by Name**—The Trust by Name mode sets the System Management Homepage to accept certain configuration changes only from servers with the HP Systems Insight Manager names designated in the Trust By Name field. The trust by name option is easy to configure, and prevents non-malicious access. For example, you could use the trust by name 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 Systems Insight Manager server name submitted.

- **Trust All**—The Trust All mode sets the System Management Homepage 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.

**Configuring Trust Mode**

The imported System Management Homepage certificates are stored in the `/opt/hp/hpsmh/certs` directory.

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

**Trust By Certificate**

To trust by certificate:

1. Click **Settings** > **System Management Homepage** > **Security**.

2. Click **Trust Mode**. The Trust Mode page appears.

3. Select **Trust by Certificate** to require trusted certificates.

4. Click **Trust Certificate** to access Trusted Management Server Certificate.
5. Click **Save Configuration** to save the current configurations, or click **Reset Values** to cancel all changes.

**Trust By Name**

The server name option must meet the following criteria:

- The overall length of the server name list is 1,024 characters.
- Each server name must be less than 64 characters.
- The following characters should not be included as part of the server name:
  
  ```
  ~ ' ! @ # $ % ^ & * ( ) + = " : ' < > ? , |
  ```

  On the Itanium platform the server name must conform to the standard described by RFC 952: it must be a list of names separated by period (.), where each name is composed by letters (upper and lower case), digits or minus sign (-). These names must start with a letter and must finish with a letter or a digit. For more information about RFC 952, refer to http://www.rfc-editor.org/rfc/rfc952.txt.

- Semicolons are used to separate server names.

To trust by name:

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

**Trust All**

To trust all servers:

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

**Trusted Management Servers**

The Trusted Management Server Certificates page 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 and the System Management Homepage.

To import certificates data:

1. Click **Settings**>**System Management Homepage**>**Security**>**Trusted Management Server**.

2. Enter the name or IP address of the HP Systems Insight Manager server that contains the certificate to be added.

3. Cut and paste the base64-encoded certificate into the text box.

4. Click **Import Certificate Data**.

**Add Certificate From Server**

To add a certificate from a server:

1. Click **Settings**>**System Management Homepage**>**Security**>**Trusted Management Server**.

2. Enter the name or IP address of the HP Systems Insight Manager 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, and if you want to add it to the Trusted Certificate list, click **Add Certificate to Trust List**.

**User Groups**

System Management Homepage 2.0 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 `root` can define operating system groups that correspond to System Management Homepage 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 System Management Homepage access level can be assigned up to five different operating system groups. The System Management Homepage installation enables you to assign the operating system groups to the System Management Homepage. If a specified operating system group is not defined when the System Management Homepage is started, the System Management Homepage log message indicates which operating system groups are not defined.
The accounts used for System Management Homepage do not need to have any elevated access on the host operating system. Any administrative System Management Homepage user can specify operating system user groups to each access level of System Management Homepage, and then all accounts in each operating system user group have the access to System Management Homepage that is specified on the User Groups page. The Linux root group automatically has administrative access to the system.

For example, the System Management Homepage 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 the System Management Homepage whether or not the accounts have any elevated access on the host operating system.

To add an Administrator Group:

The User Groups page enables you to add user groups to System Management Homepage.

The following levels of user group authorizations are available:

- **Administrator**—Users with Administrator access can view and set all information provided through the System Management Homepage. The default user group root has administrative access.

- **Operator**—Users with Operator access can view most information provided through the System Management Homepage. Some Web applications limit access to the most critical information to administrators only.

- **User**—Users with User access can view most information provided through the System Management Homepage. Some Web applications restrict viewing of critical information from individuals with User access.

To add an Administrator Group:

1. Click **Settings»System Management Homepage»Security**.
2. Click **User Groups**. The User Group page appears.
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 click **Reset Values** to cancel all changes.

To add an Operator Group:

1. Click **Settings»System Management Homepage»Security**.
2. Click **User Groups**. The User Group page appears.
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 click **Reset Values** to cancel all changes.
To add a User Group:

1. Click **Settings** ➤ **System Management Homepage** ➤ **Security**.
2. Click **User Groups**. The User Group page appears.
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.

**Tools Tab**

The Tools tab displays links to tool-oriented pages provided by participating HP Web-enabled System Management Software.

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

**Tasks Tab**

The Tasks tab displays links to task-oriented pages 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 tab is not visible.

**Log Tab**

The Logs tab includes various log information. Any logs contained in the installed HP Web-enabled System Management Software can be displayed on this tab. For example, if the HP Version Control Agent is installed, a link to the Version Control Agent log is displayed on the Logs page. You can access the entry point to the log shown by clicking the link.

**System Management Homepage Log**

The System Management Homepage Log contains primarily security-related events and is helpful when troubleshooting security problems in participating HP Web-enabled System Management Software.

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

To access the System Management Homepage Log, click **Logs** ➤ **System Management Homepage** ➤ **System Management Homepage Log**.
System Management Homepage Legacy Log

If your system had HP Web-enabled System Management Software installed before the installation of the System Management Homepage 2.0.0, then its logs are visible through the System Management Homepage Legacy Log link. This log contains historical information regarding the security-related events that occurred before the installation of the new version.

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

To access the System Management Homepage Legacy Log, click **Logs>System Management Homepage>System Management Homepage Legacy Log.**

**Troubleshooting**

**Browser Problems**

**Opening a second Mozilla browser can appear as an unauthorized login into System Management Homepage.**

**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.

**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.

**How can I tell if my browser is supported?**

**Solution**—The supported browsers are:

On IA-32 platforms:
- Internet Explorer 6.0
- Mozilla 1.5
- Mozilla 1.6

On Itanium platforms:
- Internet Explorer 6.0 or greater
Installation Problems

When installing System Management Homepage, I am getting an error that reads, 
*Another instance is running.*

**Solution**—The System Management Homepage installation attempted to install on a system 
that had files that were previously corrupted or if the installation was aborted.

To resolve this issue, navigate to the `temp` directory on the System Management Homepage 
system and delete the `smhlock.tmp` file.

When installing System Management Homepage on a Linux system, 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. You can only run one installation of the System Management Homepage 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 may access the local system at https://localhost:2381 or 
https://127.0.0.1:2381.

**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.

Why isn’t local host access denied when I set up an IP restriction?

**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 local host 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 System 
Management Homepage 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

Why doesn’t my password work after I upgraded my Web Managed Products?

**Solution**—System Management Homepage 2.0 and greater uses operating system accounts whereas previous versions used three static accounts (administrator, operator, and user). Any operating system account belonging to the root group has administrative access to the System Management Homepage. With this access, you can assign accounts in other operating system account groups to different levels of access for System Management Homepage. The System Management Homepage online help describes this process in detail.

Security Problems

Why can I not import X.509 certificates directly into System Management Homepage?

**Solution**—System Management Homepage 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 System Management Homepage by selecting **Settings**•**System Management Homepage**.

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

Why is my PKCS #7 data 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 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**•**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**•**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 the System Management Homepage.

a.

Other Problems

Why can I not install the System Management Homepage on my system?

**Solution**—The System Management Homepage install requires a Java™ version that requires at least 256 colors to load.
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. The System Management Homepage does not currently have access to that parameter and assumes the management processor is on port 80.

Why can I not install on Linux when I am not root?

Solution—You must be logged in as root for System Management Homepage to have the proper access rights.

NOTE: You cannot su- to mimic root access for reinstall on United Linux 1.0/ SuSE SLES 8.

Why can I not install System Management Homepage on my version of Linux?

Solution—The versions of Linux that the System Management Homepage supports each require their own specific set of RPM packages. To see which RPM packages are missing on your system, install the System Management Homepage RPM in verbose (non-silent) mode, and any missing RPM packages will be listed.

Glossary

cautions
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 Certification 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 they claim to be.

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

external sites
Third-party application URLs.
**graphical user interface (GUI)**

A program interface that uses the graphics capabilities of a computer to make the program easier to use. The System Management Homepage GUI is Web-enabled and displays in a Web browser.

**HP Insight Management Agent**

A program that regularly gathers information or performs some other service without the user’s immediate presence.

**HP Systems Insight Manager**

System management software that is capable of managing a wide variety of systems, including HP systems, clusters, desktops, workstations, and portables.

HP Systems Insight Manager combines the strengths of HP Insight Manager 7, HP Toptools, and HP Servicecontrol Manager to deliver a single tool for managing HP ProLiant, Integrity, and HP 9000 systems running Windows, Linux, and HP-UX. The core HP Systems Insight Manager software delivers the essential capabilities required to manage all HP server platforms. HP Systems Insight Manager can also be extended to deliver unparalleled breadth of system management with plug-ins for HP storage, power, client, and printer products. Plug-ins 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 Systems Insight Manager, go to the web address http://www.hp.com/go/hpsim.

**HP Version Control Agent**

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.

**IP range**

Systems with an IP address that falls in the specified range.

**repository**

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

**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 Task Execution

Secure execution of a task from a managed system. This feature of System Management Homepage ensures that the user requesting the task has the appropriate rights to perform the task and encrypts the request to protect data from snooping.

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 and Certificate Authority

single login

Permission granted to an authenticated user browsing to HP Systems Insight Manager to browse to any of the managed systems from within HP Systems Insight Manager without re-authenticating to the managed system. HP Systems Insight Manager is the initial point of authentication and browsing to another managed system must be from within HP Systems Insight Manager.

software update

A task to remotely update software and firmware.

status type

Systems of specified status type (Critical, Major, Minor, Normal, and Unknown).

System Management Homepage

An integrated piece of software used by the HP 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.

user

A network user with a valid login on the System Management Homepage.

user accounts

Accounts used to log in to System Management Homepage. These accounts associate a local Windows user or domain account or a Linux user group with privilege levels and paging attributes inside System Management Homepage.

version control

A feature that checks the versions of HP operating system drivers, HP Systems Insight Manager Agents, HP utilities, and firmware on the user’s system. It compares them with the Version Control Database of current software and firmware versions. Version Control then indicates that the software is current or that an upgrade is available and provides reasons for upgrading.

Version information appears as a system link for a system.