

HP System Management Homepage Installation Guide

HP-UX, Linux, and Windows Operating Systems



Legal Notices

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

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Trademark Notices

AMD and Opteron are trademarks of Advanced Micro Devices, Inc.

Adobe and Acrobat are trademarks of Adobe Systems Incorporated.

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

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

Microsoft and Windows are U.S. registered trademarks of Microsoft Corporation.

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

UNIX is a registered trademark of The Open Group.

Java™ is a registered trademark of Oracle and/or its affiliates.

Microsoft Windows XP and Microsoft Windows Server, are registered trademarks of Microsoft Corporation in the United States of America and in other countries.

Table of Contents

| | | |
|----------|---|-----------|
| 1 | Installation requirements..... | 7 |
| | Supported operating systems..... | 7 |
| | Supported browsers..... | 8 |
| | Verifying system requirements..... | 9 |
| | Obtaining HP SMH software..... | 9 |
| | HP media..... | 9 |
| | HP websites..... | 9 |
| 2 | Preparing to install HP SMH..... | 11 |
| | Installation information..... | 11 |
| 3 | Installing HP SMH on HP-UX operating systems..... | 13 |
| | System Administration Management Tool changes: SAM and HP SMH..... | 13 |
| | Installing HP SMH on HP-UX..... | 13 |
| | Installing HP SMH and dependent applications..... | 13 |
| | Installing HP SMH using the Applications media..... | 15 |
| | Installing using HP SMH Software Depot..... | 16 |
| | Configuring HP SMH..... | 16 |
| | Configuring the startup mode..... | 17 |
| | Disabling port 2301..... | 18 |
| | Patching or updating HP SMH software..... | 18 |
| 4 | Installing HP SMH on a Windows operating system..... | 21 |
| | Installing HP SMH directly on Windows..... | 21 |
| | Installing HP SMH for Windows silently..... | 32 |
| | Generating a setup.iss file..... | 32 |
| | Installing silently using the CLI..... | 32 |
| | Reinstalling silently using the CLI..... | 32 |
| | Configuring HP SMH..... | 33 |
| 5 | Installing HP SMH using HPSUM..... | 35 |
| | Installing HP SMH on a Windows operating system using HPSUM..... | 35 |
| | Installing HP SMH on a Linux operating system using the HPSUM..... | 41 |
| | Preconfiguring the HP SMH component..... | 47 |
| 6 | Installing HP SMH directly on Linux operating systems..... | 51 |
| | Installation for Linux on x86 and x86_64 operating systems..... | 51 |
| | Installing HP SMH on Linux x86 operating systems..... | 51 |
| | Installing HP SMH on x86_64 operating systems..... | 51 |
| | Configuring HP SMH..... | 51 |
| 7 | Installing HP SMH directly on Itanium-based Linux operating systems..... | 53 |
| | Installation for Itanium-based Linux operating systems..... | 53 |
| | Installing HP SMH on Itanium-based Linux operating systems..... | 53 |
| | Configuring HP SMH..... | 53 |
| 8 | Initializing the software for the first time..... | 59 |
| | Key and certificate information..... | 59 |

| | |
|--|----|
| 9 Signing in and signing out of HP SMH..... | 61 |
| Signing in with Microsoft Windows XP..... | 61 |
| Signing in with Microsoft Internet Explorer..... | 61 |
| Signing in with Mozilla and Firefox..... | 62 |
| Signing in from the HP-UX CLI..... | 62 |
| Signing out..... | 63 |
| 10 Uninstalling HP SMH..... | 65 |
| Uninstalling from an HP-UX operating system..... | 65 |
| Uninstalling from a Itanium-based Linux, x86 or x86_64 operating system..... | 65 |
| Uninstalling from a Windows operating system..... | 65 |
| Uninstalling from a Windows 2008 operating system..... | 65 |
| Uninstalling HP SMH on a CLI-based Windows system..... | 65 |
| Uninstalling manually for Windows and Linux operating systems..... | 66 |
| Uninstalling manually for HP-UX operating systems..... | 67 |
| Support and other resources..... | 69 |
| Information to collect before contacting HP..... | 69 |
| How to contact HP..... | 69 |
| Registering for software technical support and update service..... | 69 |
| How to use your software technical support and update service..... | 69 |
| Warranty information..... | 69 |
| HP authorized resellers..... | 70 |
| Documentation feedback..... | 70 |
| New and changed information in this edition..... | 70 |
| Related information..... | 70 |
| HP SMH documentation..... | 70 |
| HP-UX documentation..... | 71 |
| HP Insight Remote Support Software..... | 72 |
| Typographic conventions..... | 72 |
| Index..... | 73 |

List of Tables

| | | |
|-----|-------------------------------------|----|
| 3-1 | Bundle information..... | 13 |
| 3-2 | Variables and tags..... | 17 |
| 4-1 | Environment variables and tags..... | 33 |

1 Installation requirements

Supported operating systems

HP ProLiant servers

- Microsoft Windows Server 2011 Small Business
- Microsoft Windows 7 for x86 and x64
- Microsoft Windows Server 2008 SP2
- Microsoft Windows Server 2008 Foundation R2
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2008 R2 Server Core
- Microsoft Windows Server 2008 Essential Business
- Microsoft Windows Server 2008 Small Business SP2
- Microsoft Windows Server HPC 2008
- Microsoft Windows Server 2003 Standard Edition SP2 for x86 and x64
- Microsoft Windows Server 2003 R2 Standard Edition SP2 for x86 and x64
- Microsoft Windows Server 2003, Web Edition SP2
- Microsoft Windows Server 2003 Enterprise Edition SP2 x86 and x64
- Microsoft Windows Server 2003 R2 Enterprise Edition SP2 x86 and x64
- Microsoft Windows Server 2003 Small Business Standard and Premium R2
- Microsoft Windows Server 2003 Small Business SP2
- Microsoft Windows Vista Business Edition
- Microsoft Windows Vista Enterprise Edition
- Microsoft Windows Vista Ultimate Edition
- Microsoft Windows Vista SP2
- Microsoft Windows XP SP2
- Microsoft Windows XP SP3
- Red Hat Enterprise Linux 6 for x64
- Red Hat Enterprise Linux 6 for x86 and AMD64/EMT64T
- Red Hat Enterprise Linux 5 update 5 for x86 and AMD64/EMT64
- Red Hat Enterprise Linux 5 update 4 for x86 and AMD64/EMT64T
- Red Hat Enterprise Linux 4 update 8 or later for x86 and AMD64/EMT64T
- Oracle Enterprise Linux
- SUSE Linux Enterprise Server (SLES) 11 (SP1) for x86 and AMD64/EMT64T
- SUSE Linux Enterprise Server (SLES) 11 for x86 and AMD64/EMT64T
- SUSE Linux Enterprise Server (SLES) 10 SP3 or later for x86 and AMD64/EMT64T
- SUSE Linux Enterprise Server (SLES) 10 SP2 or later for x86 and AMD64/EMT64T
- VMware ESX 3.5 update 5
- VMware ESX 4.0 update 1
- VMware ESX 4.0 update 2
- VMware ESX 4.1
- Novell Open Enterprise Server (OES 2)

- Citrix XEN 5.6
- Citrix XEN 5.5 U2

HP Integrity servers

- Microsoft Windows Server 2008 for Itanium-based systems, 64-bit
- Microsoft Windows Server 2008 R2 for Itanium-based systems, 64-bit
- Red Hat Enterprise Linux 5.0 Update 1
- Red Hat Enterprise Linux 4.0 Update 6
- SUSE Linux Enterprise Server (SLES) 10 Service Pack 1
- SUSE Linux Enterprise Server (SLES) 9 Service Pack 4

HP-UX

- 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



NOTE: For Linux operating systems, Lightweight Directory Access Protocol (LDAP) is supported on SUSE Linux Enterprise Server 9 and SUSE Linux Enterprise Server 10.

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

HP-UX 11i v1 (B.11.11) Operating Environments are for PA-RISC systems only. HP-UX 11i v2 (B.11.23) Operating Environments (September 2004 and later). HP-UX 11i v3 (B.11.31) Operating Environments (February 2007 and later) support both PA-RISC and Itanium-based operating systems.

NOTE: To install the HP SMH application, a minimum of 100 MB free disk space is required.

Supported browsers

For HP-UX Itanium-based or PA-RISC operating systems:

- Internet Explorer 6.0 SP2
- Internet Explorer 7.0 (SMH 2.2.9 or later)
- Internet Explorer 8.0 (HP SMH 3.0.2 or later)
- Firefox 1.6, 1.7
- Firefox 1.0.2, 1.5, 2.0

For Windows Itanium-based or x86 operating systems:

- Internet Explorer 7.0 (SMH 2.1.9 or later)
- Internet Explorer 8.0 (HP SMH 6.0 or later)
- Firefox 2.0.0.x
- Firefox 3.0
- Firefox 3.5
- Firefox 3.6

For Linux Intel Itanium or x86 operating systems:

- Internet Explorer 8.0 (HP SMH 6.0 or later)
- Firefox 3.0
- Firefox 3.5
- Firefox 3.6



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.

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 was found.
- For HP-UX, Linux, and Windows, the signed in user has administrator/root rights. If the user does not have these rights, an error message appears, indicating that administrator/root rights were not detected.
- For Linux, if a dependency is not met on an Itanium-based operating system, the installation does not complete.

Obtaining HP SMH software

HP 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 6.20 or later
- HP SmartStart CD 8.20 or later
- HP ProLiant Support Pack 8.20 or later
- HP Integrity Support Pack 6.20 or later
- HP Management DVD 8.40 or later
- HP Insight Software DVD 6.0 or later

HP websites

These HP websites are accessible from any system with a web browser and access to the Internet:

- To download the latest software versions, see the HP website at <http://www.hp.com>.
- For HP-UX operating systems, you can also find the software on the Software Depot home at <http://www.hp.com/go/softwaredepot>.
- For Linux and Windows operating systems, 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, see the **Support and Drivers** tab at <http://www.hp.com>.

2 Preparing to install HP SMH

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

You can install HP SMH locally using the Windows ProLiant or Integrity Support Pack or the Linux RPM (Red Hat Package Manager) or remotely with optional preconfiguration using the HP Smart Update Manager (HPSUM) on Windows or on Linux.

Installation information

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

To change the default configuration values, type the following command at the root prompt:
`/opt/hpsmh/bin/smhconfig`

- For Linux operating systems

HP SMH is installed by an RPM package without asking you to configure any settings. After the installation is complete, run the script `/opt/hp/hpsmh/sbin/smhconfig` on a ProLiant system or `/opt/hp/hpsmh/smhconfig/hpSMHSetup.pl` on Itanium-based operating systems to set the security options used by all HP Web-based Agents on the system. Otherwise, these settings use default values.

To change the default configuration values, type the following command at the root prompt:
`/opt/hp/hpsmh/sbin/smhconfig`

- For Windows operating systems

The configuration settings are carried over from the `<System Drive>:\hp\hpsmh\conf\smhpdp.xml` file, and the wizard initiates the configuration.



NOTE: libiconv source module is placed in the SMH installation directory `<System Drive>:\hp\hpsmh\extras` for Windows x64 systems only.



NOTE: If HP SIM is installed after HP SMH is installed, the HP SMH 2048-bit key pair is replaced with the HP SIM 1024-bit key pair.

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

3 Installing HP SMH on HP-UX operating systems

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 and X-based interfaces.

Some of the key changes are:

- 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.11.31) only, a new command, *smh(1m)* is introduced (`/usr/sbin/smh`). This command 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`.

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



NOTE: After you install HP SMH, it is configured automatically for you. To change the default configuration settings, go to “Configuring HP SMH” (page 16).

Installing HP SMH and dependent applications

HP SMH requires several applications, but some applications are optional. You might have these applications installed on your system. The following bundle information will help you identify the correct bundles to download and install.

Table 3-1 Bundle information

| Product | Bundle | Path | Status | Release |
|---------|------------|----------------------------------|----------|----------------------|
| HP SMH | SysMgmtWeb | /opt/hpsmh and /var/opt/hpsmh | Required | HP-UX 11i v1, v2, v3 |

| Product | Bundle | Path | Status | Release |
|--|--|--|---|--|
| HP-UX Apache-based Web Server | hpuxwsApache | /opt/hpws/apache | Required | HP-UX 11i v1, v2, v3 NOTE: HP-UX 11i v3 version of the HP SMH can work on either the Apache 2.0 or 2.2 server. |
| HP-UX Apache-based Web Server | hpuxws22Apache | /opt/hpws22/apache | Required | HP-UX 11i v3 NOTE: HP-UX 11i v3 version of the HP SMH can work either on Apache 2.0 or 2.2 server. |
| 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 Strong Random Number Generator | KRNG11i | /usr/conf or /usr/conf/lib/libmg.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 NOTE: This version of Tomcat is compatible with Apache 2.0 server only. | /opt/hpws/tomcat | Recommended. HP SMH plug-ins such as Partition Manager require it. | HP-UX 11i v1, v2, v3 |
| HP-UX Tomcat-based Servlet Engine | hpuxws22Tomcat NOTE: This version of Tomcat is compatible with Apache 2.2 server only. | /opt/hpws22/tomcat | Recommended. HP SMH plug-ins such as Partition Manager require it. | HP-UX 11i v3 |
| HP WBEM Services | WBEMSvcS | /opt/wbem | Recommended. HP SMH plug-ins 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. HP SMH plug-ins such as Property Pages found on the Home page require it. | HP-UX 11i v1, v2, v3 |
| PropPlus (Property Page Plus) | SysMgmtPlus | /opt/hpsmh/data/ htdocs/propplus | Recommended | HP-UX 11i v3 March 2009 Release |
| HP-UX Software Distributor | HPUXBaseAux for HP-UX 11i v1 and v2. SwMgmtMin for HP-UX 11i v3. | /usr/lib/sw/wbem/ | Recommended. HP SMH plug-ins, 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. HP SMH plug-ins 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. HP SMH plug-ins such as Property Pages found on the Home page require it. | HP-UX 11i v2, v3 |

| Product | Bundle | Path | Status | Release |
|----------------------------|-----------------------------------|---|---|----------------------|
| WBEM Provider for SCSI HBA | SCSIProvider | /opt/scsiprovider/ | Optional. HP SMH plug-ins 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. HP SMH plug-ins such as Partition Manager require it. | HP-UX 11i v1, v2, v3 |
| HP-UX CDE User Interface | CDE | /usr/dt/lib/, /usr/dt/lib/hpux32/, and /usr/dt/lib/hpux64/ | Optional. HP SMH plug-ins such as DSAU require it. | HP-UX 11i v1, v2, v3 |
| HP-UX X Window Software | X11 | /opt/atok/X11, /usr/bin/X11 , and /usr/lib/X11/ | Optional. HP SMH plug-ins such as fsweb require it. | 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 installed by default. See the *HP-UX Installation and Update Guide* on the HP Technical Documentation website at <http://www.hp.com/go/hpux-core-docs> for instructions on how to install and update HP-UX, including recommended and default-installed HP application bundles. See “Installing HP SMH using the Applications media” (page 15).
- 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 “Installing HP SMH using the Applications media” (page 15).
- 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 “Installing using HP SMH Software Depot” (page 16).
- 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 need to create one image to install on multiple operating systems. See the *Ignite-UX Administration Guide* and the *Software Distributor Administration Guide* on the HP Technical Documentation website at <http://www.hp.com/go/hpux-core-docs>.

Installing HP SMH 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. If one does not exist, create a mount point for the Applications DVD.
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. Using the `mount` command, specify the DVD device name and mount point. For example, the following command mounts the `/dev/dsk/c1t0d0` device as the `/cdrom` directory:

```
mount /dev/dsk/c1t0d0 /cdrom
```


See the `mount(1M)` manpage for details.
2. Determine which products and versions are on your system, using the `swlist` command:

```
/usr/sbin/swlist -l product
```

3. Install software from the Applications DVD using the `swinstall`.
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 automatically unmounts 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.
6. Start using HP SMH.

Installing using HP SMH Software Depot

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** link.
4. Complete the registration form.
5. Review any installation instructions.
6. Save the bundle to a local directory such as `/var/temp`.
7. 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
```

8. Start using HP SMH.



NOTE: When HP SMH is installed, the user **hpsmh** and group **hpsmh** is automatically added to the `/etc/passwd` file. If you are using LDAP or any other network service to manage user and group accounts, there might be a possibility that the user ID (UID) and the group ID (GID) is already in use by the LDAP users, which can be confusing. The problem occurs in HP-UX 11i v3 on Integrity systems.

To overcome this, add a local **hpsmh** user and group using a unique UID and GID (IDs not in use by LDAP or the other network services) manually before installing the HP SMH.

1. Determine the available reserved IDs for the group (for example, 130) and the user (for example, 125).
2. Add the group using the command `/usr/sbin/groupadd -g 130 hpsmh`.
3. Add the user using the command `/usr/sbin/useradd -u 125 -g hpsmh -d /var/opt/hpsmh \ -c "System Management Homepage" hpsmh`.
4. Add the group using the command `/usr/sbin/groupadd -g 130 hpsmh`.
5. Add the user using the command `/usr/sbin/useradd -u 125 -g hpsmh -d /var/opt/hpsmh \ -c "System Management Homepage" hpsmh`.

Configuring HP SMH

The HP SMH configuration is based on environment variables and tags that are set by the following files:

- `/opt/hpsmh/sbin/envvars`
- `/opt/hpsmh/conf.common/smhp.xml`
- `/opt/hpsmh/conf/timeout.conf`
- CLI `smhconfig` tool located at `/opt/hpsmh/bin`

To change the default configuration, you can modify the files to set the value of the variables and tags described in Table 3-2 “Variables and tags” table.

Table 3-2 Variables and tags

| Variable | Description | Script |
|---------------------------------------|--|--|
| JAVA_HOME | This variable points to the /opt/hpsmh/sbin/envvars directory where JDK is installed. | /opt/hpsmh/sbin/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 stops 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 15 minutes. You can define the <session-timeout> tag using any value between 6 and 120 minutes. | /opt/hpsmh/conf/common/smhpd.xml |
| 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 stops 3 minutes after the HP SMH session timeout. If it is defined and greater than the HP SMH session timeout, then the HP SMH server stops after the time period has elapsed without any user activity. If it is not defined or equal to zero, then HP SMH starts without timeout. When the "automatic startup on boot" startup mode is in use, the timeout mechanism does not start. | /opt/hpsmh/conf/timeout.conf |
| TIMEOUT_TOMCAT | This variable defines the Tomcat timeout in minutes in the /opt/hpsmh/conf/timeout.conf file. If it is defined, Tomcat istops 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 starts without timeout. In this case, Tomcat stops only when HP SMH is stopped. | /opt/hpsmh/conf/timeout.conf |
| TOMCAT_PORT (HP-UX 11i v3) | With HP SMH running on Apache 2.2, this parameter defines the port used for communication between the Apache server and the Tomcat server. The default value is 1188. TOMCAT_PORT=1188 | /opt/hpsmh/tomcat/conf/tomcat.conf /opt/hpsmh/tomcat/conf/server.xml NOTE: The value of the Connector port in the /opt/hpsmh/tomcat/conf/server.xml file should match the port number mentioned in the /opt/hpsmh/tomcat/conf/tomcat.conf file for successful communication between the HP SMH Apache and Tomcat process. Restart the HP SMH process whenever there is a change in this port value. |

Configuring the startup mode

HP SMH supports three startup modes:

- Autostart URL

This mode is the default setting. You can start HP SMH by using a web browser and navigating to **http://hostname:2301/**. If autostart is the default, a daemon listens on **http://hostname:2301**

only (nothing listens on port 2381, so that port fails). When it contacts port 2301 (http), then the HP-UX Apache-based Web Server starts on port 2381 (https), and the page redirects.

- 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 using a web browser and navigating to `https://hostname:2381/`. Daemons listen on both `http://hostname:2301/` and `https://hostname:2381/`. If you use port 2301 (http), then the HP-UX Apache-based Web Server starts on port 2381 (https), and the page automatically redirects.



NOTE: For autostart URL and automatic startup on boot, you can use `http://hostname:2301`. This is possible on an HP-UX operating system only.

- Manual startup

- You can start HP SMH from the HP-UX CLI.

Configure the startup mode of the HP SMH server and the Tomcat instance using `/opt/hpsmh/bin/smhstartconfig` script.

Syntax: `smhstartconfig [-a {on|off} -b {on|off}] [-t {on|off}]`

Options:

- a {on|off} Enable or disable the autostart URL mode.
- b {on|off} Enable or disable the automatic startup on boot mode.
- t {on|off} Set the Tomcat startup mode where:
 - on Starts Tomcat when HP SMH starts.
 - off Starts Tomcat on demand (default).

- You can start HP SMH from the HP-UX CLI.

To configure the Apache version to be used by the HP SMH (HP-UX 11i v3), execute the following script.

```
smhstartconfig -v {2.0|2.2}
```

where, selecting:

- 2.2 starts HP SMH with Apache 2.2
- 2.0 starts HP SMH with Apache 2.0

If you do not specify an option, 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), you can start the HP-UX Apache-based Web Server processes with the `/opt/hpsmh/sbin/hpsmh start` command without rebooting.

Disabling port 2301

You can disable port 2301. In the `smhpd.xml` file the `<port2301>` tag by default is set to True. To disable port 2301, you must set the value to False. You can use the `smhconfig` command to modify the configuration.

For more information about using the `smhconfig` command, see the *smhconfig(1M)* manpage.

Patching or updating HP SMH software

HP might issue patches to HP SMH. 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 operating system, see the *Patch Management User Guide for HP-UX 11.x Systems* on the HP Technical Documentation website at <http://www.hp.com/go/hpux-core-docs>.

HP might issue software updates to HP SMH. Check the following resources for any notices regarding software updates:

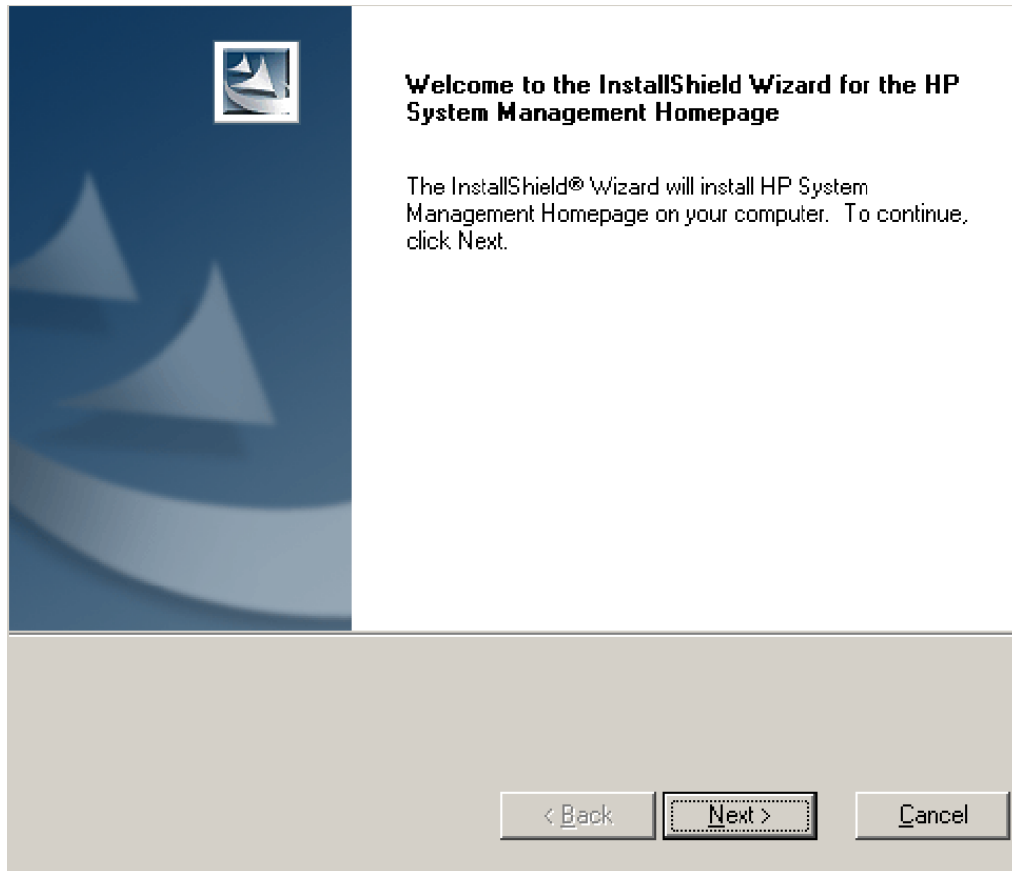
- HP-UX OE media
- HP-UX Applications media
- HP SMH web page on the Software Depot home at <http://www.hp.com/go/softwaredepot>
- HP SMH website at <http://hp.com/go/smh>

4 Installing HP SMH on a Windows operating system

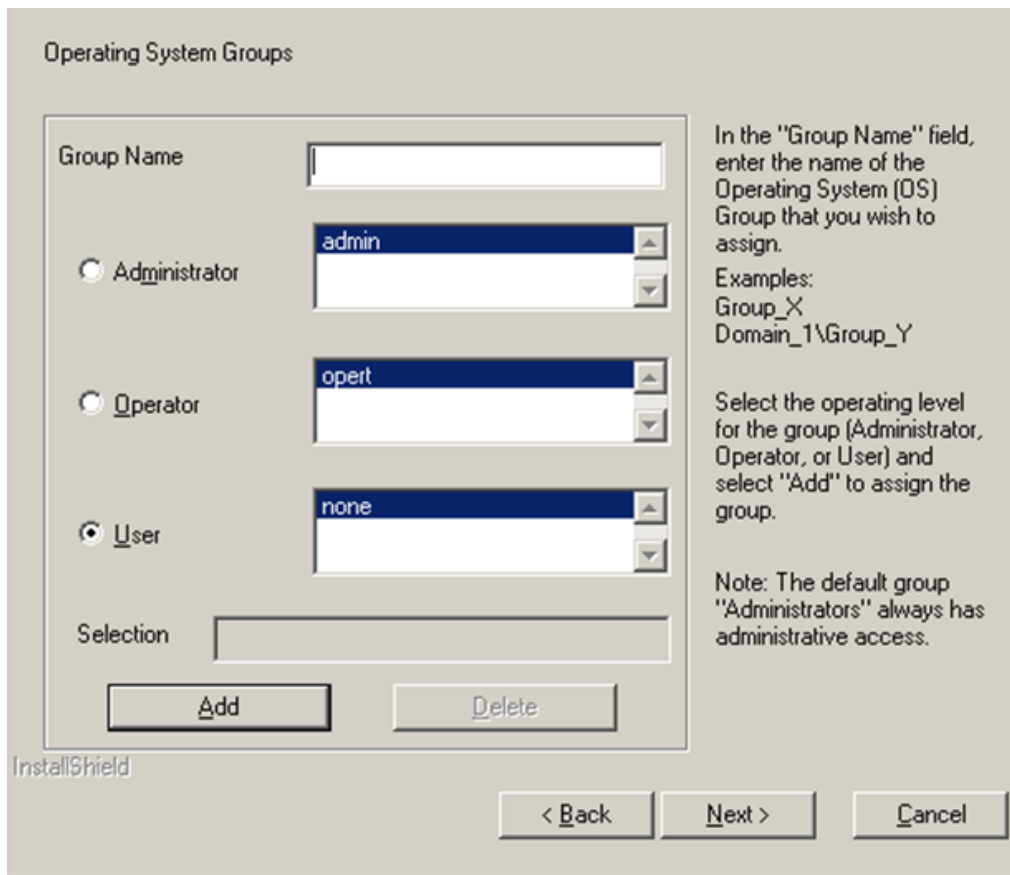
Installing HP SMH directly on Windows

Note: You can click **Cancel** at any time during configuration of HP SMH settings.

1. Initiate the `setup.exe` file to begin the installation wizard. After the wizard begins, the **Welcome** dialog box appears.



2. Click **Next**. The **OS Groups** dialog box appears.



3. 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 might lock out the administrator account. Using the administrator account, add another account with administrator privileges for Version Control Repository Manager access.

The operating system user group must be present on the system before you can add the user group to the System Management Homepage group list.

- c. Click **Add**. The group name is added. You can add a maximum of five entries for each group level.
Note: To delete a group name, select the group name and click **Delete**.
- d. Click **Next** to continue. 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** to automatically grant access to any user at the local console at the selected access level.
 - Selecting **Anonymous** enables restricted access to the unsecured pages.
 - Selecting **Administrator** grants access to both secure and unsecured pages.

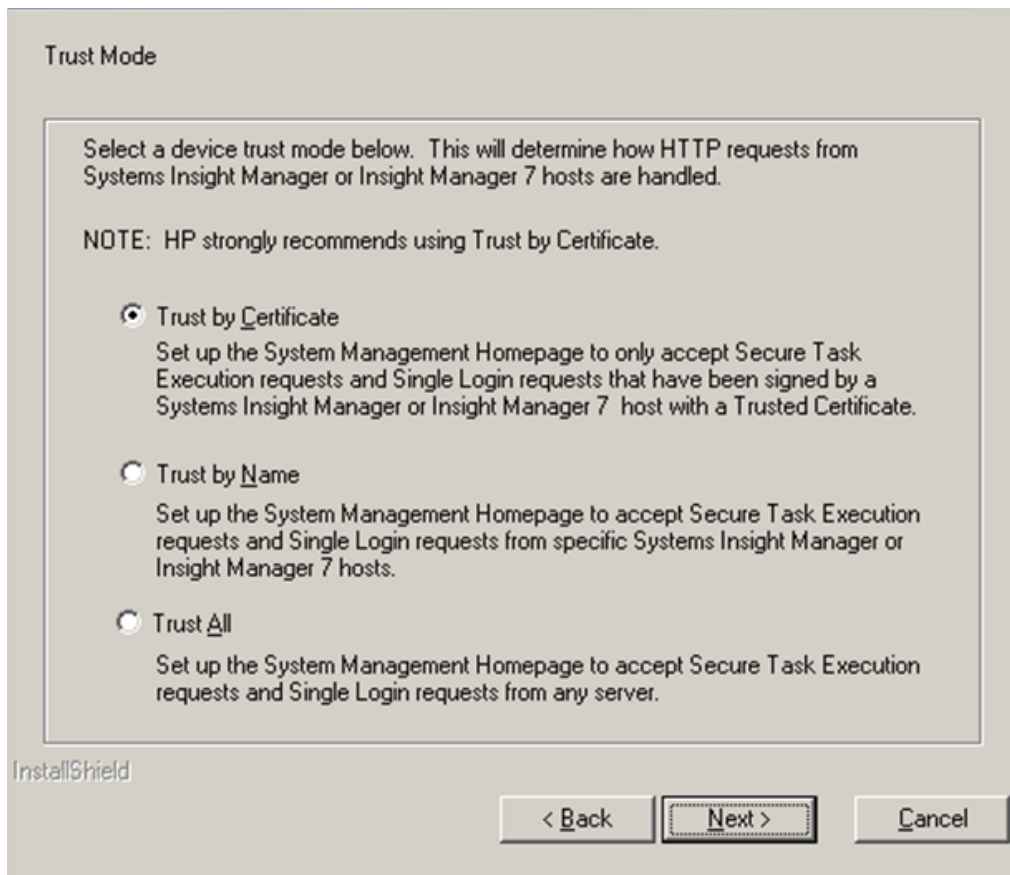
Caution: Selecting **Local Access** with administrator privileges provides all users with access to the local console full access without prompting them for a user name or password.

The **Port 2301** field provides the option to enable the port 2301. Select **Enable Port 2301** to enable the port 2301 during the installation process.

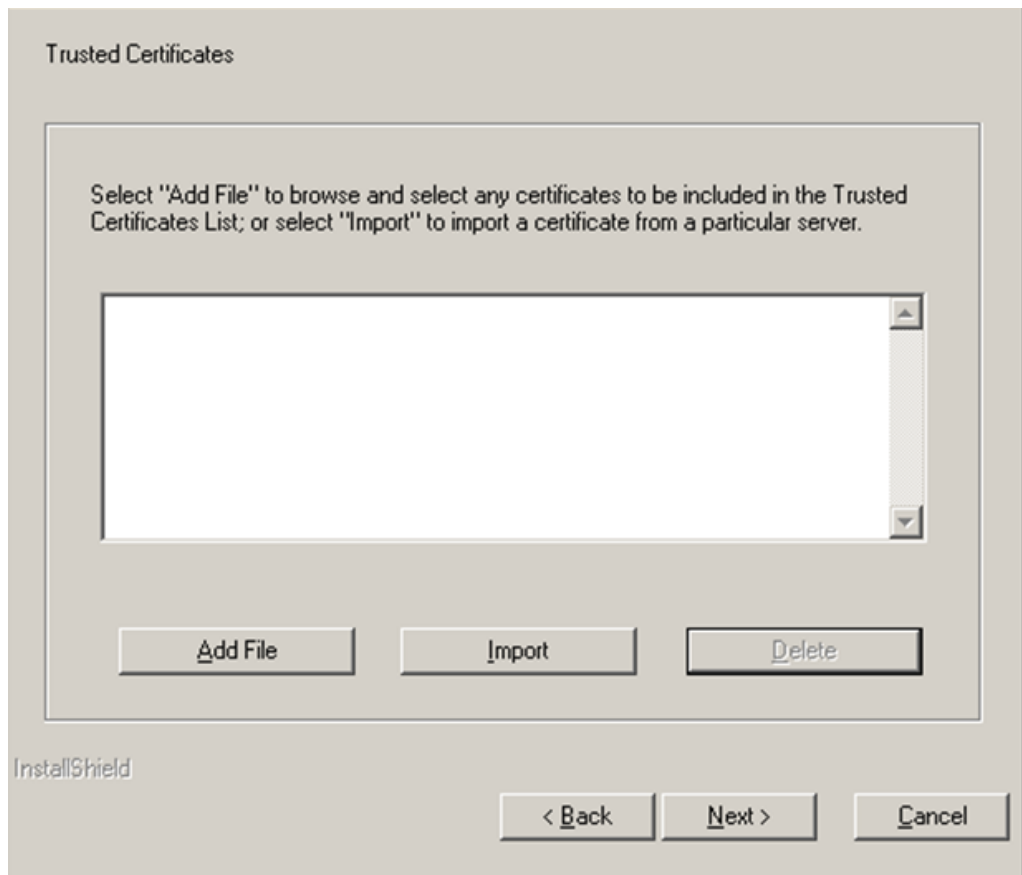


NOTE: By default, the **Port 2301** option is enabled.

4. Click **Next**. The **Trust Mode** dialog box appears.



5. Select the level of security you want to provide from one of the following trust modes:
 - Trust By Certificate
 1. Click **Next**. The **Trusted Certificates** dialog box appears. The **Trusted Certificates** dialog box allows you to add trusted certificate files to the **Trusted Certificate List**.



2. Click **Add File** to browse and select any certificates to be included in the **Trusted Certificate List**. The **Add File** dialog box appears. If you entered an invalid file name 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 SIM cannot access the HP Web-based Agents on this system. Click **OK** if you do not want HP SIM 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 Certificate** option enables the HP SMH system and the HP SIM system to establish a trust relationship using certificates. This mode is the strongest method of security because it requires certificate data and verifies the digital signature before enabling access.

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

To import a certificate:

1. Click **Import**. The **Import Server Certificate** dialog box appears.
2. Enter the name or IP address of the server whose certificate you want to import.
3. Click **Get Cert**. The certificate information appears.
4. 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 up to 128 trusted certificates.

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

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

- Trust By Name

1. Select **Trust By Name**.
2. Click **Next**. The **Trusted Server** dialog box appears.

Note: Although the **Trust By Name** mode is a slightly better security method than the **Trust All** mode, your system is still vulnerable to security attacks. The **Trust By Name** mode sets up HP SMH to accept only certain requests from servers with the HP SIM 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 on the wrong system. This option does not verify anything other than the HP SIM certificate name submitted.

3. Enter the names of the certificate of HP Systems Insight Manager servers you want to trust.
Note: The HP SIM server certificate name cannot contain the following characters: ~, !, ` , @, #, \$, %, ^, &, *, (,), +, =, \, ", :, ' , <, >, ?, ,, |, and ;.
4. Click **Add** to add the name of a certificate of HP SIM server you want to trust.
Note: You can enter a maximum of five HP SIM server names.
5. Click **Next**. The **IP Binding** dialog box appears.
Note: If you click **Next** without adding any HP SIM server certificate names to the list, an error message appears indicating that if you do not specify any trusted server names, HP SIM 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 SIM server certificate names to the list.
Note: To delete a HP SIM server certificate name, select the certificate name and click **Delete**. The selected certificate name is removed.

- Trust All

1. Select **Trust All**.
2. 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 all users in the network are trusted.

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

IP Binding

Select the IP Binding box below if you would like to bind to IP addresses that match a specific subnet and mask.

Enter the Subnet IP Address and Netmask in the designation boxes (up to 5 entries) and select "Add" to add the Subnet/Mask pair to the IP Binding List.

If IP Binding is enabled, and no Subnet/Mask pairs are configured, then the System Management Homepage will only be available on the localhost.

☐ Enable IP Binding

Subnet IP Address

Netmask

Add Delete

InstallShield

< Back Next > Cancel

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. Select **Enable IP Binding** checkbox and 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 appears 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 pair, 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.

Note: The masking field is not required for IPv6 addresses.

7. 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.

IP Restricted Logins

Access to the System Management Homepage can be restricted based on IP addresses.

Select the box below if you would like to include and/or exclude specific IP Addresses or IP Address ranges.

☒ **Enable IP Restricted Logins**

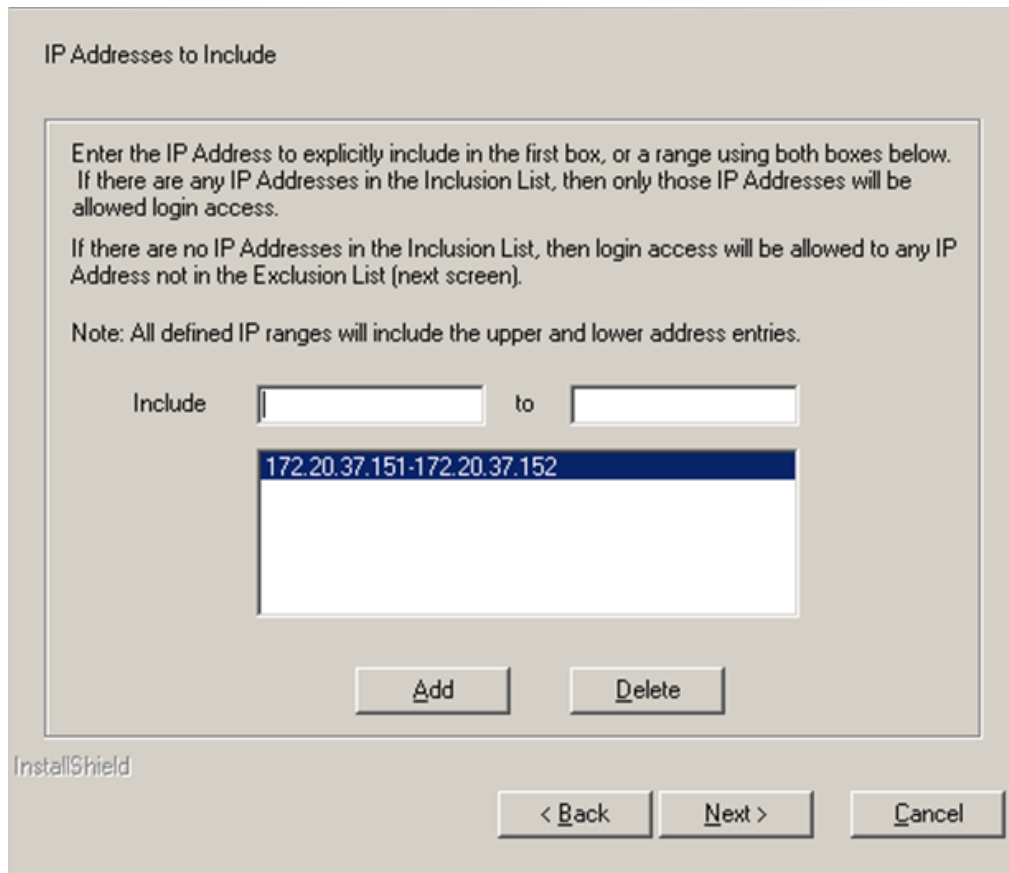
InstallShield

< Back

Next >

Cancel

8. 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 IP addresses are in the **Inclusion** list, then only those IP addresses have login privileges. If no IP addresses are in the Inclusion list, then all IP addresses that are not in the **Exclusion** list have login privileges.



The dialog box is titled "IP Addresses to Include". It contains the following text:

Enter the IP Address to explicitly include in the first box, or a range using both boxes below. If there are any IP Addresses in the Inclusion List, then only those IP Addresses will be allowed login access.

If there are no IP Addresses in the Inclusion List, then login access will be allowed to any IP Address not in the Exclusion List (next screen).

Note: All defined IP ranges will include the upper and lower address entries.

Below the text, there is a section labeled "Include" with two input boxes separated by the word "to". The first box contains the IP address "172.20.37.151" and the second box contains "172.20.37.152". Below these boxes is a list box containing the same range "172.20.37.151-172.20.37.152". At the bottom of the list box are two buttons: "Add" and "Delete".

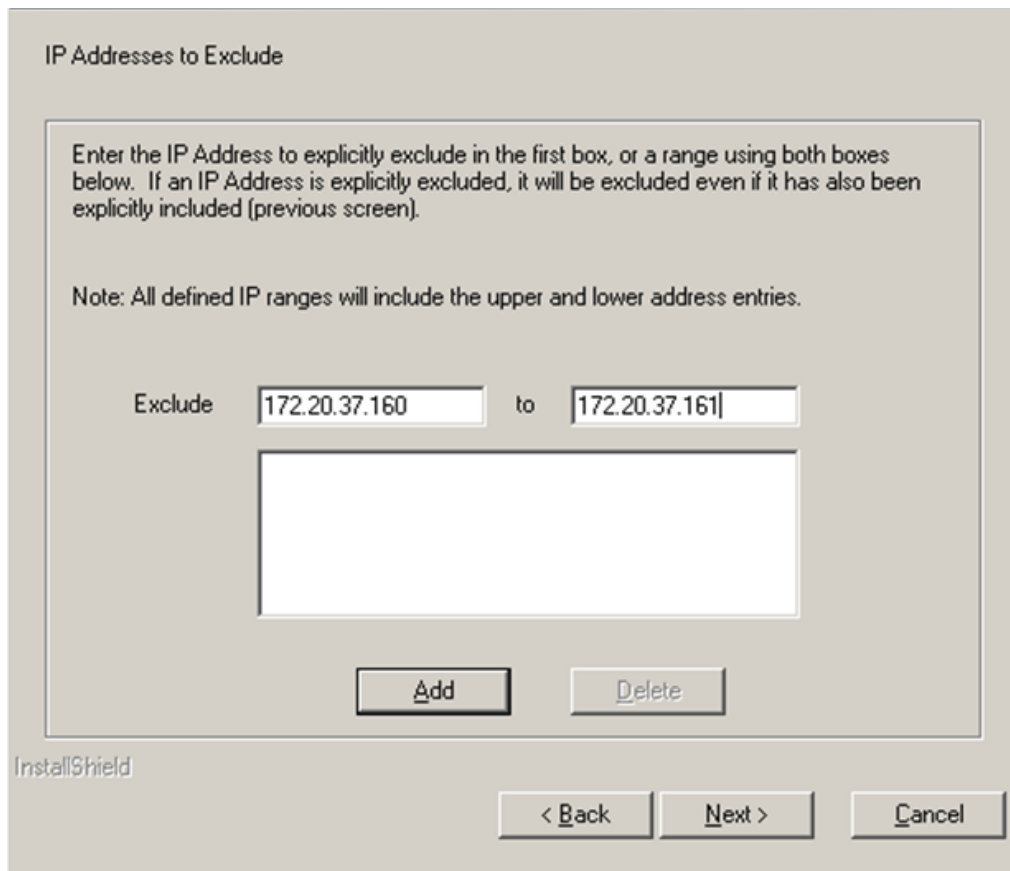
At the bottom of the dialog box, there are three buttons: "< Back", "Next >", and "Cancel".

Note: You can enter single IP address and ranges of IP addresses in the **IP Restricted Login** dialog box. Enter a single address in the first box.

- In the **Include** field, enter a beginning IP address.
- In the **To** field, enter an ending IP address. All IP addresses that fall between the beginning and ending IP addresses have login access.
- 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.

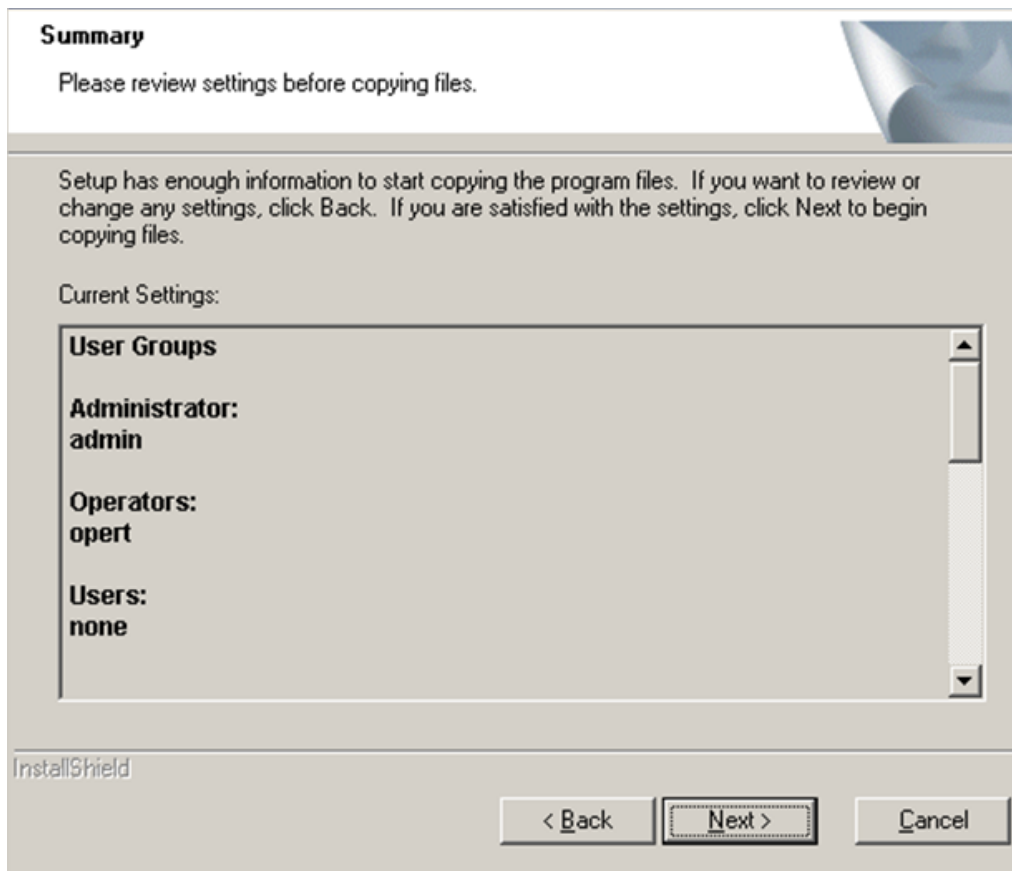
Note: If you enter an invalid IP address or IP address range, an error message appears indicating the IP address is invalid. Click **OK**. Enter a valid IP address or IP address range, and click **Add**.

9. Click **Next**. The **IP Address to Exclude** dialog box appears.



The dialog box is titled "IP Addresses to Exclude". It contains a text area with instructions: "Enter the IP Address to explicitly exclude in the first box, or a range using both boxes below. If an IP Address is explicitly excluded, it will be excluded even if it has also been explicitly included (previous screen)." Below this is a note: "Note: All defined IP ranges will include the upper and lower address entries." There are two input fields labeled "Exclude" and "to". The "Exclude" field contains "172.20.37.160" and the "to" field contains "172.20.37.161". Below these fields is a large empty rectangular box. At the bottom of the main area are two buttons: "Add" and "Delete". At the bottom of the dialog box are three buttons: "< Back", "Next >", and "Cancel". The "InstallShield" logo is in the bottom left corner.

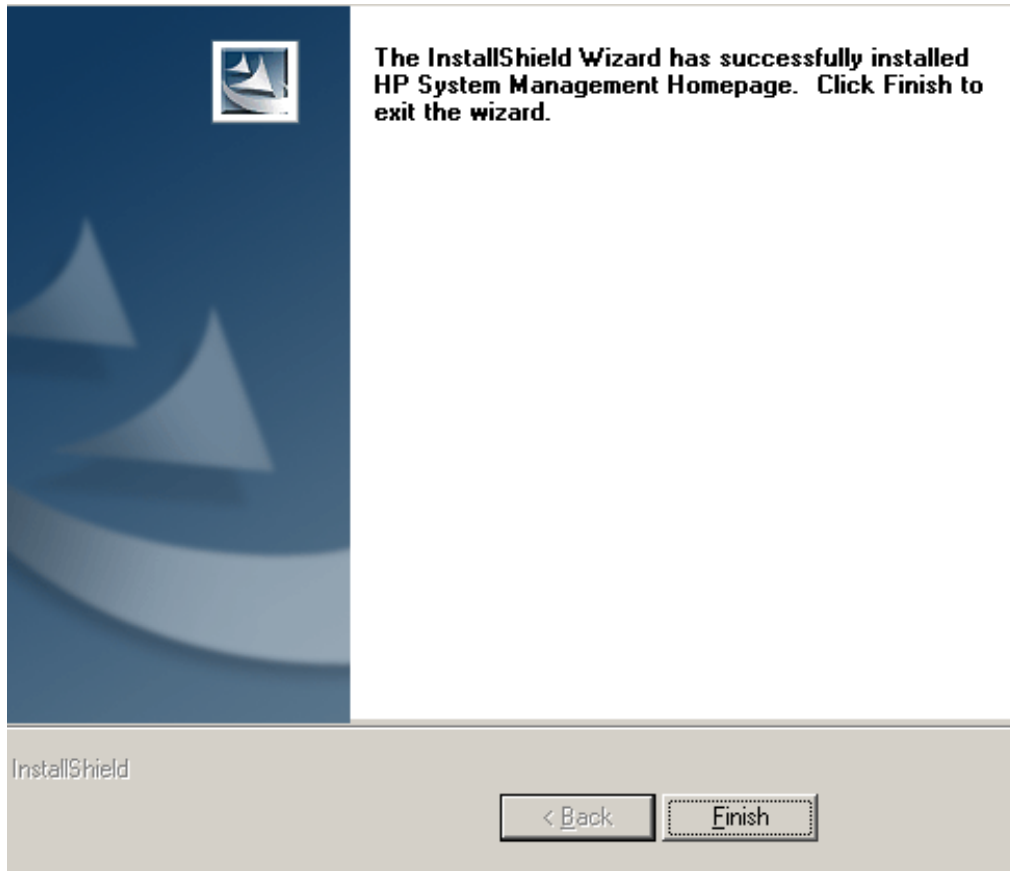
- a. In the **Exclude** field, enter a beginning IP address.
 - b. In the **To** field, enter an ending IP address. All IP addresses that fall between the beginning and ending IP addresses do not have login access.
 - c. Click **Add**. The IP address or IP address range is added to the **Exclusion** 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 you select **Next** 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 cleared, and the **Install Summary** dialog box appears.
10. Click **Next**. The **Install Summary Panel** appears. The **Install Summary Panel** lists a summary of the options that you specified during the installation.



11. Click **Next**. The installation process begins.

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 canceled.

12. 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

```
setup.exe /r
```

The HP SMH installation interface appears and records your selections.

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 /f1full_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 /f1full_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 perform an initial installation of HP SMH 3.x, the `/preserve` command preserves the pre-3.x settings.

If an HP SMH 2.x installation is 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 `SystemDrive\hp\hpsmh\smhpd.xml` file. To change the default configuration, you can modify the XML file to properly set the value of the tags. There are three ways to modify the XML file:

- Editing the XML file with a text editor application
- Using the CLI `smhconfig.exe` tool located at `SystemDrive\hp\hpsmh\bin`
- Using HP SMH interface through a browser



NOTE: Not all configurations can be accomplished using a browser.

Table 4-1 Environment variables and tags

| Variable | Description | Script |
|---|--|---|
| <code><session-timeout>15</session-timeout></code> | The <code><session-timeout></code> tag defines the HP SMH session timeout in minutes. If it is defined, then the HP SMH session stops 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 15 minutes. You can define the <code><session-timeout></code> tag using any value between 1 and 60 minutes. | <code>SystemDrive:\hp\hpsmh\conf\smhpd.xml</code> |
| <code><ui-timeout>20</ui-timeout></code> | The <code><ui-timeout></code> 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 20 seconds. You can define the <code><ui-timeout></code> tag using any value between 10 and 3600 seconds. | <code>SystemDrive:\hp\hpsmh\conf\smhpd.xml</code> |
| <code><rotate-logs-size>N</rotate-logs-size></code> | The <code><rotate-logs-size></code> tag defines the HP SMH Rotate Logs file size. To change the Rotate Logs file size, edit the configuration file <code>smhpd.xml</code> . You can define the <code><rotate-logs-size></code> tag using any value between 1 and 9, which represents the log size in megabytes. | <code>SystemDrive:\hp\hpsmh\conf\smhpd.xml</code> |
| <code><log-base-dir>path</log-base-dir></code> | The <code>log-base-dir</code> tag defines the path for <code>Error_log</code> and <code>Access_log</code> . By default, <code>Error_log</code> and <code>Access_log</code> are located in <code>SystemDrive:\hp\hpsmh\logs</code> (<code>/var/spool/opt/hp/hpsmh/logs</code> in Linux) folder. You can change the path by giving the required path in the tag and creating the logs folder under that path. | <code>SystemDrive:\hp\hpsmh\conf\smhpd.xml</code> (<code>/opt/hp/hpsmh/conf/smhpd.xml</code> in Linux). |
| <code><max-threads>value</max-threads></code> | The <code>max-threads</code> tag configures the number of threads used by Apache using the <code>smhpd.xml</code> file. <ul style="list-style-type: none"> • Default value - Windows: 250 • Max value - Windows: 512 • Min value - Windows: 64 Note: Max-thread is applicable only in the Windows environment. | |

5 Installing HP SMH using HPSUM

The HP Smart Update Manager (HPSUM) utility enables you to deploy ProLiant or Integrity Support Pack software and firmware components from a single, easy-to-use graphical user interface. The utility enables you to deploy and maintain ProLiant or Integrity Support Pack and Smart Components on a local server or one or more remote servers. 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 or Integrity Support Pack contains numerous files. All files must be present in the same directory as the HPSUM.EXE program for the PSP or ISP to be properly installed. You can install HP SMH as a part of the complete ProLiant or Integrity Support Pack, or you can install the HP SMH component individually. The HP SMH component also provides support for preconfiguration, which enables you to configure and save the configuration as part of the component itself before installing on target machines.



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

Installing HP SMH on a Windows operating system using HPSUM


1. To start the deployment, run the HPSUM.EXE. The **Source Selections** screen appears.

The screenshot shows the 'HP Smart Update Manager' window with the 'Source Selections' tab selected. The window title bar includes the HP logo and the text 'HP Smart Update Manager'. Below the title bar, the 'Source Selections' tab is active, and a help icon (?) is visible. The main content area is titled 'Choose the locations that HPSUM should check for updates.' and contains several configuration options:

- Directory:** A text box containing 'C:\Downloads\PSP\PSP 8.40' with 'Browse' and 'Default' buttons to its right.
- HP.com:** A section with two checkboxes: 'Check ftp.hp.com' (checked) and 'Use Proxy Server' (unchecked).
- Proxy Details:** A sub-section with fields for 'Server: Address', 'Port', 'Script', 'User ID', and 'Password', along with a 'Detect Proxy' button.
- Include components previously downloaded from HP.com:** An unchecked checkbox.
- Types of updates to use:** Three radio buttons: 'Both' (selected), 'Firmware Only', and 'Software Only'.

At the bottom of the window, there are two buttons: 'Exit' on the left and 'Start Inventory' on the right.

2. Click **Start Inventory** button. The **Select Installation Host(s)** screen appears when the inventory process is complete.

 HP Smart Update Manager

Select Installation Host(s)

?(h)

☒ Local Host (smh-64-bit-2k3)

☐ Remote Host or Group (Select from List)

Manage Hosts

Manage Groups

| Host Name | Type | Last Used | Description |
|--|------|-----------|-------------|
| <no remote hosts> | | | |
| To add remote hosts, use the "Manage Hosts" button | | | |

View:

☒ Only Hosts☐ Only Groups☐ Both

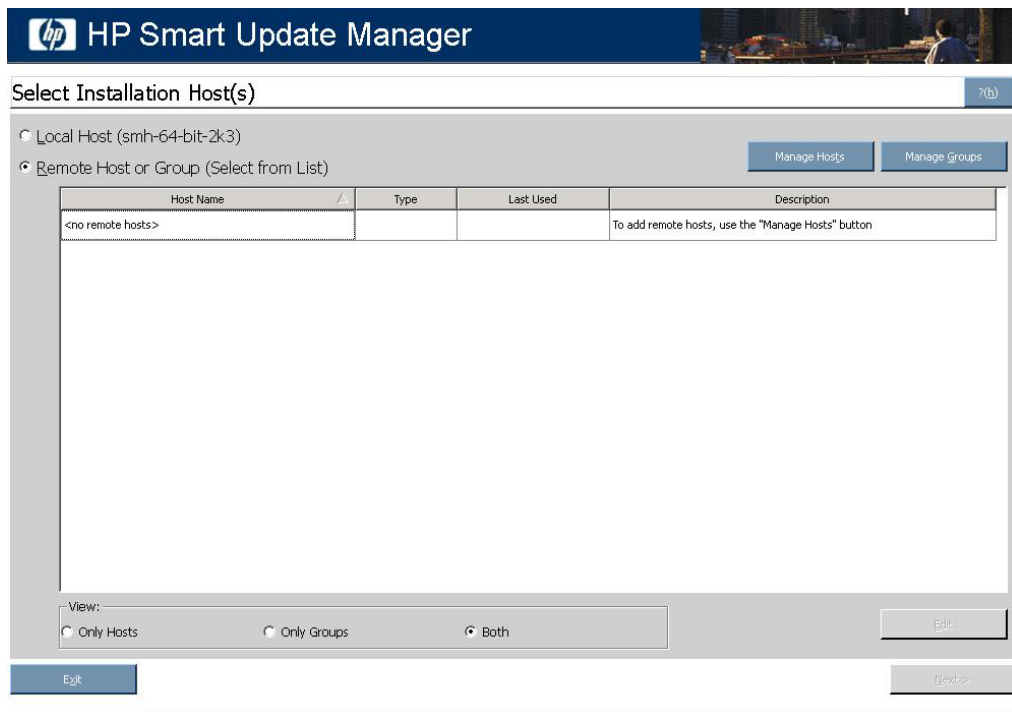
Edit

Exit

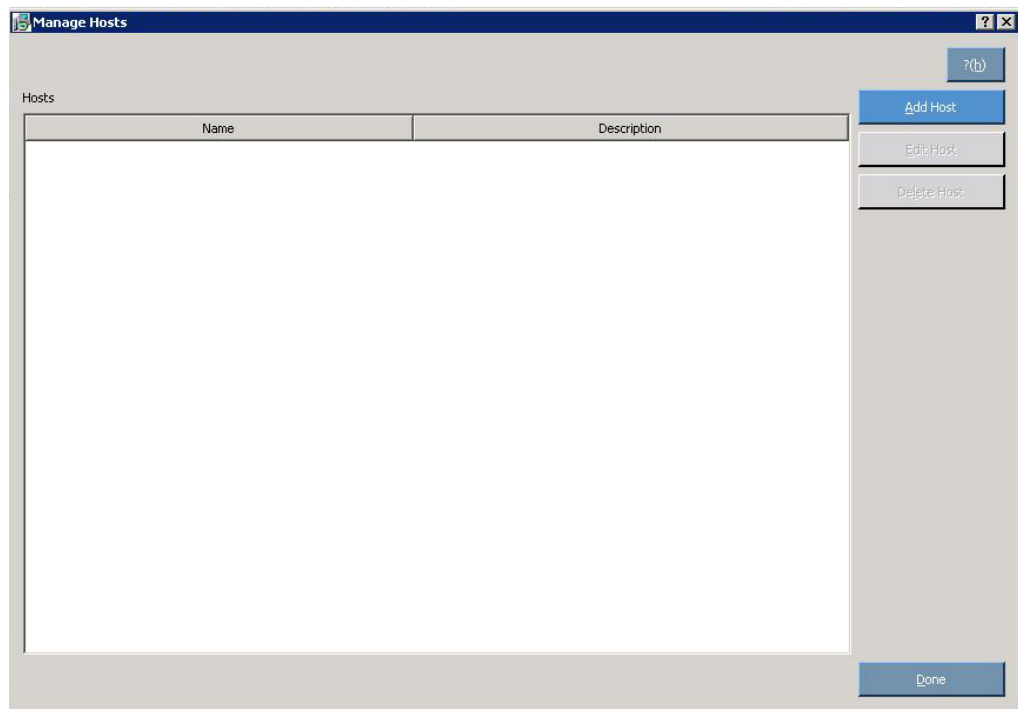
Next >

3. If you want to install HP SMH on the local server, check the **Local Host** checkbox and click **Next**.

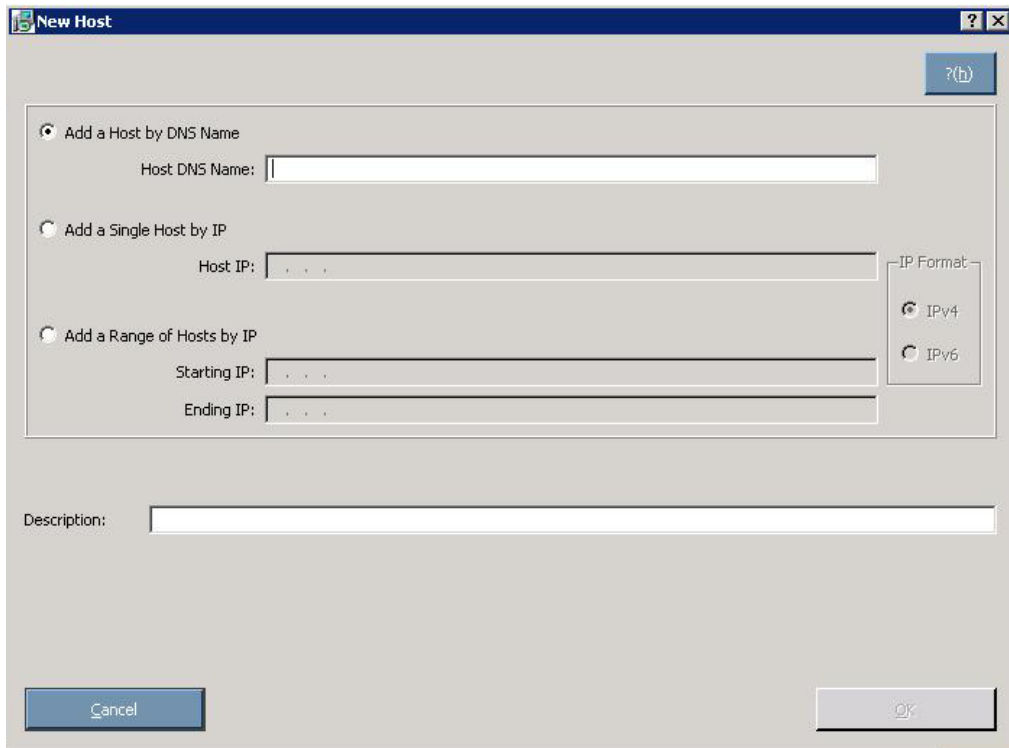
4. If you want to install HP SMH on remote servers:



- a. Select the **Remote Host or Group** checkbox and click **Manage Host**. The **Manage Host** panel appears.



- b. Click **Add Host**. You can add new hosts by DNS name or IP address, or you can add a range of IP addresses.

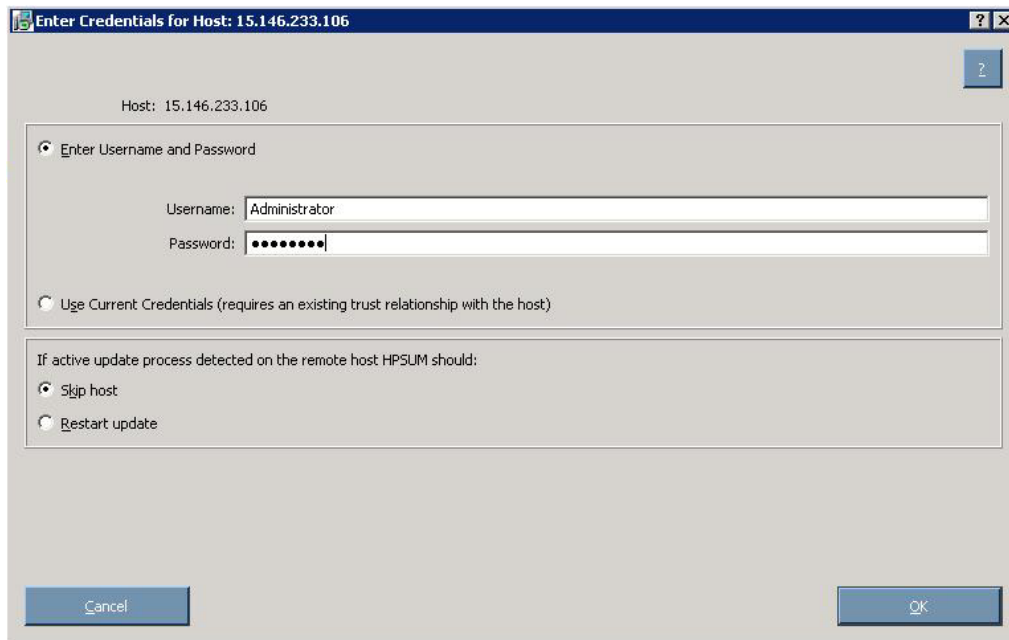


The "New Host" dialog box is shown with the following fields and options:

- ☒ Add a Host by DNS Name
 - Host DNS Name:
- ☐ Add a Single Host by IP
 - Host IP:
 - IP Format: ☒ IPv4, ☐ IPv6
- ☐ Add a Range of Hosts by IP
 - Starting IP:
 - Ending IP:
- Description:
- Buttons: Cancel, OK

- c. You can also create a group of systems on which you want to install HP SMH by selecting **Manage Groups**.

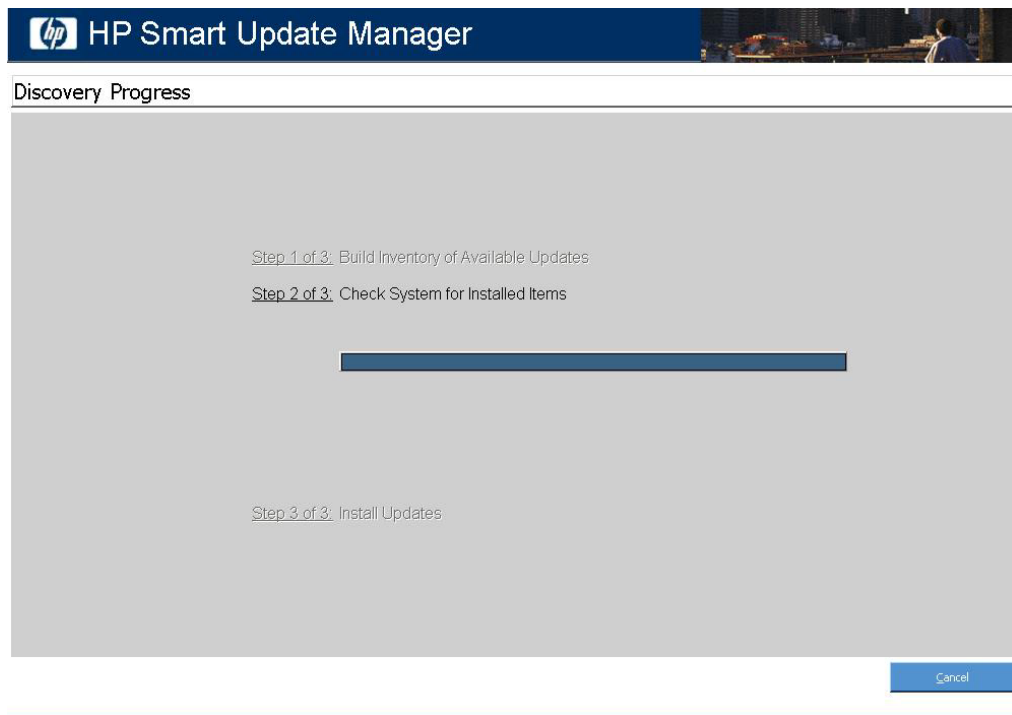
Note: If you chose to **Manage Groups**, you will need to give the Windows credentials for each remote server.



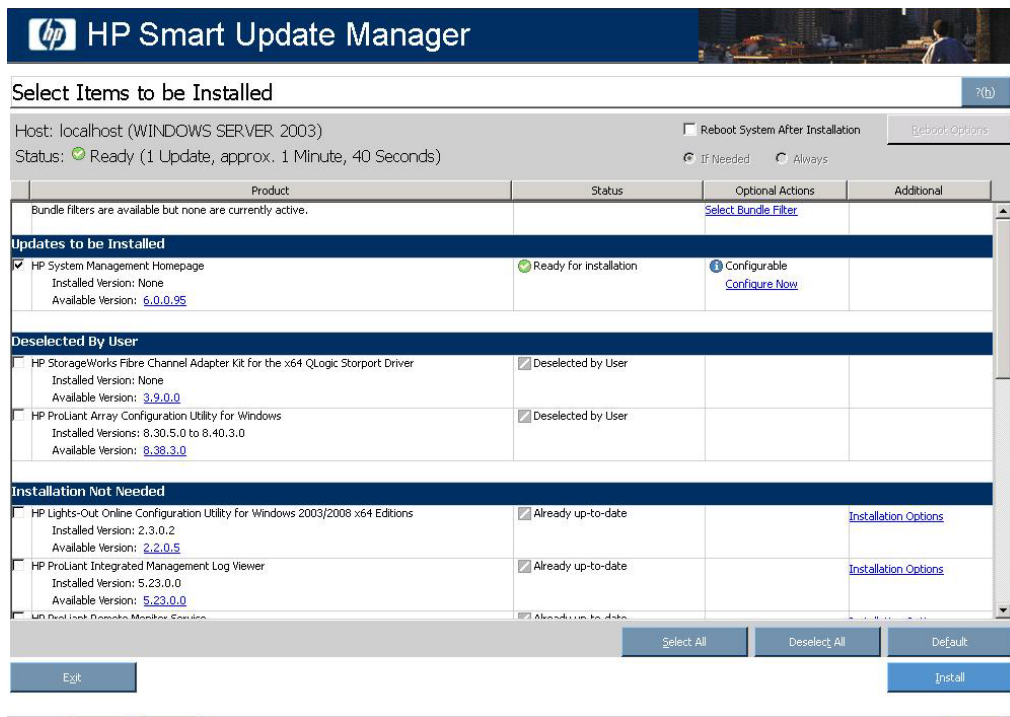
The "Enter Credentials for Host: 15.146.233.106" dialog box is shown with the following fields and options:

- Host: 15.146.233.106
- ☒ Enter Username and Password
 - Username:
 - Password:
- ☐ Use Current Credentials (requires an existing trust relationship with the host)
- If active update process detected on the remote host HPSUM should:
 - ☒ Skip host
 - ☐ Restart update
- Buttons: Cancel, OK

5. Select the target server and click **Next**. A **Discovery Progress** screen appears while the system checks for installed items. Then, the **Select Bundle Filter** page appears.



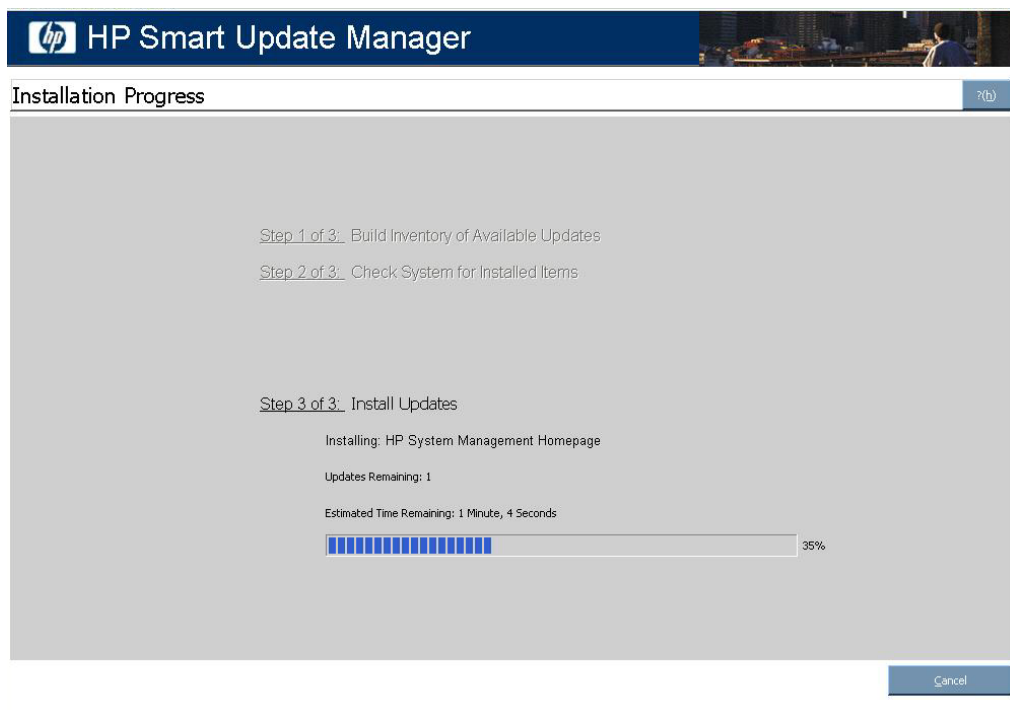
6. From the **Select Bundle Filter** page, select the appropriate PSP or ISP bundle, according to the target server operating system architecture (either x86 or x64), and select the appropriate option for the bundle filter. These options appear:
 - **Allow Non-Bundle Version** Shows other versions of the product that are in the bundle. This enables you to include updates newer than those released in the bundle.
 - **Allow Non-Bundle Products** Shows updates for products that are not part of the bundle. This option enables you to update other items on your system at the same time as applying the bundle (as a convenience or because updates in the bundle might depend on them).
 - **Force All Bundle Updates** Automatically sets the **force** flag for updates in the bundle. This option enables you to update the installation as long as the supported hardware is present and installation conditions are met.
- Note:** You do not need to select the bundle filter option when you install the HP SMH component alone.
7. Click **Next**. The **Select Items to be installed** panel appears. This panel shows the components to be installed or displays **Installation not needed** or **Excluded by filtering**.



8. Check the HP SMH component, and you can preconfigure the HP SMH component by selecting **Configure Now**.

Note: If PSP or ISP contains an older version of HP SMH than what is installed on the target server, the HP SMH component is listed under the **Installation not needed** section. In this case, click **Installation Options** for HP SMH component and select the **For Install** checkbox. The HP SMH component is listed under **Updates to be Installed**.

9. After selecting the HP SMH component, click **Install**. A screen appears showing the installation progress.



10. After installation is finished, the **Installation Result** panel appears.
In the **Installation Result** panel, the **Reboot Now** and **Exit** buttons appear.
11. To reboot the system, select **Reboot Now**. To exit the program, select **Exit**. The HP Smart Update Manager program is complete.

Installing HP SMH on a Linux operating system using the HPSUM

To install HP SMH on a Linux operating system using the HPSUM, your system must meet the minimum requirements, in addition, you must have the `psp-8.40.x.i686.en.tar` file.

1. To start the deployment, execute the command `tar -xvf psp-8.40.x.i686.en.tar`, which extracts the tar file contents to the current directory, and then execute the command `./hpsum` to run the HPSUM. The **Screen Selections** screen appears.

HP Smart Update Manager

Source Selections ?(h)

Choose the locations that HPSUM should check for updates.

Directory
/root/psp_8.4 Browse Default

HP.com
☒ Check ftp.hp.com ☐ Use Proxy Server


Proxy Details
☐ Server: Address:
Port:
☐ Script:
User ID:
Password:
Detect Proxy

☐ Include components previously downloaded from HP.com

Types of updates to use
☒ Both ☐ Firmware Only ☐ Software Only

Exit Start Inventory

2. Click **Start Inventory** button. The **Select Installation Host(s)** screen appears when the inventory process is complete.

 HP Smart Update Manager

Select Installation Host(s)

?(h)

☒ Local Host (smh-64-bit-2k3)

☐ Remote Host or Group (Select from List)

Manage Hosts

Manage Groups

| Host Name | Type | Last Used | Description |
|--|------|-----------|-------------|
| <no remote hosts> | | | |
| To add remote hosts, use the "Manage Hosts" button | | | |

View:

☒ Only Hosts

☐ Only Groups

☐ Both

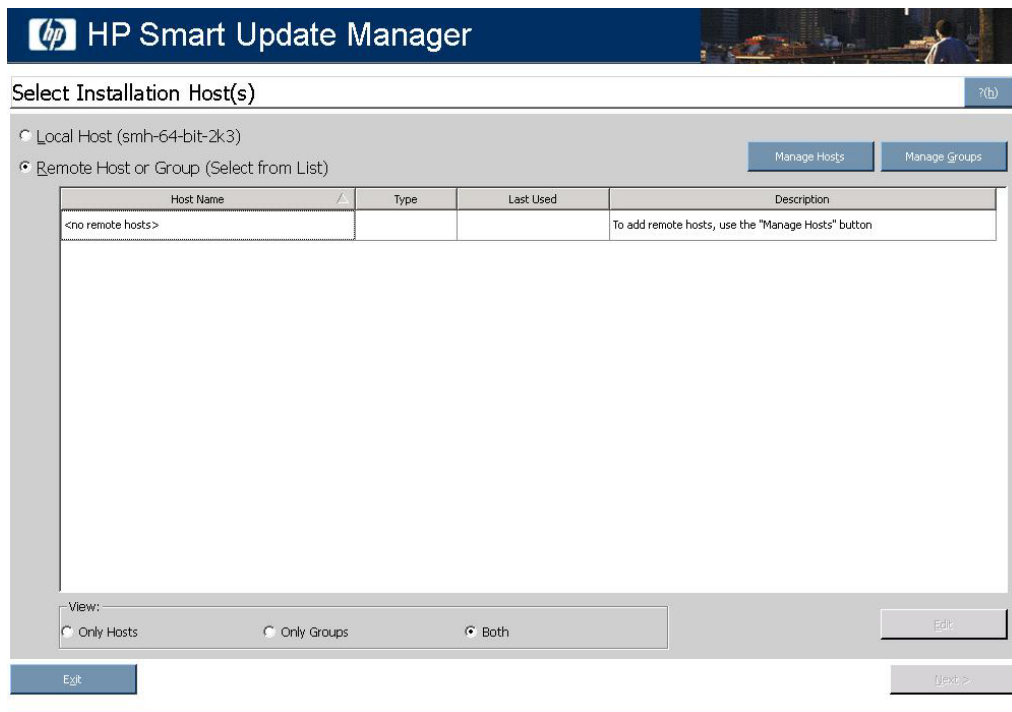
Edit

Exit

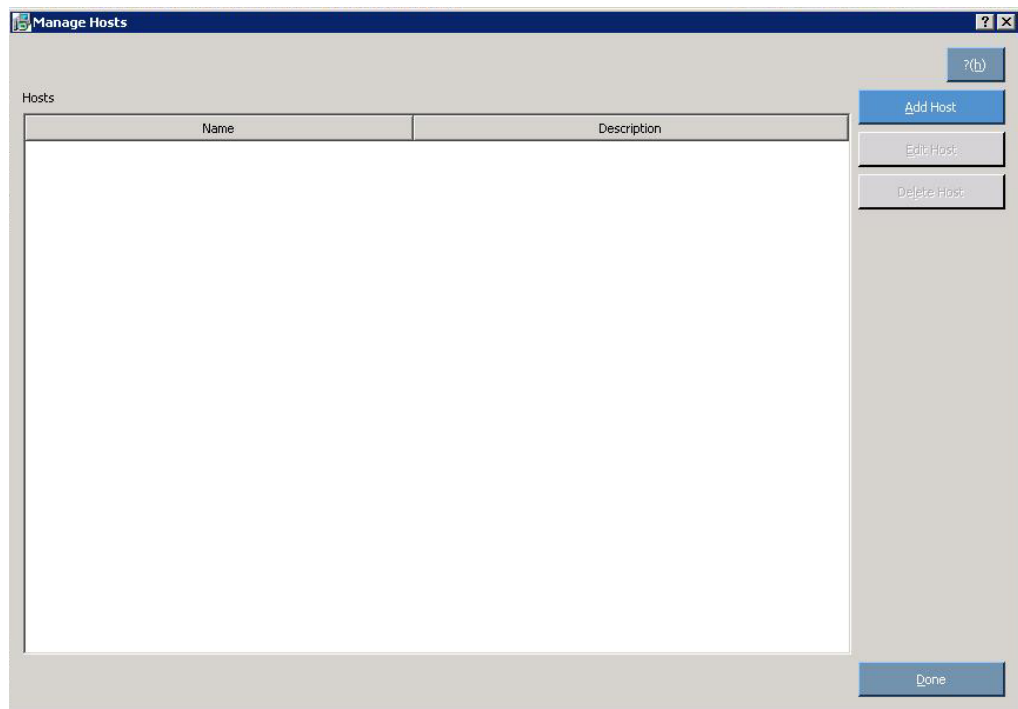
Next >

- If you want to install HP SMH on the local server, check the **Local Host** checkbox and click **Next**.

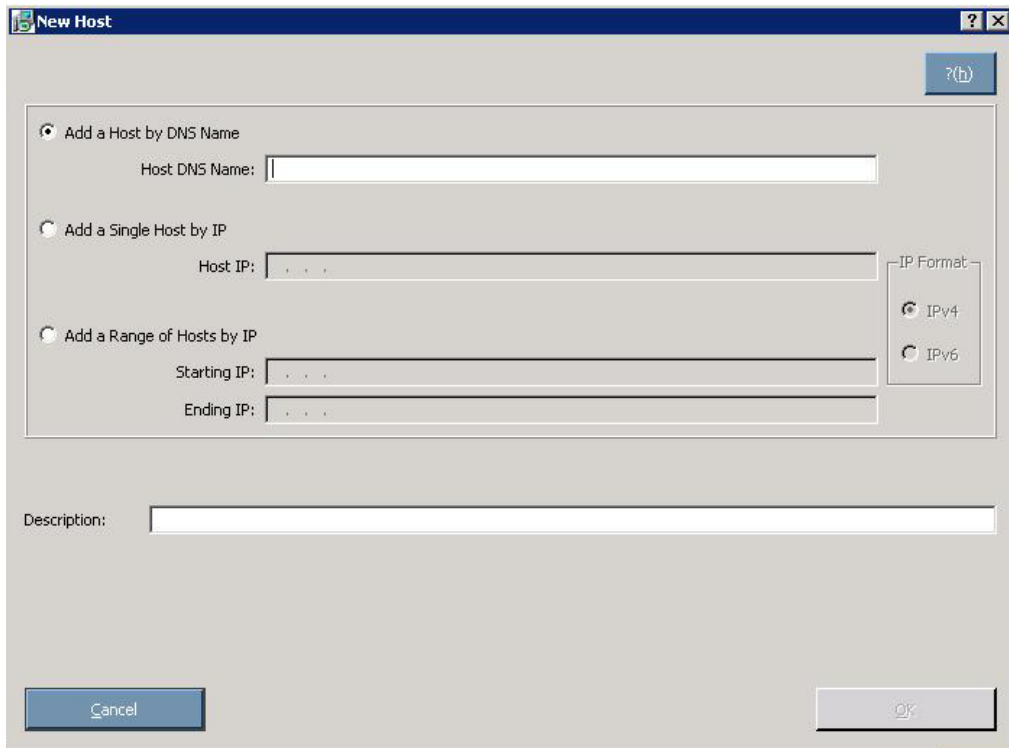
4. If you want to install HP SMH on remote servers:



- a. Select the **Remote Host or Group** checkbox and click **Manage Host**. The **Manage Host** panel appears.



- b. Click **Add Host**. You can add new hosts by DNS name or IP address, or you can add a range of IP addresses.

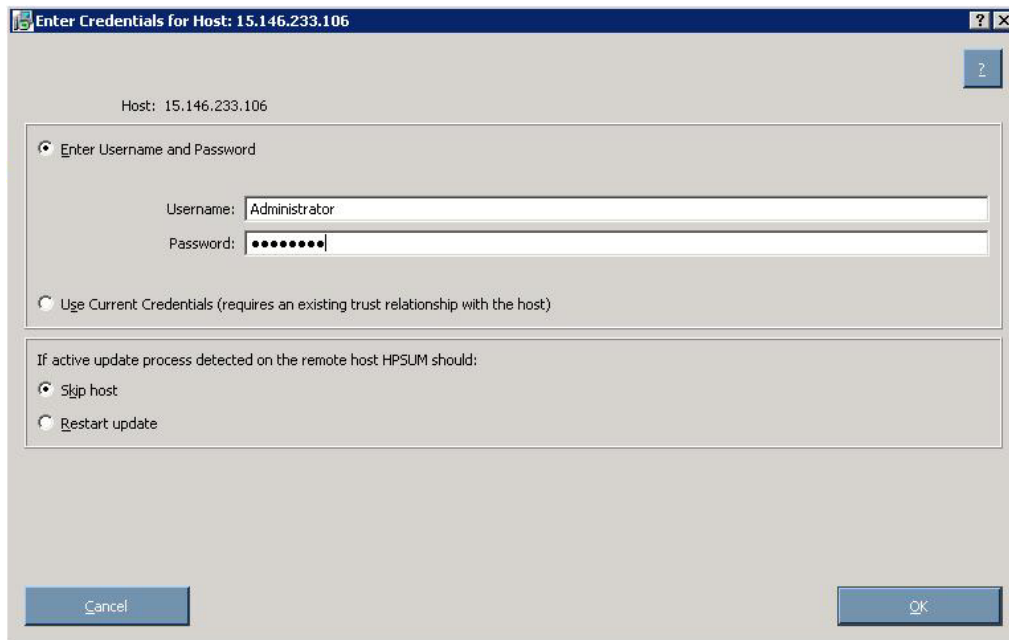


The "New Host" dialog box is shown with the following fields and options:

- ☒ Add a Host by DNS Name
 - Host DNS Name:
- ☐ Add a Single Host by IP
 - Host IP:
 - IP Format: ☒ IPv4, ☐ IPv6
- ☐ Add a Range of Hosts by IP
 - Starting IP:
 - Ending IP:
- Description:
- Buttons: Cancel, OK

- c. You can also create a group of systems on which you want to install HP SMH by selecting **Manage Groups**.

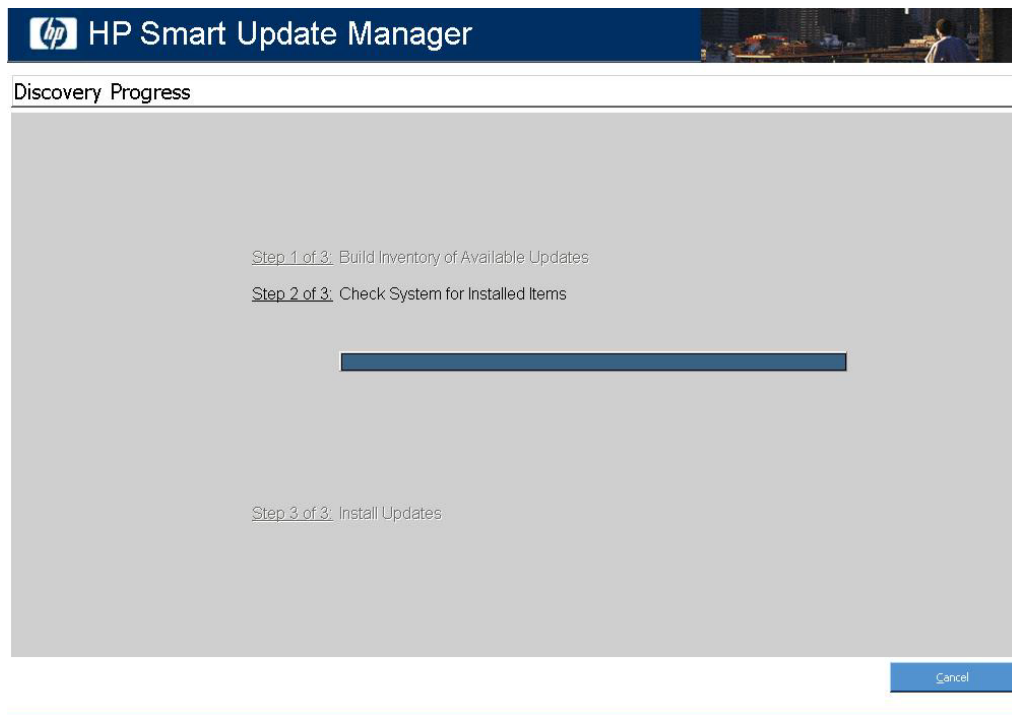
Note: If you chose to **Manage Groups**, you will need to give the Windows credentials for each remote server.



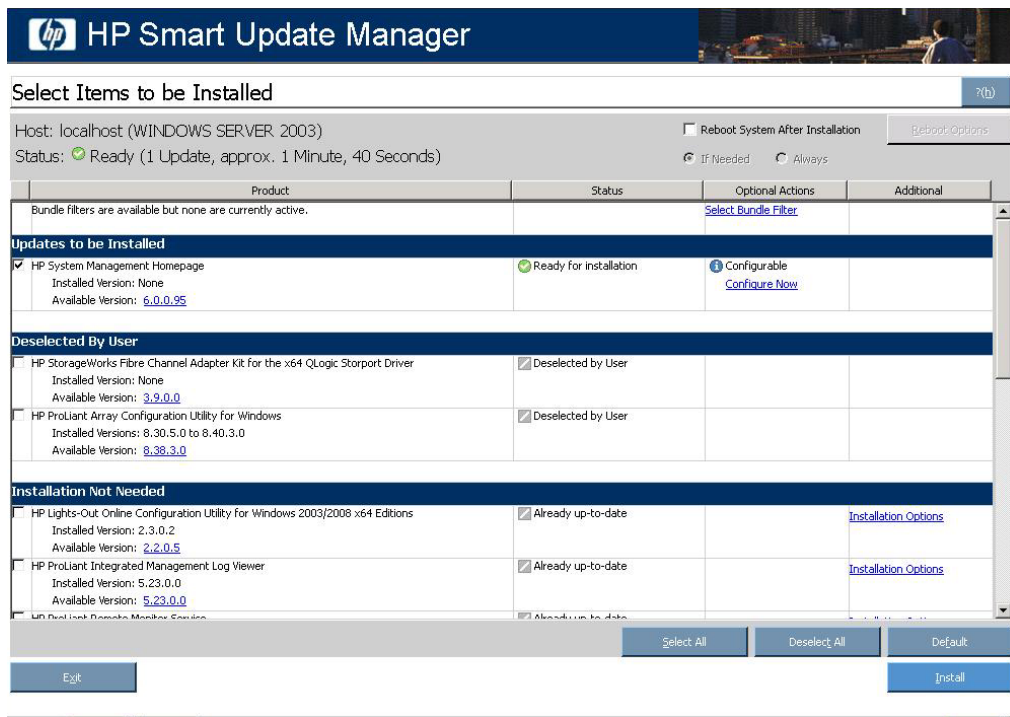
The "Enter Credentials for Host: 15.146.233.106" dialog box is shown with the following fields and options:

- Host: 15.146.233.106
- ☒ Enter Username and Password
 - Username:
 - Password:
- ☐ Use Current Credentials (requires an existing trust relationship with the host)
- If active update process detected on the remote host HPSUM should:
 - ☒ Skip host
 - ☐ Restart update
- Buttons: Cancel, OK

5. Select the target server and click **Next**. A **Discovery Progress** screen appears while the system checks for installed items. Then, the **Select Bundle Filter** page appears.



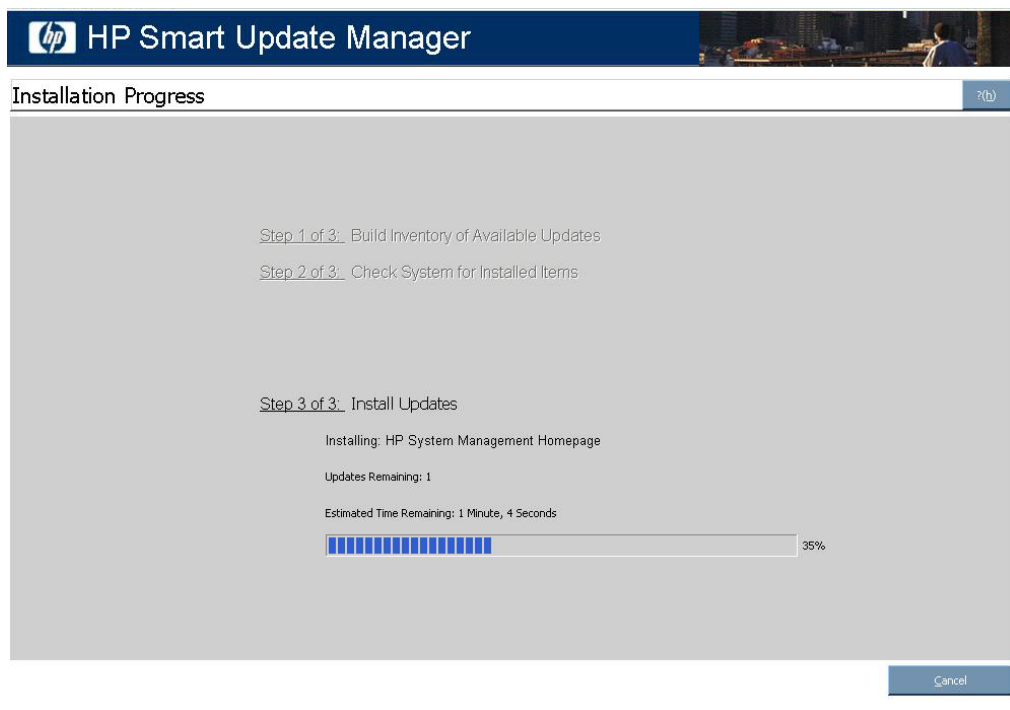
6. From the **Select Bundle Filter** page, select the appropriate PSP or ISP bundle, according to the target server operating system architecture (either x86 or x64), and select the appropriate option for the bundle filter. These options appear:
 - **Allow Non-Bundle Version** Shows other versions of the product that are in the bundle. This enables you to include updates newer than those released in the bundle.
 - **Allow Non-Bundle Products** Shows updates for products that are not part of the bundle. This option enables you to update other items on your system at the same time as applying the bundle (as a convenience or because updates in the bundle might depend on them).
 - **Force All Bundle Updates** Automatically sets the **force** flag for updates in the bundle. This option enables you to update the installation as long as the supported hardware is present and installation conditions are met.
- Note:** You do not need to select the bundle filter option when you install the HP SMH component alone.
7. Click **Next**. The **Select Items to be installed** panel appears. This panel shows the components to be installed or displays **Installation not needed** or **Excluded by filtering**.



8. Check the HP SMH component, and you can preconfigure the HP SMH component by selecting **Configure Now**.

Note: If PSP or ISP contains an older version of HP SMH than what is installed on the target server, the HP SMH component is listed under the **Installation not needed** section. In this case, click **Installation Options** for HP SMH component and select the **For Install** checkbox. The HP SMH component is listed under **Updates to be Installed**.

9. After selecting the HP SMH component, click **Install**. A screen appears showing the installation progress.



10. After installation is finished, the **Installation Result** panel appears.
In the **Installation Result** panel, the **Reboot Now** and **Exit** buttons appear.
11. To reboot the system, select **Reboot Now**. To exit the program, select **Exit**. The HP Smart Update Manager program is complete.

Preconfiguring 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 Administrator and any account under **Administrators Group** always have administrative access.
4. Click **Add** to assign the group. The new group appears under the operating system group to which it is assigned.
Note: You can add up to five entries for each 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. **Anonymous Access** enables a user to access HP SMH 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. Local Access enables a user to locally gain access to the HP SMH without being challenged for authentication. If you select **Administrator** any user with access to the local console is granted full access. If you select **Anonymous**, 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 SMH 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 to avoid importing any certificates.



NOTE: HP strongly recommends using this option because the other options are less 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 you select the certificate file, 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 HP SMH 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. This option prevents one group from installing software to the wrong system. This option verifies only the HP SIM server certificate name submitted.



CAUTION: 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 certificate name must be less than 64 characters.
- Special characters must not be included as part of the *server certificate name*: ~ ' ! @ # \$ % ^ & * () + = \ " : ' < > ? , | .

To trust by name:

1. Select **Trust by Name**, and click **Next**.
 2. In the **Trusted Server Name** field, enter the HP SIM server certificate name to be trusted.
 3. Click **Add**. The trusted HP SIM server 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 HP SMH to accept certain changes from any server.



CAUTION: 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 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 HP SMH accepts requests and provides control over which nets and subnets requests are processed.

Administrators can configure HP SMH to bind only to addresses specified in the **IP Binding** page. You can define a maximum of five subnet IP addresses and netmasks.

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



NOTE: HP SMH always binds to 127.0.0.1. If IP Binding is enabled and no subnet/mask pairs are configured, then the HP SMH is available only to 127.0.0.1. If IP Binding is not enabled, HP SMH binds 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.

Note: The masking field is not required for IPv6 addresses.

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 SMH to restrict login access based on the IP address of a system. You can set address restriction at installation time, or administrators can set address restriction 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 **Included** box, 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 SMH component is configured successfully and is ready for installation.

6 Installing HP SMH directly on Linux operating systems

Installation for Linux on x86 and x86_64 operating systems

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



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

NOTE: HP SMH already uses the user and group name hpsmh. Do not use the **hpsmh** user and group name for any other purpose.

Installing HP SMH on Linux x86 operating systems

To install HP SMH on x86 operating systems, your system must meet the minimum requirements. In addition, you must have the `hpsmh-6.x.x-y.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-6.x.x-y.i386.rpm
```

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

For more information regarding minimum requirements, see Chapter 1 “Installation requirements”.

Installing HP SMH on x86_64 operating systems

To install HP SMH on x86_64 operating systems, your system must meet the minimum requirements. In addition, you must have the `hpsmh-6.x.x-y.x86_64.rpm`.



NOTE: While installing or uninstalling HP SMH manually, `insserv: warning: script 'SCRIPT NAME' missing LSB tags and overrides may be generated` (in newer version of the servers, for example: Novell/SUSE Linux), however, these warnings do not impact HP SMH functionality or its installation or uninstallation.

If you wish to avoid such warnings, edit the `INIT INFO` block of the particular init script '`SCRIPT NAME`' per the corresponding operating system requirement.

```
rpm -ivh hpsmh-6.x.x-y.x86_64.rpm
```

Configuring HP SMH

After the HP SMH is installed, you can configure the settings. If you are migrating from a version of HP SMH prior to 3.0, the previous settings are retained. However, the retained settings are configurable.

To configure the HP SMH settings:

1. Use the CLI `smhconfig` tool located at `/opt/hp/hpsmh/sbin`.
2. Enter the following command to start the configuration: `/opt/hp/hpsmh/sbin/smhconfig`

7 Installing HP SMH directly on Itanium-based Linux operating systems

Installation for Itanium-based Linux operating systems

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



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

Installing HP SMH on Itanium-based Linux operating systems

To install HP SMH on Itanium-based operating systems, your system must meet the minimum requirements. In addition, you must have the `hpsmh-6.x.x-y.i386.rpm`.

To install HP SMH, enter the following command line:

```
rpm -ivh hpsmh-6.x.x-y.i386.rpm
```

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

For more information regarding minimum requirements, see [Chapter 1 “Installation requirements”](#).

Configuring HP SMH

After the HP SMH is installed, you can configure the settings. If you are migrating from a version of HP SMH prior to 3.0, the previous settings are retained. However, the retained settings are configurable.

To configure the HP SMH settings:

1. Enter the following command to start the configuration:

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

The **Welcome** screen indicates that you can configure security and access parameters for HP SMH and related HP web-based management tools.

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

The **Operating System Groups** screen enables you to add or delete operating system groups in HP SMH. The following options are available:

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

Note: You can add up to five existing operating system group entries for each group. Enter one of the following options to assign the operating system group to the Administrator Group List:

 - Enter 1 for Administrator.

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

 1. Enter 1 for Administrator.
 2. At the prompt, Enter the name of the operating system group: enter **admin1**.

3. Press **Enter**. **admin1** appears in the **Administrator Group List**.
4. Enter **n** to go to the next screen.
 - Enter **2** for Operator.
 - Enter **3** for User.
2. Enter **n** to go to the next screen.
- To delete a group:
 1. 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.
 2. At the prompt, enter **1**, **2**, or **3**.
 3. Enter the number next to the group name you want deleted. The group is deleted from the group list.
Note: You can delete as many groups as you want by repeating this step.
 4. Press **Enter** when you are finished deleting groups.
 5. Enter **n** to go to the next screen. The **Operating System Groups** screen appears.
 6. Enter **n** to go to the next screen. The **User Access** screen appears.
3. Configure Local and Anonymous Access. The following options are available:
 - Enter **1** to enable **Anonymous Access**.



CAUTION: HP does not recommend using anonymous access.

- Enter **2** to disable **Anonymous Access**.
- Enter **3** to disable **Local Access**.
- Enter **4** to enable **Local Access - Anonymous**. **Local Access - Anonymous** enables you to locally gain access to HP SMH without 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.
4. Enter **n** to go to the next screen or enter **p** to go to the previous screen.
 5. Enter **n** to go to the next screen. The **Trust Mode** screen appears.
 6. 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.
 - Trust by Certificate
 1. Enter **1**. You are prompted for the certificate location.
 2. Enter the file path of the trusted certificates to be added to the **Trusted Certificates List**. Press **Enter** when you are finished.
For example:

- A. Enter File: `/home/ServerName/cert1.pem` .
 - B. 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. Add as many certificates as you want by repeating these steps. Press **Enter** when you finish.
 - To import a certificate:
 1. Enter 2. You are prompted for the server name.
 2. Enter the name or IP address of the HP SIM server and press **Enter**. The certificate appears.
The following options are available:
 - Enter 1 to accept the certificate. The file is saved.
 - Enter 2 to reject the certificate. The file is not imported.
 3. Press **Enter** when you finish. The imported certificates appear in the **Trusted Certificates List**. You can import additional certificates by repeating these steps.
 4. Press **Enter** when you finish importing certificate files.
 - To delete a certificate:
 1. Enter 3. You are prompted to enter the certificate file number.
 2. Enter the certificate file number.
 3. Press **Enter** when you finish. You can delete additional certificate files by repeating these steps.
 4. Press **Enter** when you finish.
 - Trust by Name
 1. Enter 2 to **Trust by Name**. Trust Mode: Trust by Name appears.
 2. Enter 4 to **Modify Server Name** list.
To add an HP SIM server certificate name:
 - A. Enter 1. You are prompted to add an HP SIM server certificate name.
 - B. Enter the name of the certificate of HP SIM server to be trusted and press **Enter**. The certificate name appears in the **Trusted Server Names** list.
Note: You can add a maximum of five server certificate names.
 - To delete a certificate name:
 - A. From the **Server Name** list, enter 2.
 - B. Enter the number associated with the HP SIM server certificate name. The HP SIM server certificate name is removed from the **Server Name** list.
 3. Enter **n** for next. The **Trust Mode Settings** screen appears.
 - Trust All
 1. Enter 3 to **Trust All**. Trust Mode: Trust All appears.
 2. Enter **n** for next. The **IP Binding** screen appears.
 - Modify Certificate List
Enter 4 to **Modify Certificate List**.
7. Bind IP addresses that match a subnet and netmask.
The following options are available:
- Enable IP Binding
 1. Enter 1 to enable the IP Binding, which sets it to **ON**. IP Binding: ON appears.
 2. 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.
- Note:** The masking field is not required for IPv6 addresses.

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

- Disable IP Binding

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

- 8. 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:

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

To enable the IP Restricted Login:

- 1. Enter **1**. **IP Restricted Login** is set to **ON**.
- 2. Enter **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 you want to delete 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**:

- A. Enter **2** for **Exclude Login Restriction IP Address**
- B. Enter **1** to add an IP address to the **Exclusion list**.
- C. 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**.
- D. Press **Enter**. The **IP Address Exclusion List** screen appears.
- E. Enter **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:

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

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

E. Enter **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.

3. Enter **n** for next.

- To disable IP Restricted Login:

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

Note: Only IPv4 address ranges are supported for IP restricted login.

9. 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 stops and starts automatically.
10. Verify HP SMH is configured and working properly by navigating to it and verifying that it appears as you configured HP SMH during installation.

8 Initializing the software for the first time

After you have installed and configured HP SMH 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 operating systems, 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).

With HP SMH running on Apache 2.2 (HP-UX 11iv3), the Apache Tomcat communication requires certificate-based authentication through `https` connection on port 1188 (by default). The certificate `/var/opt/hpsmh/sslshare/proxy.pem`, generated during installation, is used for this purpose. For effective Apache Tomcat communication required to launch the Java plug-ins, do not alter this certificate on the system.

- In Linux operating systems, both public and private keys for HP SMH are stored in the `/etc/opt/hp/sslshare` directory. The files are called `file.pem` and `cert.pem`.
- In Windows operating systems, public and private keys are stored in the `<System Drive>:\hp\sslshare` directory of the system drive.

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



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

If the private key is compromised, you can delete the `<System Drive>:\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 occurs only the first time HP SMH starts or when no certificate and key pair exists.

A certificate from a certificate authority (CA), such as Verisign or Entrust, can replace self-generated certificates. These certificate and key files are shared with other HP Management software, such as HP SIM.

9 Signing in and signing out of HP SMH

Signing in with Microsoft Windows XP

If HP SMH is installed on a Microsoft Windows XP® system, you must enable the following security option to sign in to 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 close the **Local Security Policy Setting** dialog box.

Signing in with Microsoft Internet Explorer

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

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

To add HP SMH to Internet Explorer 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 use 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, or if you have disabled port 2301. If you keep the default-installed configuration, you can use the following URL:

`http://hostname:2301/`



NOTE: You can also use the port 1188 to access HP SMH. This port is used by the Tomcat instance of the HP SMH.

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.

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 SIM 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 SIM certificate, see the *HP System Management Homepage Online Help*.

2. Click **Yes**. The **Sign In** page appears unless you have enabled **Anonymous** access, then the **HP System Management Homepage** appears.

3. Enter a user name.

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. **Administrator** on Windows and **root** on HP-UX or Linux have administrator access on HP SMH.

4. Enter a password.
5. Click **Sign In**. HP SMH appears.

Signing in with Mozilla and Firefox

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

If you use 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 URL: `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.

The first time you browse to the HP SMH URL, 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 **Sign In** 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. **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. Click **Sign In**. HP SMH appears.

Signing in from the HP-UX CLI

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/sbin/smhstartd
```

If the daemon is not running, you can start it from the HP-UX command line using `/opt/hpsmh/sbin/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 sign 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/sbin/hpsmh start` instead to start the HP-UX Apache-based Web Server on ports 2301 (http) and 2381 (https).

Signing out

Select one of the following options:

- In the System Management Homepage banner, click **Sign Out**.
- Close every instance of the web browser that you use to sign in to HP SMH.
- You can stop HP SMH from the HP-UX command line: `/opt/hpsmh/sbin/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 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`.

10 Uninstalling HP SMH

Uninstalling from an HP-UX operating system

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

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

This method is recommended for uninstalling HP SMH.

Uninstalling from a Itanium-based Linux, x86 or x86_64 operating system

To uninstall HP SMH:

Run the following command:

```
rpm -e hpsmh
```



NOTE: When the HP SMH is uninstalled, where HP SMH directory is `/opt/hp/hpsmh`, the HP SMH directory is not deleted. The HP SMH directory contains the user-configured SMH files, and the same configuration is utilized when the HP SMH is reinstalled again.

NOTE: While installing or uninstalling HP SMH manually, `insserv: warning: script 'SCRIPT NAME' missing LSB tags and overrides` may be generated (in newer version of the servers, for example: Novell/SUSE Linux), however, these warnings do not impact HP SMH functionality or its installation or uninstallation.

If you wish to avoid such warnings, edit the `INIT INFO` block of the particular init script '`SCRIPT NAME`' per the corresponding operating system requirement.

Uninstalling from a Windows operating 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.



NOTE: When the HP SMH is uninstalled, the HP SMH directory, where HP SMH directory is `<System Drive>:\hp\hpsmh`, is not deleted. The HP SMH directory contains the user-configured SMH files, and the same configuration is utilized when the HP SMH is reinstalled again.

Uninstalling from a Windows 2008 operating system

Use the **Programs and Features** feature in Windows 2008, and complete the following steps to remove HP SMH:

1. Select **Start** ⇒ **Control Panel** ⇒ **Programs and Features**.
2. Right-click **HP System Management Homepage**.
3. Select **Uninstall**. HP SMH is uninstalled.



NOTE: When the HP SMH is uninstalled, where HP SMH directory is `<System Drive>:\hp\hpsmh`, the HP SMH directory is not deleted. The HP SMH directory contains the user-configured SMH files, and the same configuration is utilized when the HP SMH is reinstalled again.

Uninstalling HP SMH on a CLI-based Windows system

To uninstall the HP SMH application on a CLI-based Windows system, complete the following steps.

1. Stop the HP SMH service.
2. Execute the `uninstall.bat` from the command prompt to uninstall the HP SMH application. The `uninstall.bat` file is available at the location `c:\hp\hpsmh\uninstall.bat`.



NOTE: The uninstaller `uninstall.bat` batch file is shipped along with the HP SMH package.

Uninstalling manually for Windows and Linux operating 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: The `_jvm` directory is present if there is an existing HP SMH 2.0.1 or 2.0.2 installation and can be removed.



CAUTION: All HP SMH configuration settings are 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`

Important: Do not remove this file from a system that uses the Linux OS. You will lose certificates stored in this file if it is deleted.

- `\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`

Important: Do not remove this file from a system that uses the Linux OS. You will lose certificates stored in this file if it is deleted.

For **Windows**, `sslshare` is located in `SystemDrive:\hp\sslshare`

- For Linux, remove the following additional files:
`/usr/local/hp`
`/var/spool/opt/hp`
`/var/spool/compaq/wbem`
- If the HP Version Control Agent, or the HP Version Control Repository Manager, or both is installed on the operating system, remove all files and directories under `\hp\hpsmh\bin`, except `libeay32.dll` and `ssleay32.dll`.
- 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
- \HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Hewlett-Packard\System Management Homepage (if present)

Uninstalling manually for HP-UX operating systems



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

When you must uninstall HP-UX SMH, HP recommends using the `swremove` command, as described in “Uninstalling from an HP-UX operating system” (page 65).

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

On HP-UX operating systems, the `/etc/opt/hp/sslshare` directory is used by HP SIM. Do not remove the directory.

Support and other resources

Information to collect before contacting HP

Be sure to have the following information available before you contact HP:

- Software product name
- Hardware product model number
- Operating system type and version
- Applicable error message
- Third-party hardware or software
- Technical support registration number (if applicable)

How to contact HP

Use the following methods to contact HP technical support:

- In the United States, see the Customer Service / Contact HP United States website for contact options:
http://welcome.hp.com/country/us/en/contact_us.html
- In the United States, call 1-800-HP-INVENT (1-800-474-6836) to contact HP by telephone. This service is available 24 hours a day, 7 days a week. For continuous quality improvement, conversations might be recorded or monitored.
- In other locations, see the Contact HP Worldwide website for contact options:
<http://welcome.hp.com/country/us/en/wwwcontact.html>

Registering for software technical support and update service

HP Insight software includes one year of 24 x 7 HP Software Technical Support and Update Service. This service provides access to HP technical resources for assistance in resolving software implementation or operations problems.

The service also provides access to software updates and reference manuals in electronic form as they are made available from HP. Customers who purchase an electronic license are eligible for electronic updates.

With this service, Insight software customers benefit from expedited problem resolution as well as proactive notification and delivery of software updates. For more information about this service, see the following website:

<http://www.hp.com/services/insight>

Registration for this service takes place following online redemption of the license certificate.

How to use your software technical support and update service

After you have registered, you will receive a service contract in the mail containing the Customer Service phone number and your Service Agreement Identifier (SAID). You need your SAID when you contact technical support. Using your SAID, you can also go to the Software Update Manager (SUM) web page at <http://www.itrc.hp.com> to view your contract online.

Warranty information

HP will replace defective delivery media for a period of 90 days from the date of purchase. This warranty applies to all Insight software products.

HP authorized resellers

For the name of the nearest HP authorized reseller, see the following sources:

- In the United States, see the HP U.S. service locator web site:
http://www.hp.com/service_locator
- In other locations, see the Contact HP worldwide web site:
<http://welcome.hp.com/country/us/en/wwwcontact.html>

Documentation feedback

HP welcomes your feedback. To make comments and suggestions about product documentation, send a message to:

docsfeedback@hp.com

Include the document title and manufacturing part number in your message. All submissions become the property of HP.

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 website at <http://h18013.www1.hp.com/products/servers/management/agents/documentation.html>.

Related information

HP SMH documentation

For more information about HP SMH, see 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 website at <http://www.hp.com/go/hpux-core-docs>, select HP-UX 11i v3 for the latest documents and for previous versions of the documents, select either HP-UX 11i v1 or HP-UX 11i v2. Also, for Linux and Windows operating system releases, the release notes is available at the HP SMH web page at <http://h18013.www1.hp.com/products/servers/management/agents/documentation.html>.
- **HP System Management Homepage Help System** The help system provides a complete set of documentation for using, maintaining, and troubleshooting HP SMH. In HP SMH, go to the **Help** menu.
- **HP System Management Homepage Installation Guide** The installation 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 installation guide is available on the HP Technical Documentation website at <http://www.hp.com/go/hpux-core-docs>, select HP-UX 11i v3 for the latest documents and for previous versions of the documents, select either HP-UX 11i v1 or HP-UX 11i v2. Also, for Linux and Windows operating system releases, the installation 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. The user guide is available on the HP Technical Documentation website at <http://www.hp.com/go/hpux-core-docs>, select HP-UX 11i v3 for the latest documents and for previous versions of the documents, select either HP-UX 11i v1 or HP-UX 11i v2. Also, for Linux and Windows operating system releases, the user guide is available at the HP SMH web page at <http://h18013.www1.hp.com/products/servers/management/agents/documentation.html>.
- **Simplifying single-system management on HP-UX 11i – HP System Management Homepage (HP SMH)** This white paper introduces HP SMH and its various plug-ins. The use cases involving HP SMH plug-ins highlight the features provided by HP SMH. The white paper is available on the HP Technical

Documentation website at <http://www.hp.com/go/hpux-core-docs>, select HP-UX 11i v3 for the latest documents and for previous versions of the documents, select either HP-UX 11i v1 or HP-UX 11i v2, and search with the document title "Simplifying single-system management on HP-UX 11i - HP System Management Homepage (HP SMH)."

- **Safe and Powerful: Security in HP-UX System Management Homepage (SMH)** This white paper provides an overview of the security aspects in HP SMH. The white paper describes the various security features that the application provides, and includes security related tips for system administrators. The white paper is available on the HP Technical Documentation website at <http://www.hp.com/go/hpux-core-docs>, select HP-UX 11i v3 for the latest documents and for previous versions of the documents, select either HP-UX 11i v1 or HP-UX 11i v2, and search with the document title "Safe and Powerful: Security in HP-UX System Management Homepage (SMH)."
- **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 operating systems.
- **smhstartconfig (1M) manpage** For HP-UX operating system releases, the manpage is available from the CLI using the `man smhstartconfig` command. This information is not available for Linux and Windows operating systems.
- **sam (1M) manpage** For HP-UX operating system releases, the manpage is available from the CLI using the `man sam` command. This information is not available for Linux and Windows operating systems. Note SAM functionality changes in Chapter 3: "Installing HP SMH on HP-UX operating systems" (page 13).
- **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 operating system releases, the manpage is available from the CLI using the `man smh` command. This information is not available for Linux and Windows operating systems.
- **smhassist (1m) manpage** You can use the `smhassist` command to verify the configurations of SMH and see if there are any dependent software, patches or configuration errors. For HP-UX 11i v3 (B.11.31) and HP-UX 11i v2 (B.11.23) operating system releases, the manpage is available from the CLI using the `man smhassist` command. This information is not available for HP-UX 11i v1 (B.11.11), Linux, and Windows operating systems.
- **smhconfig (1m) manpage** You can use the `smhconfig` CLI to set configuration values through the command line. The CLI provides users having administrative rights access to modify configuration options, including the required security checks that allow the configuration options to be changed. For HP-UX 11i v3 (B.11.31) and HP-UX 11i v2 (B.11.23) operating system releases, the manpage is available using the `man smhconfig` command. This information is not available for HP-UX 11i v1 (B.11.11), Linux, and Windows operating systems.
- **HP System Management Homepage website** The website provides HP SMH information and product links. Go to the HP SMH website at <http://hp.com/go/smh>.
- **HP Insight Essentials software page** This web page is at <http://www.hp.com/servers/manage>.

HP-UX documentation

For more information about using HP SMH in an HP-UX environment, see the following sources. They are available on the Instant Information DVD and on the HP Technical Documentation web site at <http://www.hp.com/go/hpux-core-docs>.

- **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.
- For HP-UX operating system release documentation, check for the latest version on <http://www.hp.com/go/hpux-core-docs>.

HP Insight Remote Support Software

HP strongly recommends that you install HP Insight Remote Support software to complete the installation or upgrade of your product and to enable enhanced delivery of your HP Warranty, HP Care Pack Service or HP contractual support agreement. HP Insight Remote Support supplements your monitoring, 24x7 to ensure maximum system availability by providing intelligent event diagnosis, and automatic, secure submission of hardware event notifications to HP, which will initiate a fast and accurate resolution, based on your product's service level. Notifications may be sent to your authorized HP Channel Partner for on-site service, if configured and available in your country. The software is available in two variants:

- **HP Insight Remote Support Standard:** This software supports server and storage devices and is optimized for environments with 1-50 servers. Ideal for customers who can benefit from proactive notification, but do not need proactive service delivery and integration with a management platform.
- **HP Insight Remote Support Advanced:** This software provides comprehensive remote monitoring and proactive service support for nearly all HP servers, storage, network, and SAN environments, plus selected non-HP servers that have a support obligation with HP. It is integrated with HP Systems Insight Manager. A dedicated server is recommended to host both HP Systems Insight Manager and HP Insight Remote Support Advanced.

Details for both versions are available at:

<http://www.hp.com/go/insightremotesupport>

To download the software, go to Software Depot:

<http://www.software.hp.com>

Select Insight Remote Support from the menu on the right.

Typographic conventions

| | |
|--|--|
| <i>find(1)</i> | HP-UX manpage. In this example, "find" is the manpage name and "1" is the manpage section. |
| <i>Book Title</i> | Title of a book or other document. |
| <u><i>Linked Title</i></u> | Title that is a hyperlink to a book or other document. |
| <u>http://www.hp.com</u> | 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 <code>PATH</code> or <code>errno</code> . |
| 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. |

Index

C

- console installation
 - Linux, 51
 - Linux system preparation, 53

D

- documentation, 70

F

- features, 70

G

- getting started, 11

H

- HP Smart Update Manager
 - installation, 35
- HP-UX
 - installation, 13

I

- installation
 - HP Smart Update Manager, 35
 - HP-UX, 13
 - Linux x86_64, 51
 - operating systems, 7
 - requirements, 7, 9
 - web browsers, 8
 - Windows, 21, 35

L

- Linux
 - installation, 51
- Linux Itanium-based system
 - system preparation, 53
- Linux x86_64
 - installation, 51

M

- manpages, 70
- media, 9

O

- OpenSSH, 35
- operating systems, supported, 7

R

- removal of HP SMH, 65
- requirements
 - installation, 7
 - verifying system requirements, 9
- resources, 70

S

- setup, 11

- signing in, 61
- signing out, 61
- software, 9, 59

U

- uninstallation, 65

W

- web browsers, supported, 8
- websites, 9
- Windows
 - installation, 21
 - installation of HP Smart Update Manager, 35