HP System Management Homepage Installation Guide

HP-UX, Linux and Windows Systems

HP Part Number: 438862-007
Published: December 2007
Edition: 14

Legal Notices

Trademark Notices

Table of Contents

About this document

Intended audience

The HP System Management Homepage (HP SMH) is a web-based interface that consolidates and simplifies single system management for HP servers on HP-UX, Linux, andMicrosoft® Windows® operating systems. This installation guide is for system administrators who are installing HP SMH.

New and changed information in this edition

To review what is new and changed in this release of HP SMH, see the *HP System Management Homepage Release Notes* on the HP Technical Documentation web site at http://docs.hp.com.

Typographic conventions

find(1)	HP-UX manpage. In this example, "find" is the manpage name and "1" is the manpage section.
Book Title	Title of a book or other document.
Linked Title	Title that is a hyperlink to a book or other document.
http://www.hp.com	A Web site address that is a hyperlink to the site.
`Command`	Command name or qualified command phrase.
`user input`	Commands and other text that you type.
`computer output`	Text displayed by the computer.
Enter	The name of a keyboard key. Note that **Return** and **Enter** both refer to the same key. A sequence such as **Ctrl+A** indicates that you must hold down the key labeled **Ctrl** while pressing the **A** key.
term	Defined use of an important word or phrase.
`variable`	The name of an environment variable, for example `PATH` or `errno`.
`value`	A value that you may replace in a command or function, or information in a display that represents several possible values.
`<element>`	An element used in a markup language.
`attrib=`	An attribute used in a markup language.

Document organization

The install guide is organized as follows:

Related information

This section lists the HP SMH documentation and related HP documentation.

HP SMH documentation

For more information regarding HP SMH, refer to the following sources:

- ***HP System Management Homepage Release Notes*** The release notes provide documentation for what's new with the release, features and change notifications, system requirements, and known issues. The release notes are available on the HP Technical Documentation Web site at http://docs.hp.com.
- **HP System Management Homepage Help System** The help system provides a complete set of documentation for using, maintaining, and troubleshooting HP SMH. In the HP SMH application, go to the **Help** menu.
- ***HP System Management Homepage Installation Guide*** The install guide provides information about installing and getting started using HP SMH. It includes an introduction to basic concepts, definitions, and functionality associated with HP SMH. The install guide is available on the HP Technical Documentation web site at http://docs.hp.com. Also, for Linux and Windows releases, the install guide is available on the Management CD and at the HP SMH web page at http://h18013.www1.hp.com/products/servers/management/agents/documentation.html.
- ***HP System Management Homepage User Guide*** The user guide provides a complete set of documentation for using, maintaining, and troubleshooting HP SMH. For Linux and Windows, this user guide is available under the HP SMH Help menu, and on the HP Technical Documentation web site at http://docs.hp.com. For HP-UX, we no longer provide a printed user guide, please refer to the HP SMH online help content for information on how to use, maintain, and troubleshoot HP SMH.
- **Next generation single-system management on HP-UX 11i v2 (B.11.23)** A white paper that introduces HP SMH and its various plug-ins. The use cases involving HP SMH plug-ins described in this document highlight the features provided by HP SMH. The white paper is available on the HP Technical Documentation web site at http://docs.hp.com/en/4AA0-4052ENW/4AA0-4052ENW.pdf.
- ***hpsmh* (1m) manpage** For HP-UX releases, the manpage is available from the command line using the `man hpsmh` command. This information is not available for Linux and Windows.
- ***smhstartconfig* (1M) manpage** For HP-UX releases, the manpage is available from the command line using the `man smhstartconfig` command. This information is not available for Linux and Windows.
- ***sam*(1M) manpage** For HP-UX releases, the manpage is available from the command line using the `man sam` command. This information is not available for Linux and Windows. Please note the SAM functionality changes in Chapter 4: "Installing on HP-UX" (page 19).
- ***smh* (1m) manpage** This command is available in HP-UX 11i v3 (B.11.31) only. This is an enhanced version of the *sam*(1m) command. For HP-UX releases, the manpage is available from the command line using the `man smh` command. This information is not available for Linux and Windows.
- **HP System Management Homepage web site** The web site provides HP SMH information and product links. Go to the HP web site at http://www.hp.com or to the Software Depot

home at http://www.hp.com/go/softwaredepot and search for System Management Homepage.

- **HP ProLiant Essentials software page** This web page is at http://www.hp.com/servers/manage.

Related documentation

For more information relating to HP SMH, refer to the following sources. They are available on the Instant Information DVD and on the HP Technical Documentation web site at http://docs.hp.com.

- **HP-UX 11i Installation and Update Guides (v1, B.11.11; v2, B.11.23; v3 B.11.31)** Provide instructions on how to install or update to HP-UX.
- **HP-UX 11i Release Notes (v1, B.11.11; v2, B.11.23; v3 B.11.31)** Describe new features and functionality changes for HP-UX 11i, including information on HP SMH.

NOTE: For HP-UX release documentation, check for the latest version on http://docs.hp.com.

Publishing history

This section provides the publishing history of the document.

Manufacturing Part Number	Supported Operating Systems	Supported Versions	Edition Number	Publication Date
438862-007	Linux and Windows	See "Installation requirements" (page 11).	14	December 2007
438862-006	HP-UX	HP-UX 11i v3 (B.11.31), HP-UX 11i v2 (B.11.23), HP-UX 11i v1 (B.11.11)	13	September 2007
438862-005	Linux and Windows	See "Installation requirements" (page 11).	12	August 2007
438862-004	Linux and Windows	See "Installation requirements" (page 11).	11	June 2007
438862-003	HP-UX	HP-UX 11i v2 (B.11.23), HP-UX 11i v1 (B.11.11)	10	June 2007
438862-002	Linux and Windows	See "Installation requirements" (page 11).	9	April 2007
381372-009	HP-UX	HP-UX 11i v3 (B.11.31)	8	February 2007
438862-001	Linux and Windows	See "Installation requirements" (page 11).	7	January 2007
381372-008	HP-UX	HP-UX 11i v2 (B.11.23), HP-UX 11i v1 (B.11.11)	6	December 2006
381372-007	HP-UX	HP-UX 11i v2 (B.11.23), HP-UX 11i v1 (B.11.11)	5	September 2006

Manufacturing Part Number	Supported Operating Systems	Supported Versions	Edition Number	Publication Date
381372-006-en	HP-UX, Linux, and Windows	For HP-UX: HP-UX 11i v2 (B.11.23), HP-UX 11i v1 (B.11.11). For Linux and Windows: See "Installation requirements" (page 11).	4	June 2006
381372-005	Linux and Windows	See "Installation requirements" (page 11).	4	February 2006
381372-004-en	HP-UX	HP-UX 11i v2 (B.11.23), HP-UX 11i v1 (B.11.11)	3	December 2005
381372-002	HP-UX	HP-UX 11i v2 (B.11.23), HP-UX 11i v1 (B.11.11)	2	September 2005
381372-002	HP-UX	HP-UX 11i v2 (B.11.23), HP-UX 11i v1 (B.11.11)	2	May 2005
381372-001	Linux and Windows	See "Installation requirements" (page 11).	1	November 2004

HP encourages your comments

HP encourages your comments concerning this document. HP is committed to providing documentation that meets your needs. Send any errors found, suggestions for improvement, or compliments to: **feedback@fc.hp.com**. Include the document title, manufacturing part number, and any comment, error found, or suggestion for improvement you have concerning this document.

1 Product overview

The HP System Management Homepage (HP SMH) is a web-based interface that consolidates and simplifies single system management for HP servers running the HP-UX, Linux, and Microsoft Windows operating systems. HP SMH 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.

HP SMH 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.

Product features

HP SMH provides the following enhanced security and streamlined operations for HP servers running HP-UX, Linux, and Windows.

- Browser access using operating system-based SSL-secure authentication
- Common HTTP and HTTPS service for HP Insight 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

2 Installation requirements

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

Supported operating systems

HP SMH supports the following operating systems for the HP-UX, Linux, and Windows systems:

- HP-UX 11i v3 (B.11.31) for HP Integrity Servers and HP 9000 Servers
- HP-UX 11i v2 (B.11.23) for HP Integrity Servers and HP 9000 Servers
- HP-UX 11i v1 (B.11.11) for HP Servers and Workstations
- Red Hat Enterprise Linux 5.0 for x86 Update 1
- Red Hat Enterprise Linux 5.0 for AMD64 and Intel EM64T Update 1
- Red Hat Enterprise Linux 5.0 for AMD64 and x86 Update 1
- Red Hat Enterprise Linux 5.0 for Itanium Linux Update 1
- Red Hat Enterprise Linux 5.0 for x86
- Red Hat Enterprise Linux 5.0 for AMD64 and Intel EM64T
- Red Hat Enterprise Linux 5.0 for AMD64 and x86
- Red Hat Enterprise Linux 5.0 for Integrity Linux
- Red Hat Enterprise Linux 4.0 for x86, Update 6
- Red Hat Enterprise Linux 4.0 for AMD64 and EM64T, Update 6
- Red Hat Enterprise Linux 4.0 for AMD64 and x86 Update 6
- Red Hat Enterprise Linux 4.0 for Itanium Linux, Update 6
- Red Hat Enterprise Linux 4.0 for x86, Update 5
- Red Hat Enterprise Linux 4.0 for AMD64 and EM64T, Update 5
- Red Hat Enterprise Linux 4.0 for AMD64 and x86 Update 5
- Red Hat Enterprise Linux 4.0 for Integrity Linux, Update 5
- Red Hat Enterprise Linux 4.0 for x86, Update 4
- Red Hat Enterprise Linux 4.0 for AMD64 and EM64T, Update 4
- Red Hat Enterprise Linux 4.0 for AMD64 and x86 Update 4
- Red Hat Enterprise Linux 4.0 for Integrity Linux, Update 4
- SUSE Linux Enterprise Server 10 for x86
- SUSE Linux Enterprise Server 10 for AMD64 and Intel EM64T
- SUSE Linux Enterprise Server 10 for Itanium Linux
- SUSE Linux Enterprise Server 10 for x86 Service Pack 1
- SUSE Linux Enterprise Server 10 for AMD64 and Intel EM64T Service Pack 1
- SUSE Linux Enterprise Server 10 for Itanium Linux, Service Pack 1
- SUSE Linux Enterprise Server 9 for x86, Service Pack 4

- SUSE Linux Enterprise Server 9 for AMD64 and Intel EM64T, Service Pack 4
- SUSE Linux Enterprise Server 9 for Itanium Linux, Service Pack 4
- SUSE Linux Enterprise Server 9 for x86, Service Pack 3
- SUSE Linux Enterprise Server 9 for AMD64 and Intel EM64T, Service Pack 3
- SUSE Linux Enterprise Server 9 for Integrity Linux, Service Pack 3
- Novell Open Enterprise Server (OES) with Service Pack 1 or later
- ESX 3.0
- ESX 3.0.1
- ESX 3.0.2
- ESX 3.1
- Microsoft Windows Server 2003 SP2
- Microsoft Windows 2003 R2 Datacenter Edition (DCE)
- Microsoft Windows Server 2003 R2 SBS
- 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 Web Edition
- Microsoft Windows Server 2003, Enterprise Edition for Itanium-based Systems
- Microsoft Windows Server 2003, Datacenter Edition for Itanium-based Systems
- Microsoft Windows XP
- Microsoft Windows Server 2008
- Microsoft Windows Vista
- XenSource

NOTE: For Linux, the Lightweight Directory Access Protocol (LDAP) is supported on SUSE Linux Enterprise Server 9.

For Windows, the SmartStart CD requires that 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. The HP-UX 11i v2 (B.11.23) Operating Environments (September 2004 and later) and HP-UX 11i v3 (B.11.31) Operating Environments (February 2007 and later) support both PA-RISC and Itanium systems.

Supported browsers

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

For HP-UX Itanium or PA-RISC systems that are connecting to any server type or for HP-UX servers that display to any desktop via X, you can use the following desktop browsers :

- Mozilla 1.6, 1.7
- Firefox 1.0.2, 1.5, 2.0

For Windows Itanium or x86 systems that are connecting to any server type, you can use the following desktop browsers:

- Internet Explorer 6.0, 7.0
- Mozilla 1.5, 1.6, 1.7
- Firefox 1.0.2, 1.5, 2.0

For Linux Intel Itanium or x86 systems that are connecting to any server type, you can use the following desktop browsers:

- Mozilla 1.5, 1.6, 1.7
- Firefox 1.0.2, 1.5, 2.0

NOTE: Installation of HP SMH 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 x86 platform

HP SMH supports the following Red Hat Package Managers (RPM) for each of the Linux operating systems on the x86 platform.

Operating system	RPM
SUSE Linux Enterprise Server 10 (x86)	• glibc 2.3.90 or later • pam 0.99 or later • perl 5.8.8 or greater • zlib 1.2.3 or greater
SUSE Linux Enterprise Server 9 (x86)	• 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 Enterprise Linux 4.0 (x86)	• 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

HP SMH supports the following RPMs for each of the Linux operating systems on the AMD64 and EM64T platform.

Operating system	RPM
SUSE Linux Enterprise Server 9 (AMD64 and EM64T)	• 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 4.0 (AMD64 and EM64T)	• 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 Itanium platform

HP SMH supports the following RPMs for each of the Linux operating systems on the Itanium platform.

Operating system	RPM
Red Hat Enterprise Linux 4.0 and 5.0 (Integrity platforms)	• glibc-2.3.4 • j2sdk-1-4-2 (version 2.1.7 and earlier) • jrockit-R27.1.0-jdk1.5.0 • net-snmp-utils-5.1.2-11.EL4.6hp • net-snmp-perl-5.1.2-11.EL4.6hp • openssl-0.9.7a-43.8 or greater • pam-0.77-66.14 or greater • perl-5.8.5 or greater
SUSE Linux Enterprise Server 9 and 10 for Integrity Linux	• glibc-2.3.3 or greater • j2sdk-1-4-2 (version 2.1.7 and earlier) • jrockit-R27.1.0-jdk1.5.0 • openssl-0.9.7d-15 or greater • net-snmp-5.1-80.16hp • pam-0.77-221 • perl-5.8.3 • zlib-1.2.1-70 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.

The IPF is an Intel Itanium 64-bit processor.

Verifying system requirements

Before installation begins, the installation utility verifies whether:

- For HP-UX, Linux, and Windows, the operating system meets the minimum requirements. If HP SMH does not support the operating system on a system, an error message appears, indicating that an invalid operating system is found.
- For HP-UX, Linux, and 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.
- For Linux, during a Linux installation on an x86 platform, if the Linux dependencies are not met, the missing dependencies are displayed.
- For Linux, if a dependency is not met on an Itanium platform, the installation will not complete.

Obtaining the HP SMH software

You can obtain HP SMH software from the following HP media and web sites:

HP media

HP SMH is available on the following media:

- HP-UX 11i v3 (B.11.31) Operating Environment DVD, February 2007 or later
- HP-UX 11i v3 (B.11.31) Applications DVD, February 2007 or later
- HP-UX 11i v2 (B.11.23) Operating Environment DVD, May 2005 or later
- HP-UX 11i v2 (B.11.23) Applications DVD, September 2005 or later
- HP-UX 11i v1 (B.11.11) Operating Environment DVD, September 2005 or later
- HP-UX 11i v1 (B.11.11) Applications DVD, May 2005 or later
- HP SmartSetup CD 4.6 or later
- SmartStart CD 7.20 or later
- Support Pack 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, HP SMH 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 and Troubleshooting** link on http://www.hp.com.

3 Initial setup

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

Additionally, you can install HP SMH locally 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.

Installation information

- For HP-UX systems

  HP SMH is installed or updated using the HP-UX Operating Environment (OE) media or Applications 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/smhpd.xml` file.

- For Linux systems

  HP SMH is installed by an RPM package without asking you to configure any settings. After the installation is complete, run the `perl` script utility (`/opt/hp//hpsmh/hpSMHSetup.pl` on ProLiant or `/opt/hp/hpsmh/smhconfig/hpSMHSetup.sh` on Itanium) to set the security options used by all of the HP Web-based 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/smhpd.xml` file.

- For Windows systems

  The configuration settings are carried over from the`\hp\hpsmh\conf\smhpd.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 HP SMH is installed, the HP SMH 2048-bit key pair will be replaced with the HP Systems Insight Manager 1024-bit key pair.

You can also install HP SMH on Integrity servers from the HP SmartSetup CD.

4 Installing on HP-UX

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

System Administration Management Tool changes: SAM and HP SMH

The HP-UX System Administration Manager (SAM) is deprecated in HP-UX 11i v3. HP SMH is the system administration tool for managing HP-UX 11i. HP SMH provides web-based systems management functionality, at-a-glance monitoring of system component health and consolidated log viewing. HP SMH also provides a Terminal User Interface (TUI). SAM continues to provide access to TUI (Terminal User Interface) and X-based interfaces. More details on HP SMH are available in the *Next generation single-system management on HP-UX 11i v2 (B.11.23)* white paper located at http://docs.hp.com/en/4AA0-4052ENW/4AA0-4052ENW.pdf.

Some of the key changes are described below:

- The SAM Functional Area Launcher (FAL) is replaced by the HP SMH web-based Graphical User Interface (GUI).
- The enhanced TUI offers improved look and feel, online viewing of manpages, command previews, and other improvements.
- For HP-UX 11i v3 (B.11.131) only, a new command, *smh*(1m) is introduced (`/usr/sbin/smh`). This is an enhanced version of the *sam*(1m) command (`/usr/sbin/sam`).
- The `sam` command in `/usr/sbin/sam` is deprecated. Any invocation of `/usr/sbin/sam` will display the deprecation message and launch `/usr/sbin/smh` automatically.

Installing on HP-UX

To install HP SMH on HP-UX, you have several options:

- Installing from the HP-UX 11i v3 (B.11.31) OE media (February 2007 or later) and from the HP-UX 11i v3 (B.11.31) Applications media (February 2007 or later)
- Installing from the HP-UX 11i v2 (B.11.23) OE media (May 2005 or later) and from the HP-UX 11i v2 (B.11.23) Applications media (September 2005 or later)
- Installing from the HP-UX 11i v1 (B.11.11) OE media (September 2005 or later) and from the HP-UX 11i v1 (B.11.11) Applications media (May 2005 or later)
- Installing from the HP SMH web site, which you can find on the Software Depot home at http://www.hp.com/go/softwaredepot .

NOTE: After you install HP SMH, it is already configured for you to start using immediately. To change the default configuration settings, go to "Configuring HP SMH" (page 23).

Installation requirements

To install HP SMH, your system must meet the minimum requirements. The following list provides a general review of requirements. For detailed information regarding minimum requirements, see Chapter 2: "Installation requirements" (page 11).

- HP-UX 11i v1 (B.11.11) for HP Servers and Workstations

  HP-UX 11i v2 (B.11.23) for HP Integrity Servers and HP 9000 Servers

  HP-UX 11i v3 (B.11.31) for HP Integrity Servers and HP 9000 Servers
- Mozilla or Firefox browser
- Administrator privileges on system
- Dependent applications (see next section)

Installing HP SMH and dependent applications

HP SMH requires several applications, but some applications are optional. You might 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	Path	Status	Release
HP SMH	`SysMgmtWeb`	`/opt/hpsmh` and `/var/opt/hpsmh`	Required	HP-UX 11i v1, v2, v3
HP-UX Apache-based Web Server	`hpuxwsApache`	`/opt/hpws/apache`	Required	HP-UX 11i v1, v2, v3
HP-UX Strong Random Number Generator	`KRNG11i`	`/usr/conf` or `/usr/conf/lib/libmng.a`, `/usr/share`, `/usr/include`, `/sbin/init.d`, `/sbin/rc1.d`	Recommended	HP-UX 11i v1 You can find this application on the Software Depot Home at http://www.hp.com/go/softwaredepot The `KRNG11i` bundle requires a system reboot.
HP-UX Tomcat-based Servlet Engine	`hpuxwsTomcat`	`/opt/hpws/tomcat`	Recommended: Certain HP SMH plugins, such as Partition Manager require it.	HP-UX 11i v1, v2, v3
HP WBEM Services	`WBEMSvcs`	`/opt/wbem`	Recommended: Certain HP SMH plugins, such as Property Pages found on the Home page require it.	HP-UX 11i v1, v2, v3
HP-UX System Fault Management	`SysFaultMgmt`	`/opt/sfm/`	Recommended: Certain HP SMH plugins, such as Property Pages found on the Home page require it.	HP-UX 11i v1, v2, v3

Product	Bundle	Path	Status	Release
HP-UX Software Distributor	HPUXBaseAux for HP-UX 11i v1 and v2. SwMgmtMin for HP-UX 11i v3.	/usr/lib/sw/wbem/	Recommended: Certain HP SMH plugins, such as Property Pages found on the Home page require it.	HP-UX 11i v1, v2, v3
LAN Provider for Ethernet LAN interfaces	WBEMP-LAN-00	/opt/lanprovider/	Recommended: Certain HP SMH plugins, such as Property Pages found on the Home page require it.	HP-UX 11i v1, v2, v3
WBEM Provider for FC HBAs	FCProvider	/opt/fcprovider/	Optional: Certain HP SMH plugins, such as Property Pages found on the Home page require it.	HP-UX 11i v2, v3
WBEM Provider for SCSI HBA	SCSIProvider	/opt/scsiprovider/	Optional: Certain HP SMH plugins, such as Property Pages found on the Home page require it.	HP-UX 11i v2, v3
Java	Java2 1.4 SDK for HP-UX (T1456AA)	/opt/java1.4	Optional: Certain HP SMH plugins, such as Partition Manager require it.	HP-UX 11i v1, v2, v3
OpenSSL	OpenSSL	/opt/openssl	Required	HP-UX 11i v1, v2, v3
HP-UX Common System Management Enablers	SysMgmtBase	usr/sam and /opt/hpsmh/lib	Required	HP-UX 11i v2, v3
HP-UX CDE User Interface	CDE	/usr/dt/lib/, /usr/dt/lib/hpux32/, and /usr/dt/lib/hpux64/	Optional: Certain HP SMH plugins require it; e.g., DSAU.	HP-UX 11i v1, v2, v3
HP-UX X Window Software	X11	/opt/atok/X11, /usr/bin/X11 , and /usr/lib/X11/	Optional: Certain HP SMH plugins require it; e.g., fsweb.	HP-UX 11i v1, v2, v3

If you do not have these applications on your system, you can use the following resources to install them before or after you install HP SMH:

- If you installed or updated HP-UX 11i v3 (B.11.31) from the media, then the applications were recommended to install. If you installed or updated HP-UX 11i v1 (B.11.11) or HP-UX 11i v2 (B.11.23) from the 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 recommended and default-installed HP application bundles. See "Using the Applications media" (page 22).
- You can use swinstall to install or update the bundles (for example, hpuxwsApache and hpuxwsTomcat) using the HP-UX 11i v1 (B.11.11), HP-UX 11i v2 (B.11.23), and HP-UX 11i v3 (B.11.31) media. See "Using the Applications media" (page 22).
- 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 22).
- You can also download the bundles to a depot on your network and use Ignite-UX and Software Distributor to install them. This process 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 Applications media

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

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

      Use the `ioscan -funC disk` command to list disk devices, including the DVD devices.

   b. Create a mount point for the Applications 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.

   c. Use the `mount` command to mount the DVD.

      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
      ```

      See 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 Applications DVD.

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

   See the *swinstall*(1M) manpage for details.
4. Select and install software from the Applications DVD.

   The `swinstall` program has an interface for selecting and installing software from the DVD.
5. Unmount and eject the Applications 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. See the *umount*(1M) manpage for details.

TIP: After the installation is complete, you can start using HP SMH immediately.

Using Software Depot

To install HP SMH 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. Click the **Receive for Free** 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:

   `swinstall -s /var/temp/ depot_filename.depot bundlename`

   For example: `swinstall -s \`
   `/var/temp/SysMgmtHomepage_A2214_HP-UX_B.11.23_IA+PA.depot SysMgmtWeb`

TIP: After the installation is complete, you can start using HP SMH immediately.

Configuring HP SMH

The HP SMH configuration is based on environment variables and tags that are set by the `/opt/hpsmh/lbin/envvars`, `/opt/hpsmh/conf.common/smhpd.xml` and `/opt/hpsmh/conf/timeout.conf` files. To change the default configuration, you can modify the files to properly set the value of the following variables and tag.

Variable	Description	Script
JAVA_HOME	Points to the `/opt/hpsmh/lbin/envvars` directory where JDK is installed.	`/opt/hpsmh/lbin/envvars`
<session-timeout>15</session-timeout>	The <session-timeout> tag defines the HP SMH session timeout in minutes. If it is defined, then the HP SMH session is stopped after the time period has elapsed without any user activity. If it is not defined, then the default for the HP SMH session timeout is set to 15 minutes. You can define the <session-timeout> tag using any value between 1 and 120 minutes.	`/opt/hpsmh/conf.common/smhpd.xml`

Variable	Description	Script
TIMEOUT_SMH	The TIMEOUT_SMH environment variable defines the HP SMH server timeout in minutes. If it is defined and lower than the HP SMH session timeout, the HP SMH server will be stopped three minutes after the HP SMH session timeout. If it is defined and greater than the HP SMH session timeout, then the HP SMH server is stopped after the time period has elapsed without any user activity. If it is not defined or equal to zero, then HP SMH is started without timeout. When the "automatic startup on boot" startup mode is in use, the timeout mechanism will not be started.	`/opt/hpsmh/conf/timeout.conf`
TIMEOUT_TOMCAT	Defines the Tomcat timeout in minutes in the `/opt/hpsmh/conf/timeout.conf` file. If it is defined, 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. If it is not defined or equal to zero, then Tomcat is started without timeout. In this case, Tomcat is stopped only when HP SMH is stopped.	`/opt/hpsmh/conf/timeout.conf`

Configuring the startup mode

HP SMH supports three startup modes:

- Autostart URL

  This mode is the default setting for startup. You can start HP SMH 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 mode starts HP SMH automatically during system initialization. If the automatic startup on boot start mode is enabled and the system was rebooted using this configuration, you can access HP SMH 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 HP SMH from the HP-UX command line.

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

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

Options:

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

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

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

- `on` Start Tomcat when HP SMH 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, see the *smhstartconfig*(1M) manpage:

`man smhstartconfig` or **`man sam`**

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

Patching or updating the software

HP may issue patches to HP SMH. 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 and Applications 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 11.x Systems* on the HP Technical Documentation web site at http://docs.hp.com.

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

- HP-UX OE media
- HP-UX Applications media
- HP SMH web page on the Software Depot home at http://www.hp.com/go/softwaredepot

5 Installing on Windows

This chapter provides steps to install HP System Management Homepage (HP SMH) on the Windows operating system.

The next chapter provides steps to install HP SMH on the Windows operating system using the ProLiant Remote Deployment Utility:

Installing HP SMH 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.
2. Click **Next**. The **OS Groups** dialog box appears. You can 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 HP SMH 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: You must 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 because it could potentially lock out the administrator account. 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.

   Select one of 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 HP SMH to automatically grant local IP addresses at the selected access level.

     Caution: Selecting **Local Access** with administrator privileges provides all 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:
   a. Trust By Certificate
      i. 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**.
      ii. 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 Web-based Agents on this system. Click **OK** if you do not want HP Systems Insight Manager to access the HP Web-based 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 HP SMH 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.

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

      or

      i. Click **Import**. The **Import Server Certificate** dialog box appears.
      ii. Enter the name or IP address of the server whose certificate you want to import.
      iii. Click **Get Cert**. The certificate information appears.
      iv. 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.

      v. 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.

   b. Trust By Name
      i. Select **Trust By Name**.
      ii. 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 HP SMH to only accept certain requests from servers with the HP Systems Insight Manager certificate names designated in the **Trust By Name** field. The **Trust By Name** option is easy to configure and can prevent unauthorized 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 certificate name submitted.

      iii. Enter the names of the certificate of HP Systems Insight Manager servers you want to trust.

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

iv. Click **Add** to add the name of a certificate of HP Systems Insight Manager server you want to trust.

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

Note: If you click **Next** without adding any HP SIM server's certificate names to the list, an error message appears, indicating that if you do not specify any trusted server names, HP Systems Insight Manager cannot access the HP Web-based Agents on this system. Click **OK** to proceed without trusting any systems, or click **Cancel** to close the dialog box and add HP Systems Insight Manager server's certificate names to the list.

Note: To delete a HP Systems Insight Manager server's certificate name, select the certificate name and click **Delete**. The selected certificate name is removed.

c. Trust All

i. Select **Trust All**.

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

Note: The **Trust All** option leaves your system vulnerable to security attacks and sets up HP SMH 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. If you enter an invalid Subnet IP Address/Netmask, an error message appears indicating the `Subnet IP address or Netmask is invalid`. Click **OK**. Enter a valid Subnet IP address/Netmask and click **Add** again.

9. Click **Next**. The **IP Restricted Login** dialog box appears. The **IP Restricted Login** dialog box enables you to select specific IP addresses or IP address ranges to include or exclude from gaining login access. Although optional, HP SMH can restrict login access based on the IP addresses of the machine attempting to gain access.

10. Select **IP Restricted Login**, 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 Restricted Login** 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 addresses 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 enter 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 enter 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 Summary** dialog box appears.

12. Click **Next**. The **Install Summary Panel** appears. The **Install Summary Panel** lists a summary of the options that you specified during the installation.
13. Click **Next**. The installation process is started.

    Note: During the installation of HP SMH, the **Cancel** button is disabled. Even if you click **X** in the upper-right corner of the box, the current operation cannot be cancelled.

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

Installing HP SMH for Windows silently

The HP SMH installation for Windows enables you to silently install HP SMH. After the installation is complete, you can configure HP SMH settings.

NOTE: Do not copy or import certificates when using the `setup.exe /r` option.

Generating a setup.iss file

To generate your own `setup.iss`, run the following command:

1. `setup.exe /r`
2. The HP SMH 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, use the following command:

`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 HP SMH. The `/s /preserve` command preserves the existing `smhpd.xml` settings.

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

If an HP SMH 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.

Configuring HP SMH

The HP SMH configuration is based on environment variables and tags that are set by the `%SystemDrive%\hp\hpsmh\conf\smhpd.xml`, file. To change the default configuration, you can modify the files to properly set the value of the following variables and tags.

Variable	Description	Script
<session-timeout>15</session-timeout>	The <session-timeout> tag defines the HP SMH session timeout in minutes. If it is defined, then the HP SMH session is stopped after the time period has elapsed without any user activity. If it is not defined, then the default for the HP SMH session timeout is set to 15 minutes. You can define the <session-timeout> tag using any value between 1 and 120 minutes.	`%SystemDrive%\hp\hpsmh\conf\smhpd.xml`
<ui-timeout>20</ui-timeout>	The <ui-timeout> tag defines the HP SMH GUI timeout in seconds. If it is defined, then HP SMH limits the loading time of the webapps. If it is not defined, then the default for the HP SMH GUI timeout is set to 20 seconds. You can define the <ui-timeout> tag using any value between 10 and 3600 seconds.	`%SystemDrive%\hp\hpsmh\conf\smhpd.xml`
<rotate-logs-size>N</rotate-logs-size>	The <rotate-logs-size> tag defines the HP SMH Rotate Logs file size. To change the Rotate Logs file size, you will need to edit the configuration file smhpd.xml. You can define the <rotate-logs-size> tag using any value between 1 and 99, which represents the log size in megabytes.	`%SystemDrive%\hp\hpsmh\conf\smhpd.xml`
<log-base-dir>path</log-base-dir>	The log-base-dir tag defines the path for Error_log and Access_log. By default Error_log and Access_log will be located in <systemdrive>:\hp\hpsmh\logs (/var/spool/opt/hp/hpsmh/logs in Linux) folder. The path can be changed by giving the required path in the tag and create the logs folder under that path.	<Systemdrive>:\hp\hpsmh\conf\smhpd.xml (/opt/hp/hpsmh/conf/smhpd.xml in Linux).
<max-threads>value</max-threads>	The max-threads tag configures the number of threads used by apache via the smhpd.xml file. • Default value - WIndows: 250 and Linux: 25 • Max value - Windows: 512 and Linux: 64 • Min value - Windows: 64 and Linux: 25	<Systemdrive>:\hp\hpsmh\conf\smhpd.xml (/opt/hp/hpsmh/conf/smhpd.xml in Linux).

6 Installing HP SMH using the ProLiant Remote Deployment Utility

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

- "Installing remotely on Windows using ProLiant Remote Deployment Utility" (page 34)

The previous chapter provides steps to install HP SMH in-place on the Windows operating system.

- "Installing HP SMH in-place on Windows" (page 27)

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 Setup.exe which is present as part of the ProLiant Support Pack. 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. HP SMH can be installed as a part of the complete ProLiant Support Pack, or you can install the HP SMH component individually. The HP SMH component also provides support for preconfiguration, which allows the configurations of the component to be configured and saved as part of the component itself before installing on target machines. This feature facilitates the installation of the preconfigured component without any user intervention, and the installed component has the configurations, which are saved during preconfiguration.

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

NOTE: Installation of a preconfigured component overwrites the configuration settings of any existing HP SMH installation. If you want to retain existing settings, do not preconfigure the component.

To preconfigure the HP SMH component:

1. Under **All configurable components**, right-click on the **HP System Management Homepage** component and select **Configure**. The **Welcome** wizard appears.
2. Click **Next**. The **Operating System Group** dialog box appears providing you with an option to add the groups and select the **Operating** level.
3. To add HP SMH groups:
   a. 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: You must 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 because it could potentially lock out the administrator account. Using the administrator account, add another account with administrator privileges to be used for Version Control Repository Manager access.

   b. Select an **Operating Level** from the dropdown list. This level determines the privileges assigned to this group.
   c. 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 before the group name.

4. Click **Next**. The **User Access** dialog box appears.
5. The **User Access** dialog box enables you to configure HP SMH 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 HP SMH to automatically grant local IP addresses at the selected access level.

     Caution: Selecting **Local Access** with administrator privileges provides all 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:
   a. Trust By Certificate
      i. Select **Trust By Certificate**.
      ii. 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**.
      iii. Click **Browse** to select the certificate file. After the certificate file is selected, the certificate data appears on the screen.
      iv. Click **Add**. The certificate appears under **Certificate File**. To delete a certificate file from the screen, click the **X** located before the certificate file.
      v. **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 Web-based Agents on this system. Click **OK** if you do not want HP Systems Insight Manager to access the HP Web-based 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 HP SMH 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.

      vi. Click **Next**. The **IP Binding** dialog box appears.
   b. Trust By Name
      i. Select **Trust By Name**.
      ii. 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 HP SMH to only accept certain requests from servers with the HP Systems Insight Manager's certificate 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 certificate name submitted.

      iii. Enter the names of the certificate of SIM servers you want to trust.

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

      iv. Click **Add** to add the certificate name of a SIM server you want to trust. The certificate name appears under **Trusted Server**. To delete a server's certificate name, click the **X** located before the certificate name.
      v. Click **Next**. The **IP Binding** dialog box appears.

         Note: If you click **Next** without adding any HP Systems Insight Manager server's certificate names to the list, an error message appears, indicating that if you do not specify any trusted server names, HP Systems Insight Manager cannot access the HP Web-based Agents on this system. Click **OK** to proceed without trusting any systems, or click **Cancel** to close the dialog box and add HP Systems Insight Manager server's certificate names to the list.

   c. Trust All
      i. Select **Trust All**.

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

Note: The **Trust All** option leaves your system vulnerable to security attacks and sets up HP SMH 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 appears in the **IP Binding** list. To delete a Subnet IP Address/Netmask, click the **X** located before the **Subnet IP Address/Netmask** pair. The Subnet IP Address/Netmask is deleted from the **IP Binding** list.

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

      Note: If you enter an invalid Subnet IP Address/Netmask, an error message appears indicating the Subnet IP address or Netmask is invalid. Click **OK**. Enter a valid Subnet IP address/Netmask and click **Add** again.

9. Click **Next**. The **IP Restricted Login** dialog box appears. The **IP Restricted Login** dialog box enables you to select specific IP addresses or IP address ranges to include or exclude from gaining login access. Although optional, HP SMH can restrict login access based on the IP addresses of the machine attempting to gain access.
10. Select **IP Restricted Login**.
    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 appears 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 appears indicating the IP address is invalid.

       Note: If **Finish** is clicked without adding any IP addresses to 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 click **OK**, the IP Restricted Login option on the **IP Restricted Login** dialog box is deselected

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

You can install this preconfigured component to target systems without the need to configure settings in HP SMH after installation. For more information about using the ProLiant Remote Deployment Utility, see the *HP ProLiant Support Pack and Deployment Utilities User Guide*.

7 Installing HP SMH using the HP Smart-Update Manager (HPSUM)

This chapter provides steps to install HP System Management Homepage (HP SMH) on the Windows operating system using the HP Smart-Update Manager (HPSUM).

The previous chapter provides steps to install HP SMH using the ProLiant Remote Deployment Utility.

The HP Smart-Update Manager utility enables you to deploy PSP software and firmware components from a single, easy-to-use interface. Using a graphical interface, the utility enables you to deploy and maintain ProLiant Support Packs and Smart Components on a local server or one or more remote servers accessible over a network connection. This utility enables legacy support of existing software and firmware components while simplifying the overall deployment process. The utility also provides installation logic and version control that automatically check for dependencies, installing only the correct updates for optimal configuration.

ProLiant Support Pack contains numerous files. All files must be present in the same directory as the HPSUM.EXE program for the PSP to be properly installed. HP SMH can be installed as a part of the complete ProLiant Support Pack, or you can install the HP SMH component individually. The HP SMH 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 feature 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.

NOTE: Installation of a pre-configured component overwrites the configuration settings of an existing HP SMH installation. If you want to retain existing settings, do not pre-configure the component.

Installing HP SMH remotely on Windows using HP Smart-Update Manager (HPSUM)

1. To start the deployment, run HPSUM.EXE. The **Inventory Progress** screen is displayed while the HP Smart-Update Manager builds an inventory of available updates.
2. The **Select Installation Host(s)** screen appears when the inventory process is complete.
3. If you want to install HP SMH on the local server, check the **Local Host** checkbox and click **Next**.
4. If you want to install HP SMH on remote server(s):
   a. Select the **Remote Host or Group** checkbox and click **Manage Host**. The **Manage Host** panel is displayed.
   b. Click **Add Host**. Here, you can add a new host(s) by DNS name or IP Address or you have the option to add a range of IP Addresses.
   c. You can also create a group of systems on which you want to install HP SMH by selecting **Manage Groups**.

      Note: If you chose to **Manage Groups**, you will need to give the Windows credentials for each remote server.

5. After selecting the target server, click **Next**. This will show **Discovery Progress** while the system is checked for installed items. Then, the **Select Bundle Filter** page is displayed.
6. From the **Select Bundle Filter** page, select the appropriate PSP bundle, addording to the target server's operating system architecture (either x86 or x64), and check the appropriate option for the bundle filter. There are three options provided:
   I. **Allow Non-Bundle Version:** Shows other versions of the product that are in the bundle. This lets you include updates that may be newer than those released in the bundle.
   II. **Allow Non-Bundle Products:** Shows updates for products that are not part of the bundle. This lets you update other items on your system at the same time as applying the bundle (as a convenience or because updates in the bundle may depend on them).
   III. **Force All Bundle Updates:** Automatically sets the **force** flag for updates in the bundle. This causes the update to install even if it is not necessary as long as the supported hardware is present and installation conditions are met.

   Note: Selecting the bundle filter option is not required when the HP SMH component is being installed alone.
7. Click **Next**. This will take you to the **Select Items to be installed** panel. This panel shows the components to be installed or displays **Installation not needed** or **Excluded by filtering**.
8. Check the System Management Homepage component and you can pre-configure the HP SMH component by selecting **Configure Now**.

   Note: If the PSP contains an older version of HP SMH than what is already installed on the target server, the HP SMH component will be listed under **Installation not needed** section. In this case, click **Installation Options** for HP SMH component and check the **For Install** checkbox. The HP SMH component will now be listed under **Updates to be Installed**.
9. After selecting the HP SMH component, click **Install**. This will show the installation progress.
10. After installation is finished, the **Installation Result** panel will be displayed.
11. In the **Installation Result** panel, you will see two buttons **Reboot Now** and **Exit**.
12. If you want to reboot the system, select **Reboot Now**. If you want to exit the program, select **Exit**. This will complete the HP Smart-Update Manager program.

To preconfigure the HP SMH component:

1. From the **Welcome to the Configuration Wizard for the HP System Management Homepage Component** page, click **Next**. The **Operating Systems Groups** page appears.

2. In the **Group Name** field, enter the name of an operating system group that you want to assign (for example, **`vcadmin`**).
3. In the **Operating Level** field, select the appropriate level for the new group from the dropdown list.

   Note: The default **Administrators Groups** always have administrative access.
4. Click **Add** to assign the group. The new group appears under the operating system group to which it was assigned.

   Note: You can add up to five entries per operating system group.
5. Click **Next**. You can click **Save** to save your changes up to this point or click **Cancel** to discard the changes and close the wizard.
6. Select one of the following options:
   - **Anonymous Access** Anonymous Access is disabled by default. Enabling **Anonymous Access** enables a user to access the HP System Management Homepage without logging in. Select this option to allow anonymous access.

     Caution: HP does not recommend the use of anonymous access.
   - **Local Access** Local Access is disabled by default. Enabling Local Access enables a user to locally gain access to the HP System Management Homepage without being challenged for authentication, which means that any user with access to the local console is granted full access if **Administrator** is selected. If **Anonymous** is selected, any local user has access limited to unsecured pages without being challenged for a user name and password.

     Caution: HP does not recommend the use of local access unless your management server software enables it.
7. Click **Next**. You can click **Save** to save your changes up to this point, or click **Cancel** to discard the changes and close the wizard.
8. Select one of the following Trust Mode security options:
   - **Trust by Certificate** Sets the HP System Management Homepage to accept configuration changes only from HP SIM servers with trusted certificates. This mode requires the submitted server to provide authentication by means of certificates. This mode is the strongest method of security because it requires certificate data and verifies the digital signature before allowing access. If you do not want to enable any remote configuration changes, leave **Trust by Certificate** selected, and leave the list of trusted systems empty by avoiding importing any certificates.

     

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

     To trust by certificate:
     1. Select **Trust by Certificate**, and click **Next**.
     2. In the **Certificate Name** field, click **Browse** to select the certificate file. After the certificate file is selected, the certificate data appears on the screen.
     3. Click **Add**. The certificate appears under **Certificate Files**. You can click **Save** to save your changes up to this point or click **Cancel** to discard the changes and close the wizard.
     4. Click **Next**. The **IP Binding** page appears.
   - **Trust by Name** Sets the HP System Management Homepage to accept certain configuration changes only from servers with the HP SIM certificate names designated in the **Trust By Name** field. The **Trust By Name** option is easy to configure. For example, you might use the **Trust By Name** option if you have a secure network with two separate groups of administrators in two separate divisions. It prevents one group from installing

software to the wrong system. This option verifies only the HP SIM server's certificate name submitted.

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

The server name option must meet the following criteria:

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

To trust by name:

1. Select **Trust by Name**, and click **Next**.
2. In the **Trusted Server Name** field, enter the HP SIM server's certificate name to be trusted.
3. Click **Add**. The trusted HP SIM server's certificate name appears under the **Trusted Servers** list. You can click **Save** to save your changes up to this point or click **Cancel** to discard the changes and close the wizard.
4. Click **Next**. The **IP Binding** page appears.

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

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

To trust all servers:

1. Select **Trust All**. You can click **Save** to save your changes up to this point or click **Cancel** to discard the changes and close the wizard.
2. Click **Next**. The **IP Binding** page appears.

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

   Administrators can configure the HP System Management Homepage to only bind to addresses specified in the **IP Binding** page. A maximum of five subnet IP addresses and netmasks can be defined.

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

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

   To configure IP Binding:

   1. Select **IP Binding**. The **IP Binding** page appears.
   2. Enter the IP address.
   3. Enter the netmask.
   4. Click **Add**. The IP binding configuration is saved and appears under the **IP Binding List**.
   5. Click **Next**. The **IP Restricted Login** page appears.

10. The IP Restricted Login enables the HP System Management Homepage to restrict login access based on the IP address of a system.

    You can set address restriction at installation time or by it can be set by administrators from the **IP Restricted Login** page

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

    To include or exclude IP addresses:

    1. In the **From** field, enter the IP addresses to include or exclude. You can enter an IP address range to be included or excluded by entering a beginning IP address in the **From** field and an ending IP address in the **To** field.
    2. From the **Type** field, select **Include** or **Exclude**.
    3. Click **Add** to add the IP address or IP address range to the **Inclusion List** or **Exclusion List**.
    4. Click **Save**. The **HP System Management Homepage Login** page for the HP System Management Homepage system appears.

8 Installing in-place on Linux

This chapter provides steps to install HP System Management Homepage (HP SMH) in-place on Linux x86 systems and x86_64 systems.

The next chapter provides steps to install HP SMH in-place on Linux systems using the Linux Deployment Utility.

Installation for Linux on x86 and x86_64

The HP SMH installation for Linux enables you to silently install HP SMH on x86 and x86_64 systems. After the installation is complete, you can configure the HP SMH settings.

NOTE: To install HP SMH, you must be logged in as root user.

Installing HP SMH on Linux x86 systems

To install HP SMH on x86 systems, your system must meet the minimum requirements. For more information regarding minimum requirements, see Chapter 2 "Installation requirements". In addition, you must have the `hpsmh-2.x.x.linux.i386.rpm`.

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

To install HP SMH, enter the following command line:

```
rpm -ivh hpsmh-2.x.x-linux.i386.rpm
```

A message appears indicating that HP SMH installed successfully with default configuration values.

Installing HP SMH on x86_64

To install HP SMH on x86_64 systems, your system must meet the minimum requirements. For more information regarding minimum requirements, see Chapter 2 "Installation requirements". In addition, you must have the `hpsmh-2.x.x.linux-release.x86_64.rpm`

To install HP SMH, enter the following command line:

```
rpm -ivh hpsmh-2.x.x-linux-release.x86_64.rpm
```

A message appears indicating that HP SMH installed successfully with default configuration values.

Configuring HP SMH

After HP SMH 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 HP SMH settings:

1. Enter the following command to start the configuration:

   ```
   perl /opt/hp/hpsmh/hpSMHSetup.pl
   ```

   Enter the following command to start the configuration for Itanium systems:

   ```
   perl /opt/hp/hpsmh/hpSMHSetup.sh
   ```

   The **Welcome** screen appears, indicating that you can configure security and access parameters on the following screens.

2. The Welcome screen indicates that you can configure security and access parameters for HP System Management Homepage and related HP web-based management tools.

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

3. The **Operating System Groups** screen enables you to add operating system groups to HP SMH.

   Add or delete operating system groups in HP SMH. The following options are available:

   a. To add groups:

      i. 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:

           A. Enter `1` for Administrator.
           B. At the prompt, `Enter the name of the operating system group:` enter **admin1**.
           C. Press **Enter**. **admin1** appears in the **Administrator Group List**.
           D. Enter **n** to go to the next screen.

         - Enter `2` for Operator.
         - Enter `3` for User.

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

   b. To delete a group:

      i. Enter `2` to delete a group.

         The following options are available:

         - Enter `1` for Administrator. The **Administrator Group List** appears.
         - Enter `2` for Operator. The **Operator Group List** appears.
         - Enter `3` for User. The **User Group List** appears.

      ii. At the prompt, enter `1`, `2`, or `3`.

      iii. 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 you want by repeating this step.

      iv. Press **Enter** when you are finished deleting to go to the next screen.

      v. Enter **n** to go to the next screen. The **Operating System Groups** screen appears.

      vi. Enter **n** to go to the next screen. The **User Access** screen appears.

4. 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 HP SMH 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. 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 appears.
7. Configure the HP SMH trust mode.

   Enter `1` for **Trust by Certificate**. `Trust Mode: Trust by Certificate` appears.

   The following options are available: Trust by Certificate, Trust by Name, Trust All and Modify Certificate List.

a. Trust by Certificate
   i. To add a certificate file:
      A. Enter `1`. You are prompted for the certificate location.
      B. Enter the file path of the trusted certificates to be added to the **Trusted Certificates List**. Press **Enter** when you are finished.

         For example:

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

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

      C. You can add as many certificates as you want by repeating these steps. Press **Enter** when you are finished adding certificate files.
   ii. To import a certificate:
      A. Enter `2`. You are prompted for the server name.
      B. Enter the name or IP address 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.

      C. 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.
      D. Press **Enter** when you are finished importing certificate files.
   iii. To delete a certificate:
      A. Enter `3`. You are prompted to enter the number associated with the certificate file to be deleted.
      B. Enter the number of the certificate file to be deleted.
      C. Press **Enter** when you are finished. You can delete as many certificate files as you want by repeating these steps.
      D. Press **Enter** when you are finished deleting certificate files.

b. Trust by Name
   i. Enter `2` to **Trust by Name**. `Trust Mode: Trust by Name` appears.
   ii. Enter `4` to **Modify Server Name** list.

      To add an HP Systems Insight Manager server's certificate name:

      A. Enter `1`. You are prompted to add an HP Systems Insight Manager server's certificate name.
      B. Enter the name of the certificate of HP Systems Insight Manager server to be trusted and press **Enter**. The certificate name appears in the **Trusted Server Names** list.

         Note: You can add as many server certificate names as you want.

      To delete a certificate name:

      A. From the **Server Name** list, enter `2`.
      B. Enter the number associated with the name of the certificate of the HP SIM server to be deleted. The HP SIM server's certificate name is removed from the **Server Name** list.
   iii. Enter **n** for next. The **Trust Mode Settings** screen appears.

c. Trust All
   i. Enter `3` to **Trust All**. `Trust Mode: Trust All` appears.
   ii. Enter **n** for next. The **IP Binding** screen appears.

d. Modify Certificate List

   Enter `4` to **Modify Certificate List**.

8. Bind IP addresses that match a subnet and netmask.

   The following options are available:

   a. Enable IP Binding
      i. Enter `1` to enable the IP Binding, which sets it to **ON**. `IP Binding: ON` appears.
      ii. Enter **n** to go to the next screen.

      The following options are available:

      To add an IP address:

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

      B. Enter the IP address to be added. `IP Address: YourIPAddress` appears. You are prompted for the netmask.

      C. Enter the netmask. `netmask: YourNetmask` appears.

      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 to be deleted. The IP address or netmask is removed from the IP address or netmask list.

      iii. Enter **n** to go to the next screen. The **IP Restricted Login** screen appears.

   b. Disable IP Binding
      i. Enter `2` to disable the IP Binding, which sets it to **OFF**. `IP Binding: OFF` appears.
      ii. Enter **n** to go to the next screen or enter **p** to go to the previous screen. The **IP Restricted Login** screen appears.

9. Configure HP SMH to restrict login access based on the IP address of the system from which the login is attempted.

   The following options are available:

   a. Enter `1` to enable an IP Restricted Login, which sets it to **ON**. **IP Restricted Login:ON** appears.

      To enable the IP Restricted Login:

      i. Enter `1`. **IP Restricted Login** is set to **ON**.

      ii. Press **n** for next. The **Set IP Address Restrictions** screen appears.

         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 appears 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 from the Inclusion list:

         A. Enter `2`.

         B. 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**.

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

         1. Enter `2` for Exclude Login Restriction IP Address

         2. Enter `1` to add an IP address to the Exclusion List.

         3. 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**.

         4. Press `Enter` . The **IP Address Exclusion List** screen appears.

         5. Press `n` for next. The **IP Address Inclusion List** and **IP Address Exclusion List** appears.

         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.

         3. Press **Enter**. The IP address is deleted from the **IP Address Exclusion List**.

         4. Press **Enter**. The **IP Address Exclusion List** screen appears.

         5. Press `n` for next. The **IP Address Inclusion** list and **IP Address Exclusion** list appears.

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

      iii. Enter **n** for next.

   b. Enter `2` to disable IP Restricted Login, which sets it to **OFF**. `IP Restricted Login: OFF` appears.

      To disable IP Restricted Login:

      Enter `2` to disable the IP Restricted Login. The IP Restricted Login is set to **OFF**.

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

9 Installing directly on Linux

Installing in-place on Linux Itanium

This chapter provides steps to install HP System Management Homepage (HP SMH) in-place on Linux Itanium.

The next chapter provides steps to install HP SMH in-place on Linux systems using the Linux Deployment Utility.

Installation for Linux Itanium

The HP SMH installation for Linux enables you to silently install HP SMH on Itanium systems. After the installation is complete, you can configure the HP SMH settings.

NOTE: To install HP SMH, you must be logged in as root user.

Installing HP SMH on Linux Itanium systems

To install HP SMH on Itanium systems, your system must meet the minimum requirements. For more information regarding minimum requirements, see Chapter 2 "Installation requirements". In addition, you must have the `hpsmh-2.x.x.-xx.linux.ia64.rpm`.

To install HP SMH, enter the following command line:

```
rpm -ivh hpsmh-2.x.x-xx-linux.ia64.rpm
```

A message appears indicating that HP SMH installed successfully with default configuration values.

Configuring HP SMH

After HP SMH 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 HP SMH settings:

1. Enter the following command to start the configuration:

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

   The **Welcome** screen appears, indicating that you can configure security and access parameters on the following screens.

2. The Welcome screen indicates that you can configure security and access parameters for HP System Management Homepage and related HP web-based management tools.

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

3. The **Operating System Groups** screen enables you to add operating system groups to HP SMH.

   Add or delete operating system groups in HP SMH. The following options are available:

   a. To add groups:
      i. 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:

           A. Enter `1` for Administrator.
           B. At the prompt, `Enter the name of the operating system group:` enter **admin1**.
           C. Press **Enter**. **admin1** appears in the **Administrator Group List**.
           D. Enter **n** to go to the next screen.
         - Enter `2` for Operator.
         - Enter `3` for User.

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

   b. To delete a group:
      i. Enter `2` to delete a group.

         The following options are available:

         - Enter `1` for Administrator. The **Administrator Group List** appears.
         - Enter `2` for Operator. The **Operator Group List** appears.
         - Enter `3` for User. The **User Group List** appears.

      ii. At the prompt, enter `1`, `2`, or `3`.
      iii. 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 you want by repeating this step.

      iv. Press **Enter** when you are finished deleting to go to the next screen.
      v. Enter **n** to go to the next screen. The **Operating System Groups** screen appears.
      vi. Enter **n** to go to the next screen. The **User Access** screen appears.

4. 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 HP SMH 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. 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 appears.
7. Configure the HP SMH trust mode.

   Enter `1` for **Trust by Certificate**.

   The line with `1 Trust by Certificate` (selected) becomes yellow.

   The following options are available: Trust by Certificate, Trust by Name, Trust All and Modify Certificate List.

   a. Trust by Certificate
      i. To add a certificate file:
         A. Enter `1`. You are prompted for the certificate location.
         B. Enter the file path of the trusted certificates to be added to the **Trusted Certificates List**. Press **Enter** when you are finished.

            For example:

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

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

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

      ii. To import a certificate:
         A. Enter `2`. You are prompted for the server name.
         B. Enter the name or IP address 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.

         C. 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.
         D. Press **Enter** when you are finished importing certificate files.

      iii. To delete a certificate:
         A. Enter `3`. You are prompted to enter the number associated with the certificate file to be deleted.
         B. Enter the number of the certificate file to be deleted.
         C. Press **Enter** when you are finished. You can delete as many certificate files as you want by repeating these steps.
         D. Press **Enter** when you are finished deleting certificate files.

b. Trust by Name

i. Enter `2` to **Trust by Name**.

The line with `2 Trust by Certificate` (selected) becomes yellow.

ii. Enter `4` to **Modify Server Name** list.

To add an HP Systems Insight Manager server's certificate name:

A. Enter `1`. You are prompted to add an HP Systems Insight Manager server's certificate name.

B. Enter the name of the certificate of HP Systems Insight Manager server to be trusted and press **Enter**. The certificate name appears in the **Trusted Server Names** list.

Note: You can add as many server certificate names as you want.

To delete a certificate name:

A. From the **Server Name** list, enter `2`.

B. Enter the number associated with the name of the certificate of HP SIM server to be deleted. The HP SIM server's certificate name is removed from the **Server Name** list.

iii. Enter **n** for next. The **Trust Mode Settings** screen appears.

c. Trust All

i. Enter `3` to **Trust All**.

The line with `3 Trust by Certificate` (selected) becomes yellow.

ii. Enter **n** for next. The **IP Binding** screen appears.

d. Modify Certificate List

Enter `4` to **Modify Certificate List**.

8. Bind IP addresses that match a subnet and netmask.

The following options are available:

a. Enable IP Binding

i. Enter `1` to enable the IP Binding, which sets it to **ON**. `IP Binding: ON` appears.

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

The following options are available:

To add an IP address:

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

B. Enter the IP address to be added. `IP Address: YourIPAddress` appears. You are prompted for the netmask.

C. Enter the netmask. `netmask: YourNetmask` appears.

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 to be deleted. The IP address or netmask is removed from the IP address or netmask list.

iii. Enter **n** to go to the next screen. The **IP Restricted Login** screen appears.

b. Disable IP Binding

i. Enter `2` to disable the IP Binding, which sets it to **OFF**. `IP Binding: OFF` appears.

ii. Enter **n** to go to the next screen or enter **p** to go to the previous screen. The **IP Restricted Login** screen appears.

9. Configure HP SMH to restrict login access based on the IP address of the system from which the login is attempted.

   The following options are available:

   a. Enter `1` to enable an IP Restricted Login, which sets it to **ON**. **IP Restricted Login:ON** appears.

      To enable the IP Restricted Login:

      i. Enter `1`. **IP Restricted Login** is set to **ON**.

      ii. Press **n** for next. The **Set IP Address Restrictions** screen appears.

         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 appears 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 from the Inclusion list:

         A. Enter `2`.

         B. 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**.

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

         1. Enter `2` for Exclude Login Restriction IP Address

         2. Enter `1` to add an IP address to the Exclusion List.

         3. 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**.

         4. Press `Enter` . The **IP Address Exclusion List** screen appears.

         5. Press `n` for next. The **IP Address Inclusion List** and **IP Address Exclusion List** appears.

         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.

         3. Press **Enter**. The IP address is deleted from the **IP Address Exclusion List**.

         4. Press **Enter**. The **IP Address Exclusion List** screen appears.

         5. Press `n` for next. The **IP Address Inclusion** list and **IP Address Exclusion** list appears.

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

      iii. Enter **n** for next.

   b. Enter `2` to disable IP Restricted Login, which sets it to **OFF**. `IP Restricted Login: OFF` appears.

      To disable IP Restricted Login:

      Enter `2` to disable the IP Restricted Login. The IP Restricted Login is set to **OFF**.

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

10 Installing in-place on Linux using Linux Deployment Utility

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

The previous chapter provides steps to install HP SMH in-place on Linux x86 systems and x86_64 systems.

Installing HP SMH with preconfiguration

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 preconfiguring the HP SMH component is optional.

Preconfiguring the HP SMH component

Note: All preconfiguration settings are saved in the component XML file.

To preconfigure the HP SMH component:

1. Run the `install###.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 on **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 five names, separated by semicolon or space)** field, enter the operating system group name for administrator-level access.

   Note: You can enter up to five 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 five names, separated by semicolon or space)** field, enter the operating system group name for operator-level access.

   Note: You can enter up to five 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 five names, separated by semicolon or space)** field, enter the operating system group name for user-level access.

   Note: You can enter up to five 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 select **TrustByCert** 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 select **TrustByName** from the **Trust Mode** dropdown menu, enter the names of the trusted HP SIM servers' certificate and separate multiple entries with a semicolon in the list of trusted **Host 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 pairs separated by semicolons. For example, *IPAddress1/Netmask1;IPAddress2/Netmask2*.
13. In the **Enable IP Restricted Login** field, enter **YES** to enable IP restricted logins or **NO** to disable IP restricted logins.
14. In the **Enter include IP Addresses, or ranges** field, enter the IP addresses or range of IP address to be included.
15. In the **Enter exclude IP Addresses, or ranges** field, enter the IP addresses or range of IP address to be excluded.
16. Click **Save** to save your configuration, or click **Cancel** to discard your configuration.
17. Click **OK** to close the **HP ProLiant Linux Deployment Utility** screen.
18. After preconfiguration 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 independent.

Installing HP SMH as a single component

You can install HP SMH independent of other components included in the ProLiant Support Pack.

To install HP SMH as a single component:

1. Select all components *except* the HP SMH component.
2. Right-click all other components and select **Do Not Install component**.
3. Installs the HP SMH component with the configurations that are provided through the Linux Deployment Utility.

   For more information about using the Linux Deployment Utility, see the *HP ProLiant Support Pack and Deployment Utilities User Guide*.

4. The HP SMH component can also be installed by invoking the following command from the shell prompt: `./install###.sh –c hpsmh>version<.linux.i???.rpm`.

Installing HP SMH without preconfiguration

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

11 Initializing the software for the first time

After HP System Management Homepage (HP SMH) 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.

Key and certificate information

- In HP-UX, both public and private keys for HP SMH 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 HP SMH are stored in the `/opt/hp/sslshare` directory or `/etc/opt/hp/sslshare` directory in HP SMH 2.1.3 and later. 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 HP SMH 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 HP SMH to generate a new certificate and private key.

NOTE: Certificate and private key generation only occur the first time HP SMH 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.

12 Logging in and logging out of HP SMH

This chapter provides browser and command line instructions for logging in to and out of HP System Management Homepage (HP SMH).

Logging in with Windows XP

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

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 and security model for local accounts** and select **Properties**. The **Local Security Policy Setting** dialog box appears.

   Note: The **Network Access** item may be worded differently, depending on your environment.
5. Select **Classic - local users authenticate as themselves**.
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 HP SMH with Internet Explorer:

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

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

   To add HP SMH to Internet Explorer's Trusted Sites:

   a. From Internet Explorer, click **Tools** ⇒ **Internet Options**.
   b. Click the **Security** tab. The Security tab appears.
   c. Select the **Trusted sites** icon.
   d. Click **Sites...**. The Trusted sites dialog box appears.
   e. In the **Add this website to the zone** field, enter **`https://hostname:2381/`** and click **Add**.
   f. Click **OK** to save your changes and close the Trusted sites dialog box.
   g. 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 HP SMH 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 HP SMH.

   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 HP SMH, 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, see the *HP System Management Homepage Online Help*.

3. Click **Yes**.

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

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

   If you have not yet added user groups into HP SMH 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 HP SMH.

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

Logging in with Mozilla and Firefox

To log in to HP SMH with Mozilla and Firefox:

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

   If you are using Mozilla or Firefox 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 HP SMH 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 HP SMH 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 **HP System Management Homepage** appears.

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

   If you have not yet added user groups into HP SMH 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 HP SMH.

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

Logging in from the HP-UX command line

You can verify whether the autostart daemon is running with the following 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:2301`**.

You can also use the `samweb` command to automatically start the default browser in the main HP SMH page.

After the daemon is running and the HP-UX Apache-based Web Server is started with autostart, you can log in to HP SMH with either http://*hostname*:2301 or https://*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

Select one of the following 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 use to log in to HP SMH.
- You can stop HP SMH 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 HP SMH through 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).

  For more information, go to the *hpsmh*(1m) manpage: **`man hpsmh`**.

13 Uninstalling HP SMH

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

Uninstalling from an HP-UX system

To uninstall HP SMH on an HP-UX system, use the following `swremove` command:

```
swremove -x enforce_dependencies=false SysMgmtHomepage
```

This is the recommended HP-UX method of uninstalling HP SMH.

Uninstalling from a Linux Itanium, x86 or x86_64 system

To uninstall HP SMH:

Run the following command:

```
rpm -e hpsmh
```

Uninstalling from a Windows system

Use the **Add/Remove Programs** feature in Windows, and complete the following steps to remove HP SMH:

1. Select **Start** ⇒ **Control Panel** ⇒ **Add or Remove Programs**.
2. Select **HP System Management Homepage**.
3. Click **Remove**. HP SMH is uninstalled.

Uninstalling from multiple Windows systems silently

You can write a script to uninstall HP SMH silently on multiple Windows systems simultaneously. To uninstall HP SMH 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, use the following command:

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

Uninstalling manually for Windows and Linux systems

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

Note: Items marked *if present* are present if there is an existing HP SMH 2.0.1 or 2.0.2 installation.

CAUTION: All HP SMH configuration settings will be lost after uninstalling manually!

To manually uninstall HP SMH:

1. Stop the HP SMH service.
2. Remove the following directories and files on the system drive:
   - \hp\hpsmh\csicon.ico
   - \hp\hpsmh_jvm (if present)
   - \hp\hpsmh\certs
   - \hp\hpsmh\conf
   - \hp\hpsmh\data
   - \hp\hpsmh\lib
   - \hp\hpsmh\logs
   - \hp\hpsmh\modules
   - \hp\hpsmh\namazu
   - \hp\hpsmh\session\
   - \hp\sslshare\

     For **Linux**, sslshare is located in `/etc/opt/hp/sslshare`

     For **Windows**, sslshare is located in `<systemdrive>:\hp\sslshare`
   - For Linux you will need to remove the following additional files:

     /usr/local/hp

     /var/spool/opt/hp

   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`

Uninstalling manually for HP-UX systems

This section describes how to manually uninstall HP SMH on an HP-UX system.

CAUTION: Manually uninstalling HP-UX SMH is not recommended.

When it is necessary to uninstall HP-UX SMH, HP recommends using the `swremove` command, as described in "Uninstalling from an HP-UX system" (page 67).

The following procedure manually uninstalls HP SMH on an HP-UX system.

1. Stop the HP SMH service.
2. Remove (using `rm -rf`) the following directories:
   - `/var/opt/hpsmh`
   - `/opt/hpsmh/session`
   - `/opt/hpsmh/certs`
   - `/opt/hpsmh/cookies`
   - `/opt/hpsmh/sslshare`
   - `/opt/hpsmh/tmp`

CAUTION: On HP-UX systems, do not remove all files under the `/opt/hpsmh` directory because files for SMH HP-UX web applications also are stored there. Only remove the directories listed above.

Also on HP-UX systems, the `/etc/opt/hp/sslshare` directory is used by HP SIM and should not be removed.

Index