

HP System Management Homepage



Manufacturing Part Number: 365395-004

May 2005, Edition 2

©Copyright 2005 Hewlett-Packard

Table of Contents

Product Overview	4
Product Overview	4
Additional Resources	4
Related Topics	4
Getting Started	5
Related Procedures	5
Related Topics	5
Logging In	5
Logging Out	8
Automatically Importing Certificates	8
Navigating the Software	10
Introduction	10
Header frame	10
Data frame	10
Information Areas	10
Related Topics	11
Tabs	11
System Management Homepage Overview	12
Related Topics	12
The Home Tab	13
System Status Summary	13
Software Status	13
Organizational menu	13
Related Topics	14
The Settings Tab	15
System Management Homepage section	15
Related Procedures	15
Related Topics	15
Credits	15
Security	15
IP Binding	16
IP Restricted Login	17
Local Server Certificate	18
Local and Anonymous Access	20
Trust Mode	21
Trusted Management Servers	23
User Groups	24
The Tasks Tab	27
Related Topics	27
The Tools Tab	28
Related Topics	28
The Logs Tab	29
Related Procedures	29
Related Topics	29
System Management Homepage Log	29
System Management Homepage Legacy Log	30
Troubleshooting	31
Browser Problems	31
Installation Problems	33
IP Address Problems	34
Login Problems	34

Security Problems	37
Other Problems	39
Service and Support	40
Glossary	42
Index	46

Product Overview

Product Overview

The System Management Homepage is a Web-based application that provides a consolidated interface for single system management. By aggregating the data from HP Web-based agents and management utilities, the System Management Homepage 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.

The System Management Homepage can be installed on HP-UX, Microsoft® Windows®, and Linux operating systems (IA32 and Intel Itanium).

- On HP-UX Operating Environments, System Management Homepage is installed with default settings. You can change the configuration by modifying the environment variables set in the `/opt/hpsmh/sbin/envvars` and `/opt/hpsmh/conf/timeout.conf` scripts.
- On Linux operating systems, System Management Homepage is installed with default settings. The settings are configurable by way of the perl script located at `/usr/local/hp`.
- On Windows operating systems, the installation enables you to configure the System Management Homepage settings during installation.

Note:



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

Additional Resources

For additional resources, go to these links:

- System Management Homepage on the Software Depot home at <http://www.hp.com/go/softwaredepot>
- HP Proliant Server Management Software page at <http://www.hp.com/servers/manage>

Related Topics

- System Management Homepage Overview
- Getting Started

Getting Started

To get started with System Management Homepage, use the following steps as a guideline for configuring the System Management Homepage 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 and Anonymous Access"

Related Procedures

- Logging In
- Logging Out

Related Topics

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

Logging In

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

To log in to the System Management Homepage with Internet Explorer:

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

Note:



If you are using Internet Explorer to browse to an HP-UX system, then you can use port 2381 if you changed the default configuration to have `autostart` disabled and `start on boot` enabled. If you keep the default-installed configuration, you can use the following URI:

`http://hostname:2301/`

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

You can find procedures on how to change the configuration variables in the *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 link, 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 the System Management Homepage.

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**.

If you are accessing this page through a link from HP Systems Insight Manager and the **Trust By Certificate** option is enabled in the System Management Homepage, the **Automatically Import Management Server Certificate** option appears if trust has not been previously configured. For more information regarding automatically importing the HP Systems Insight Manager certificate, refer to "Automatically Importing Certificates" .

3. Click **Yes**.

The **Login** page appears.

If you have enabled **Anonymous** access, 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 **Administrators** group for Windows or the operating system group **root** (which in turn contains the user root by default) for HP-UX and Linux. If the credentials cannot be authenticated, the user is denied access.

Note:



In most cases, the **administrator** on Windows and **root** on HP-UX or Linux have administrator access on the System Management Homepage.

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

The **System Management Homepage** appears.

To log in to the System Management Homepage with Mozilla:

1. Navigate to **http://hostname:2381/**.

If you are using Mozilla to browse to an HP-UX system, then you can use port 2381 if you changed the default configuration to have `autostart` disabled and `start on boot` enabled. If you keep the default-installed configuration, you can use the following URI:

http://hostname:2301/

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

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

The first time you browse to the System Management Homepage 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 unless you have enabled **Anonymous** access, then the **System Management Homepage** appears.

3. 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 **Administrators** group for Windows or the operating system group **root** (which in turn contains the user `root` by default) for HP-UX and Linux. If the credentials cannot be authenticated, the user is denied access.

Note:



In most cases, the **administrator** on Windows and **root** on HP-UX and Linux have administrator access on the System Management Homepage.

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

The **System Management Homepage** appears.

Related Topics

- Logging Out
- Automatically Importing Certificates

Logging Out

To log out of the System Management Homepage, you have several options:

- In the System Management Homepage banner, for HP-UX click **Sign Out** and for Linux and Windows click **logout**.

The System Management Homepage Login Window appears.

- Close every instance of the Web browser that you used to log in to System Management Homepage.

Related Topic

- Logging 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 Manager 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 (Settings-Security-Trust Mode window), and a certificate for the HP Systems Insight Manager 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 Systems Insight Manager certificate details.

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 log-in credentials.

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 log-in credentials.

3. Leave **Automatically Import Management Server Certificate** selected, enter your System Management Homepage credentials, and click **Login** to automatically import the certificate.

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

Related Topics

- Logging In
- Logging Out
- Local and Anonymous Access
- Local Server Certificate
- Trusted Management Servers
- User Groups

Navigating the Software

Introduction

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 Software Status section in the The Home Tab for more information.

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 displays the path you are currently viewing.

Data frame

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

Information Areas

Depending on your operating systems (HP-UX, Linux, or Windows), you will see the following information areas in the Header or Data Frames:

- **Tabs** The System Management Homepage Tabs include:
 - The Home Tab
 - The Settings Tab
 - The Tasks Tab
 - The Tools Tab
 - The Logs Tab
- **Support.** The Support link takes you to the ProLiant Server Management page. The purpose of the HP Support page is to provide you with a variety of products, services, and support related resources. To access support, go to <http://www.hp.com/servers/manage>.
- **Forums.** Contact the HP Support Forum to get answers to your questions about HP products. To access the HP Support Forum, go to <http://forums.itrc.hp.com>.

- **Help.** The Help link 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.** The System Model displays the model of the system. The System Model displays **Unknown** if the HP Insight Management Agent for servers are not installed on the system.
- **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 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.

Related Topics

- The Home Tab
- The Settings Tab
- The Tasks Tab
- The Tools Tab
- The Logs Tab

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 **Tasks** tab and the **Tools** tab are only visible if HP Web-enabled System Management Software provides information for them.

The System Management Homepage tabs that may display are:

- The Home Tab
- The Settings Tab
- The Tasks Tab
- The Tools Tab
- The Logs Tab

Related Topics

- The Home Tab
- The Settings Tab
- The Tasks Tab
- The Tools Tab
- The Logs Tab

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 Software Status section on the The Home Tab for more information.

For information regarding navigating in the System Management Homepage, refer to Navigating the Software.

Related Topics

- [Tabs](#)
- [The Home Tab](#)
- [The Settings Tab](#)
- [The Tasks Tab](#)
- [The Tools Tab](#)
- [The Logs Tab](#)

The Home Tab

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

- System Status Summary
- Software Status
- Organizational menu

Note:



Depending on what information is available from the HP Web-enabled System Management Software, you may see other boxes of information including computer system, operating system, and networking.

System Status Summary

The **System Status Summary** 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 **System Status Summary** 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.





Status Box Indicators

Indicator	Description
Blue	Unknown
Green	OK
Yellow	Degraded
Orange	Failed
Gray	No status

Organizational menu

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

- **System Model.** For HP-UX only, it lists the model of the system running System Management Homepage.

- **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 the **Remote Insight Lights-Out Edition (RILOE)** board or the **Integrated Lights-Out (iLO)** board. This information is provided by HP Insight Management Agent. If no HP Web-enabled System Management Software is installed that provides this information, then **None** is displayed.
- **Other Software/Other Links.** Provides information regarding value-added software as well as links to pages on <http://www.hp.com/servers/proliantessentials> that contain software information, including ProLiant Essentials Value Added Software.
- **KEY/Legend.** Displays a listing of status icons and a brief description of each.
 -  **OK**
 -  **Degraded**
 -  **Failed**
 -  **Unknown**

Related Topics

- The Settings Tab
- The Tasks Tab
- The Tools Tab
- The Logs Tab

The 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 and provides links to the following:

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

Related Procedures

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

Related Topics

- The Home Tab
- The Tasks Tab
- The Tools Tab
- The Logs Tab

Credits

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

Related Topics

- The Home Tab
- The Settings Tab
- The Tasks Tab
- The Tools Tab
- The Logs Tab

Security

The **System Management Homepage Security** link provides the following security options:

- **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 and Anonymous Access.** Select **Settings->System Management Homepage->Security ->Local and 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.**

Related Procedures

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

Related Topics

- The Home Tab
- The Settings Tab
- The Tasks Tab
- The Tools Tab
- The Logs Tab

IP Binding

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

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 is bound 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:

Setting this value requires restarting the 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

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

IP Restricted Login

The IP Restricted Login enables the System Management Homepage to restrict log-in access based on the IP address of a system.

You can set address restriction at installation time or by it can be set 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 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**. The **IP Restricted Login** page appears.
3. Select **IP Restricted Login** 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 System Management Homepage which may require you to log in again.

7. Click **OK**.

Related Topics

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

Local Server Certificate

The **Local Server Certificate** page 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 System Management Homepage is replaced with one that was issued by a Certificate Authority (CA).

- The first step of the process is to cause the System Management Homepage 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 the System Management Homepage.
- After the **PKCS #7 data** data has been successfully imported, the original `\hp\sslshare\cert.pem` certificate file for Windows, and the `/opt/hpsmh/sslshare/cert.pem` file for HP-UX and 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** and/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` for Linux, and `c:\hp\sslshare\req_cr.pem` 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. In this case, skip the next step.
8. Click **Import PKCS #7 Data**. A message appears indicating whether the customer-generated certificate was successfully imported.
9. Restart the **System Management Homepage**.
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/req_cr.pem` for HP-UX, `/opt/hp/sslshare/req_cr.pem` for Linux, and `c:\hp\sslshare\req_cr.pem` for Windows; then restart the System Management Homepage.

Related Topics

- IP Binding
- IP Restricted Login
- Local and Anonymous Access
- Trust Mode
- Trusted Management Servers
- User Groups

Local and Anonymous Access

Local and **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 System Management Homepage without logging in.

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 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 username and password.

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

Enabling Anonymous and Local Access

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.

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. 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

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

Trust Mode

The **Trust Mode** options 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 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 strongly recommends using this option as it is more secure.

- **Trust by Name.** 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. For example, you might 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.

Note:



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

- **Trust All.** Sets the System Management Homepage to accept certain configuration changes from any system.

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

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

For Windows, the imported HP Systems Insight Manager certificates are stored in the `systemdrive\hp\hpsmh\certs` directory.

Note:



You must have administrative authority to access this directory.

Trust By Certificate

To trust by certificate:

1. Select **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 **Trusted Certificate** to access the Trusted Management server certificate.
5. Click **Save Configuration** to save the current configurations or **Reset Values** to cancel all changes.

Trust By Name

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 `server name`: `~ ' ! @ # $ % ^ & * () + = \ " : ' < > ? , |`
- Semicolons are used to separate `server names`

To trust by name:

1. Select **Settings>System Management Homepage>Security**.
2. Click **Trust Mode**. The **Trust Mode** page is displayed.
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 **Reset Values** to cancel all changes.

Trust All

To trust all servers:

1. Select **Settings>System Management Homepage>Security**.
2. Click **Trust Mode**. The **Trust Mode** page is displayed.
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
- IP Binding
- IP Restricted Login
- Local and Anonymous Access
- Local Server Certificate
- Trusted Management Servers
- User Groups

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.
- **Add Certificate From Server.** You can add a trusted certificate from an HP Systems Insight Manager server.

Importing Certificates

To import a certificate to the trusted certificates list:

1. Select **Settings>System Management Homepage>Security>Trusted Management Servers**.

2. Enter the name or IP address of the HP Systems Insight Manager system that contains the certificate to be added. Add it in the **Add Certificate From Server** box.
3. Cut and paste the Base64 encoded certificate into the text box.
4. Click **Import Certificate Data**.

Adding a Certificate from a Server

To add a certificate from a server:

1. Select **Settings->System Management Homepage->Security->Trusted Management Servers**.
2. Enter the name of the HP Systems Insight Manager server that contains the certificate to be added. Add it in the **Add Certificate From Server** box.
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 the Certificate** window, and if you want to add it to the trusted certificate list, click **Add Certificate to Trust List**.

Related Topics

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

User Groups

System Management Homepage 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 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 Windows administrators group and the HP-UX and Linux root group automatically have 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 the accounts have any elevated access on the host operating system.

Adding User Groups

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 all information provided through the System Management Homepage. The appropriate default user group, **Administrators** for Microsoft 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 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.

Adding an Administrator Group

To add an Administrator Group:

1. Select **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 **Reset Values** to cancel all changes.

Adding an Operator Group

To add an Operator Group:

1. Select **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 **Reset Values** to cancel all changes.

Adding a User Group

To add a User Group:

1. Select **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.

Related Topics

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

The 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.

Related Topics

- The Home Tab
- The Settings Tab
- The Tools Tab
- The Logs Tab

The 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.

Related Topics

- The Home Tab
- The Settings Tab
- The Tasks Tab
- The Logs Tab

The Logs 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.

The Logs tab provides the following log options:

- Select **Logs->System Management Homepage->System Management Homepage Log**.
- For Linux and Windows only, select **Logs->System Management Homepage->System Management Homepage Legacy Log**.

Related Procedures

- System Management Homepage Log
- System Management Homepage Legacy Log

Related Topics

- The Home Tab
- The Settings Tab
- The Tasks Tab
- The Tools Tab

System Management Homepage Log

The **System Management Homepage Log** primarily contains 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, select **Logs->System Management Homepage->System Management Homepage Log**.

Related Topics

- The Logs Tab
- System Management Homepage Legacy Log
- The Settings Tab
- The Tasks Tab
- The Tools Tab

System Management Homepage Legacy Log

If your Linux or Windows system had HP Web-enabled System Management Software installed prior to the installation of the System Management Homepage 2.0.0, then their logs are visible by way of the **System Management Homepage Legacy Log** link. This log contains historical information regarding the security-related events that occurred prior to the installation of the new version.

Note:



You must be a member of the System Management Homepage **Administrators** group to access the **System Management Homepage Log**.

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

Note:



HP-UX does not include a Legacy Log.

Related Topics

- The Logs Tab
- System Management Homepage Log

Troubleshooting

Note:



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

Browser Problems

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 System Management Homepage?

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 the System Management Homepage 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 System Management Homepage. 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 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.

I get security messages or partially displayed pages when browsing into System Management Homepage 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.

How can I tell if my browser is supported?

Solution: The supported browsers are:

You can use the following desktop browser running on an HP-UX Itanium or PA-RISC system that is connecting to any server type, or a browser running locally on the HP-UX server and displayed to any desktop via X :

- Mozilla 1.6

You can use the following desktop browsers running on a Windows Itanium or x86 system that are connecting to any server type :

- Internet Explorer 6.0 or greater
- Mozilla 1.5
- Mozilla 1.6

You can use the following desktop browsers running on a Linux IPF or x86 system that are connecting to any server type :

- Mozilla 1.5
- Mozilla 1.6

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

Solution: By default, HP-UX is installed with the `autostart` feature enabled. A daemon listens on port 2301 and only starts the System Management Homepage 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 `localhost`.

HP recommends using the following URL to resolve this issue:

`https://localhost:2381`

After updating my Windows XP system with Service Pack 2, I am unable to access 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 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.

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

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 indicated above. 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.

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 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, 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 System Management Homepage 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://localhost:2381** or **https://127.0.0.1:2381**. For HP-UX, you can access the local system at **http://hostname:2301** if you kept 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 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

I cannot log in to System Management Homepage on my Windows operating system.

Solution: 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 System Management Homepage operating system groups.

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 on next logon option** selected.

Any login created in the future can be added by the operating system Administrator without selecting the **user must change the password on next logon option**. In addition, if this option is selected,

you can change the password through the operating system before logging in to the System Management Homepage.

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 administrators group (root group in Linux) 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. Please note that this does not apply to HP-UX.

I created new Windows accounts, using default settings, for use with the System Management Homepage 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 on next login**. This option must be deselected before the account can be used to log in to the System Management Homepage.

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 the System Management Homepage. 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 System Management Homepage 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 Web site to the zone**, enter the IP address of the System Management Homepage system. For example, enter **https://ipaddress** .
6. Click **Add**.
7. Click **OK**.
8. Click **OK**.
9. Click **OK**. The changes are saved.

After updating my Windows XP system with Service Pack 2, I am unable to access 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 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.

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

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 indicated above. 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.

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 may 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 indicated above. 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 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 the `\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 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->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. 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 System Management Homepage?

Solution: To use a Windows 2003 Certificate Authority to create a certificate for System Management Homepage:

1. Create the PKCS#10 data packet by clicking **Settings->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`.

Other Problems

Why can't I 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. Please 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. The System Management Homepage does not currently have access to that parameter and assumes the management processor is on port 80.

Why can't I install on HP-UX or 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 to reinstall on United Linux 1.0 or SuSE SLES 8.

Why can't I 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 are listed.

Why can I not access the System Management Homepage after I installed some McAfee products?

Solution: McAfee has announced (through its Web site) an incompatibility that might render its own products and several Web-based products unusable. The list of incompatible products includes the HP System Management Homepage. This incompatibility can be seen on Windows 2000. The McAfee Web site described the issue:

"Internet connectivity issues caused by incompatible Layered Service Providers:

- (LSP) CR13346

Product Versions

- All McAfee VirusScan 7 versions
- All McAfee Internet Security 5 versions
- All McAfee Firewall 4 versions

Operating Systems

- Windows 2000/XP
- Windows 98/Millennium
- System Information

Connection to the Internet:

You might experience Internet connectivity issues when McAfee Products are used in conjunction with other applications, which include a Layered Service Provider (LSP.) Most applications, which include a LSP, do coexist successfully. Those that are known to conflict with the McAfee LSP are listed below:"

- "Either uninstall the third-party application or uninstall the McAfee product."

McAfee is a business unit of Network Associates, Inc.

When I select Partition Manager Help from the System Management Homepage Help menu, why is the page blank?

Solution: Under certain circumstances, a blank page will appear in the Web browser when selecting Partition Manager Help from the System Management Homepage Help menu. If this occurs, use your browser's **Reload** button to correct the problem.

Service and Support

Support for System Management Homepage is provided as an adjunct to support of the underlying hardware. The purpose of the HP Support page is to provide you with a variety of product, service, and support related resources. In particular, you can use this page to:

- Access the HP ProLiant Server Management 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 System Management Homepage page at <http://software.hp.com>.
- 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. 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

Glossary

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 Certification Authority (CA) to bind the key and subject identification together.
Certificate Authority	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	The set of commands that you can execute directly from the command shell of an operating system.
Domain Name Service	A service that translates domain names into IP addresses.
external sites	Third-party application URLs.
graphical user interface	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.
in-place	Locally. For example to install in-place means to install locally.
HP Systems Insight Manager	<p>System management software that is capable of managing a wide variety of systems, including HP systems, clusters, desktops, workstations, and portables.</p> <p>HP Systems Insight Manager combines the strengths of HP Insight Manager 7, HP Tootools, 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 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 http://www.hp.com/go/hpsim.</p>
HP Insight Management Agent	A program that regularly gathers information or performs some other service without the user's immediate presence.
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.

	<p>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.</p>
HP Version Control Repository Manager	<p>An Insight Management Agent that allows a customer to manage HP-provided software stored in a user-defined directory/repository.</p>
HP Web-enabled System Management Software	<p>Software that manages HP Web-enabled products.</p>
Integrity Support Pack	<p>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.</p>
Internet Protocol (IP) range	<p>Systems with an IP address that falls in the specified range.</p>
ProLiant Support Pack	<p>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.</p>
Public-key infrastructure	<p>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.</p>
repository	<p>The database that stores vital information about the managed cluster, including users, nodes, node groups, roles, tools, and authorizations.</p>
Red Hat Package Manager	<p>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.</p>
search criteria	<p>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.</p>
Secure HTTP	<p>An extension to the HTTP protocol that supports sending data securely over the Web.</p>
Secure Shell	<p>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</p>

	<p>one system to another, and it provides authentication and secure communications over insecure channels.</p>
Secure Sockets Layer	<p>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.</p>
Secure Task Execution	<p>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.</p>
self-signed certificate	<p>A certificate that is its own Certificate Authority (CA), so that the subject and the CA are the same. See Also certificate, Certificate Authority.</p>
single login	<p>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.</p>
software update	<p>A task to remotely update software and firmware.</p>
status type	<p>Systems of specified status type (Critical, Major, Minor, Normal, and Unknown).</p>
survey utility	<p>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.</p>
System Management Homepage	<p>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.</p>
URI	<p>Provides methods to access a resource on the Internet. A Uniform Resource Locator (URL) is a type of Uniform Resource Indicator (URI).</p>
URL	<p>A global address of resources on the World Wide Web. A Uniform Resource Locator (URL) is a type of Uniform Resource Indicator (URI).</p>
user	<p>A network user with a valid login on the System Management Homepage.</p>
user accounts	<p>Accounts used to log in to System Management Homepage. These accounts associate a local Windows user, domain account, or an HP-UX or Linux user group with privilege levels and paging attributes inside System Management Homepage.</p>

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 (VCDB) of current software and firmware versions. Version control then indicates that the software is up to date or that an upgrade is available and provides reasons for upgrading.

Version information appears as a system link for a system.

Index

C

- certificates
 - auto import certificate, 8
 - trust mode, 21
 - trusted management server certificates, 23
- credits
 - System Management Homepage, 15

G

- getting started
 - login, 5
 - logout, 8

H

- home
 - System Management Homepage, 13

L

- logs
 - System Management Homepage, 29
 - System Management Homepage legacy log, 30
 - System Management Homepage log, 29

N

- navigating
 - System Management Homepage, 10

O

- overview
 - getting started, 5
 - System Management Homepage, 12

R

- reference
 - troubleshooting, 40

S

- security
 - anonymous, 20
 - auto import certificate, 8
 - IP Binding, 16
 - IP Restricted Login, 17
 - local access, 20
 - local server certificate, 18
 - System Management Homepage, 15
 - trust mode, 21
 - trusted management server certificates, 23
 - user groups, 24

- settings
 - System Management Homepage, 15
- System Management Homepage
 - anonymous access, 20
 - credits, 15
 - getting started, 5
 - home, 13
 - IP Binding, 16
 - IP Restricted Login, 17
 - legacy log, 30
 - local access, 20
 - local server certificate, 18
 - login, 5
 - logout, 8
 - logs, 29
 - navigating, 10
 - overview, 12
 - security, 15
 - settings, 15
 - tabs, 11
 - tasks, 27
 - tools, 28
 - user groups, 24

T

- tabs
 - System Management Homepage, 11
- tasks
 - System Management Homepage, 27
- tools
 - System Management Homepage, 28
- troubleshooting
 - reference, 40