

HP System Management Homepage Installation Guide

HP-UX, Linux, and Windows Systems



Manufacturing Part Number: 381372-002
May 2005, Edition 2

©Copyright 2005 Hewlett-Packard

Legal Notices

The information in this document is subject to change without notice.

Hewlett-Packard makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental, or consequential damages in connection with the furnishing, performance, or use of this material.

Warranty

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

U.S. Government License

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

Copyright Notices

©Copyright 1983-2005 Hewlett-Packard Development Company, L.P. All rights reserved. Reproduction, adaptation, or translation of this document without prior written permission is prohibited, except as allowed under copyright laws.

Trademark Notices

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

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

Intel® and Itanium® are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

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

Java™ is a US trademark of Sun Microsystems, Inc.

Microsoft®, Windows®, and Windows NT® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

Red Hat® is a registered trademark of Red Hat, Inc. in the United States and other countries.

SuSE® is a registered trademark of SuSE Linux AG.

Publication History

The manual publication date and part number indicate its current edition. The publication date will change when a new edition is released. The manual part number will change when extensive changes are made.

To ensure that you receive the latest edition, you should subscribe to the appropriate product support service. See your HP sales representative for details.

Please direct comments regarding this guide to:

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

Or, use this web form to send us feedback:

<http://docs.hp.com/assistance/feedback.html>

Revision History

Revision Edition 2

May 2005

MPN: 381372-002. The second edition provided installation instructions for the HP-UX Operating Environments.

Revision Edition 1

November 2004

MPN: 381372-001. The first edition provided installation instructions for the Linux and Windows operating systems.

Typographic Conventions

We use the following typographical conventions.

| | |
|--------------------------|---|
| <code>audit(5)</code> | HP-UX manpage. <i>audit</i> is the name and <i>5</i> is the section in the <i>HP-UX Reference</i> . On the web and on the Instant Information DVD, it may be a hot link to the manpage itself. From the HP-UX command line, you can enter " man audit " or " man 5 audit " to view the manpage. See <code>man(1)</code> . |
| <i>Book Title</i> | Title of a book. On the web and on the Instant Information DVD, it may be a hot link to the book itself. |
| Command | Command name or qualified command phrase. |
| <code>ComputerOut</code> | Text displayed by the computer. |
| <i>Emphasis</i> | Text that is emphasized. |
| Emphasis | Text that is strongly emphasized. |
| KeyCap | Name of a keyboard key. Note that Return and Enter both refer to the same key. |
| <i>Term</i> | Defined use of an important word or phrase. |
| UserInput | Commands and other text that you type. |
| <i>Variable</i> | Name of a variable that you may replace in a command or function or information in a display that represents several possible values. |
| [] | Contents are optional in formats and command descriptions. If the contents are a list separated by , you must choose one of the items. |
| { } | Contents are required in formats and command descriptions. If the contents are a list separated by , you must choose one of the items. |
| ... | Preceding element may be repeated an arbitrary number of times. |
| | Separates items in a list of choices. |

Table of Contents

| | |
|---|----|
| 1. Product Overview | 6 |
| 2. Installation Requirements | 7 |
| Supported Operating Systems | 7 |
| Supported Browsers | 8 |
| RPMs Supported on the IA-32 Platform | 9 |
| RPMs Supported on the AMD64 and EM64T Platform | 11 |
| RPMs Supported on the Itanium Platform | 11 |
| Verifying System Requirements | 13 |
| Obtaining the System Management Homepage Software | 13 |
| HP Media | 13 |
| HP Web Sites | 13 |
| 3. Initial Setup | 15 |
| 4. Installing on HP-UX | 16 |
| Installation Requirements | 16 |
| Installing System Management Homepage and Dependent Applications | 17 |
| Using the Application Release (AR) Media | 18 |
| Using Software Depot | 19 |
| Configuring System Management Homepage | 20 |
| Configuring the Startup Mode | 20 |
| Patching or Updating the Software | 22 |
| 5. Installing on Windows | 23 |
| Installing the System Management Homepage In-Place on Windows | 23 |
| Installing the System Management Homepage for Windows Silently | 27 |
| Generating a setup.iss file | 27 |
| Installing silently using the CLI | 27 |
| Reinstalling silently using the CLI | 28 |
| 6. Using the ProLiant Remote Deployment Utility | 29 |
| Installing Remotely on Windows Using ProLiant Remote Deployment Utility | 29 |
| 7. Installing In-Place on Linux | 33 |
| Installation for Linux on IA-32 and x86_64 | 33 |
| Installing System Management Homepage on Linux IA_32 Systems | 33 |
| Installing System Management Homepage on x86_64 | 34 |
| Configuring System Management Homepage | 34 |
| 8. Installing In-Place on Linux Using Linux Deployment Utility | 41 |
| Installing System Management Homepage with Pre-configuration | 41 |
| Pre-configuring the System Management Homepage Component | 41 |
| Installing the System Management Homepage as a Single Component | 43 |
| Installing the System Management Homepage without Pre-configuration | 43 |
| 9. Initializing the Software for the First Time | 44 |
| 10. Logging In and Logging Out of System Management Homepage | 45 |
| Logging In with Windows XP | 45 |
| Logging In with Internet Explorer | 45 |
| Logging In with Mozilla | 47 |
| Logging In from the HP-UX Command Line | 48 |
| Logging Out | 48 |
| 11. Uninstalling the System Management Homepage | 49 |
| Uninstalling from an HP-UX System | 49 |
| Uninstalling from a Linux IA-32 or x86_64 System | 49 |
| Uninstalling from a Windows System | 49 |
| Uninstalling from Multiple Windows Systems Silently | 49 |
| Uninstalling Manually for Windows Systems | 50 |

| | |
|----------------|----|
| Glossary | 52 |
| Index | 56 |

Chapter 1. Product Overview

The HP System Management Homepage is a Web-based interface that consolidates and simplifies single system management for HP servers running the HP-UX, Linux, and Microsoft Windows operating systems. The System Management Homepage aggregates and displays data from Web Agents and other HP Web-enabled System Management Software that includes HP Insight Diagnostics, the Array Configuration Utility, and the HP Software Version Control Agents.

The System Management Homepage enables IT administrators to view in-depth hardware configuration and status data, performance metrics, system thresholds, diagnostics, and software version control information using a single intuitive interface.

System Management Homepage provides enhanced security and streamlined operations for HP servers running HP-UX, Linux, and Windows.

- Browser access using OS-based SSL-secure authentication
- Common HTTP and HTTPS service for HP management agents and utilities, for reduced complexity and system resource requirements
- Simplified architecture for implementing HTTP security and HP management updates
- Greater access control through NIC binding and advanced configuration features for individual and groups of users
- Broader operating system and browser support

Chapter 2. Installation Requirements

This chapter provides requirements for the HP-UX, Linux, and Windows systems to run System Management Homepage:

- “Supported Operating Systems” (page 7)
- “Supported Browsers” (page 8)
- “RPMs Supported on the IA-32 Platform” (page 9)
- “RPMs Supported on the AMD64 and EM64T Platform” (page 11)
- “RPMs Supported on the Itanium Platform” (page 11)
- “Verifying System Requirements” (page 13)
- “Obtaining the System Management Homepage Software” (page 13)
 - “HP Web Sites” (page 13)
 - “HP Media” (page 13)

Supported Operating Systems

This section lists the supported operating systems for the HP-UX, Linux, and Windows systems:

- HP-UX 11i V2 (B.11.23) for HP Integrity Servers, HP Workstations, and HP 9000 Servers
- HP-UX 11i V1 (B.11.11) for HP Servers and Workstations
- Red Hat Enterprise Linux 4.0 for x86
- Red Hat Enterprise Linux 4.0 for AMD64 and EM64T
- Red Hat Enterprise Linux 3 for x86
- Red Hat Enterprise Linux 3 for AMD64 and Intel EM64T
- Red Hat Enterprise Linux 2.1
- Red Hat Linux Advanced Server 2.1 Update 3 or later
- Red Hat Enterprise Linux 3 Update 2 or later for AMD64 and x86
- SUSE Linux Enterprise Server (SLES) 8 for x86
- SUSE Linux Enterprise Server (SLES) 9 for x86
- SUSE Linux Enterprise Server (SLES) 9 for AMD64 and Intel EM64T
- SUSE Linux Enterprise Server (SLES) 8 for AMD64

- SUSE Linux Enterprise Server (SLES) 8 with Service Pack 3 or later for AMD64
- SUSE Linux Enterprise Server (SLES) 9 for x86
- SUSE Linux Enterprise Server (SLES) 9 for AMD64 and EM64T
- UnitedLinux 1.0 Service Pack 3
- Microsoft Windows Server 2003 Slipstream, Standard Edition
- Microsoft Windows Server 2003 Slipstream, Web Edition RTM
- Microsoft Windows Server 2003 Slipstream, Enterprise Edition RTM
- Microsoft Windows Server 2003 SBS, Standard and Premium
- Microsoft Windows Server 2003, Enterprise Edition for 64-bit Itanium based Systems
- Microsoft Windows Server 2003, Datacenter Edition for 64-bit Itanium based Systems
- Microsoft Windows Server 2003, Enterprise Edition with Service Pack 1 for Itanium based Systems
- Microsoft Windows Server 2003, Datacenter Edition with Service Pack 1 for Itanium based Systems
- Microsoft Windows 2000 Server with Service Pack 4 or later
- Microsoft Windows 2000 Advanced Server with Service Pack 4 or later
- Microsoft Windows 2000 Server Slipstream with Service Pack 4 or later
- Microsoft Windows 2000 Advanced Server Slipstream with Service Pack 4 or later
- Microsoft Windows XP

Note:

For Linux, the Lightweight Directory Access Protocol (LDAP) is not supported. During SUSE Linux Enterprise Server (SLES) 9 installation, LDAP is used by default, so you must disable it.



For Windows, the SmartStart CD requires all systems have a minimum of 256 MB of RAM.

The HP-UX 11i V1 (B.11.11) Operating Environments are for PA-RISC systems only, while the HP-UX 11i V2 (B.11.23) Operating Environments (September 2004 and later) include PA-RISC and Itanium systems.

Supported Browsers

This section lists the supported browsers for the HP-UX, Linux, and Windows systems:

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

Note:



Installation of the System Management Homepage does not require a browser.

The HP Web-enabled System Management Software is hardware dependent. For the installation to complete successfully, your system must support at least 256 colors.

RPMs Supported on the IA-32 Platform

The System Management Homepage supports the following RPMs for each of the Linux operating systems on the IA-32 platform.

| Operating System | RPM |
|---|--|
| SUSE Linux Enterprise Server (SLES) 8 (x86) | <ul style="list-style-type: none">● expat 1.95.4-41 or greater● glibc 2.2.5● pam 0.76-70 or greater● perl 5.8.0 or greater● zlib 1.1.4-53 or greater |

Installation Requirements

| | |
|--|--|
| SUSE Linux Enterprise Server (SLES) 9 (x86) | <ul style="list-style-type: none">● expat 1.95.7-37 or later● glibc 2.3.3-98 or later● pam 0.77-221 or later● perl 5.8.0 or greater● zlib 1.2.1 or greater |
| Red Hat Linux Advanced Server 2.1 (x86) | <ul style="list-style-type: none">● expat 1.95.1-7 or greater● glibc v2.2.4● pam 0.75-46.7.3 or greater● perl 5.6.1 or greater● zlib 1.1.4-8 or greater |
| Red Hat Enterprise Linux 3 (x86) | <ul style="list-style-type: none">● expat 1.95.5-6 or greater● glibc v2.3.2● pam 0.75-51 or greater● perl 5.8.0 or greater● zlib 1.1.4-8.1 or greater |
| Red Hat Enterprise Linux 4.0 (x86) | <ul style="list-style-type: none">● expat 1.95.7-4 or greater● glibc 2.3.3-36● pam 0.77-47 or greater● perl 5.8.0 or greater● zlib 1.2.1-3 or greater |
| Red Hat Enterprise Linux 4.0 (AMD64 and EM64T) | <ul style="list-style-type: none">● expat 1.95.7-4 or greater● glibc 2.3.3-36● pam 0.77-47 or greater● perl 5.8.0 or greater● zlib 1.2.1-3 or greater |

RPMs Supported on the AMD64 and EM64T Platform

The System Management Homepage supports the following RPMs for each of the Linux operating systems on the AMD64 and EM64T platform.

| Operating System | RPM |
|---|---|
| SUSE Linux Enterprise Server (SLES) 8 (AMD64) | <ul style="list-style-type: none"> ● expat 1.95.4-67 or greater ● glibc 2.2.5 ● pam 0.76-74 or greater ● perl 5.8.0 or greater ● zlib 1.1.4-124 or greater |
| SUSE Linux Enterprise Server (SLES) 9 (AMD64 and EM64T) | <ul style="list-style-type: none"> ● expat 1.95.7-37 or greater ● glibc 2.3.3-98 or greater ● pam 0.77-221 or greater ● perl 5.8.0 or greater ● zlib 1.2.1-70 or greater |
| Red Hat Enterprise Linux 3 (AMD64 and EM64T) | <ul style="list-style-type: none"> ● expat 1.95.5-6 or greater ● glibc 2.3.2 ● pam 0.75-56 or greater ● perl 5.8.0 or greater ● zlib 1.1.4-8.1 or greater |

RPMs Supported on the Itanium Platform

The System Management Homepage supports the following RPMs for each of the Linux operating systems on the Itanium platform.

| Operating System | RPM |
|------------------|-----|
|------------------|-----|

| | |
|---|--|
| Red Hat Linux Advanced Server 2.1 (IPF) | <ul style="list-style-type: none"> ● expat 1.95.1-7 or greater ● glibc v2.2.4 ● iproute ● jrockit-j2se 8.1.1.1-2 or greater (IPF only) ● pam 0.75-46.7.3 or greater ● perl 5.6.1 or greater ● ucd-snmp 4.2.4 or greater ● zlib 1.1.4-8 or greater |
| Red Hat Enterprise Linux 3 (IPF) | <ul style="list-style-type: none"> ● expat 1.95.5-6 or greater ● glibc v2.3.2 ● jrockit-j2se 8.1.1.1-2 or greater (IPF only) ● net-snmp 5.0.9 or greater ● net-snmp-perl 5.0.9 or greater ● openssl 0.9.7a-22.1 or greater ● pam 0.75-51 or greater ● perl 5.8.0 or greater ● zlib 1.1.4-8.1 or greater |
| SUSE Linux Enterprise Server (SLES) 8 (IPF) | <ul style="list-style-type: none"> ● expat 1.95.4-41 or greater ● glibc 2.2.5 ● iproute2 ● jrockit-j2se 8.1.1.1-2 or greater (IPF only) ● openssl 0.9.6g-73 or greater ● pam 0.76-70 or greater ● perl 5.8.0 or greater ● ucdsnmp 4.2.5 or greater ● zlib 1.1.4-53 or greater |

Note:



The AMD64 is an AMD Opteron Processor.

The EM64T is an Intel Xeon Processor with Extended Memory 64 Technology.

The x86 is an Intel Pentium III/IV/Xeon 32 bit Processor (IA32).

The IPF is an Intel Itanium 64 bit Processor (IA64).

Verifying System Requirements

Before installation begins, the installation utility verifies whether:

- HP-UX/Linux/Windows: The operating system meets the minimum requirements. If the System Management Homepage does not support the operating system on a system, an error message appears, indicating that an invalid operating system is found.
- HP-UX/Linux/Windows: The user is logged in with administrator/root rights. If the user is not logged in with these rights, an error message appears, indicating that administrator/root rights were not detected.
- Linux: During a Linux installation on an IA-32 platform, if the Linux dependencies are not met the missing dependencies are displayed.
- Linux: If a dependency is not met on an Itanium platform, the installation will not complete.

Obtaining the System Management Homepage Software

You can obtain the System Management Homepage software from the following HP Web sites and media:

HP Media

The System Management Homepage is available on the following media:

- HP-UX 11i V2 (B.11.23) Operating Environment DVD, May 2005 or later
- HP-UX 11i V2 (B.11.23) Application Release DVD, May 2005 or later
- HP-UX 11i V1 (B.11.11) Application Release DVD, May 2005 or later
- SmartStart CD 7.20 or later
- Management CD 7.20 or later

HP Web Sites

The HP Web sites are accessible from any system with a Web browser and access to the Internet:

- To download the latest software versions, go to the HP Web site at <http://www.hp.com>.
- For HP-UX, you can also find the software on the Software Depot home at <http://www.hp.com/go/softwaredepot>.
- For Linux and Windows, the System Management Homepage is available in the ProLiant Support Pack and Integrity Support Pack. To download the latest version of the ProLiant Support Pack or Integrity Support Pack, go to the Support & Drivers page at <http://www.hp.com/support/files>.

Chapter 3. Initial Setup

You can install the System Management Homepage on systems running HP-UX, Linux, and Windows.

Additionally, you can install the System Management Homepage in-place using the Windows ProLiant Support Pack or the Linux RPM (Red Hat Package Manager), or remotely with optional preconfiguration using the ProLiant Remote Deployment Utility or the Linux Deployment Utility.

- For HP-UX Systems

The System Management Homepage is installed or updated using the HP-UX Operating Environment (OE) media or Applications Release (AR) media. You do not have to configure any settings to run the product.

For HP-UX, the configuration settings are preserved in the `/opt/hpsmh/conf.common/smhp.d.xml` file.

- For Linux Systems

The System Management Homepage is installed by an RPM package without asking you to configure any settings. After the installation is complete, run the `perl` script 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.

For Linux systems, the configuration settings are carried over from the `/opt/hp/hpsmh/conf/smhp.d.xml` file, and the wizard initiates the configuration.

- For Windows Systems

The configuration settings are carried over from the `\hp\hpsmh\conf\smhp.d.xml` file, and the wizard initiates the configuration.

Note:



If a Management HTTP Server is currently installed on the machine, the configuration settings are carried over to that system.

If HP Systems Insight Manager is installed after System Management Homepage is installed, the System Management Homepage 2048-bit key pair will be replaced with the HP Systems Insight Manager 1024-bit key pair.

Chapter 4. Installing on HP-UX

This chapter provides steps to install System Management Homepage on the HP-UX Operating Environments (OEs):

- “Installation Requirements” (page 16)
- “Installing System Management Homepage and Dependent Applications” (page 17)
- “Using the Application Release (AR) Media” (page 18)
- “Using Software Depot” (page 19)
- “Configuring System Management Homepage” (page 20)
- “Patching or Updating the Software” (page 22)

To install System Management Homepage on HP-UX, you have several options:

- Installing from the HP-UX V2 (B.11.23) Operating Environment (OE) media (May 2005 or later)
- Installing from the HP-UX 11i V1 (B.11.11) Application Release (AR) media or the HP-UX V2 (B.11.23) Application Release (AR) media (May 2005 or later)
- Installing from the System Management Homepage Web site, which you can find on the Software Depot home at <http://www.hp.com/go/softwaredepot>

Note:



After you install System Management Homepage, it is already configured for you to start using immediately. To change the default configuration settings, go to “Configuring System Management Homepage” (page 20).

Installation Requirements

To install System Management Homepage, your system must meet the minimum requirements. The following list provides a general review of requirements. For detailed information regarding minimum requirements, refer to Chapter 2: “Installation Requirements” (page 7).

- HP-UX 11i V1 (B.11.11) for HP Servers and Workstations
HP-UX 11i V2 (B.11.23) for HP Integrity Servers, HP Workstations, and HP 9000 Servers
- Mozilla browser
- Administrator privileges on system
- Dependent applications (see next section)

Installing System Management Homepage and Dependent Applications

There are several applications that System Management Homepage requires and some that are optional. You may already have these applications installed on your system. The following bundle information will help you identify the correct bundles to download and install:

| Product | Bundle Tag | Path | Status | Release |
|--------------------------------------|-----------------------------------|--|---|---|
| System Management Homepage | SysMgmtWeb | /opt/hpsmh and /var/opt/hpsmh | Required | HP-UX 11i V1 and V2 |
| HP-UX Apache-based Web Server | hpuxwsApache | /opt/hpws/apache | Required | HP-UX 11i V1 and V2 |
| HP-UX Strong Random Number Generator | KRNG11i | /usr/conf or /usr/conf/lib/lib/krng, /usr/share, /usr/include, /sbin/init.d, /sbin/rc1.d | Required | HP-UX 11i V1 You can find this application on the Software Depot Home at http://www.hp.com/go/swdepot or the IT Resource Center at http://itrc.hp.com . The KRNG11i bundle requires a system reboot. |
| HP-UX Tomcat-based Servlet Engine | hpuxwsTomcat | /opt/hpws/tomcat | Optional: Certain System Management Homepage plugins, such as PartitionManager require it. | HP-UX 11i V1 and V2 |
| HP WBEM Services | B8465BA | /opt/wbem | Optional: Certain System Management Homepage plugins, such as Property Pages found on the Home page require it. | HP-UX 11i V1 and V2 |
| Java | Java2 1.4 SDK for HP-UX (T1456AA) | /opt/java1.4 | Optional: Certain System Management Homepage plugins, such as PartitionManager require it. | HP-UX 11i V1 and V2 |

| Product | Bundle Tag | Path | Status | Release |
|---------|------------|--------------|----------|---------------------|
| OpenSSL | OpenSSL | /opt/openssl | Required | HP-UX 11i V1 and V2 |

If you do not have these applications on your system, you can use the following resources to install them before or after you instal System Management Homepage:

- If you installed or updated HP-UX 11i V1 (B.11.11) from the AR media or HP-UX 11i V2 (B.11.23) from the AR or OE media, then the applications were default installed. See the *HP-UX Installation and Update Guide* on the HP Technical Documentation Web site at <http://docs.hp.com> for instructions on how to install and update HP-UX, including the default-installed HP application bundles. Also see “Using the Application Release (AR) Media” (page 18).
- You can use **swinstall** to install or update the bundles (for example, `hpuxwsApache` and `hpuxwsTomcat`) using the HP-UX 11i V1 (B.11.11) AR media and the HP-UX 11i V2 (B.11.23) AR or OE media. See “Using the Application Release (AR) Media” (page 18).
- You can go to the Software Depot Home at <http://www.hp.com/go/softwaredepot> to search for and download the application bundles. You can then use **swinstall** to install the applications. See “Using Software Depot” (page 19).
- You can also download the bundles to a depot on your network, then use Ignite-UX and Software Distributor to install them. This is helpful if you are creating one image to install on multiple systems. See the *Ignite-UX Administration Guide* and the *Software Distributor Administration Guide* on the HP Technical Documentation Web site at <http://docs.hp.com>.

Using the Application Release (AR) Media

To install System Management Homepage and other HP Applications, you must have root privileges. These instructions assume you are installing from a DVD.

1. Mount the Application DVD. To install software from the Application DVD, you must mount the DVD as a file system that HP-UX 11i can access:

- Determine the DVD device name.

Use the **ioscan -func disk** command to list disk devices, including the DVD devices.

- Create a mount point for the Application DVD, if one does not yet exist.

The mount point is a directory that HP-UX uses as an access point for the DVD. Often a `/cdrom` directory is used. If this directory does not exist, create it using the **mkdir** command.

- Use the **mount** command to mount the DVD.

Using the **mount** command, specify the DVD device name and mount point. For example, the following command mounts the `/dev/dsk/c1t0d0` device as the `/cdrom` directory:
mount /dev/dsk/c1t0d0 /cdrom

Refer to the `mount (1M)` manpage for details.

2. To determine which products and versions are on your system, use the **swlist** command:
`/usr/sbin/swlist -l product`

3. Use **swinstall** to install software from the Application DVD.

The following example uses **swinstall** to install software from the source mounted at `/cdrom`:
`/usr/sbin/swinstall -s /cdrom bundlename`

Refer to the `swinstall(1M)` manpage for details.

4. Select and install software from the Application DVD.

The **swinstall** program has an interface for selecting and installing software from the DVD.

5. Unmount and eject the Application DVD.

You must unmount the DVD before you can eject it from the DVD-ROM drive. The DVD is automatically unmounted whenever the server reboots.

Use the **umount** command to unmount the DVD. For example, `umount /cdrom` unmounts the `/cdrom` file system. Refer to the `umount(1M)` manpage for details.

Tip:



After the installation is complete, you can start using the System Management Homepage immediately.

Using Software Depot

To install System Management Homepage and other HP Applications, you must have root privileges.

1. Go to the Software Depot Home at <http://www.hp.com/go/softwaredepot>.
2. Find the product that you want to download. Each product has a Web page with information and download links.
3. Select the **download** link.
4. Fill out the registration form.
5. Review any installation instructions.
6. Save the bundle to a local directory such as `/var/temp`.
7. Use the **swinstall** command to install the product to your system. For example, `swinstall -s /var/temp bundlename`

Tip:

After the installation is complete, you can start using the System Management Homepage immediately.

Configuring System Management Homepage

The HP-UX System Management Homepage configuration is based on environment variables that are set by `/opt/hpsmh/sbin/envvars` and `/opt/hpsmh/conf/timeout.conf` scripts. To change the default configuration, you can modify the scripts to properly set the value of the following variables.

| Variable | Description | Script |
|----------------|--|---|
| JAVA_HOME | Points to the directory where JDK is installed. | <code>/opt/hpsmh/sbin/envvars</code> |
| TIMEOUT_SMH | Defines the SMH timeout in minutes. If it is not defined or equal to 0 (zero), then SMH is started without timeout. If present, then SMH is stopped after this time period has elapsed without any user-activity. | <code>/opt/hpsmh/conf/timeout.conf</code> |
| TIMEOUT_TOMCAT | Defines the Tomcat timeout in minutes. If it is not defined or equal to 0 (zero), then Tomcat is started without timeout. In this case, Tomcat is stopped only when SMH is stopped. If present, Tomcat is stopped after this time period has elapsed without any request to a Java web application. By default, the timeout for the HP-UX Tomcat-based Servlet Engine is 20 minutes and the timeout for the HP-UX Apache-based Web Server is 30 minutes. | <code>/opt/hpsmh/conf/timeout.conf</code> |

Configuring the Startup Mode

System Management Homepage supports three startup modes:

- autostart URL

This is the default setting for startup.

You can start System Management Homepage by using a Web browser and navigating to **http://hostname:2301/**. If autostart is configured as the default, there is a daemon listening on `http://hostname:2301` only (nothing is listening on port 2381 so that port will fail). When it contacts port 2301 (http), then the HP-UX Apache-based Web Server is started on port 2381 (https) and the page is automatically redirected.

- automatic startup on boot

This starts System Management Homepage automatically during the system initialization. If the automatic startup on boot start mode is enabled and the system was rebooted using this configuration, you can access the System Management Homepage by using a Web browser and navigating to **https://hostname:2381/**. Daemons are listening on both `http://hostname:2301/` and `https://hostname:2381/`. If you use port 2301 (http), then the HP-UX Apache-based Web Server is started on port 2381 (https) and the page is automatically redirected.

Note:



For autostart URL and automatic startup on boot, you can use `http://hostname:2301`, as it works in both cases. This is possible on an HP-UX system only.

- manual startup

You can start System Management Homepage from the HP-UX command line.

Use the `/opt/hpsmh/bin/smhstartconfig` script to configure the startup mode of the System Management Homepage server and of the Tomcat instance that the System Management Homepage uses.

Syntax: **smhstartconfig** [**-a** <on|off> **-b** <on|off>] [**-t** <on|off>]

Options:

-a Enable/disable the autostart URL mode.
 <on|off>

-b Enable/disable the automatic startup on boot mode.
 <on|off>

-t Set the Tomcat startup mode where:
 <on|off>

| | |
|-----|--|
| on | Start Tomcat when System Management Homepage starts. |
| off | Start Tomcat on demand (default). |

If no options are specified, then `smhstartconfig` displays the current startup mode. The `smhstartconfig` command does not accept **-a on** and **-b on** options simultaneously.

For more information, go to the `smhstartconfig(1M)` manpage: **man smhstartconfig** or **man sam**

After changing the autostart mode to "on boot" (with the `smhstartcommand -b on -a off` command), without rebooting you can start the HP-UX Apache-based Web Server processes with the `/opt/hpsmh/sbin/hpsmh start` command.

Patching or Updating the Software

HP may issue patches to the System Management Homepage. If this is the case, you can adopt a proactive patch management strategy and regularly check the standard patch resources:

- IT Resource Center (ITRC) at <http://itrc.hp.com>
- standard HP-UX patch bundles on the OE media, the AR media, and the ITRC

For a detailed guide on how to patch your HP-UX system, see the *Patch Management User Guide for HP-UX Systems* on the HP Technical Documentation Web site at <http://docs.hp.com>.

HP may issue software updates to the System Management Homepage. If this is the case, check the following resources for any notices regarding software updates:

- HP-UX OE media
- HP-UX AR media
- System Management Homepage Web page on the Software Depot home at <http://www.hp.com/go/softwaredepot>

Chapter 5. Installing on Windows

This chapter provides steps to install System Management Homepage on the Windows operating system.

- “Installing the System Management Homepage In-Place on Windows” (page 23)
- “Installing the System Management Homepage for Windows Silently” (page 27)

The next chapter provides steps to install System Management Homepage on the Windows operating system using the ProLiant Remote Deployment Utility:

- “Using the ProLiant Remote Deployment Utility” (page 29)

Installing the System Management Homepage In-Place on Windows

1. Initiate the `setup.exe` file to invoke the installation wizard. After the wizard initiates, the **Welcome** dialog box appears with a message explaining what product is being installed, the company name, and website.
2. Click **Next**. The **OS Groups** dialog box appears. Click **Cancel** to cancel the installation process. If you click **Cancel**, a message appears, giving you the option to continue installation or to exit the installation.
3. To add the System Management Homepage group names:
 - a. In the **Group Name** field, enter a name for the operating system group.
 - b. Select an operating level to include **Administrator**, **Operator**, or **User**.

Note: It is necessary to assign an account to an operating system user group with administrator privileges to access the Version Control Repository Manager from the Version Control Agent. Do not use the Administrator account to connect from the Version Control Agent to the Version Control Repository Manager as it could potentially lock the Administrator account out. Using the Administrator account, add another account with administrator privileges to be used for Version Control Repository Manager access.

4. Click **Add**. The group name is added. A maximum of five entries can be added for each group level.

Note: To delete a group name, select the group name and click **Delete**.

5. Click **Next** to continue or **Back** to return to the previous page. The **User Access** dialog box appears.

The **User Access** dialog box enables you to configure the System Management Homepage from the following access types:

- Select **Anonymous Access** to enable anonymous access to unsecured pages.

- Select **Local Access Anonymous** or **Local Access Administrator** to set up the System Management Homepage to automatically grant local IP addresses at the selected access level.

Caution: Selecting **Local Access** with Administrator privileges provides any users with access to the local console full access without prompting them for a user name or password.

6. Click **Next**. The **Trust Mode** dialog box appears.
7. Select the level of security you want to provide from one of the following trust modes:
 - Trust By Certificate
 - a. Click **Next**. The **Trusted Certificates** dialog box appears. The **Trusted Certificates** dialog box allows trusted certificate files to be added to the **Trusted Certificate List**.
 - b. Click **Add File** to browse and select any certificates to be included in the **Trusted Certificate List**. The **Add File** dialog box appears. If an invalid file name is entered in the file name field, an error message appears, indicating the file does not exist. Click **OK** to select another file, or click **Cancel** to close the dialog box. The **Trusted Certificate List** appears.

Note: If you click **Next** without adding any certificates to the list, and no certificates exist from a previous installation, a message appears indicating that if you do not specify any trusted certificates, HP Systems Insight Manager cannot access the HP Insight Management Agents on this system. Click **OK** if you do not want HP Systems Insight Manager to access the Insight Management Agents on this system, or click **Cancel** to close the dialog box and add the trusted certificates to the list.

Note: The **Trust By Certificates** option enables the System Management Homepage system and the HP Systems Insight Manager system to establish a trust relationship 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.
 - c. Click **Next**. The **IP Binding** dialog box appears.

or
 - a. Click **Import**. The **Import Server Certificate** dialog box appears.
 - b. Enter the name or IP address of the server whose certificate you want to import.
 - c. Click **Get Cert**. The certificate information appears.
 - d. Verify the certificate information. If you want to add this certificate to the **Trusted Certificate List**, click **Accept** and the certificate is added to the **Trusted Certificate List**, or click **Cancel** if you do not want to add it to the **Trusted Certificate List**. The **Trusted Certificate List** appears.

Note: You can add an unlimited number of trusted certificates.
 - e. Click **Next**. The **IP Binding** dialog box appears. Click **Back** to return to the **Trust Mode dialog** box.

Note: To delete a certificate, select the certificate and click **Delete**. The selected certificate is removed.

- Trust By Name

- a. Select **Trust By Name**.
- b. Click **Next**. The **Trusted Server** dialog box appears.

Note: Although the **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 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 can prevent non-malicious access. For example, you might 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.

- c. Enter the names of the servers you want to trust.

Note: The server name cannot contain the following characters: ~, !, ` , @, #, \$, %, ^, &, *, (,), +, =, ", :, ' , <, >, ?, ,, |, and ;.

- d. Click **Add** to add the name of a server you want to trust.
- e. Click **Next**. The **IP Binding** dialog box appears.

Note: If you click **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 cannot access the Insight Management Agents on this system. Click **OK** to proceed without trusting any systems, or click **Cancel** to close the dialog box and add server names to the list.

Note: To delete a server name, select the server name and click **Delete**. The selected server name is removed.

- Trust All

- a. Select **Trust All**.
- b. Click **Next**. The **IP Binding** dialog box 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. For example, you might want to use **Trust All** if you have a secure network, and everyone in the network is trusted.

8. Select **IP Binding** to enable the Subnet IP Address and NetMask.

The **IP Binding** dialog box enables you to bind to specific IP addresses that match a specific Subnet IP Address or NetMask. It restricts the subnet you want to manage.

- a. Enter the **Subnet IP Address** in the designated field.
- b. Enter the **NetMask** in the designated field.
- c. Click **Add**, and the Subnet IP Address/NetMask is displayed in the dialog box. To delete a Subnet IP Address/Netmask from the dialog box, select a **Subnet IP Address/NetMask**, and click **Delete**. The Subnet IP Address/Netmask is removed from the dialog box.

Note: You can add up to five Subnet IP Address/NetMask pairs.

9. Click **Next**. The **IP Restricted Logins** dialog box appears. The **IP Restricted Logins** dialog box enables you to select specific IP addresses or IP address ranges to include or exclude 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.
10. Select **IP Restricted Logins**, and click **Next**. The **IP Address to Include** dialog box appears. This dialog box enables you to specify the IP address or IP address ranges to grant login access permission. If there are IP addresses in the **Inclusion** list, then only those IP addresses are enabled for login privileges. If there are no IP addresses in the Inclusion list, then login privileges are permitted to all IP addresses that are not in the **Exclusion** list.

Note: A single address and ranges of addresses can be accepted in the **IP Restriction Logins** dialog box. Enter the single address in the first box.

- a. In the **Include** field, enter a beginning IP address to which you want to grant login access.
- b. In the **To** field, enter an ending IP address to which you want to grant login access. All IP address that fall between the beginning and ending IP addresses are granted login access.
- c. Click **Add**. The IP address or IP address range is added to the **Inclusion** list. To delete an IP address or IP address range, select an IP address or IP address range, and click **Delete**. The IP address or IP address range is deleted from 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. Click **OK**. Enter a valid IP address or IP address range, and click **Add** again.

11. Click **Next**. The **IP Address to Exclude** dialog box appears.
 - a. In the **Exclude** field, enter a beginning IP address to which you want to deny login access.
 - b. In the **To** field, enter an ending IP address to which you want to deny login access. All IP addresses that fall between the beginning and ending IP addresses are denied login access.
 - c. Click **Add**. The IP address or IP address range is added to the **Exclusion** list. To delete an IP address or IP address range, select an IP address or IP address range, and click **Delete**. The IP address or IP address range is deleted from the **Exclusion** list.

Note: If you entered an invalid IP address or IP address range, an error message appears, indicating the IP address is invalid. Click **OK**. Enter a valid IP address or IP address range, and click **Add** again.

Note: If **Next** is selected without adding any IP addresses to either the **Include** or **Exclude** lists, a warning message appears stating, IP Restricted Login checkbox will be marked as disabled. Do you want to proceed without adding any IP Address restrictions? If you select **OK**, the **IP Restricted Login** option on the **IP Restricted Login** dialog box is deselected, and the **Install Preview** dialog box appears.

12. Click **Next**. The **Install Preview Panel** appears. The **Install Preview Panel** lists the location where the System Management Homepage is installed, the amount of space the installation requires, and the summary of the options that you specified during the installation.

13. Click **Next**. The installation process is started.

Note: During the installation of the System Management Homepage, **Cancel** is disabled. If you click the **X** in the upper-right corner of the box, an error message appears, stating the current operation cannot be canceled.

14. Click **Finish** to complete the installation.

Installing the System Management Homepage for Windows Silently

The System Management Homepage installation for Windows enables you to silently install the System Management Homepage. After the installation is complete, you can configure the System Management Homepage settings.

Generating a setup.iss file

To generate your own `setup.iss`:

1. Run the following CLI:

```
setup.exe /r
```

2. The System Management Homepage Installation interface appears and records your selections.

3. The `setup.iss` file is placed into the Windows directory. You can move this file to the location of your choice.

Installing silently using the CLI

To install silently using the CLI:

```
setup.exe /s /f1<full_path_to_setup.iss_file>
```

For example, you might enter `setup.exe /s /f1c:\mydirectory\setup.iss`.

Note: There are no spaces between `f1` and the path.

Reinstalling silently using the CLI

To reinstall silently using the CLI:

```
setup.exe /s /reinst /f1<full_path_to_setup.iss_file>
```

Note: The **/s /reinst** command reinstalls the same version of System Management Homepage. The **/s /preserve** command preserves the existing `hpsmh.xml` settings.

If you are performing an initial installation of System Management Homepage 2.x, the **/preserve** command preserves the pre-2.x settings if present in the `compaq\wbem` directory.

If a System Management Homepage 2.x installation is already present, you must enter **setup.exe /s /reinst /preserve /f1<full_path_to_setup.iss>**. If you do not include **/preserve**, the `setup.iss` is applied.

Chapter 6. Using the ProLiant Remote Deployment Utility

This chapter provides steps to install System Management Homepage on the Windows operating system using the ProLiant Remote Deployment Utility.

- “Installing Remotely on Windows Using ProLiant Remote Deployment Utility” (page 29)

The previous chapter provides steps to install System Management Homepage in-place on the Windows operating system.

- “Installing the System Management Homepage In-Place on Windows” (page 23)

The ProLiant Remote Deployment Utility for Windows is a graphical application that provides enhanced ProLiant Support Pack deployment capabilities. Using a graphical interface, the utility enables you to deploy and maintain ProLiant Support Packs and Smart Components on a local server or remote server accessible over a network connection.

To run the ProLiant Remote Deployment Utility, invoke the Setup.exe which is present as part of the ProLiant Support Pack corresponding to each operating system. The ProLiant Support Pack is identified based on the operating system installed on the server. The components that are supported for installation are listed in the right side of the frame. The System Management Homepage can be installed as a part of the complete ProLiant Support Pack, or you can install the System Management Homepage component individually. The System Management Homepage component also provides support for pre-configuration, which allows the configurations of the component to be configured and saved as part of the component itself before installing on target machines. This facilitates the installation of the pre-configured component without any user intervention, and the installed component has the configurations, which are saved during pre-configuration.

All configurable components are listed at the top of the left frame under All configurable components.

Note:



Installation of a pre-configured component overwrites the configuration settings of any existing System Management Homepage installation. If you wish to retain existing settings, do not preconfigure the component.

Installing Remotely on Windows Using ProLiant Remote Deployment Utility

To pre-configure the System Management Homepage component:

1. Under **All configurable components**, right-click on the **System Management Homepage** component and select **Configure....** The **Welcome** wizard is displayed.
2. Click **Next**. The **Operating System Group** dialog box is displayed providing you with an option to add the groups and select the **Operating** level.

3. To add System Management Homepage groups:
 1. In the **Group Name** field, enter a name for the group. For example, you might want to use *vcAdmin* for a Version Control Administrator group.

Note: It is necessary to assign an account to an operating system user group with administrator privileges to access the Version Control Repository Manager from the Version Control Agent. Do not use the **Administrator** account to connect from the Version Control Agent to the Version Control Repository Manager as it could potentially lock the Administrator account out. Using the Administrator account, add another account with administrator privileges to be used for Version Control Repository Manager access.
 2. Select an **Operating Level** from the dropdown list. This level determines the privileges assigned to this group.
 3. Click **Add**. The group name is added. A maximum of five entries can be added for each group level.

After a group name is added, you can delete it by clicking the **X** located next to the group name.
4. Click **Next**. The **User Access** dialog box appears.
5. The **User Access** dialog box enables you to configure the System Management Homepage from the following access types:
 - Select **Anonymous Access** to enable anonymous access to unsecured pages.
 - Select **Local Access Anonymous** or **Local Access Administrator** to set up the System Management Homepage to automatically grant local IP addresses at the selected access level.

Caution: Selecting **Local Access** with Administrator privileges provides any users with access to the local console full access without prompting them for a user name or password.
6. Click **Next**. The **Trust Mode** dialog box appears.
7. Select the level of security you want to provide from one of the following trust modes:
 - Trust By Certificate
 - a. Select **Trust By Certificate**.
 - b. Click **Next**. The **Trusted Certificates** dialog box appears. The **Trusted Certificates** dialog box allows trusted certificate files to be added to the **Trusted Certificate List**.
 - c. Click **Browse** to select the certificate file. After the certificate file is selected, the certificate data is displayed on the screen.
 - d. Click **Add**. The certificate is displayed under **Certificate File**. To delete a certificate file from the screen, click the **X** located next to the certificate file.
 - e. Click **Add File** to browse and select any certificates to be included in the **Trusted Certificate List**. The **Add File** dialog box appears. If an invalid file name is entered in the file name field, an error message appears, indicating the file does not exist.

Click **OK** to select another file, or click **Cancel** to close the dialog box. The **Trusted Certificate List** appears.

Note: If you click **Next** without adding any certificates to the list, and no certificates exist from a previous installation, a message appears indicating that if you do not specify any trusted certificates, HP Systems Insight Manager cannot access the HP Insight Management Agents on this system. Click **OK** if you do not want HP Systems Insight Manager to access the Insight Management Agents on this system, or click **Cancel** to close the dialog box and add the trusted certificates to the list.

Note: The **Trust By Certificates** option enables the System Management Homepage system and the HP Systems Insight Manager system to establish a trust relationship 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.

f. Click **Next**. The **IP Binding** dialog box appears.

● Trust By Name

a. Select **Trust By Name**.

b. Click **Next**. The **Trusted Server** dialog box appears.

Note: Although the **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 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 can prevent non-malicious access. For example, you might 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.

c. Enter the names of the servers you want to trust.

Note: The server name cannot contain the following characters: ~, !, ` , @, #, \$, %, ^, &, *, (,), +, =, ", :, ', <, >, ?, ,, |, and ;.

d. Click **Add** to add the name of a server you want to trust. The server name is displayed under **Trusted Server**. To delete a server name, click the **X** located next to the server name.

e. Click **Next**. The **IP Binding** dialog box appears.

Note: If you click **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 cannot access the Insight Management Agents on this system. Click **OK** to proceed without trusting any systems, or click **Cancel** to close the dialog box and add server names to the list.

Note: To delete a certificate, select the certificate and click **Delete**. The selected certificate is removed.

- Trust All
 - a. Select **Trust All**.
 - b. Click **Next**. The **IP Binding** dialog box 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. For example, you might want to use **Trust All** if you have a secure network, and everyone in the network is trusted.

8. Select **IP Binding** to enable the Subnet IP Address and NetMask.

The **IP Binding** dialog box enables you to bind to specific IP addresses that match a specific Subnet IP Address or NetMask. It restricts the subnet you want to manage.

- a. Enter the **Subnet IP Address** in the designated field.
- b. Enter the **NetMask** in the designated field.
- c. Click **Add**. The Subnet IP Address/NetMask is displayed in the dialog box. To delete a Subnet IP Address/Netmask, select a **Subnet IP Address/NetMask**, and click **Delete**. The Subnet IP Address/Netmask is deleted from the dialog box.

Note: You can add up to five Subnet IP Address/NetMask pairs.

9. Click **Next**. The **IP Restricted Logins** dialog box appears. The **IP Restricted Logins** dialog box enables you to select specific IP addresses or IP address ranges to include or exclude 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.

10. Select **IP Restricted Logins**.

- a. Enter the IP address or IP address range.
- b. Select to **Include** or **Exclude**.
- c. Click **Add**. The IP address or IP address range is displayed under the **Inclusion** or **Exclusion** list. To delete an IP address or IP address range, click the **X** located next to the IP address or IP address range. The IP address or IP address range is removed from the list.

Note: You can add as many IP addresses or IP address ranges as you want.

Note: If you enter an invalid IP address or IP address range, an error message is displayed indicating the IP address is invalid.

11. Click **Finish** to save the configurations for the component.

You can install this pre-configured component to target systems without the need to configure settings in the System Management Homepage after installation. For more information regarding using the ProLiant Remote Deployment Utility, refer to the *HP ProLiant Support Pack and Deployment Utilities User Guide*.

Chapter 7. Installing In-Place on Linux

This chapter provides steps to install System Management Homepage in-place on Linux IA-32 systems and x86-64 systems.

- “Installation for Linux on IA-32 and x86_64” (page 33)
 - “Installing System Management Homepage on Linux IA_32 Systems” (page 33)
 - “Installing System Management Homepage on x86_64” (page 34)
 - “Configuring System Management Homepage” (page 34)

The next chapter provides steps to install System Management Homepage in-place on Linux systems using the Linux Deployment Utility.

- “Installing System Management Homepage with Pre-configuration” (page 41)
 - “Pre-configuring the System Management Homepage Component” (page 41)
 - “Installing the System Management Homepage as a Single Component” (page 43)
- “Installing the System Management Homepage without Pre-configuration” (page 43)

Installation for Linux on IA-32 and x86_64

The System Management Homepage installation for Linux enables you to silently install the System Management Homepage on IA-32 and x86_64 systems. After the installation is complete, you can configure the System Management Homepage settings.

Note:



To install System Management Homepage, you must be logged in as root user.

Installing System Management Homepage on Linux IA_32 Systems

To install System Management Homepage on IA_32 systems, your system must meet the minimum requirements. For more information regarding minimum requirements, refer to

Chapter 2. *Installation Requirements*. In addition, you must have the `hpsmh-2.0.0.linux.i386.rpm`.

Note: The general 32-bit RPM List is not installed by default.

To install System Management Homepage, enter the following command line:

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

A message appears indicating the System Management Homepage installed successfully with default configuration values.

Installing System Management Homepage on x86_64

To install System Management Homepage on x86_64 systems, your system must meet the minimum requirements. For more information regarding minimum requirements, refer to

Chapter 2. *Installation Requirements* . In addition, you must have the `hpsmh-2.0.0-linux-release.x86_64.rpm`

Note: Red Hat Enterprise Linux 3 installs the 32-bit `compat-db-4.0.14-5.i386.rpm` by default on 64-bit systems. It displays in an rpm **query all** command, such as `compat-db-4.0.14-5`. Before installing System Management Homepage, ensure that the `compat-db-4.0.14-5.x86_64.rpm` is loaded from the distribution CD 3.

To verify 64-bit is loaded on Red Hat Linux 3:

Enter the following command:

```
rpm --qi --provides compat-db-4.0.14-5 | grep libdb-
```

If x86_64 bit is installed, `libdb-4.0.so() (64bit)` is displayed.

To install System Management Homepage, enter the following command line:

```
rpm -ivh hpsmh-2.0.0-linux-release.x86-64.rpm
```

A message appears indicating the System Management Homepage installed successfully with default configuration values.

Configuring System Management Homepage

After the System Management Homepage is installed, you can configure the settings. If you are migrating from Management HTTP Server, the Management HTTP Server settings are retained. However, the retained settings are configurable.

To configure System Management Homepage settings:

1. Enter the following command line to start the configuration:

```
perl /usr/local/hp/hpSMHSetup.pl
```

The **Welcome** screen appears.

2. The Welcome screen indicates that you can configure security and access parameters on the following screens.

Press **Enter**. The **Operating System Groups** screen appears.

3. The **Operating System Groups** screen enables you to add operating system groups to System Management Homepage.

The following options are available:

- 1 - Add Groups

To add groups:

1. At the prompt, enter **1** to add a group. The **Add Operating System Groups** screen displays the operating system group lists.

Note: You can add up to five entries per group.

Enter one of the following options to assign the operating system group to the Administrator Group List:

- Enter **1** for Administrator.

For example, to add **admin1** to the **Administrator** operating system group:

1. Enter **1** for Administrator.
2. At the prompt, **Enter the name of the operating system group:**, enter **admin1**.
3. Press **Enter**. **admin1** is displayed in the **Administrator Group List**.
4. Enter **n** to go to the next screen.

- Enter **2** for Operator.

- Enter **3** for User.

2. Enter **n** to go to the next screen.

- 2 - Delete Groups

To delete a group:

1. Enter **2** to delete a group.

The following options are available:

- Enter **1** for Administrator. The **Administrator Group List** is displayed.
- Enter **2** for Operator. The **Operator Group List** is displayed.

- Enter **3** for User. The **User Group List** is displayed.
- 2. At the prompt, enter **1**, **2**, or **3**.
- 3. Enter the number next to the group name to be deleted. The group is deleted from the group list.
Note: You can delete as many groups as needed by repeating the applicable step below.
- 4. Press **Enter** when you are finished deleting to go to the next screen.
- 5. Enter **n** to go to the next screen. The **Operating System Groups** screen is displayed.
- 6. Enter **n** to go to the next screen. The **User Access** screen appears.

4. The **User Access** screen enables you to configure Local and Anonymous Access

The following options are available:

- Enter **1** to enable **Anonymous Access**.

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

- Enter **2** to disable **Anonymous Access**.

- Enter **3** to disable **Local Access**.

- Enter **4** to enable **Local Access - Anonymous**. **Local Access** enables you to locally gain access to the System Management Homepage without being challenged for authentication. 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.

- Enter **5** to enable **Local Access - Administrator**. This option grants full access to secure and unsecure pages. This means that any user with access to the local console is granted full access.

5. Enter **n** to go to the next screen or enter **p** to go to the previous screen.

6. Enter **n** to go to the next screen. The **Trust Mode** screen is displayed.

7. The **Trust Mode** screen enables you to configure the System Management Homepage trust mode.

The following options are available:

- Enter **1** to **Trust by Certificate**. **Trust Mode:Trust by Certificate** is displayed.

The following options are available:

- 1 - Trust by Certificate

The following options are available:

□ 1 - Add File

To add a certificate file:

1. Enter **1**. You are prompted for the certificate location.
2. Enter the file path of the trusted certificates to be added to the **Trusted Certificates List**. Press **Enter** when you are finished.

For example:

1. **File:** `/home/ServerName/cert1.pem` .
2. Press **Enter**. The `cert1.pem` is added to the **Trusted Certificates List**.

If the certificate file does not exist, a message is displayed indicating the `/home/ServerName/cert1.pem` does not exist.

3. You can add as many certificates as you want by repeating these steps. Press **Enter** when you are finished adding certificate files.

□ 2 - Import

To import a certificate:

1. Enter **2**. You are prompted for the server name.
2. Enter the name of the HP Systems Insight Manager server and press **Enter**. The certificate is retrieved and displayed.

The following options are available:

- Enter **1** to accept the certificate. The file is saved.
- Enter **2** to reject the certificate. The file is not imported.

3. Press **Enter** when you are finished. The imported certificates display in the **Trusted Certificates List**. You can import as many certificates as you want by repeating these steps.
4. Press **Enter** when you are finished importing certificate files.

□ 3 - Delete

1. Enter **3**. You are prompted to enter the number associated with the certificate file to be deleted.
2. Enter the number of the certificate file to be deleted.
3. Press **Enter** when you are finished. You can delete as many certificate files as you want by repeating these steps.

4. Press **Enter** when you are finished deleting certificate files.

○ 2 - Trust by Name

1. Enter **2** to **Trust by Name**. **Trust Mode: Trust by Name** is displayed.

2. Enter **4** to **Modify Server Name** list.

To add an HP Systems Insight Manager server name:

a. Enter **1**. You are prompted to add an HP Systems Insight Manager server.

b. Enter the name of the HP Systems Insight Manager server to be trusted and press **Enter**. The server name is displayed in the **Trusted Server Names** list.

Note: You can add as many servers as you want.

To delete a server name:

i. From the **Server Name** list, enter **2**.

ii. Enter the number associated with the name of the server to be deleted. The server name is removed from the **Server Name** list.

c. Enter **n** for next. The **IP Binding** screen is displayed.

○ 3 - Trust All

1. Enter **3** to **Trust All**. **Trust Mode: Trust All** is displayed.

2. Press **Enter**.

3. Enter **n** for next. The **IP Binding** screen is displayed.

8. The **IP Binding** screen enables you bind IP addresses that match a subnet and netmask.

The following options are available:

● 1 - Enable IP Binding

1. Enter **1** to enable the IP Binding, which sets it to **ON**. **IP Binding: ON** is displayed.

2. Enter **n** to go to the next screen.

The following options are available:

○ 1 - Add

To add an IP address:

1. Enter **1** to add an IP address. You are prompted for the IP address.

2. Enter the IP address to be added. **IP Address: YourIPAddress** is displayed. You are prompted for the netmask.
3. Enter the netmask. **netmask: YourNetmask** is displayed.

Note: You can add or delete as many IP addresses as you want.

To delete an IP address:

- a. Enter **2**.
 - b. Enter the number of the IP address or netmask ask to be deleted. The IP address or netmask is removed from the IP address or netmask list.
4. Enter **n** to go to the next screen. The **IP Restricted Logins** screen is displayed.

● 2 - Disable IP Binding

1. Enter **2** to disable the IP Binding, which sets it to **OFF**. **IP Binding: OFF** is displayed.
2. Enter **n** to go to the next screen or enter **p** to go to the previous screen. The **IP Restricted Logins** screen is displayed.

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

The following options are available:

- Enter **1** to enable IP Restricted Logins, which sets it to **ON**. **IP Restricted Logins:OFF** is displayed.

To enable the IP Restricted Logins:

1. Enter **1**. **IP Restricted** is set to **ON**.
2. Press **Enter** for next. The **Set IP Address Restrictions** screen is displayed.

To add IP addresses to the Inclusion List:

- a. Enter **1** for **Include Login Restriction IP Address**.
- b. Enter **1** for **Add**.
- c. Enter the IP address or IP address range you want to add to the Inclusion List. The IP address or IP address range is displayed under the **IP Address Inclusion List**.

Note: You can add or delete as many IP addresses or IP address ranges as you want.

To delete an IP address or IP address range:

- i. Enter **2**.
 - ii. Enter the number associated with the IP address or IP address range to be deleted and press **Enter**. The IP address or IP address range is deleted from the **Inclusion List**.
- d. Enter **n** for next.
- Enter **2** to disable IP Restricted Logins, which sets it to **OFF**. **IP Restricted Logins: OFF** is displayed.

To disable IP Restricted Logins:

- Enter **2** to disable the IP Restricted Logins. The IP Restricted Logins is set to **OFF**.

To add an IP address or IP address range to the Exclusion List:

- a. Enter **1** to add an IP address to the Exclusion List.
- b. Enter the IP address or IP address range to be added to the Exclusion List. The IP address or IP address range is added in the **IP Address Exclusion List**.
- c. Enter **n** for next.

Note: You can add or delete as many IP addresses or IP address ranges as you want.

To delete an IP address or IP address range from the Exclusion List:

1. Enter **2** to delete an IP address from the Exclusion List.
2. Enter the number associated with the IP address or IP address range to be deleted. Press **Enter**. The IP address is deleted from the **IP Address Exclusion List**.

10. Enter **n** to go to the next screen. The configuration completes, and a message is displayed indicating the System Management Homepage is successfully set up. The System Management Homepage service is stopped and started automatically.
11. Verify the System Management Homepage is configured and working properly by navigating to it and verifying that it displays correctly.

Chapter 8. Installing In-Place on Linux Using Linux Deployment Utility

This chapter provides steps to install System Management Homepage in-place on the Linux operating system using the Linux Deployment Utility.

- “Installing System Management Homepage with Pre-configuration” (page 41)
 - “Pre-configuring the System Management Homepage Component” (page 41)
 - “Installing the System Management Homepage as a Single Component” (page 43)
- “Installing the System Management Homepage without Pre-configuration” (page 43)

The previous chapter provides steps to install System Management Homepage in-place on Linux IA-32 systems and x86-64 systems.

- “Installation for Linux on IA-32 and x86_64” (page 33)
 - “Installing System Management Homepage on Linux IA_32 Systems” (page 33)
 - “Installing System Management Homepage on x86_64” (page 34)
 - “Configuring System Management Homepage” (page 34)

Installing System Management Homepage with Pre-configuration

The Linux Deployment Utility provides an easy and efficient method to upgrade and manage system software. The utility enables you to deploy and maintain ProLiant Support Pack software on local servers through use of the terminal window and on remote servers through use of the ssh (secure shell) utility. The Linux Deployment Utility is shipped with the Linux ProLiant Support Pack, which is available on the SmartStart CD. The Linux Deployment Utility enables you to install components or ProLiant Support Packs in-place, but not remotely.

The Linux Deployment Utility parses the .XML files associated with each component and verifies whether the installation of those components is supported on the specific environment. The components that are supported for installation are listed with a status icon indicating whether the component should to be installed, and whether it should be configured. Configuring or pre-configuring the System Management Homepage component is optional.

Pre-configuring the System Management Homepage Component

Note: All pre-configuration settings are saved in the component XML file.

To pre-configure the System Management Homepage component:

1. Run the `install1720.sh` script. The **HP ProLiant Linux Deployment Utility** screen is displayed asking you to wait while component XML files are parsed.
2. Under **Component Name**, select **HP System Management Homepage for Linux**.
3. Right-click **HP System Management Homepage for Linux** and select **Configure Component**. The **Configuration Option** screen is displayed.
4. In the **Please enter the Operating System (OS) Group Names for Administrator level access. (Max 5 names, separated by semicolon or space)** field, enter the operating system group name for administrator-level access.
Note: You can enter up to 5 operating system group names for administrator-level access. Separate the group names with a semicolon (;) or space.
5. In the **Please enter the Operating System (OS) Group Names for operator-level access. (Max 5 names, separated by semicolon or space)** field, enter the operating system group name for operator-level access.
Note: You can enter up to 5 operating system group names for operator-level access. Separate the group names with a semicolon (;) or space.
6. In the **Please enter the Operating System (OS) Group Names for user-level access. (Max 5 names, separated by semicolon or space)** field, enter the operating system group name for user-level access.
Note: You can enter up to 5 operating system group names for user-level access. Separate the group names with a semicolon (;) or space.
7. In the **Allow Local Access** field, enter **YES** to allow local access or **NO** to disallow local access.
8. Select the local access type, **Anonymous** or **Administrator**, from the **Local Access Type** dropdown menu.
9. In the **Allow Anonymous Access** field, enter **YES** to allow anonymous access or **NO** to disallow anonymous access.
10. Select the trust mode from the **Trust Mode** dropdown menu.
 - If you selected **TrustByCer** from the **Trust Mode** dropdown menu, enter the names of the certificate files and separate multiple entries with a semicolon in the **List of File or Host names separated by semicolon** field. For example, `cert.pem;cert2.pem;ServerName` .
 - If you selected **TrustByName** from the **Trust Mode** dropdown menu, enter the names of the trusted servers and separate multiple entries with a semicolon in the **Server Names** field. For example, `Server1;Server2`.
11. In the **IP Binding** field, enter **YES** to enable IP Binding or **NO** to disable IP Binding.
12. In the **IP Binding List** field, enter the IP address and netmask and separate multiple pairs by a semicolon. For example, `IPAddress1/Netmask1;IPAddress2/Netmask2`.

13. In the **Enable IP restricted logins** field, enter **YES** to enable IP restricted logins or **NO** to disable IP restricted logins.
14. In the **IP Binding List** field, enter the IP address and netmask pairs separated by semicolons. For example, **IPAddress1/Netmask1; IPAddress2/Netmask2**.
15. In the **Enable IP restricted logins** field, enter **YES** to enable IP restricted logins or **NO** to disable IP restricted logins.
16. In the **Enter include IP Addresses, or ranges** field, enter the IP addresses or range of IP address to be included.
17. In the **Enter exclude IP Addresses, or ranges** field, enter the IP addresses or range of IP address to be excluded.
18. Click **Save** to save your configuration. Click **Cancel** to discard your configuration.
19. Click **OK** to close the **HP ProLiant Linux Deployment Utility Utility** screen.
20. After pre-configuration is complete, installation can be initiated through the Linux Deployment Utility as part of the complete ProLiant Support Pack or the single component can be installed independently.

Installing the System Management Homepage as a Single Component

You can install the System Management Homepage independently of other components included in the ProLiant Support Pack.

To install the System Management Homepage as a single component:

1. Select all components except the System Management Homepage component.
2. Right-click all other components and select **Do Not Install component**. The System Management Homepage component can also be installed by invoking the following command from the shell prompt: `./install###.sh -c hpsmh>version<.linux.i???.rpm`.
3. This process installs the component with the configurations that are provided through the Linux Deployment Utility.

For more information regarding using the Linux Deployment Utility, refer to the *HP ProLiant Support Pack and Deployment Utilities User Guide*.

Installing the System Management Homepage without Pre-configuration

You can install the System Management Homepage component without any configurations by clicking **Install**. You can configure the System Management Homepage settings at any time by logging into the System Management Homepage with root privileges.

Chapter 9. Initializing the Software for the First Time

This chapter provides an overview of how to initialize the System Management Homepage.

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 HP-UX, both public and private keys for the System Management Homepage are stored in the `/var/opt/hpsmh/sslshare` directory. The files are called `file.pem` (private key) and `cert.pem` (server certificate).
- 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`.
- In Windows, public and private keys are stored in the `\hp\sslshare` directory of the system drive.

To protect the key, this subdirectory is only accessible to administrators if the file system allows such security. For private key security reasons, HP highly recommends that Windows installations of the System Management Homepage be installed on New Technology File System (NTFS).

Important:



For Windows operating systems, the file system must be NTFS for the private key to have administrator only access through the file.

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 occur the first time the System Management Homepage is started or when no certificate and key pair exists.

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.

Chapter 10. Logging In and Logging Out of System Management Homepage

This chapter provides browser and command line instructions for logging in to System Management Homepage and for logging out.

- “Logging In with Windows XP” (page 45)
- “Logging In with Internet Explorer” (page 45)
- “Logging In with Mozilla” (page 47)
- “Logging In from the HP-UX Command Line” (page 48)
- “Logging Out” (page 48)

Logging In with Windows XP

If the System Management Homepage is installed on a Windows XP system, the following security option must be enabled to log into the System Management Homepage:

1. Select **Control Panel->Administrative Tools Local Security Policy**. The **Local Security Settings** dialog box appears.
2. Select **Local Policies**.
3. Select **Security Options**.
4. Right-click **Network Access: Sharing & Security model for local Accounts to Classic from Guest Only** and select **Security...**. The **Local Security Policy Setting** dialog box appears.
5. Select **Enabled**.
6. Click **OK** to save your settings and close the **Local Security Policy Setting** dialog box.

Logging In with Internet Explorer

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

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

To avoid an active scripting error, HP recommends that you add the System Management Homepage URL to Internet Explorer's Trusted Sites.

To add the System Management Homepage to Internet Explorer's Trusted Sites:

1. From Internet Explorer, click **Tools->Internet Options**.

2. Select the **Security** tab. The Security tab appears.
3. Select the **Trusted sites** icon.
4. Click **Sites....** The Trusted sites dialog box appears.
5. In the **Add this Web site to the zone** field, enter `https://hostname:2381/` and click **Add**.
6. Click **OK** to save your changes and close the Trusted sites dialog box.
7. Click **OK** to close the Internet Options dialog box.

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 previous chapters of this guide.

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.

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 the *System Management Homepage Online Help*.

3. Click **Yes**.

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 **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. 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.

Logging In with Mozilla

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 previous chapters of this guide.

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. 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.

Logging In from the HP-UX Command Line

You can check whether the autostart daemon is running with the command:

```
$ ps -ef | grep smh
  root 1789      1  0  Mar 31  ?        0:00 /opt/hpsmh/lbin/smhstartd
```

If the daemon is not running, you can start it from the HP-UX command line using `/opt/hpsmh/lbin/hpsmh autostart`, then use a Web browser to navigate to `http://hostname:2381`.

You can also use the `samweb` command to automatically start the default browser in the main System Management Homepage page.

After the daemon is running and the HP-UX Apache-based Web Server is started with autostart, you can log in to System Management Homepage with either `http://hostname:2301` or `http://hostname:2381`.

Note:



If the autostart daemon is not configured (see the `smhstartconfig -a off -b on`), use the command `/opt/hpsmh/lbin/hpsmh start` instead to start the HP-UX Apache-based Web Server on ports 2301 (http) and 2381 (https).

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**.
- Close every instance of the Web browser that you used to log in to System Management Homepage.
- You can stop the System Management Homepage from the HP-UX command line:
`/opt/hpsmh/lbin/hpsmh stop`

This will not stop the mini-daemon `smhstartd`, but will stop the HP-UX Apache-based Web Server. The next time you contact System Management Homepage via `http://hostname:2301`, the HP-UX Apache-based Web Server will again start up on port 2381 (https). If autostart is configured, the HP-UX Apache-based Web Server times out automatically after 30 minutes (default setting).

Chapter 11. Uninstalling the System Management Homepage

This chapter provides instructions on how to uninstall System Management Homepage from HP-UX, Linux, and Windows systems. It also provides instruction on how to uninstall it manually.

- “Uninstalling from an HP-UX System” (page 49)
- “Uninstalling from a Linux IA-32 or x86_64 System” (page 49)
- “Uninstalling from a Windows System” (page 49)
- “Uninstalling Manually for Windows Systems” (page 50)
- “Uninstalling from Multiple Windows Systems Silently” (page 49)

Uninstalling from an HP-UX System

To uninstall the System Management Homepage, use the **swremove** command: `# swremove SysMgmtWeb`

Uninstalling from a Linux IA-32 or x86_64 System

To uninstall the System Management Homepage:

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

Or run: `rpm -e hpsmh`

Uninstalling from a Windows System

Use the **Add/Remove Programs** feature in Windows, and complete the following steps to remove System Management Homepage:

1. **Select Start->Control Panel Add or Remove Programs.**
2. Select **System Management Homepage.**
3. Click **Remove.** The **System Management Homepage** is uninstalled.

Uninstalling from Multiple Windows Systems Silently

You can write a script to uninstall System Management Homepage silently on multiple Windows systems simultaneously. To uninstall the System Management Homepage for Windows silently, you

must use your existing `setup.iss` file or you must generate one before proceeding with the silent uninstall.

To uninstall silently using the CLI:

```
setup.exe /s /removeonly /f1<full_path_to_setup.iss_file>
```

Uninstalling Manually for Windows Systems

Uninstalling manually duplicates the actions of the System Management Homepage uninstaller, which can be accessed through **Add/Remove Programs** in the **Control Panel**. Use this procedure if you wish to completely uninstall the System Management Homepage, and the uninstaller has been inadvertently removed or corrupted.

Note: Items marked *if present* are present if there is an existing System Management Homepage 2.0.1 or 2.0.2 installation.

Caution:



All System Management Homepage configuration settings will be lost after uninstalling manually!

To manually uninstall the System Management Homepage:

1. Stop the System Management Homepage service.
2. Remove the following directories and file on the system drive:
 - `\hp\hpsmh\csicon.ico`
 - `\hp\hpsmh_jvm` (if present)
 - `\hp\hpsmh_uninst`, and any other directory beginning with `_uninst` (if present)
 - `\hp\hpsmh\certs`
 - `\hp\hpsmh\conf`
 - `\hp\hpsmh\include`
 - `\hp\hpsmh\lib`
 - `\hp\hpsmh\logs`
 - `\hp\hpsmh\modules`
 - `\hp\hpsmh\namazu`
 - `\hp\hpsmh\session\`

- a. If the HP Version Control Agent and/or the HP Version Control Repository Manager is installed on the system, remove all files and directories under `\hp\hpsmh\bin` except `libeay32.dll` and `ssleay32.dll`.
 - b. If the Version Control Agent, Version Control Repository Manager, or both are not installed on the system, remove the entire `\hp\hpsmh\bin` directory.
3. Delete the following registry keys:
- `\HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\System Management Homepage`
 - `\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\System Management Homepage (if present)`
 - `\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{3C4DF0FD-95CF-4F7B-A816-97CEF616948F}`
 - `\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\System\HP System Management Homepage`
 - `\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SysMgmtHP`

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

console install
Linux, 33
conventions, typographic, 3
copyright notices, 2

G

getting started, 15
government license, 2

H

HP-UX
install, 16

I

initial setup, 15
initialize software, 44
install
HP-UX, 16
Linux, 41
Linux IA_32, 33
Linux x86_64, 33
operating systems, 7
ProLiant Remote Deployment Utility, 29
requirements, 7
RPMs on AMD64 and EM64T, 11
RPMs on IA-32, 9
RPMs on Itanium, 11
verify requirements, 13
web browsers, 8
Windows, 23, 29
Itanium
RPMs, 11

L

legal notices, 2
Linux
install, 33
Linux Deployment Utility install, 41
Linux IA_32
install, 33
Linux x86_64
install, 33
logging in, 45
logging out, 45

M

media

System Management Homepage, 13

O

operating systems
supported, 7
overview
System Management Homepage, 6

P

product overview, 6
ProLiant Remote Deployment Utility
install, 29
publication history, 2

R

remove System Management Homepage , 49
remove System Management Homepage on Linux
IA-32
remove System Management Homepage on Linux,
49
remove System Management Homepage on Windows,
49
removing, 49
requirements
install, 7
verify, 13
revision history, 3
RPMs
supported, 9, 11

S

setup, 15
software, 44
System Management Homepage, 13
System Management Homepage
HP-UX install, 16
install requirements, 7
Linux Deployment Utility install, 41
Linux install, 33, 41
logging in, 45
logging out, 45
media, 13
operating systems, 7
overview, 6
ProLiant Remote Deployment Utility install, 29
RPMs on AMD64, 11
RPMs on EM64T, 11
RPMs on IA-32, 9
RPMs on Itanium, 11
setup, 15
software, 13, 44
uninstall, 49

- verify install requirements, 13
- web browsers, 8
- web sites, 13
- Windows install, 23, 29

T

- trademark notices, 2
- typographic conventions, 3

U

- uninstalling, 49

W

- warranty, 2
- web browsers
 - supported, 8
- web sites
 - System Management Homepage, 13
- Windows
 - install, 23
 - install ProLiant Remote Deployment Utility, 29