HP ProLiant Firmware Maintenance CD User Guide



Part Number 447788-009
December 2009 (9th Edition)

© Copyright 2007, 2009 Hewlett-Packard Development Company, L.P.

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.

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.

Microsoft, Windows, Windows Server, Windows XP, and Windows Vista are U.S. registered trademarks of Microsoft Corporation.

Intended audience

This guide is intended for individuals who are familiar with the configuration and operation of Microsoft® Windows®, Windows Server® 2003, Windows Server® 2008, Linux, smart components, and deployment of firmware and software to systems and options. Because of the risk of data loss, only individuals experienced with using firmware and software should implement the procedures in this guide.

Contents

Introduction 5
HP ProLiant Firmware Maintenance CD overview 5
Minimum requirements 5
New features 6
Supported firmware 7
Obtaining the HP ProLiant Firmware Maintenance CD 8
Deployment options 8
Online deployment 9
Offline deployment 9
HP USB key utility 9
Using a hard drive 11
Deployment of components not on Firmware Maintenance CD 11
Trusted Platform Module 11
TPM scenarios 13
Firmware Maintenance CD powered by HP Smart Update Manager 15
Deployment scenarios 15
Graphical deployment on a local host 16
Scripted deployment on a local host 16
Deployment to multiple remote hosts 16
Keyboard support 17
Local host installations using the GUI 17
Selecting the location to check for updates 17
Selecting an installation host 20
Selecting components to install 22
Viewing the installation results 30
Multiple-host installations using the GUI 32
Selecting remote hosts or groups 32
Selecting components to install on multiple hosts 42
Viewing the installation results for multiple hosts 44
Scripted deployment 46
Command line interface 46
Command line syntax 46
Command line arguments 46
Component configuration for Windows components only 51
Command line examples 51
HP Smart Update Manager return codes 52
Creating HP Smart Update Manager input files 54
Input file format and rules 55
File encoding 56
Error reporting 56
Input file parameters 56
Advanced topics 61
Deploying firmware and software simultaneously 61
Server virtualization detection and support 62

Configuring IPv6 networks with HP Smart Update Manager....62
Configuring IPv6 for Windows Server 2003....62
Configuring IPv6 for Windows Server 2008....65
Configuring IPv6 for Linux....67
Troubleshooting....70
Recovering from a failed ROM upgrade....70
Recovering from a failed system ROM upgrade....70
Recovering from a failed option ROM upgrade....71
Recovering from an installation failure....72
Collecting trace directories....72
Recovering from a discovery failure....73
Troubleshooting connection errors....73
Recovering from a loss of Linux remote functionality....74
Configuring firewall settings....74
Recovering from a blocked program on Microsoft Windows....75
Configuring Windows firewall settings....75
Enabling ports in HP Smart Update Manager....75
Recovering from operating system limitations when using a Japanese character set....77
Displaying the user-specified reboot message using a Japanese character set when running on a Linux operating system....77
Rebooting with the user-specified reboot message using a Japanese character set when running on a Windows operating system....77
Recovering from Fatal Error - application will exit message....78
Running in a directory path containing double-byte characters....78
Recovering from a missing reboot message when running on SUSE LINUX Enterprise Server 9....78
Running HP Smart Update Manager on SUSE LINUX Enterprise Server 9....78
Recovering a lost HP Smart Update Manager connection....79
Mounting the Firmware Maintenance CD on virtual media....79
Troubleshooting HP Smart Update Manager in IPv6 networks....79
Troubleshooting HP Smart Update Manager in IPv6 Windows Server 2003 environment....79
Troubleshooting HP Smart Update Manager in IPv6 Windows Server 2008 environment....80
Troubleshooting HP Smart Update Manager in IPv6 Red Hat and Novell SUSE-based Linux environments....80
Technical support....82
Reference documentation....82
Operating system information....82
HP contact information....82
Acronyms and abbreviations....83
Index....85

Introduction

HP ProLiant Firmware Maintenance CD overview

The HP ProLiant Firmware Maintenance CD provides a collection of HP Smart Update Manager and firmware in an ISO image that can be used either in an offline, interactive mode, or online in either a scripted or interactive mode. The Firmware Maintenance CD provides firmware for supported HP servers and options. The Firmware CD contains all the firmware for the BladeSystem enclosures with the exception of the Virtual Connect firmware. The Virtual Connect firmware is not available on the Firmware Maintenance CD because of its size.

To deploy the Firmware Maintenance CD contents, see "Online deployment (on page 9)" and "Offline deployment (on page 9)." In offline mode, the Firmware Maintenance CD boots a small Linux kernel and enables firmware updates to take place on a single server using the embedded HP Smart Update Manager software. Because of the special boot environment, support for remote servers and hosts is not available. In online mode, users can leverage the autorun utility to launch HP Smart Update Manager or browse the CD to the \compaq\swpackages directory and execute it directly.

All firmware smart components are placed in the \compaq\swpackages directory for use by HP Smart Update Manager. If additional firmware smart components are needed, the Firmware Maintenance CD can be copied to a USB key, and these additional components added to the \compaq\swpackages directory. If HP Smart Update Manager supports the type of firmware added, it is automatically picked up the next time HP SUM is executed.

△ **CAUTION:** The Firmware Maintenance CD and its contents should be used only by individuals who are experienced and knowledgeable in their use. Before using HP Smart Update Manager to update firmware, be sure to back up the target server and take all other necessary precautions so that mission-critical systems are not disrupted if a failure occurs.

HP Smart Update Manager stores host and group information from session to session. However, user names, passwords, and existing credentials are not stored.

Use OA version 2.51 or later to get a list of all major firmware versions deployed in your enclosure using the Rack Firmware link on the main OA web page. HP supports the current and two previous versions of the Firmware Maintenance CD.

Minimum requirements

NOTE: HP Smart Update Manager requires a true Administrator login and not an elevated RUN AS Administrator. If you are unable to perform the net use * \\server\ADMIN$ for Microsoft Windows® target servers, you do not have sufficient privileges to run HP Smart Update Manager.

To successfully deploy HP Smart Update Manager on target systems based on a Windows® operating system, the following must be available:

- A local administrative system with 512 MB of memory, running a supported Windows® operating system

- Sufficient hard-drive space of at least twice the file size of the components to be deployed
- WMI enabled

> **NOTE:** When attempting to use the remote deployment functionality of HP Smart Update Manager on any edition of Windows Server® 2008, you must ensure that the File and Print Services feature is enabled and that the File and Print Services exception has been enabled in the Windows® firewall. Failure to do so prevents HP Smart Update Manager from deploying remote Windows® target servers.

To successfully deploy HP Smart Update Manager on target systems based on a Linux operating system, the following must be available:

- A local administrative system with 512 MB of memory, running a supported Linux operating system
- glibc 2.2.4-26 or later
- gawk 3.1.0-3 or later
- sed 3.02-10 or later
- pciutils-2.1.8-25.i386.rpm or later

To successfully update HP Smart Update Manager on remote target systems based on a Linux operating system, the following must be available:

- tcl-8.x package
- tcl-5.x package
- expect-5.x package

To successfully execute HP Smart Update Manager on any local or remote target systems running a SUSE Enterprise Linux 11 operating system on x86 or x64 architectures, the following library must be available:

- compat-libstdc++-296-2.96-132.7.2.i386.rpm or another compatibility library that provides the /usr/lib/libstdc++-libc6.2-2.so.3 file

Without this library, HP Smart Update Manager does not complete discovery and return "Discovery Failed" messages.

To perform Linux deployments, a root equivalent user account must be used. SSH support must be enabled and firewall opened to enable SSH communications on remote Linux servers or HP Smart Update Manager is not able to deploy updates. By default, SUSE LINUX Enterprise Server 10 and 11 block SSH support through the firewall. To enable SSH support if it has been disabled in the firewall, use the yast2 command to open the necessary ports in the firewall.

> **NOTE:** Beginning with the Firmware Maintenance CD v8.50, HP Smart Update Manager no longer runs on SUSE Enterprise Linux 9.



> **IMPORTANT:** The HP Smart Update Manager does not support cross-platform deployments (for example, deployments from Linux systems to Windows® systems).

New features

The Firmware Maintenance CD 8.70 has the following new features:

- Enables report generation from the command line

- /report generates a target summary and how the components in the repository affect the target (For example, whether each component applies to the target or not.)
- /inventory_report generates a report of the components in the specified repository.

- Accepts command line parameters from an input file

Supported firmware

The Firmware Maintenance CD provides the means to update the following firmware.

Firmware type	Supported by HP Firmware Maintenance CD
System ROM	Yes
iLO 2 firmware	Yes, local and remote
Broadcom NIC firmware	Yes
Intel NIC firmware	No
NetXen NIC firmware	No
Power PIC firmware	Yes, beginning with Firmware Maintenance CD 8.60
Smart Array controller firmware	Yes
SAS and SATA hard drive firmware behind Smart Array controllers	Yes
SAS and SATA hard drive firmware behind non-Smart Array controllers	No
Emulex, QLogic, and Brocade Fibre Channel Host Bus Adapter firmware	Yes, offline only
Tape blade firmware	Yes
Onboard Administrator firmware	Yes, online only
Virtual Connect firmware*	Yes, online only and components must be downloaded from the web and added to the CD
HP StorageWorks 600 Modular Disk System (MDS600)**	Yes, offline only
HP 3Gb SAS BL Switch firmware***	No

*Virtual Connect firmware components are not shipped with the HP Firmware Maintenance CD because of their size (approximately 50 MB per component). However, if the Virtual Connect firmware components are downloaded from the HP website, they can be added to the Firmware Maintenance CD by creating a USB key using the USB Key Utility. The latest version can be obtained from the HP BladeSystem Firmware Maintenance website (http://www.hp.com/go/bladesystemupdates).

**MDS600 firmware update requires HP Smart Update Manager 3.6.0 or later. All blades in an enclosure with Smart Array P700M controllers, except the blade doing the update, must be turned off before the firmware update process is initiated. MDS600 firmware can only be updated using the Firmware Maintenance CD in offline mode.

***The HP 3Gb SAS BL Switch firmware can only be updated by uploading a bin file through the Virtual Storage Manager (VSM) product. This firmware is currently delivered as a binary image file on the HP website and must be downloaded and manually upgraded.

Because firmware might be able to update only in online or offline mode for some components, you might need to execute the HP Firmware Maintenance CD both online and offline to update all the firmware in an enclosure.

Obtaining the HP ProLiant Firmware Maintenance CD

The ProLiant Firmware Maintenance CD can be downloaded at no cost from the HP website (http://www.hp.com/support) and as part of the ProLiant Essentials Foundation Pack. The HP Smart Update Manager utility is available from the ProLiant Firmware Maintenance CD.

Deployment options

You can run the Firmware Maintenance CD either online or offline.

When performing an online deployment, you must boot the server from the operating system that is already installed and running.

Deployment	Supported systems
Online deployment	HP Smart Update Manager supports online deployments of all ROM flash components for both Windows® and Linux operating systems including: • HP Onboard Administrator for HP c-Class BladeSystem • HP Virtual Connect Ethernet and Fibre Channel Modules for c-Class BladeSystem • System hard-drive (SAS and SATA) • Array-controller • Lights-Out Management ROM flash components

NOTE: The Onboard Administrator and Virtual Connect Ethernet and Fibre Channel Modules are supported only in online deployments.

When performing an offline deployment, you can boot the server from the Firmware Maintenance CD or a USB drive key that contains the Firmware Maintenance CD contents.

Deployment	Supported systems
Offline deployment	HP Smart Update Manager supports offline deployments of all ROM flash components including: • System hard-drive • Array-controller • QLogic and Emulex Fibre Channel HBA • Lights-Out Management ROM flash components

NOTE: You can add firmware components to the USB drive key in the /compaq/swpackages directory.

Online deployment

To deploy components online:

1. Choose one of the following options:
   - Insert the Firmware Maintenance CD. The Firmware Maintenance CD interface opens.

     NOTE: In Linux, if the autostart is not enabled, you must manually start the Firmware Maintenance CD.

   - Insert the USB drive key. Manually start the interface and open a CLI. To access the Firmware Maintenance CD, enter one of the following commands:
     - In Windows®, enter _autorun\autorun_win
     - In Linux, enter /autorun

     NOTE: If you are using a USB drive key with multiple cd images, navigate to the appropriate CD subfolder to launch autorun for the Firmware Maintenance CD.
2. Read the End-User License Agreement. To continue, **click Agree.** The Firmware Maintenance CD interface appears.
3. Click the **Firmware Update** tab.
4. Click **Install Firmware.** The HP Smart Update Manager is initiated.
5. Select, and then install the desired components. For more information, see "Local host installations using the GUI (on page 17)" or "Multiple-host installations using the GUI (on page 32)."

Offline deployment

To deploy components offline:

1. Boot the server from the Firmware Maintenance CD or a USB drive key.
2. At the prompt, select a language and keyboard.
3. Click **Continue.**
4. Read the End-User License Agreement. To continue, click **Agree**. The Firmware Maintenance CD interface appears.
5. Click the **Firmware Update** tab.
6. Click **Install Firmware.** The HP Smart Update Manager is initiated.
7. Select, and then install the desired components. For more information, see "Local host installations using the GUI (on page 17)" or "Multiple-host installations using the GUI (on page 32)."

HP USB key utility

The HP USB Key Utility enables you to copy the Firmware Maintenance CD contents to a USB memory key. You can then run the Firmware Maintenance applications from a USB key instead of from the CD. Insert a USB key containing the Firmware CD ISO image created by using the HP USB Key Creator for Windows utility into a usb port of your server or through the SUV (Serial-USB-Video) cable attached to the server to be updated if the server supports the SUV cable.

For Windows® operating systems, the HP USB Key Creator for Windows utility must be downloaded from the HP website (http://www.hp.com) and installed on a workstation. After installation, the utility places a shortcut in the HP System Tools folder in the Programs start menu.

To create your bootable drive key and copy the contents of the CD:

1. Place your HP USB drive key in an available USB port.
2. Select the **HP USB Key Utility** shortcut in the HP System Tools folder.
3. Complete each step presented by the application.
4. The HP USB Key Creator formats the USB key, therefore files on the key are lost. Ensure that you are using a USB key that is at least 1GB in size and does not contain any valuable files.

For Linux, the USB key can be created manually:

1. Obtain SYSLINUX 3.2 or higher from freshmeat.net or syslinux.zytor.com and download to a Linux workstation.
2. Install the SYSLINUX RPM obtained in step 1.
3. Create a directory for the USB key mountpoint, if one does not already exist.

   For example, `mkdir /usbkey`.
4. Insert the USB key and mount it. The device mountpoint can vary depending on whether other SCSI drives are also installed on the server. Therefore, the device mountpoint can be sdb1, sdc1, and so forth.

   ```
   mount /dev/sda1 /usbkey
   ```
5. Issue the command `./syslinux /usbkey` to have SYSLINUX write out the boot partition to the USB key. Failure to issue this command might lead to a key that does not boot the Firmware CD until the SYSLINUX command is successful.
6. Create a directory to mount the CD image. For example, `mkdir /cd_mount_point`.
7. Insert the Firmware CD or mount the Firmware CD ISO through a loopback:

   `mount /dev/cdrom /cd_mount_point` or `mount -t iso9660 firmware-<version>.iso /cd_mount_point -o loop`
8. Change to the /usb directory on the CD.

   ```
   cd /cd_mount_point/usb
   ```
9. Execute the usbcreator.sh shell script passing in the CD mount point and the USB mount point to move the Firmware CD files to the USB key

   ```
   ./usbcreator.sh /cd_mount_point /usbkey
   ```
10. If additional components must be added to the USB, copy the components into the /compaq/swpackages (Linux) or the \compaq\swpackages (Windows) directory and HP Smart Update Manager picks them up automatically if the version can support the type of components added.
11. Unmount the CD and the USB key. This must match the initial mount point in step 4.

    ```
    umount /dev/cdrom
    umount /dev/sda1
    ```
12. Remove the USB key and CD from the workstation used to create the USB key.

NOTE: To remove a CD image from your USB drive key, delete the subfolder containing the CD image and edit the syslinux.cfg file at the root of the USB drive key to remove the section referencing that subfolder name.

Using a hard drive

1. Copy the contents of the \compaq\swpackages directory from the CD or ISO image to a directory on the hard drive where HP Smart Update Manager will be executed.
2. Ensure that execute privileges are available in Linux by using the `chmod 700 *` command. By default, the files are copied off the CD in Linux as read-only with no execution privileges.
3. Copy any updated files into the same directory where the files were copied in step 1.
4. Execute HP Smart Update Manager to have the new firmware components recognized.

Deployment of components not on Firmware Maintenance CD

If you have components that are not on the Firmware Maintenance CD that you want to deploy, you can include other smart components to HP Smart Update Manager environment. To deploy software and firmware components that are not on the Firmware Maintenance CD:

1. Obtain the components from the HP website (http://www.hp.com).
2. Create a bootable USB key ("HP USB key utility" on page 9), or copy the \compaq\swpackages directory to the hard drive, and then remove the read-only bit.
3. Add the additional components to the \compaq\swpackages directory on the USB key or to the directory on the hard drive with the components from the Firmware Maintenance CD.
4. Start HP Smart Update Manager.
5. On the Source Selection screen, you can specify the directory where all of the components are located as well as select the **Check ftp.hp.com** box if you want to include the latest version of software and firmware components from the HP website (http://www.hp.com).

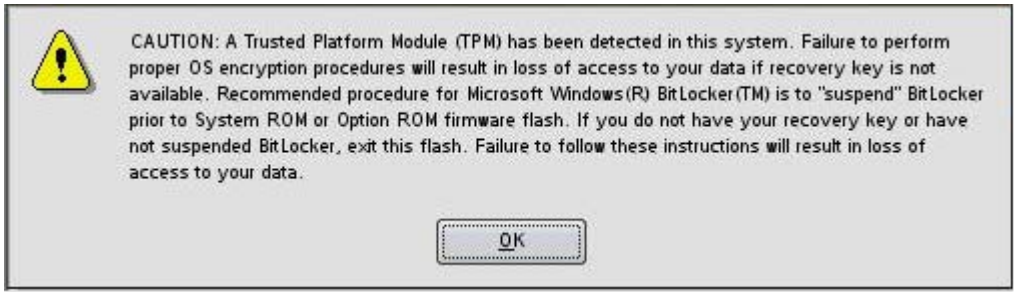
Trusted Platform Module

The TPM, when used with BitLocker, measures a system state and, upon detection of a changed ROM image, restricts access to the Windows® file system if the user cannot provide the recovery key. HP Smart Update Manager detects if a TPM is enabled in your system. If a TPM is detected in your system or with any remote server selected as a target, for some newer models of ProLiant, HP Smart Update Manager utilities for iLO, Smart Array, NIC, and BIOS warn users prior to a flash. If the user does not temporarily disable BitLocker and does not cancel the flash, the BitLocker recovery key is needed to access the user data upon reboot.

A recovery event is triggered if:

- The user does not temporarily disable BitLocker before flashing the System BIOS when using the Microsoft BitLocker Drive Encryption.
- The user has optionally selected to measure iLO, Smart Array, and NIC firmware.

If HP Smart Update Manager detects a TPM, a pop-up warning message appears.



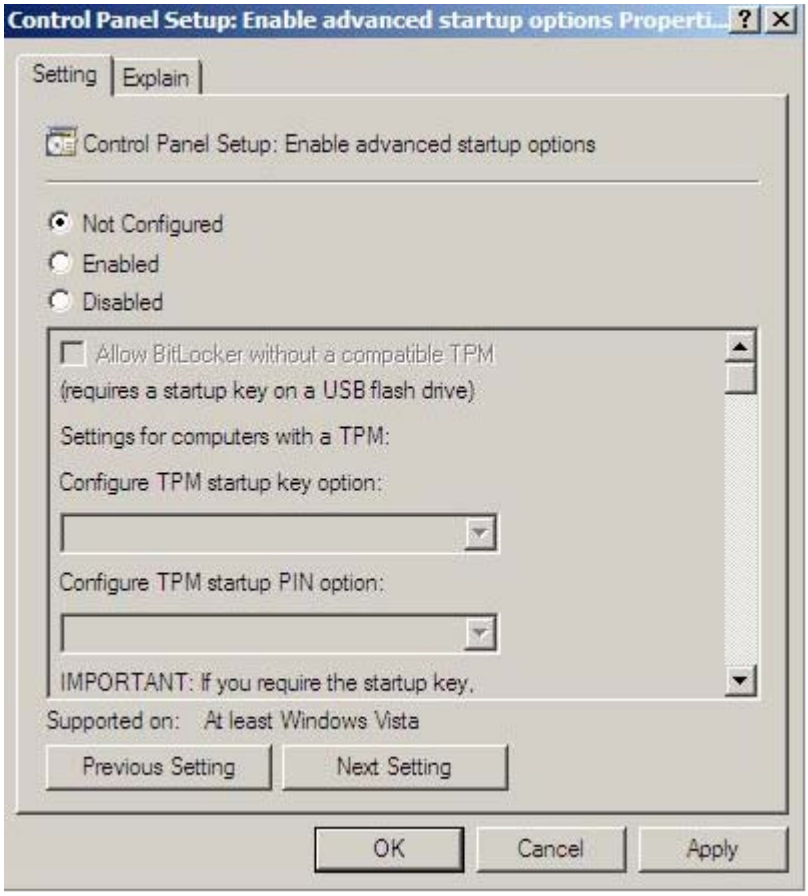
To enable firmware updates without the need to type in the TPM password on each server, the BitLocker Drive Encryption must be temporarily disabled. Disabling the BitLocker Drive Encryption keeps the hard drive data encrypted. However, BitLocker uses a plain text decryption key that is stored on the hard drive to read the information. After the firmware updates have been completed, the BitLocker Drive Encryption can be re-enabled. Once the BitLocker Drive Encryption has been re-enabled, the plain text key is removed and BitLocker secures the drive again.

> **NOTE:** Temporarily disabling BitLocker Drive Encryption can compromise drive security and should only be attempted in a secure environment. If you are unable to provide a secure environment, HP recommends providing the boot password and leaving BitLocker Drive Encryption enabled throughout the firmware update process. This requires the /tpmbypass parameter for HP Smart Update Manager or the firmware update is blocked.

To temporarily disable BitLocker support to allow firmware updates, perform the following:

1. Click **Start,** and then search for gpedit.msc in the Search Text box.
2. When the Local Group Policy Editor starts, click **Local Computer Policy.**
3. Click **Computer Configuration>Administrative Templates>Windows Components>BitLocker Drive Encryption.**
4. When the BitLocker settings are displayed, double-click **Control Panel Setup: Enable Advanced startup options.**
5. When the dialog box appears, click **Disable.**

6. Close all the windows, and then start the firmware update.



To enable advanced startup options, use the following command:

```
cscript manage-bde.wsf -protectors -disable c:
```

When the firmware update process is completed, the BitLocker Drive Encryption support can be re-enabled by following steps 1 through 4 but clicking **Enabled** in step 5 instead. The following command can be used to re-enable BitLocker Drive Encryption after firmware deployment has completed.

```
cscript manage-bde.wsf -protectors -enable c:
```

TPM scenarios

The following table discusses the TPM detection scenarios that you might encounter.

Scenario	Result
If the TPM is detected and enabled, the installation is not silent, and a system ROM must be updated.	A pop-up warning message appears. After **OK** is selected, you can continue. The installation is not canceled.
If the TPM is detected and enabled, the installation is silent, the /tpmbypass switch is not given, and any firmware updated must be applied to the server.	No pop-up warning appears. A new log file is generated (%systemdrive%\cpqsystem\log\cpqstub.log). Because the installation is silent, the installation is terminated and cannot continue.

If the TPM is detected and enabled with Option ROM Measuring, the installation is not silent, and a system ROM must be updated.	A pop-up warning message appears. After **OK** is selected, you can continue. The installation is not canceled.
If the TPM is detected and enabled with Option ROM Measuring, the installation is silent; the /tpmbypass switch is not given, and any firmware updated must be applied to the server.	No pop-up warning appears. A new log file is generated (%systemdrive%\cpqsystem\log\cpqstub.log). Because the installation is silent, the installation is terminated and cannot continue.
If the TPM is detected and enabled, the installation is silent, and the /tpmbypass switch is supplied.	The installation occurs.

Other scenarios do not affect the normal installation procedure.

Firmware Maintenance CD powered by HP Smart Update Manager

Deployment scenarios

HP Smart Update Manager deploys smart firmware components on a local host or one or more remote hosts. The remote hosts must be online and running the same operating system as the system running HP Smart Update Manager. For example, when the remote hosts are running Linux, the HP Smart Update Manager must also be running on a Linux operating system. HP Smart Update Manager supports the following operating systems:

- Windows Server® 2003
- Windows Server® 2003 x64
- Windows Server® 2008
- Windows Server® 2008 x64
- Windows Server® 2008 R2 x64
- Red Hat Enterprise Linux 4
- Red Hat Enterprise Linux 5
- SUSE Linux Enterprise Server 10
- SUSE Linux Enterprise Server 11

The following table describes typical HP Smart Update Manager deployment scenarios.

Scenario	Description
Graphical deployment on a local host	Use this scenario when you: • Are not familiar with command line tools. • Are deploying components on a local, single host. • Do not require scripting.
Scripted deployment on a local host	Use this scenario when you: • Are familiar with command line tools. • Are deploying components on a local, single host. • Must perform a customized, scripted deployment.
Graphical deployment to a remote host	Use this scenario when you: • Are not familiar with command line tools. • Are deploying components on one or more remote hosts. • Do not require scripting.
Scripted deployment to a remote host	Use this scenario when you: • Are familiar with command line tools. • Are deploying components on one or more hosts. • Must perform a customized, scripted deployment to one or

Scenario	Description
	more host systems.

Graphical deployment on a local host

To deploy components to a single local host, use the HP Smart Update Manager GUI.

1. Ensure all minimum requirements are met as described in "Minimum requirements (on page 5)."
2. Ensure that the components to be deployed are accessible to the local host.

For information about performing the deployment using the GUI, see "Local host installations using the GUI (on page 17)."

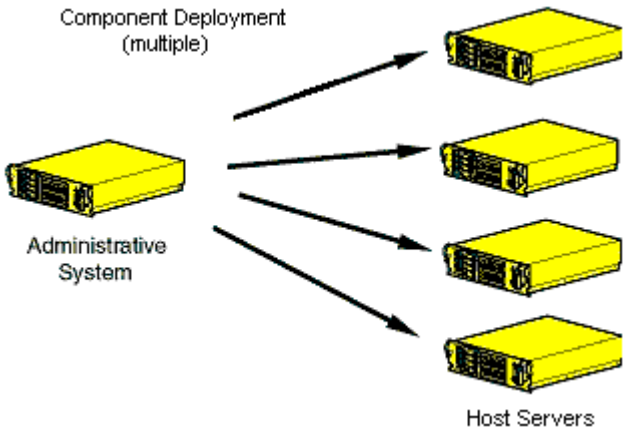
Scripted deployment on a local host

To deploy components to a local host using the command line interface:

1. Ensure all minimum requirements are fulfilled as described in "Minimum requirements (on page 5)."
2. Ensure that the components to be deployed are accessible to the local host.
3. Create a script to customize the deployment. See "Scripted deployment (on page 46)" for more information.
4. Execute the script.

Deployment to multiple remote hosts

NOTE: A remote host can be the IP address or DNS name of a remote server, remote iLO NIC port, Virtual Connect Ethernet or Fibre Channel Module for c-Class BladeSystem, or BladeSystem Onboard Administrator.



To deploy components to multiple remote hosts using the GUI:

1. Ensure that all minimum requirements are met as described in "Minimum requirements (on page 5)."
2. Ensure that the components to be deployed are accessible to the administrative system.

For more information about performing the deployment using the graphical interface, see "Multiple-host installations using the GUI (on page 32)."

To deploy components to multiple remote hosts using the CLI:

1. Ensure that all minimum requirements are met as described in "Minimum requirements (on page 5)."
2. Ensure that the components to be deployed are accessible to the administrative system.
3. Create a script to customize the deployment. For more information, see "Scripted deployment (on page 46)."
4. Execute the script.

Keyboard support

The HP Smart Update Manager graphical user interface has accelerator keys that enable you to manage and control common tasks quickly. To ensure proper navigation, the following are a few reminders.

- Depending on the operating system, you must press **ALT** to see the task corresponding to the underlined letter.
- The accelerator keys work by pressing **ALT + the underlined letter**.
- Press **Space** to select items such as hosts or groups.
- Press **Tab** to select from a list, and then press the **arrow keys** to toggle radio buttons.

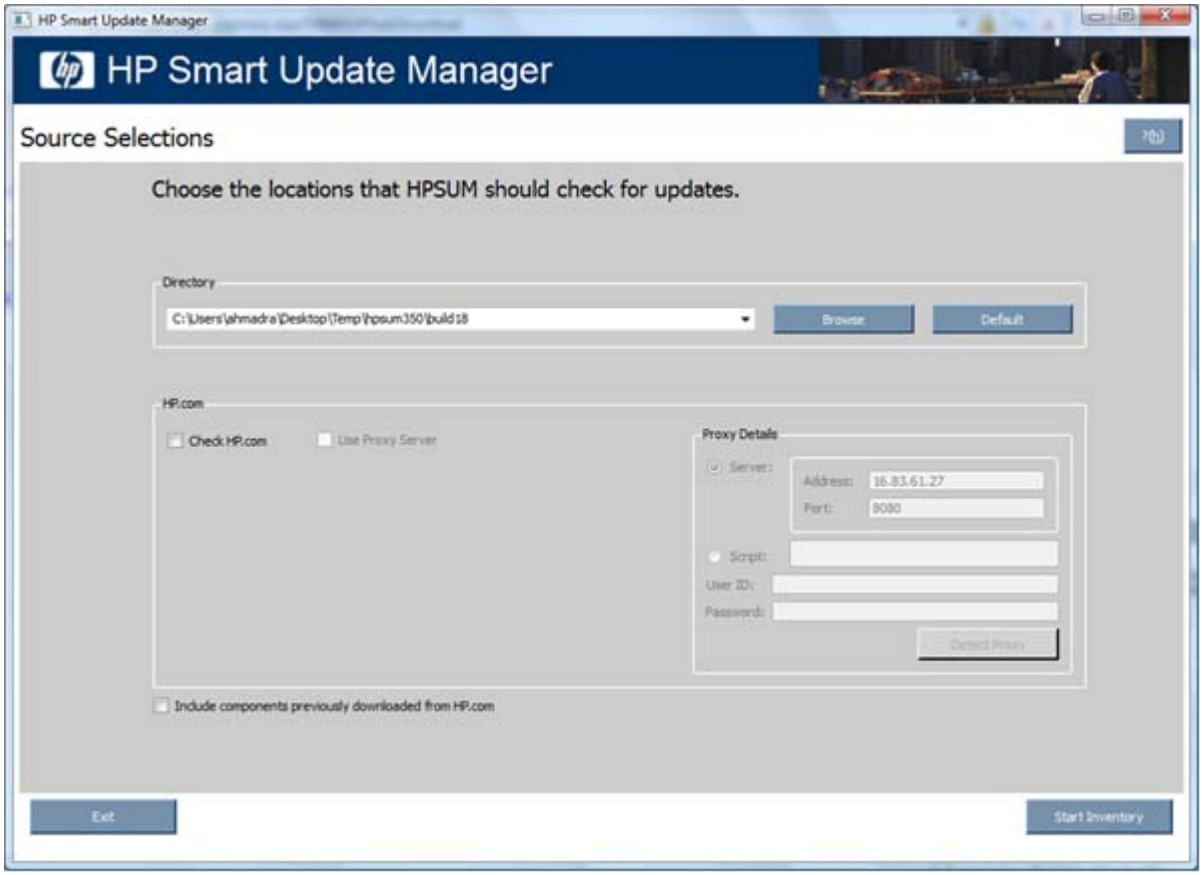
Local host installations using the GUI

HP Smart Update Manager can deploy smart components on a local host or on one or more remote hosts. You can deploy components on a local host by using the HP Smart Update Manager GUI. To access the HP Smart Update Manager, see Deployment Options (on page 8).

Selecting the location to check for updates

The Source Selections screen enables you to select components from a directory and the HP FTP site (ftp://ftp.hp.com) as a location for obtaining updates to your systems. You can also select components that have already been downloaded. You can use up to all three of the following methods simultaneously.

NOTE: For offline deployments, the Source Selections screen does not appear.



The Source Selections screen allows you to specify where to get components for updating the targets by using one or more of the following methods:

- Directory—This option enables you to select the directory where the components you want to deploy are located. It can be located on a locally accessible file system. The default location is the directory from where HP Smart Update Manager is executed. To change the directory value, click the **Browse** button to launch a select-directory menu. To set the field back to its initial value, click the **Default** button.
- Check ftp.hp.com—This option enables you to get firmware and software components located on the HP FTP site (ftp://ftp.hp.com). The HP FTP site contains the latest versions of the firmware and software components available from HP. The components, which are applicable (denoted with an HP.com icon) are available for selection on the Select Items to be Installed screen. When using this method, both firmware and software components are available for selection depending on the options set on the Set Bundle Filter screen when ProLiant Support Packs are included in the components to be deployed. To limit only the appearance of available firmware components, use the `/romonly` command line argument and use the `/softwareonly` command line argument for software components. The components are not downloaded from the HP FTP site to a target until the Install button is actually selected unless the component is needed to discover supported devices. If components are needed for discovery, you are prompted to allow this action. If components are already up-to-date, the components are not seen.
  - The Check ftp.hp.com checkbox is cleared by default. To pull updates from the web, select the **Check ftp.hp.com** checkbox. To use a proxy server and enable the proxy details group box, select the **Use Proxy Server** checkbox.

- Proxy Details—Enter the proxy information in the Proxy Details group box to be used to access the HP FTP site. To auto-detect the proxy information, click the **Detect Proxy** button. If you use a proxy server in accessing the HP FTP site, the proxy information is saved and prepopulated on the next deployment.

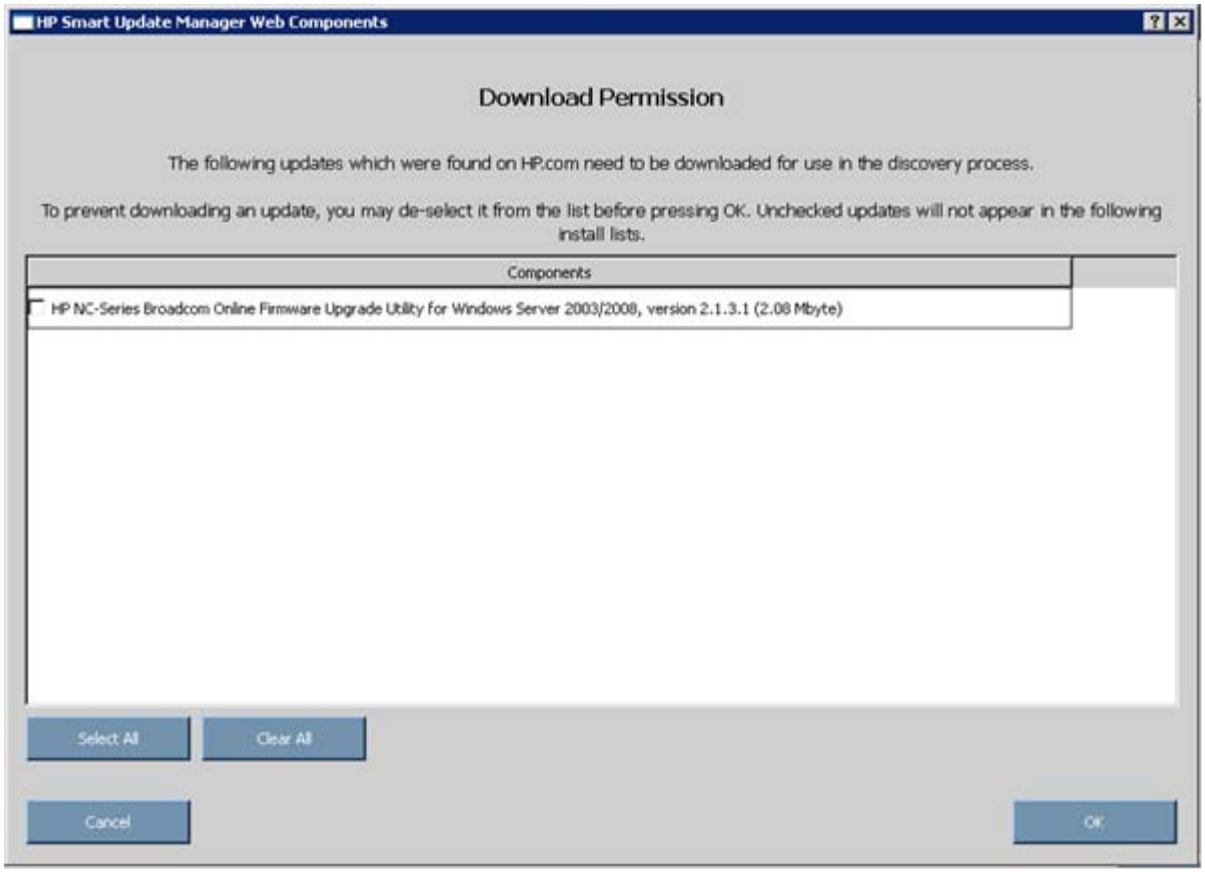
  NOTE: HP Smart Update Manager does not support FTP over HTTP proxy. FTP downloaded from HTTP proxy fails. Components from the HP FTP site is only presented for selection on the Select Items to Install screen if their versions are newer than what is already on the system. If a system has all of the latest versions of firmware and software, no components from HP.com is presented on the Select Items to be Installed screen.

- Include components previously downloaded from HP.com—This option includes the components that have been previously downloaded from the HP ftp site as available for selection on the Select Items to be Installed screen. The default location for the previously downloaded components is %TEMP%\hp_sum\RepositoryManager\Repxx\<component_number> directory. To use components already downloaded from HP.com, select this checkbox.

To begin the inventory process, click **Start Inventory.** The Inventory Progress screen appears while the HP Smart Update Manager builds an inventory of available updates.

Download Permission

Before starting any discovery, HP Smart Update Manager searches the web digest for self-discovery components that need to be downloaded for the discovery process. Self-discovered components are components including but not limited to NIC firmware and tape firmware that HP Smart Update Manager uses to discover the hardware in the system. The Download Permission screen appears.



The Download Permission screen lists the available updates found on the HP FTP site. You can select or clear the updates you are allowing to download. The Download Permission screen includes the following buttons:

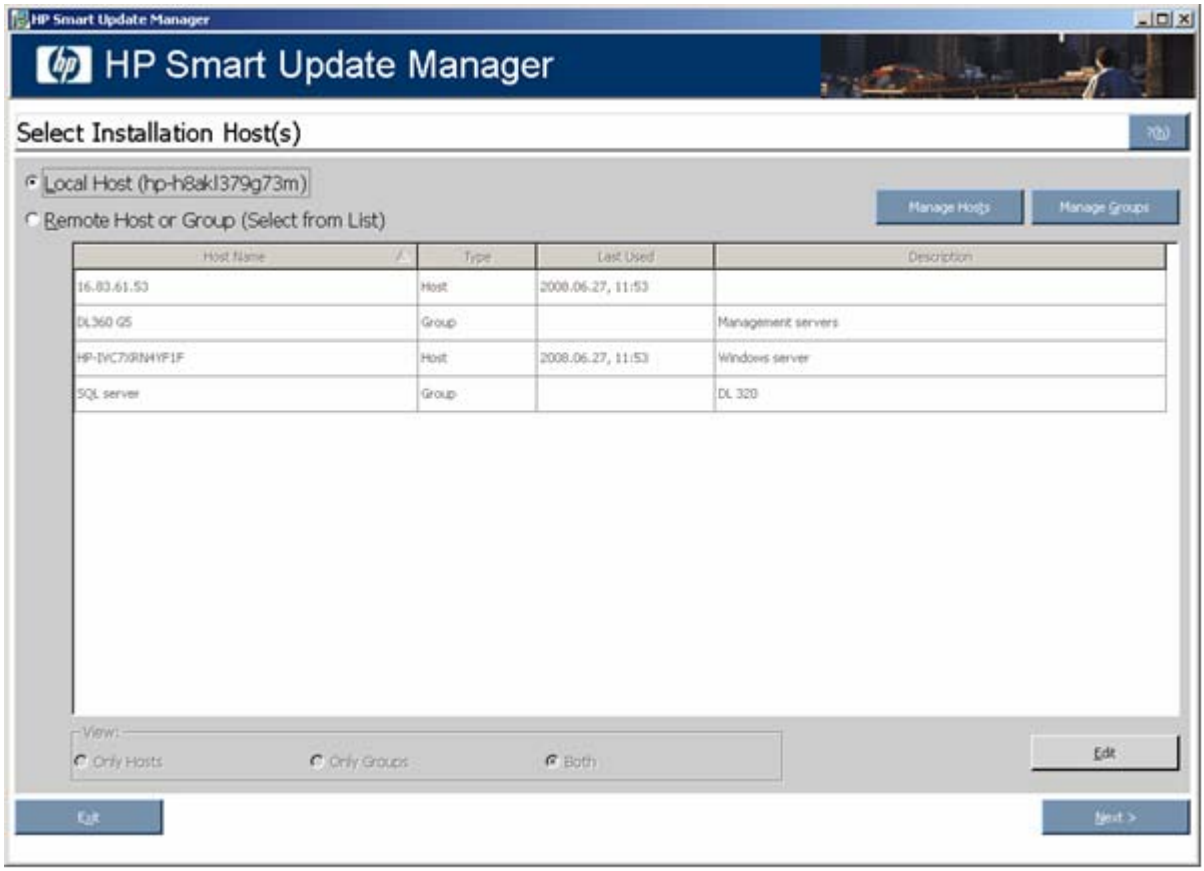
- Select All—Selects all available components for download.
- Clear All—Clears all components selected for download.
- Cancel—Exits the Download Permission screen and returns to the Source Selections screen.
- OK—Downloads all selected components.

> **NOTE:** Emulex HBAs, Qlogic HBAs, and offline-only components cannot be retrieved from the HP website and can only be installed offline. These components do not appear on the web components list.

For more information on selecting the location for updates, see Selecting the location to check for updates (on page 17).

Selecting an installation host

The Select Installation Host(s) screen appears when you have selected the location to obtain your updates from.



The Select Installation Host(s) screen enables you to choose a host for component installation. By default, the first time you run HP Smart Update Manager on a particular system, the only host available is the local host. However, you can also select remote hosts as your targets. For more information about using the graphical interface for multiple remote deployments, see Multiple-host installations using the GUI (on page 32).

The following columns are included in the Select Installation Host(s) screen:

- Host Name—Displays the host IP address or DNS name.
- Type—Categorizes the system as a host or group.
- Last Used—Enables you to sort the list by the most recently used hosts.
- Description—Displays the user-defined description given to a host.

When the Remote Host or Group option in the Select Installation Host(s) screen is selected, you can sort your view of the host list by selecting Only Hosts, Only Groups, or Both.



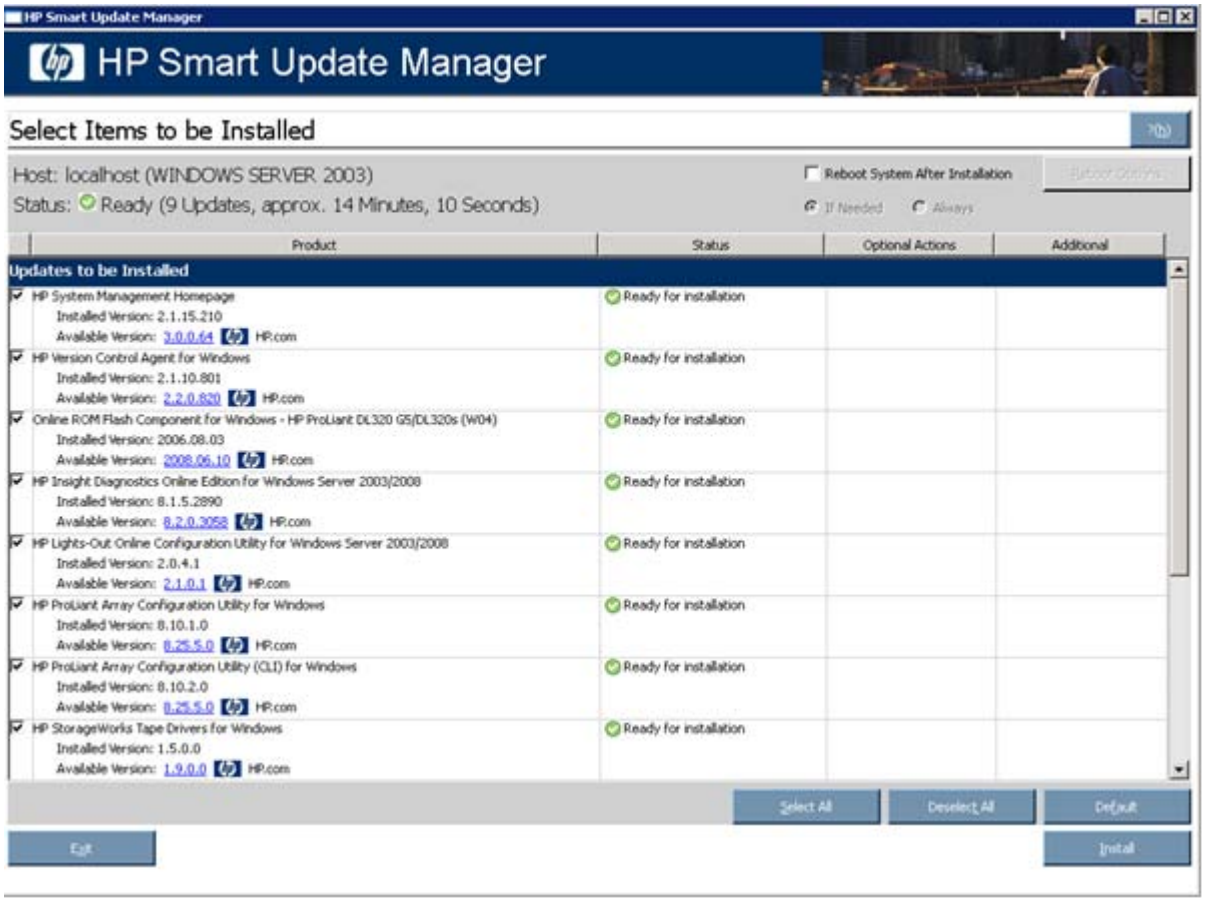
The Select Installation Host(s) screen also includes the following buttons:

- Manage Hosts—Enables you to add, edit, and delete hosts.
- Manage Groups—Enables you to add, edit, and delete groups.
- Edit—Enables you to edit the selected host.
- Next—Proceeds to the next step in the installation process where the local or remote system checks for already installed items.
- Exit—Exits HP Smart Update Manager.

To continue selecting an installation host, click **Next.** For multiple remote deployments, enter the credentials for the host. When the credentials have been successfully entered, the discovery process occurs.

Selecting components to install

When the discovery process ("Selecting an installation host" on page 20) is complete, the Select Items to be Installed screen appears. The Select Items to be Installed screen displays information about which components are available for installation on your system and enables you to select or deselect components to install.



The Select Items to be Installed screen includes the following sections:

- Product—Lists the system on which the selected items are installed.
- Status—Indicates if the installation is ready.
- Optional Actions—Indicates whether the component configuration is optional or required but has already been updated.
- Reboot section—Enables you to specify reboot settings and determine when reboots occur.
- Component selection pane—Enables you to specify which components to install.

When updating installation for some but not all NIC components, select the devices to be updated in the window that appears. If the NIC firmware listed for the device does not have a version, you cannot add that firmware to the device using HP Smart Update Manager.

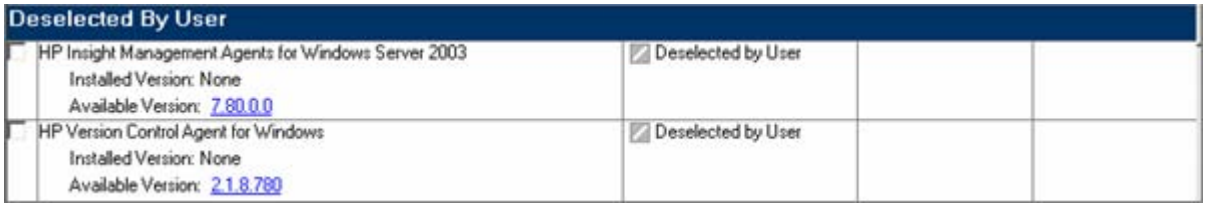
When multiple hardware devices such as hard drives or array controllers exist in a single server, HP Smart Update Manager lists each device only once. If the devices have different firmware versions, then the versions are listed from earliest to latest in a range. When multiple instances of the firmware are available for installation, the instances are listed from latest to earliest. If necessary, all hardware device firmware is flashed to the selected version.

The Select Items to be Installed screen also includes the following buttons:

- Select All—Selects all available components for installation.
- Deselect All—Clears all components selected for installation.
- Default—Restores the selections in the product installation pane to the default view, which is based on the existing configuration of the local system.
- Exit—Exits HP Smart Update Manager.
- Install—Installs all selected components.
- Add Supplemental—Enables you to deploy additional components from a removable device. The additional components must be located on the root of the device. This button is available only for offline deployments.

The component selection pane in the Select Items to be Installed screen is divided into sections, which might vary depending on your system. These sections include the following headings:

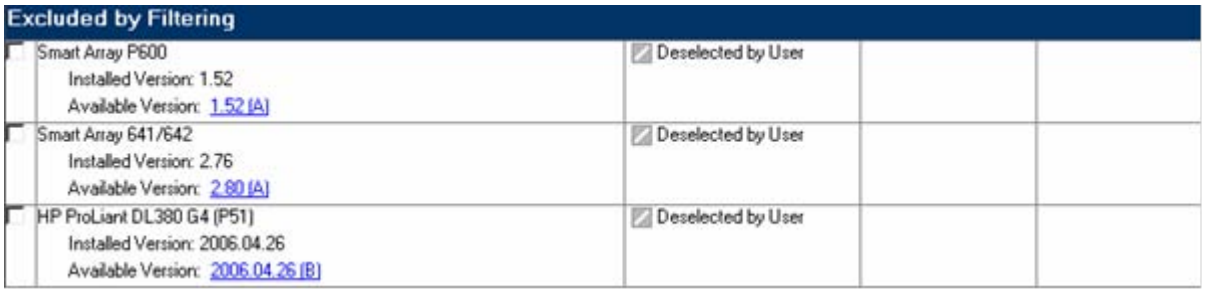
- Deselected By User—You have deselected the components in this section, and the components are not installed.



- Installation Not Needed—The components in this section do not need to be updated, but can be. To update the components, select the components, and then click **Installation Options.**



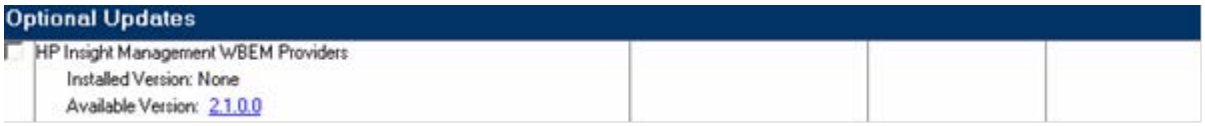
- Excluded by Filtering—The components in this section were excluded through your filtering options. You can use the Select Bundle Filter option or one of the command line arguments, `/romonly` or `/softwareonly`, to change the exclusion on a single target. For multiple targets, this must be repeated on each additional target. The Select Bundle Filter option screen is only available when there are bundles such as ProLiant Support Packs included in the location where the components to be downloaded are.



- Updates to be Installed—The components in this section can be installed on your system.



- Optional Updates—The components in this section are not selected for installation by default, even if the product is not already installed or is installed but not up-to-date. To include the component in the installation set, you must select the component.



- No Device Driver Installed—The devices supported by the components in this section are detected on the system, but HP Smart Update Manager requires a device driver before the component can be made available for installation. Install the device driver.



Multi-session installation appears on the Source Selections screen under certain combinations of dependencies between the components selected for installation.

- Component B depends on the product in component A, in a way that requires the product to be already installed and active for component B to install.
- Component A needs a reboot after installation to become active.
- There is not an already-installed version of the product in component A, or at least not one of the correct version to satisfy the dependency.

If all of the above conditions are true, then HP Smart Update Manager detects it and a notification to reboot appears in order to continue the installation. All installable components appear in the original update list, but only the components shown before the notification is installed. You must reboot to complete the installation and then restart HP Smart Update Manager to continue the installation process.

Status field



The Status field of the Select Items to be Installed screen displays information about whether the installation is ready to proceed or not.

Icon	Text	Description
	Ready	All selected components are ready to be installed.
	Already up-to-date	No component installation is required.
	None Selected	No components are selected for installation.

Icon	Text	Description
	*x* Critical Action	*X* components are not ready for installation due to failed dependencies, where *x* is the number of components. The installation cannot proceed until the dependencies are met or the component is deselected for installation.

Reboot section

The reboot section of the Select Items to be Installed screen enables you to specify preferred reboot behavior.

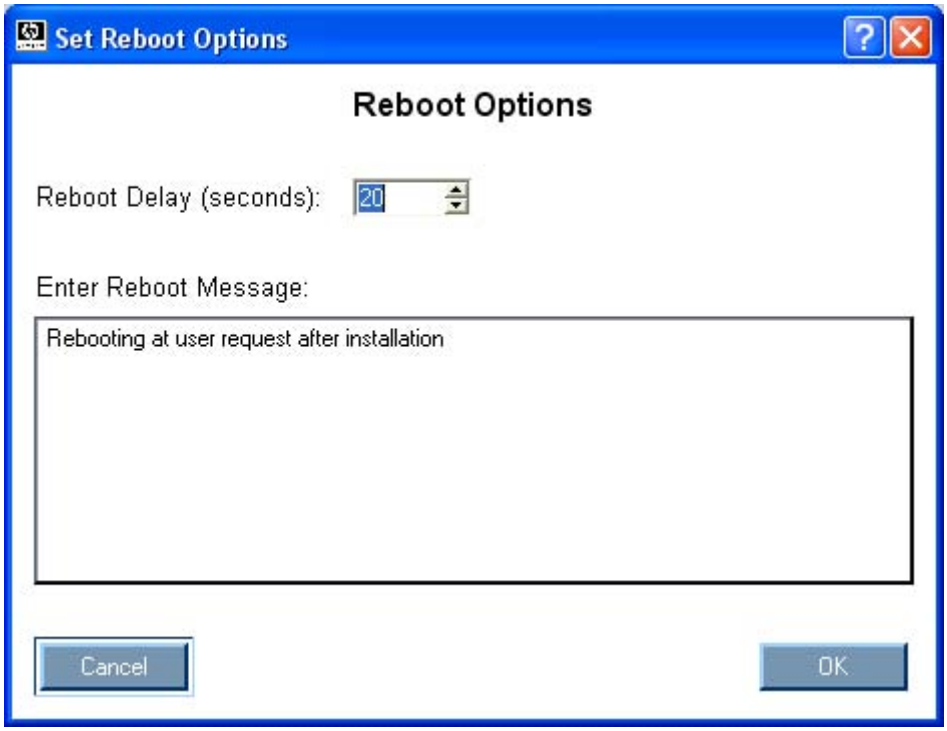


To instruct the system to reboot after updates are installed:

1. Click **Reboot System After Installation.**
2. Click **Always** or **If Needed**.

If **Always** is selected, then the system will always be rebooted unless there is a component installation failure. If **If Needed** is selected, then the system will be rebooted if needed by at least one component unless there is a component installation failure.

To change the delay before reboot or the reboot message, click **Reboot Options.** The Set Reboot Options screen appears.



NOTE: In Linux, the Reboot Delay time is automatically converted from seconds to minutes. Any value under a full minute, 59 seconds or less, will be rounded to the next minute for Linux.

Make any changes, and click **OK.**

Component selection pane

The component selection pane of the Select Items to be Installed screen displays (by component number order, unless a dependency causes the installation order to change) all components available for installation based on your server and hardware options. The HP Smart Update Manager checks each component for dependencies, if the component is already installed on the system, or if it requires a reboot after installation. Items available for installation are selected by default. You can deselect any components you do not want to install.

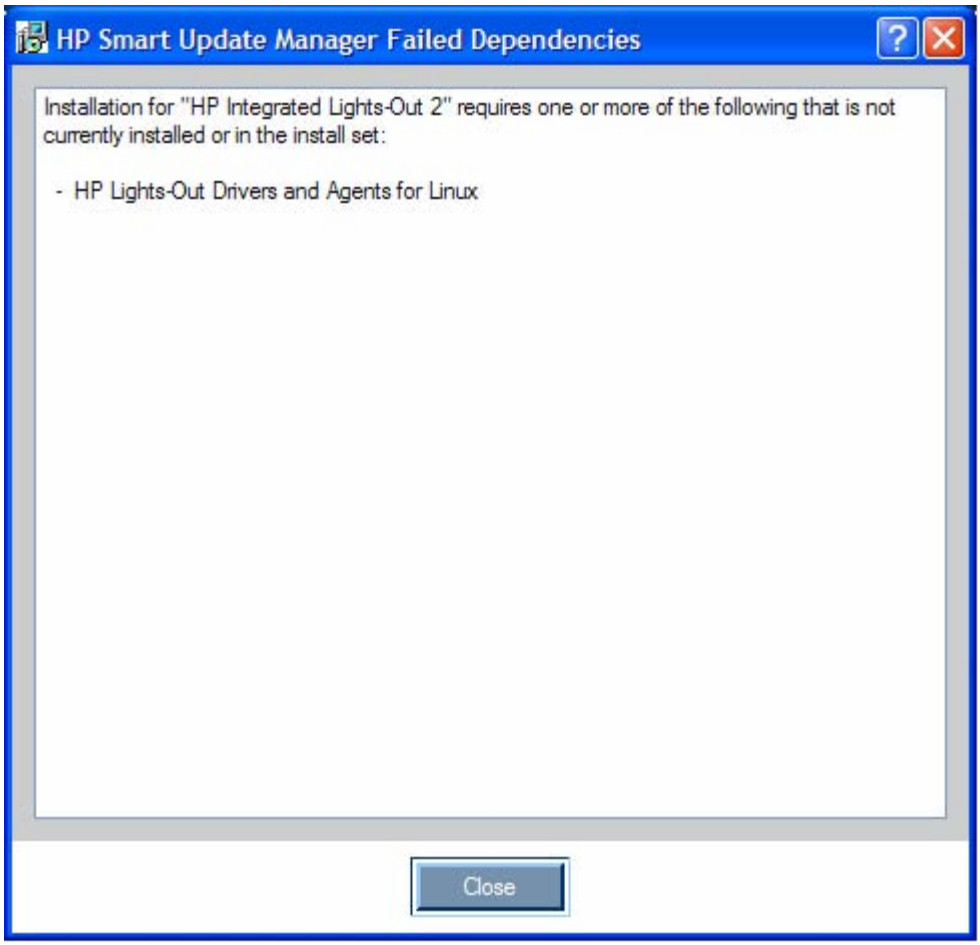
The component selection pane is divided into the following columns:

- Product—Specifies the name of the component, version number, and new component version number. To view the component version history, click the new version number.
- Status—Displays the status of the component.

Icon	Text	Description
	Ready for installation	The component is ready for installation.
	Not selected for installation	The component has not been selected for installation.
	Already up-to-date	The component is already up-to-date. To downgrade or rewrite a component, click **Installation Options.**
	No device driver installed	The firmware devices supported by the components in this section are detected on the system but require a device driver. Install the device driver.
	Deselected by user	The component has not been selected for installation.
	Failed dependencies	The component has a dependency that has not been met. To determine the nature of the failed dependency, click **View Failed Dependencies.**

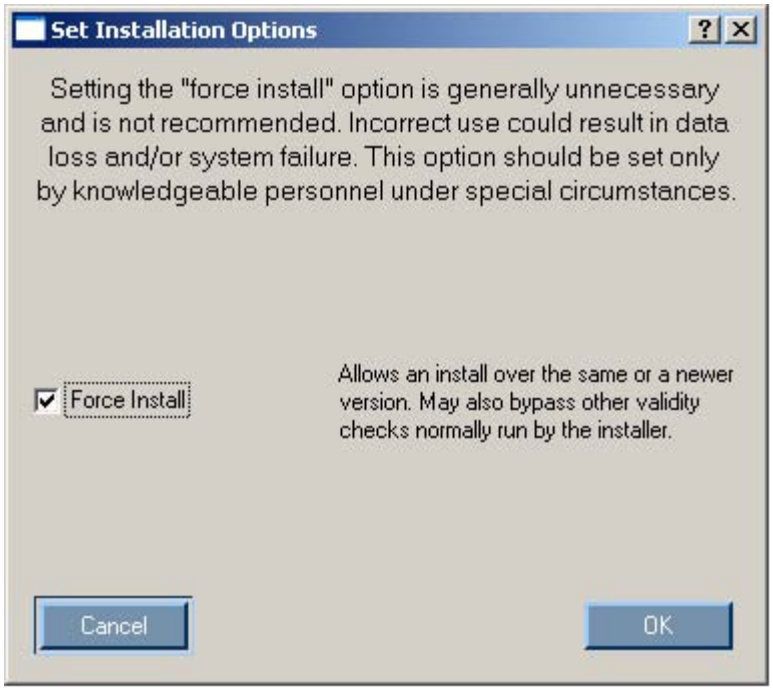
- Optional Actions—Reserved for future use.
- Additional—Contains the installation options and additional information for the components.

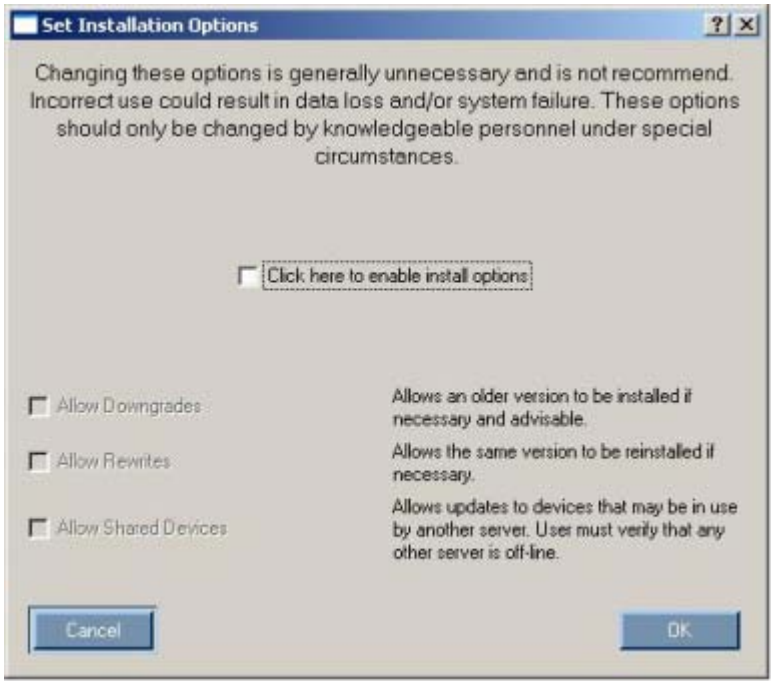
If a failed dependency occurs, you must resolve it before proceeding with the installation. Depending on the issue, you must locate software or firmware components in the Firmware Maintenance CD or HP website (http://www.hp.com). The following figure shows the Failed Dependencies screen.



Installation options

You can specify firmware upgrade behavior for installable components by selecting one or more options from the Additional Options field. Depending on the component type, one of the following screens appears. The first screen applies to firmware and software components and the second screen applies only to firmware.





△ **CAUTION:** Updating the firmware while a shared device is in use can lead to data loss. Before enabling the **Allow Shared Devices** option, be sure any other servers sharing the selected devices are offline.

- Select **Allow Downgrades** to downgrade the current firmware to an older version.

- Select **Allow Rewrites** to enable HP Smart Update Manager to overwrite the current firmware version with the same version.
- Select **Allow Shared Devices** to upgrade firmware in a shared storage environment.

NOTE: HP Smart Update Manager does not support Allow Downgrades or Allow Rewrites for the HP Virtual Connect Ethernet and Fibre Channel Modules for c-Class BladeSystem firmware component.

The following table illustrates how changing the options for firmware upgrade behavior can change the firmware upgrade results. In this example, the array controller is assumed to be an HP Smart Array 6402 controller.

If the existing array controller has firmware version 3.00 installed, then updating the firmware produces results as described in the following table.

	Default	**Allow downgrades**	**Allow rewrites**
Firmware upgrade v3.05	3.05	3.05	3.05
Firmware upgrade v3.10	3.10	3.10	3.10

If the existing array controller has firmware version 3.10 installed, then updating the firmware produces results as described in the following table.

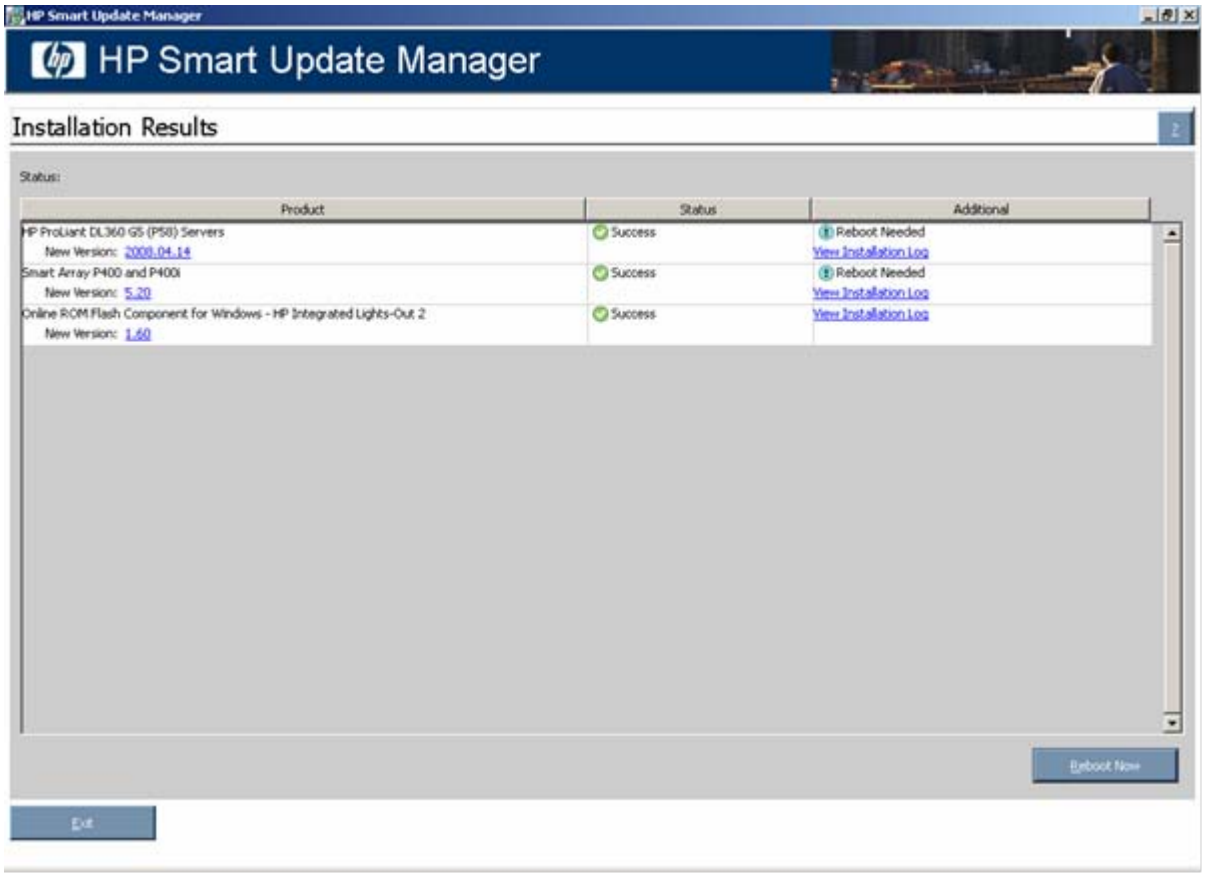
	Default	**Allow downgrades**	**Allow rewrites**
Firmware upgrade v3.05	No change	3.05	3.10
Firmware upgrade v3.10	No change	No change	3.10

NOTE: When updating installation for NIC components, select the devices to be updated in the window that appears.

After you have selected all the components that you want to install, click **Install** to proceed with the installation. The Installation Progress screen appears.

Viewing the installation results

When the installation is complete, the Installation Results screen appears.



The Installation Results screen is divided into the following columns:

- Product—Specifies the name of the installed component. To see the component version history, click the version number.
- Status—Specifies the installation status of the component.

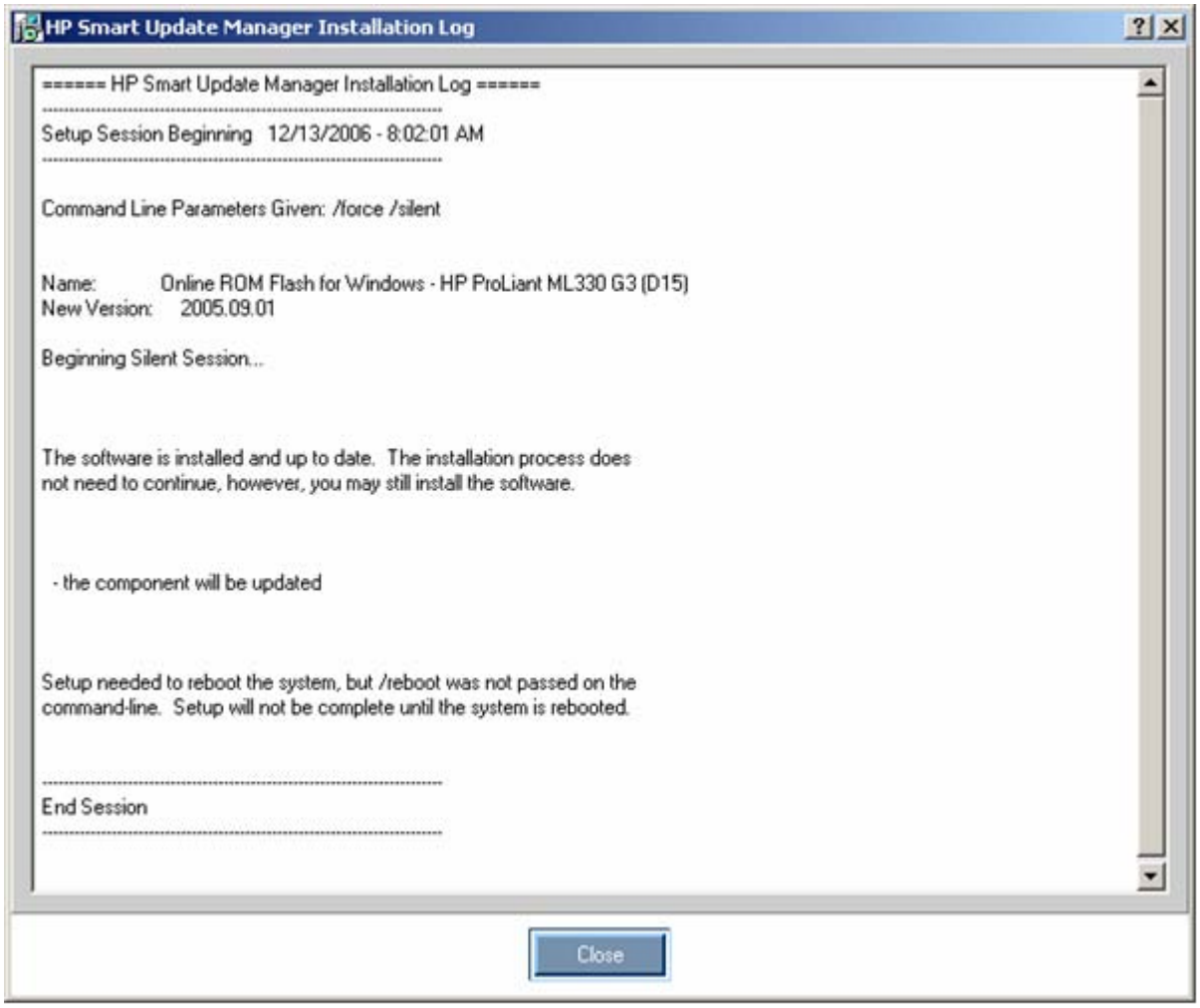
The following icons may appear in the Status column.

Icon	Text	Description
	Success	The component was installed successfully.
	Same/older version successfully installed	The existing component was successfully downgraded or reflashed to the same or older version.
	Update returned an error	An update error has occurred. See the HP Smart Update Manager log file for details.
	Installation failed	The component was not installed. To see additional details, click **View Installation Log**.

- Additional—Enables you to view the installation log for each component and reminds you if a reboot is needed.

Icon	Text	Description
	Reboot Needed	The server must be rebooted for the component to take effect.

To see additional details, click **View Installation Log.**



The Installation Results screen also includes the following buttons:

- Reboot Now—Reboots the server. (This button is available for local installations only.)
- Exit—Exits the HP Smart Update Manager.

NOTE: After updating hard drives in external enclosures such as MSA20, you must power cycle the external enclosures. The Reboot button in HP Smart Update Manager only reboots the server but never power cycles an external enclosure.

There are installation logs named hpsum_log.txt and hpsum_detail_log.txt, which contain information about the installation activity for each host being updated. The hpsum_log.txt log contains a brief summary of the installation activity. The hpsum_detail_log.txt log contains all of the installation details, including errors, for each component installed.

The log files can be found in the following locations:

- For Windows® operating systems, these files are located in subdirectories named according to the IP address of each host in the \CPQSYSTEM\hp\log subdirectory on the boot partition of the local host. The directory containing the local host information is named localhost instead of being named after the IP address.

- For Linux operating systems, these files are located in subdirectories named according to the IP address of each host in the /var/hp/log subdirectory of the local host. The directory containing the local host information is named localhost instead of being named after the IP address.

There is a new file that contains detailed information on the execution of HP Smart Update Manager.

- For Windows® operating systems, the filename is C:\cpqsystem\hp\log\hpsum_execution_log_<date>_<time>.log.
- For Linux operating systems, the filename is /var/hp/log/hpsum_execution_log_<date>_<time>.log.

> **NOTE:** Using the offline environments provided by the Firmware Maintenance CD and HP BladeSystem Firmware Deployment Tool results in the log files being written to the Linux location.

HP Smart Update Manager also creates trace logs of its installation that can be used to debug problems. These trace files are located in the following places:

- For Windows Server® 2003/XP/Vista, %TEMP%\hp_sum\.
- For Windows Server® 2008, %TEMP%\<number>\hp_sum. Normally, the <number> is 1.
- For Linux, /tmp/hp_sum.

HP Smart Update Manager creates a separate trace log for each target server. These are captured in subdirectories under the trace log directories. The directories start with Target_0, Target_1, and so forth. These contain the target specific trace information. No passwords or sensitive data is stored in this trace logs.

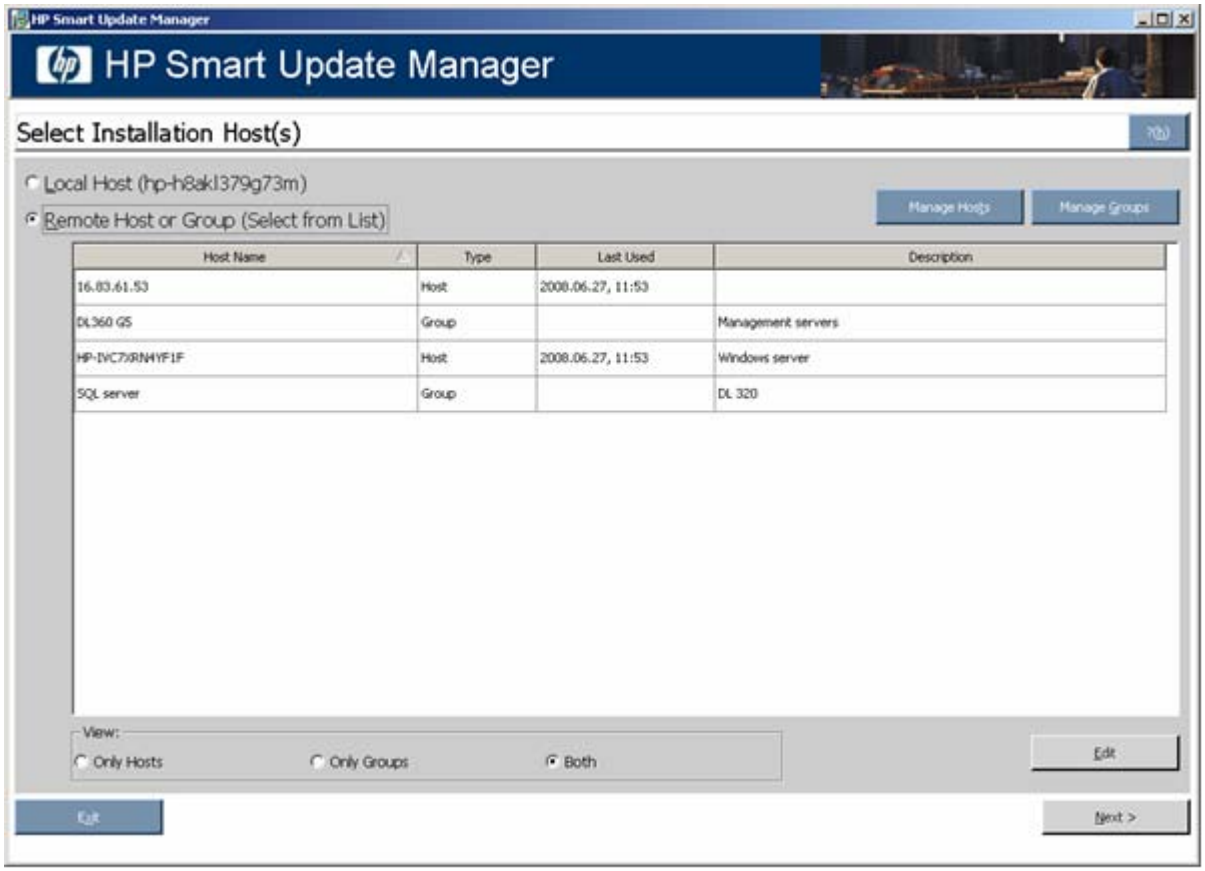
Multiple-host installations using the GUI

HP Smart Update Manager provides an easy-to-use graphical interface that enables you to deploy and maintain firmware components. To access HP Smart Update Manager, see "Deployment options (on page 8)." After you start HP Smart Update Manager, the Source Selection screen ("Selecting the location to check for updates" on page 17) appears which allow you to specify where the components that you want to deploy can be found. After selecting the where the components can be found, the Inventory Progress screen appears while HP Smart Update Manager builds an inventory of available updates. When the inventory process is complete, the Select Installation Host(s) screen appears.

Selecting remote hosts or groups

The Select Installation Host(s) screen enables you to choose multiple hosts and groups for component installation. A remote host can be the IP address or DNS name of a remote server, remote iLO NIC port, Virtual Connect Ethernet or Fibre Channel Module for c-Class BladeSystem, or BladeSystem Onboard Administrator.

> **NOTE:** Local hosts cannot be included in a list with remote hosts or in a group. When selecting an iLO or iLO2 as a host, only the iLO firmware can be updated. The server host must also be selected to update all other firmware and software components on the same physical server. The iLO firmware can be updated by either selecting the iLO or the server host.



To add hosts, see "Managing hosts (on page 33)." To add groups, see "Managing groups (on page 37)."

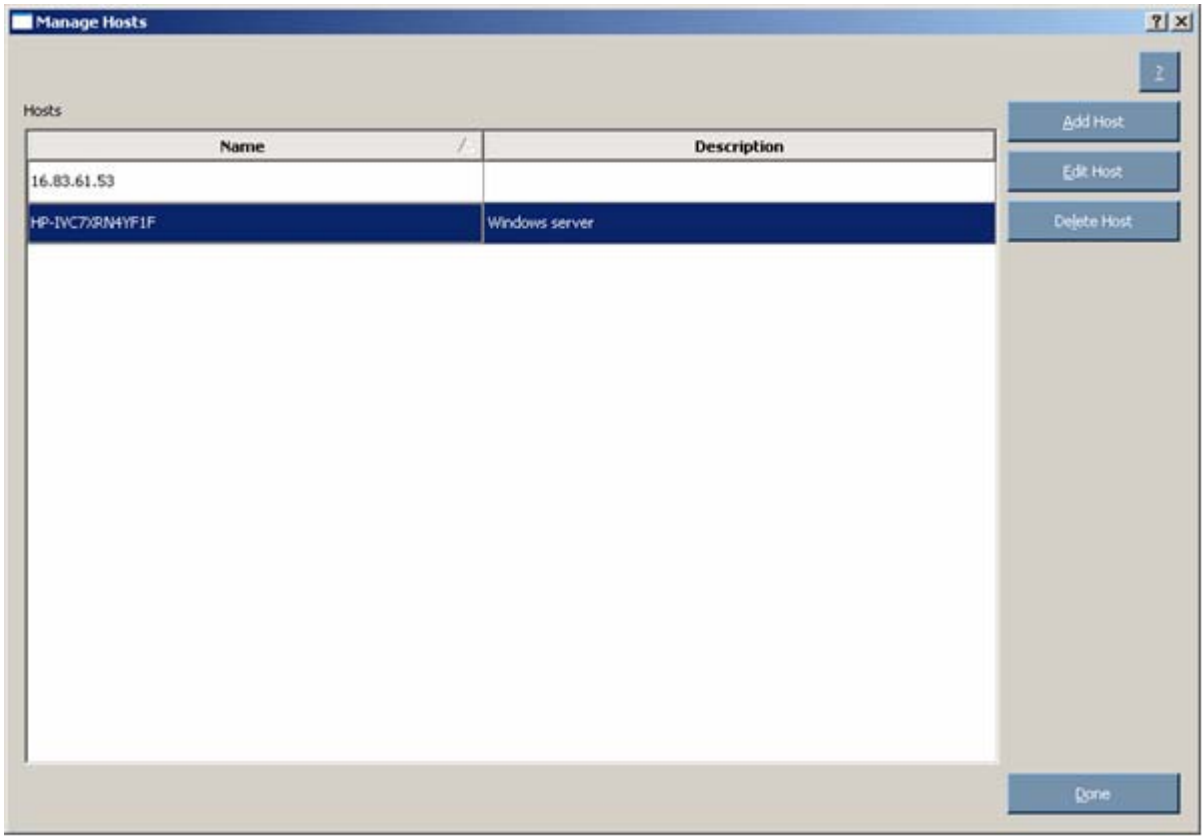
To continue with the deployment process:

1. Select one or more hosts or groups.
2. To continue, click **Next.**
3. Enter the credentials for the host ("Entering credentials for hosts" on page 40).
4. Click **OK** to proceed, as described in Selecting components to install on multiple hosts (on page 42).
5. When the installation is complete, the Installations results for multiple hosts screen ("Viewing the installation results for multiple hosts" on page 44) appears.

Managing hosts

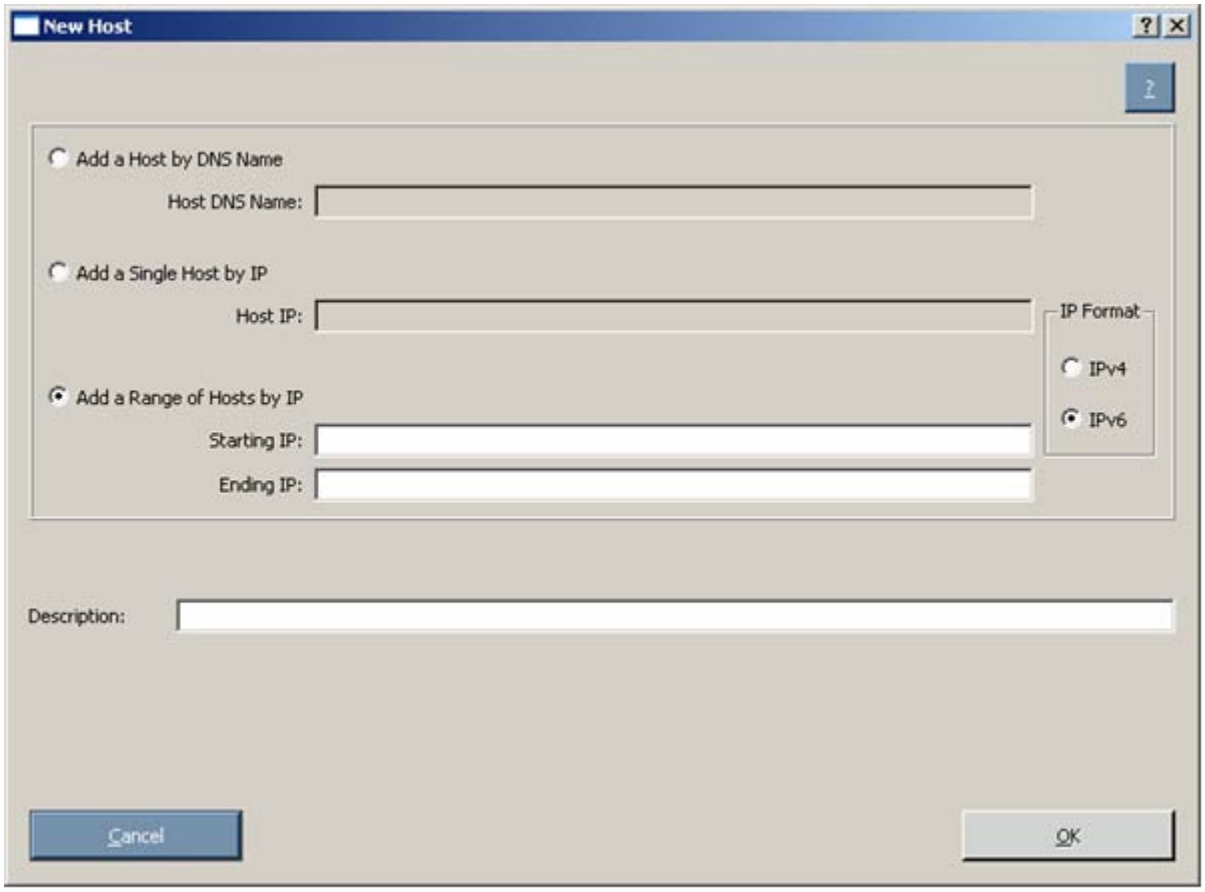
To add, edit, or delete hosts, click the **Manage Hosts** button. The Manage Hosts screen appears. A remote host can be the IP address or DNS name of a remote server, remote iLO NIC port, Virtual Connect Ethernet or Fibre Channel Module for c-Class BladeSystem, or BladeSystem Onboard Administrator.

NOTE: Local hosts cannot be included in a list with remote hosts or in a group. When selecting an iLO or iLO2 as a host, only the iLO firmware can be updated. The server host must be selected to update all other firmware and software components. The iLO firmware can be updated by either selecting the iLO or the server host.


Manage Hosts
?
Hosts
Name
Description
16.83.61.53
HP-IVC7\RN4YF1F
Windows server
Add Host
Edit Host
Delete Host
Done

To add a host:

1. Click **Add Host.** The New Host dialog box appears.



2. Select the method to add a host from the following:
   - Enter the DNS name of the host you want to add.
   - Enter the IP address of the host you want to add.
   - Enter the IP address range of the hosts you want to add. The starting and ending IP addresses must both be on the same subnet. When using the IPv6 format, the last field in the ending address is limited to 32 targets.

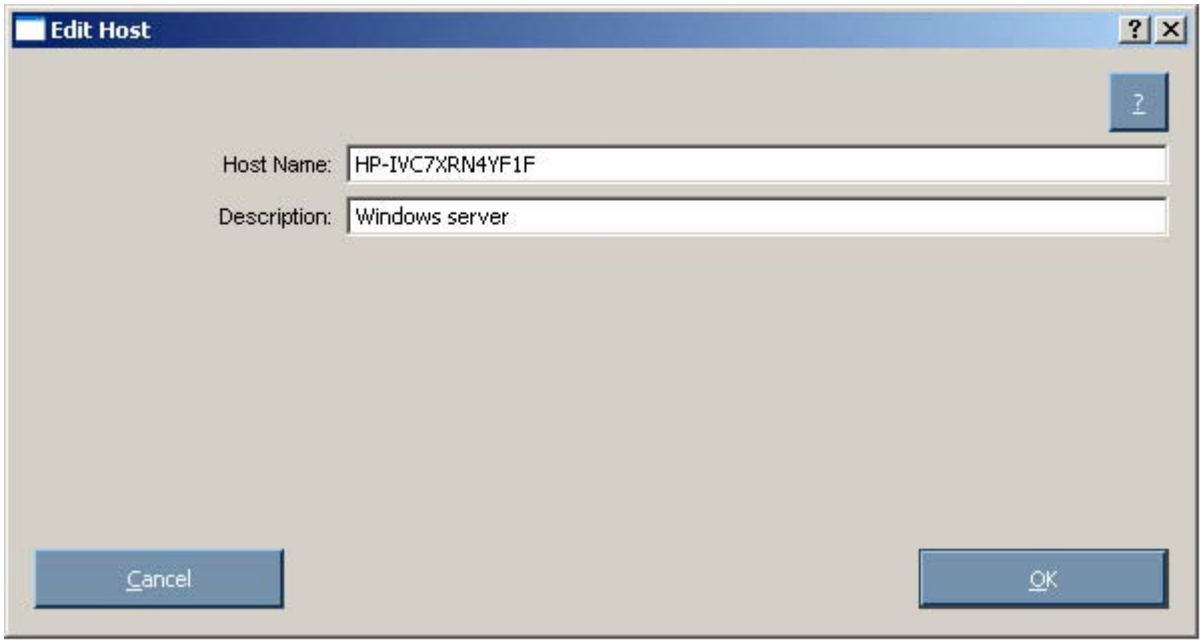
     NOTE: When adding hosts using either IP address option, you can select from the IP format options: IPv4 or IPv6. The IPv4 format is the default option since it is the current Internet protocol. The IPv6 format is the next generation Internet protocol.

3. Enter an optional user-defined description given to the host you want to add.
4. Click **OK.**

The new host is added to the list on the Select Installation Host(s) screen.

To edit an existing host:

1. On the Manage Hosts screen, click the **Edit Host** button. The Edit Host dialog box appears.



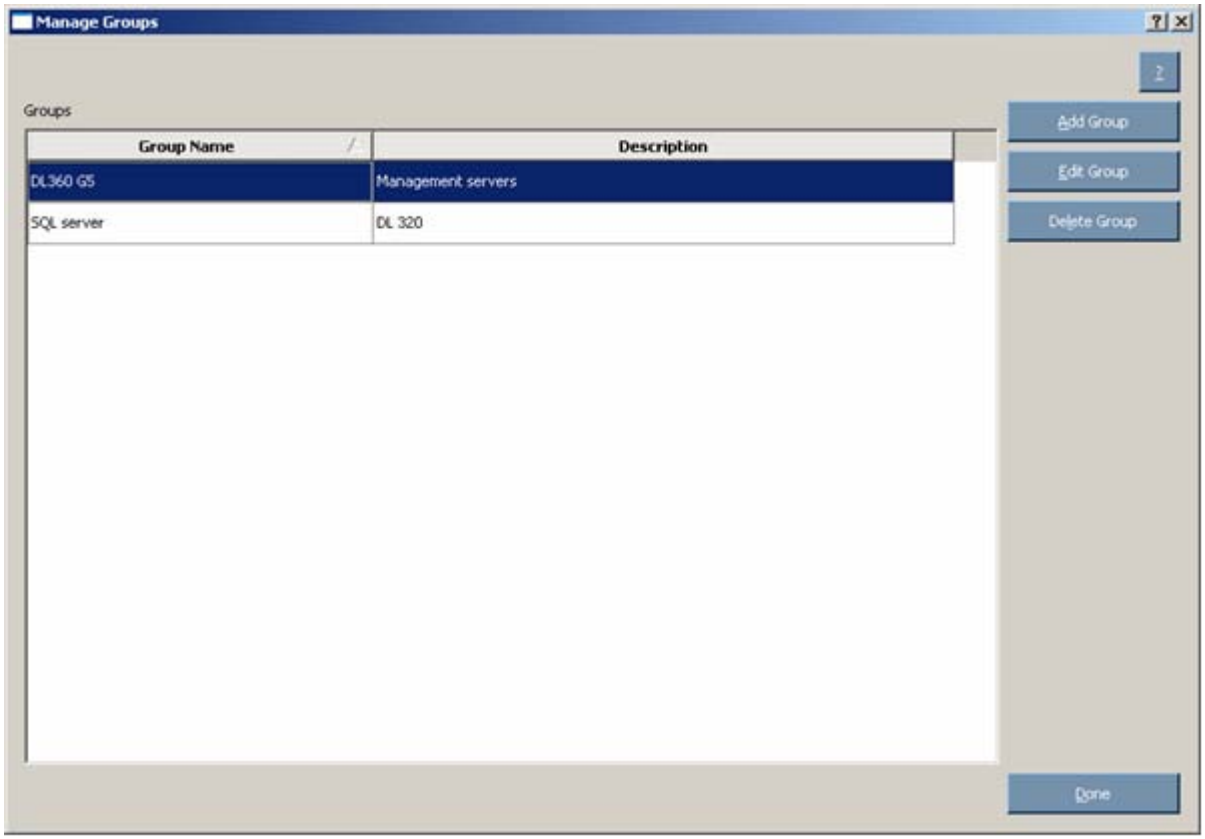
2. Edit the Host Name and Description.
3. Click **OK.**

To delete a host:

1. On the Manage Hosts screen, click the **Delete Host** button.
2. When the confirmation screen appears, click **Yes.**

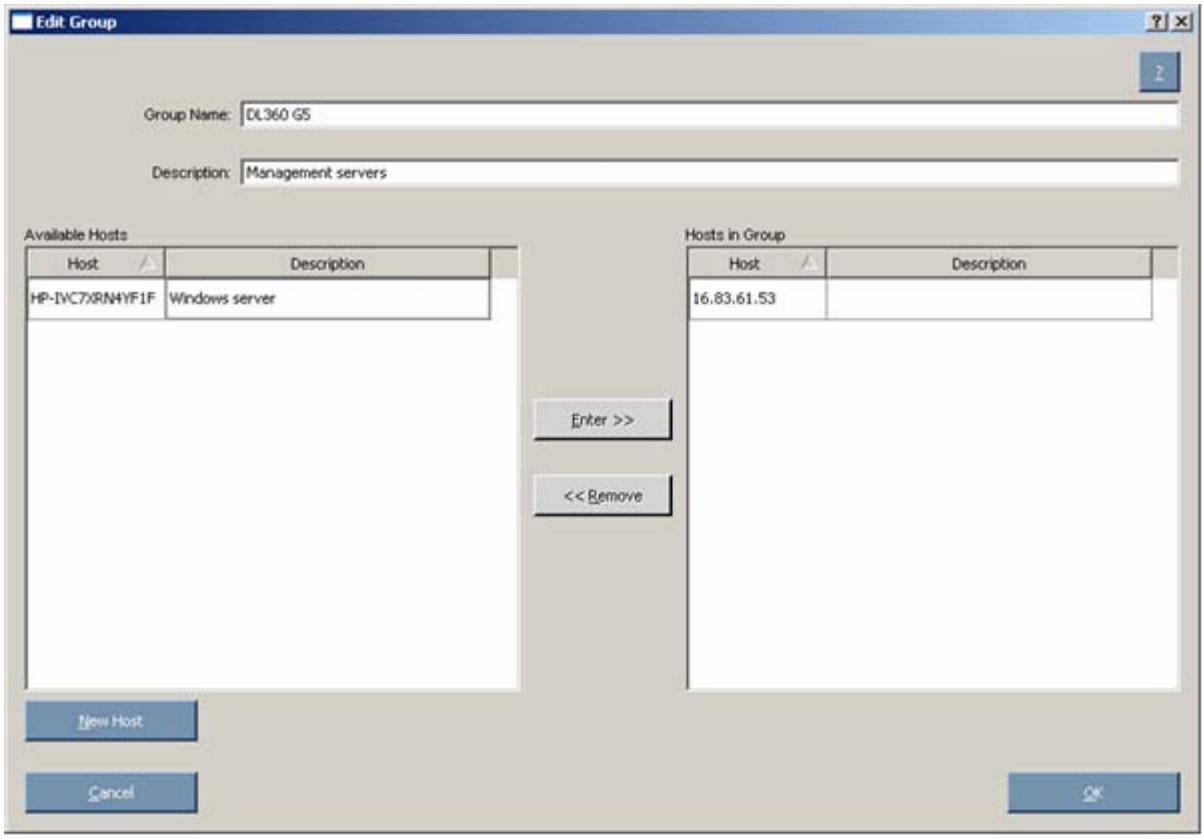
Managing groups

To add, edit, or delete groups, click the **Manage Groups** button. The Manage Groups screen appears.



To add a group:

1. Click **Add Group.** The Edit Group dialog box appears.

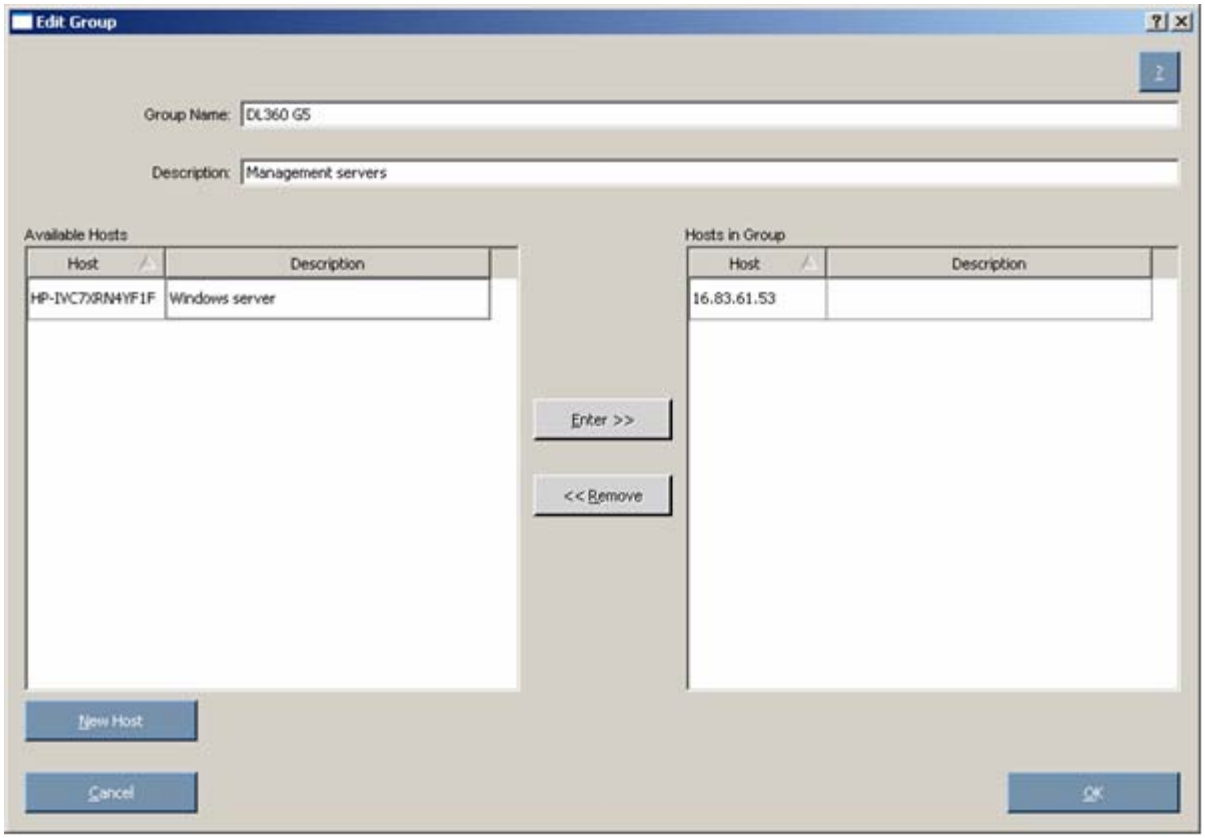


2. Enter a group name.
3. Enter an optional user-defined description given to the group to be added.
4. Select the hosts to be added to the group from the Available Hosts pane. You can add new hosts from this screen by clicking the **New Host** button. For more information on adding hosts, see "Managing hosts (on page 33)."
5. Click the **Enter** button to move the selected hosts to the new group.
6. Click **OK.**

The new group is added to the list on the Select Installation Host(s) screen.

To edit an existing group:

1. Select the group, and then on the Manage Groups screen, click the **Edit Group** button. The Edit Group dialog box appears.



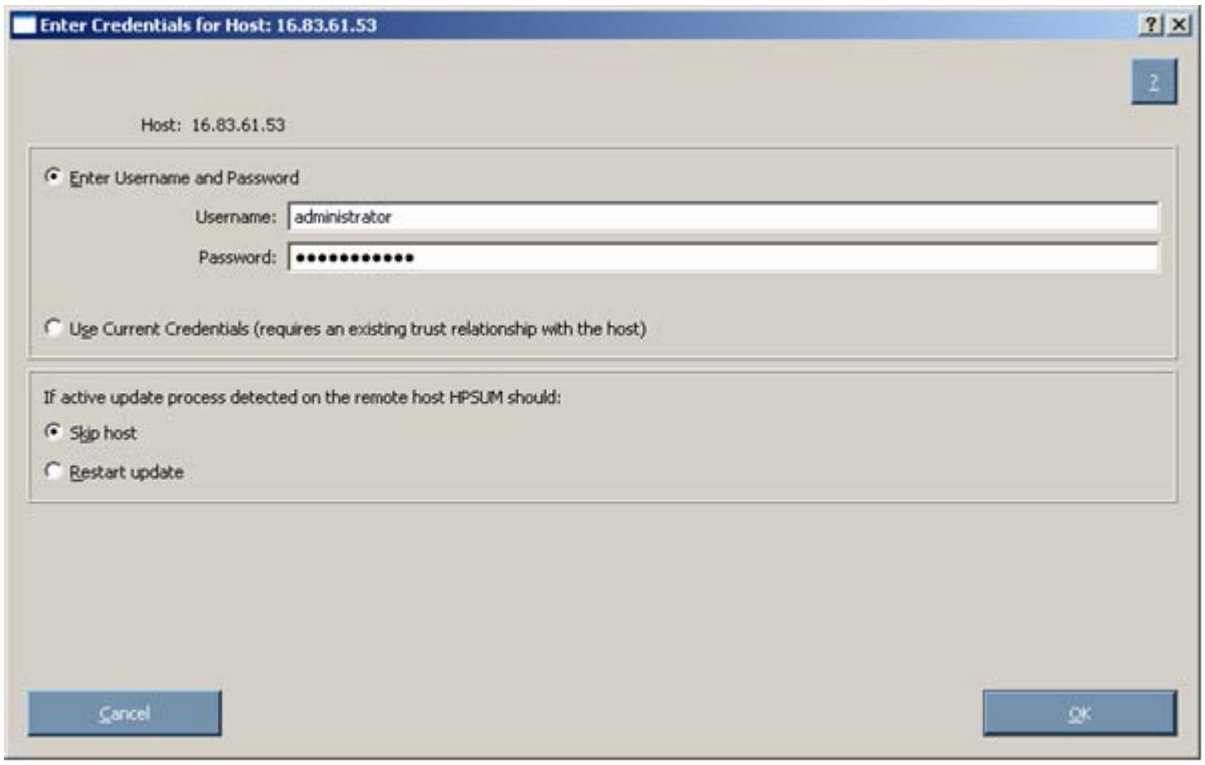
2. Edit the group name as needed.
3. Edit the optional user-defined description given to the host as needed.
4. Click the **Enter** and **Remove** buttons to add or remove hosts as needed.
5. Click **OK.**

To delete a group:

1. Select the group on the Manage Groups screen, and then click the **Delete Group** button.
2. When the confirmation screen appears, click **Yes.**

Entering credentials for hosts

When you select a single remote host, the Enter Credentials for Host screen appears. You must enter your username and password as the credentials for the host.



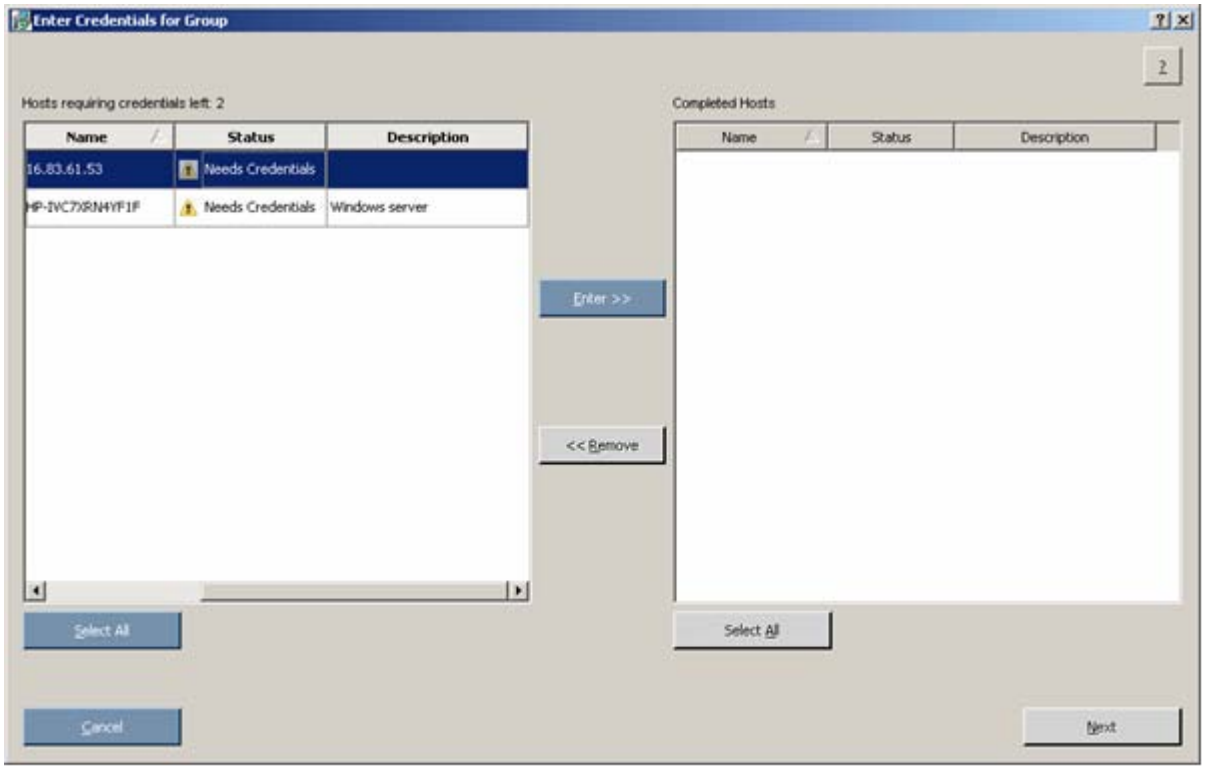
To enter the credentials for the host, choose one of the following:

- Select **Enter Username and Password**, and then enter the username and password.
- Select **Use Current Credentials** to use the currently logged-in user's credentials.

If an active update process is detected on the remote host, you can select **Skip host** or **Restart update.** Skip host causes the host to be ignored for the rest of the update process, and Restart update causes any existing or in-progress installation to be terminated.

To continue, click **OK.**

When you select a group or multiple hosts, the Enter Credentials for Group screen appears.



The screen separates the remaining hosts that still require credentials from the completed hosts.

Each pane is divided into the following columns:

- Name—Specifies the name of the host.
- Status—Specifies the credentials status of the host.

Icon	Text	Description
	Entered	The credentials for the host have been entered.
	Needs Credentials	The credentials for the host have not been entered.
	Credentials Failed	The credentials entered for the host have failed.
	Unable to access host	The host cannot be accessed using the credentials entered, or the host cannot be found on the network.
	Host Skipped Due to Existing HPSUM Session	The host is skipped due to an existing HP Smart Update Manager session. The skipped hosts can be accessed if the appropriate CLI switch is used or if **Restart Update** is selected on the Enter credentials for host screen.

- Description—Displays the user-defined description given to the host.

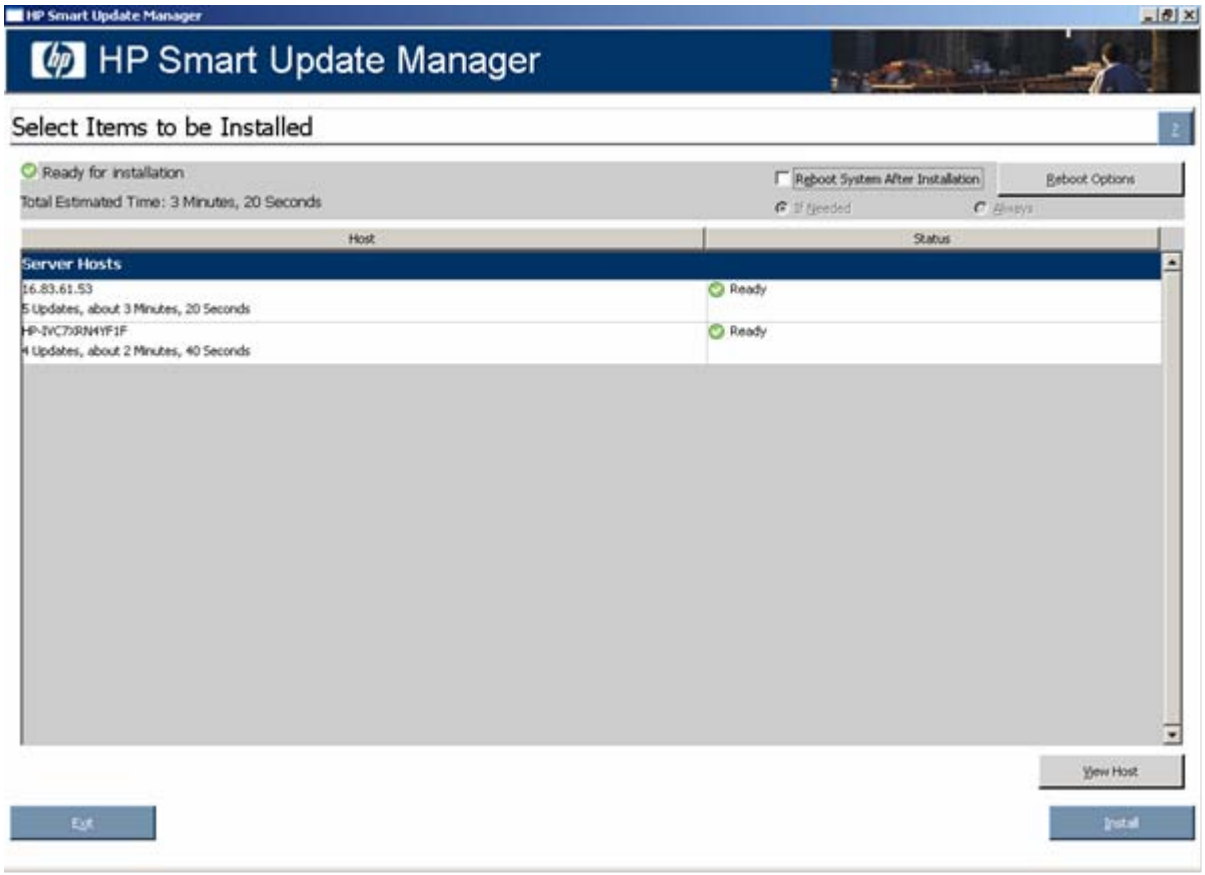
To enter the credentials for the host:

1. In the left pane, select the host from the list of hosts requiring credentials. If all credentials are the same, to select all the hosts on the list, click **Select All.**
2. To enter the required credentials and move the selected host to the Completed Hosts pane, click the **Enter** button.
3. To continue, click **Next.**

NOTE: If a TPM is detected and enabled, an HP Smart Update Manager pop-up warning message appears after the Discovery Progress screen. You must read the message and determine how to proceed. For more information, see Trusted Platform Module (on page 11).

Selecting components to install on multiple hosts

The Select Items to be Installed screen displays the server hosts and their status information.



The Select Items to be Installed screen includes the following buttons:

- View Host—Enables you to view additional information about a host after you select it.
- Install—Installs all selected components on all remote hosts. The Install button is grayed out when a dependency failure occurs.
- Exit—Exits HP Smart Update Manager.

The server host pane of the Select Items to be Installed screen displays summary information for the server hosts available for installation and features a drilldown of individual hosts.

The server host pane is divided into the following columns:

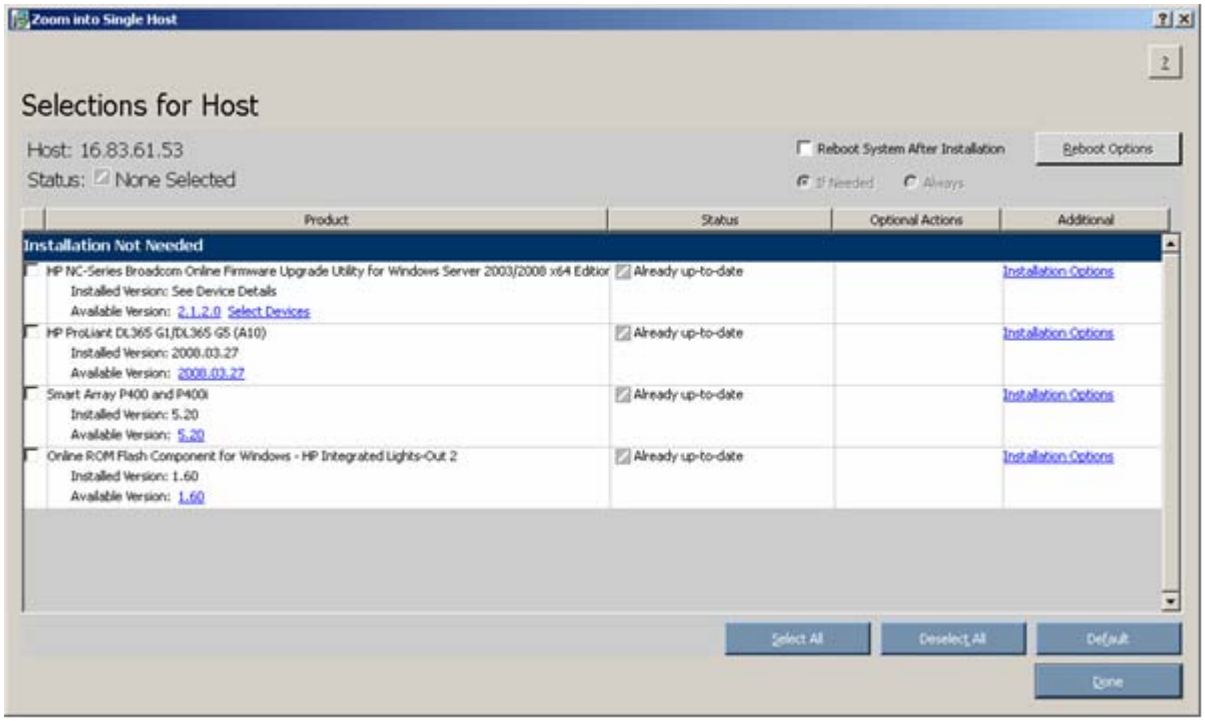
- Host—Specifies the name of the system, number of updates available, and the estimated time for the installation.
- Status—Specifies the status of the host.

Icon	Text	Description
	Ready	The host is ready for installation.

Icon	Text	Description
	Nothing to Install	The host is already up-to-date.
	Host Skipped Due to Existing HPSUM Session	The host is skipped due to an existing HP Smart Update Manager session.
	Action Required	The host is not ready for installation. Click **View Host** for additional information.
	Discovery Failed	The host is not ready for installation. The detection of installed hardware, software, and firmware has failed.

NOTE: The default reboot behavior after updates are installed might also appear in the Status column.

To zoom in to single host selections, click **View Host** on the Select Items to be Installed screen. The Selections for Single Host screen appears.

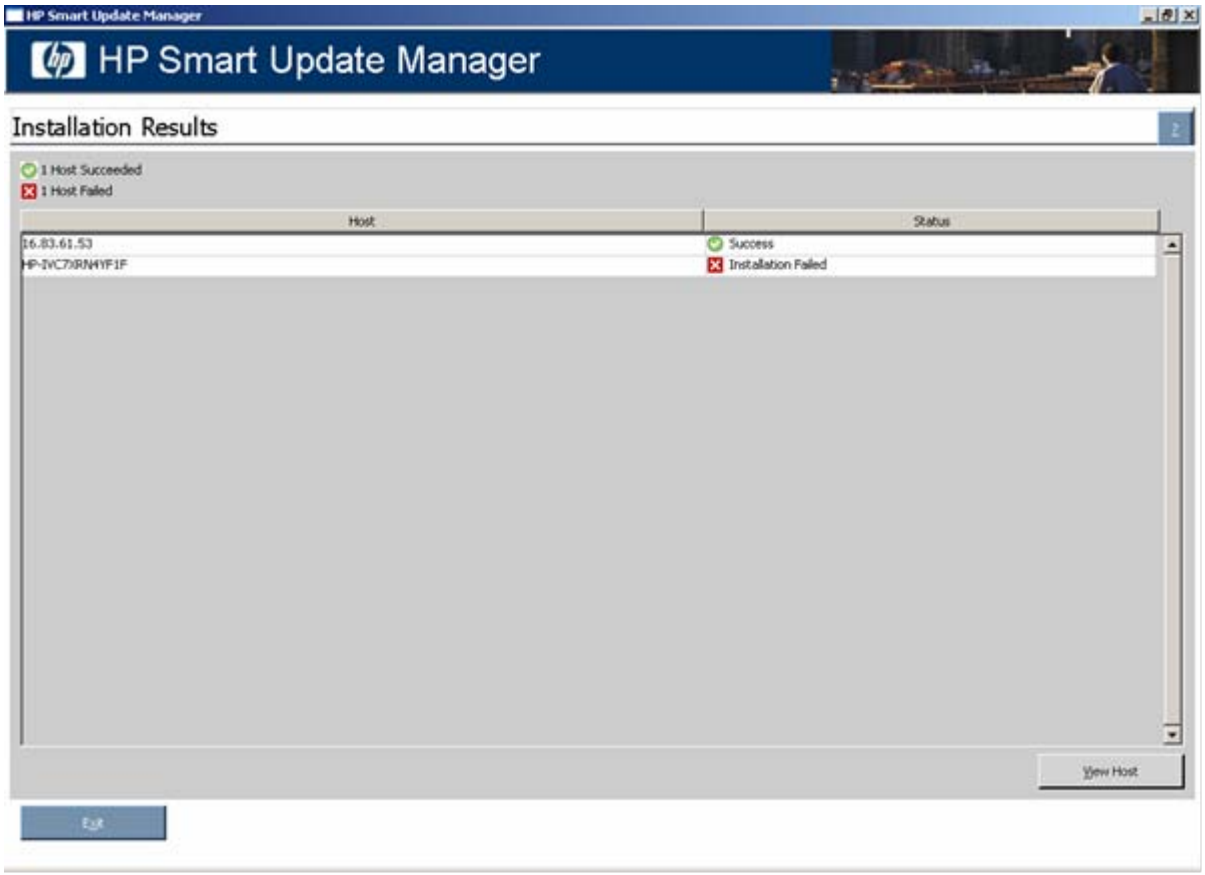


To set single-host selections, proceed as described in "Selecting Components to Install (on page 22)."

After setting the single-host selections for all hosts to be updated, on the Select Items to be Installed screen, to proceed with the installation, click **Install**.

Viewing the installation results for multiple hosts

When the installation is complete, the Installation Results screen appears.



The Installation Results screen is divided into the following columns:

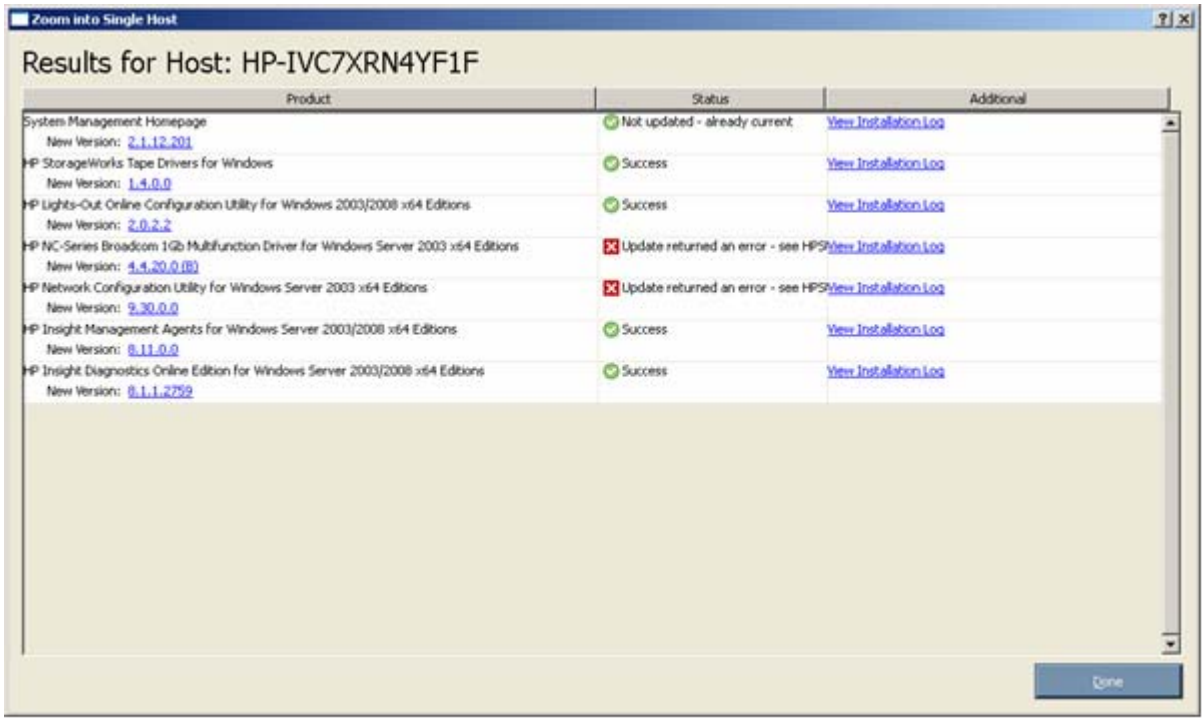
- Host—Specifies the IP address or DNS name of the host.
- Status—Specifies the overall installation status of the components on the remote host.

Icon	Text	Description
	Success	The host was updated successfully.
	Nothing to install	The host is already up-to-date.
	Installation canceled by user	The installation was canceled and cannot continue the process.
	Installation failed	One or more of the component installations have failed.

The Installation Results screen also includes the following buttons:

- View Host—Enables you to view the installation results for the selected host.
- Exit—Exits HP Smart Update Manager.

To view single-host installation results, double-click the host or select the host, and click **View Host.**



Proceed as described in "Viewing the installation results (on page 30)."

Scripted deployment

Command line interface

The HP Smart Update Manager command line interface enables you to script custom installations.

Command line syntax

The general command line syntax for HP Smart Update Manager is:

```
hpsum [/h[elp]] [/?] [/f[orce]] [/f[orce]:bundle] [/f[orce]:rom]
[/f[orce]:software] [/f[orce]:all ] [/g (/downgrade)] [/e (/rewrite)]
[/m[utual])] [/r[eboot]] [/reboot_message "reboot message"]
[/reboot_delay timeout_in_seconds] [/reboot_always] [/s[ilent]]
[/c[omponent] <component_to_install>] [/group "group_name"]
[/b[undle] <bundle_to_install>] [/allow_update_to_bundle]
[/allow_non_bundle_components] [/use_latest] [/use_location
"file_share"] [/use_web] [/use_d[ownloaded]] [/tpmbypass] [/ignore_tpm]
[/use_snmp] [/use_wmi] [/romonly] [/softwareonly] [/dryrun]
[/continue_on_error <error>] [/override_existing_connection]
[/express_install] [/user <username> or /username <username>] [/passwd
<password>] [/current_credential] [/target "netAddress"] [/logdir
"path"] [<component1_to_install> <component2_to_install> ...]
[<bundle1_to_install> <bundle2_to_install> ...]  [/v[erbose]]
[/veryv[erbose]]  [/report] [/inventory_report] [/inputfile "filename"]
```

The HP Smart Update Manager with Onboard Administrator requires a user ID and password to log in. The user ID must be an Administrator equivalent ID and not an operator or user equivalent level ID.

> **NOTE:** All arguments and information enclosed in brackets are optional. The arguments may be prefixed with either a '-' or '/' character. These examples show only the '/'.

On Windows® operating systems, use a slash (/) before each argument. On Linux operating systems, use a hyphen (-) before each argument.

If no command line arguments are executed on the command line, the component GUI appears.

> **NOTE:** Command line syntax does not support double-byte character sets. Any messages entered through the command line using a double-byte character set will not be displayed correctly.

Command line arguments

HP Smart Update Manager recognizes the following command line arguments. These arguments prepopulate the GUI in the Select Items to be Installed screen. If you specify the host or group, the Select Items to be Installed screen does not appear.

You cannot use some arguments such as `/romonly` and `/softwareonly` together.

Command line argument	Description
`/h[elp] or /?`	This argument displays command line Help information.
`/f[orce]`	This argument enables you to override or downgrade an existing component installation. This argument produces the same results as `/f:software`.
`/f[orce]:bundle`	This argument enables you to override or downgrade the existing installation of components in the selected bundle.
`/f[orce]:rom`	This argument enables you to override or downgrade the existing installation of the selected firmware components. (Applies to firmware only.)
`/f[orce]:software`	This argument enables you to override or downgrade the existing installation of the selected software components.
`/f[orce]:all`	This argument enables you to override or downgrade the existing installation of the selected software components, firmware components, and bundles.
`/g or /downgrade`	This argument enables you to downgrade to an earlier version of firmware for multi-target devices such as hard drives and array controllers. (Applies to firmware only.)
`/e or /rewrite`	This argument enables you to rewrite the same version of firmware only for multi-target devices such as hard drives and array controllers. (Applies to firmware only.)
`/m[utual]`	If the device you want to flash is in a shared storage environment, then this argument informs the firmware flash engine to flash the firmware. If the device to be flashed is in a shared storage environment, and the `/m` option is not passed, then the component installation fails. (Applies to firmware only.)
`/r[eboot]`	If the following conditions are met, then this argument causes the server (or host server in a remote installation) to reboot: • The `/reboot` option is selected or given as a command line argument. • All components selected for installation are successfully installed. • At least one of the installed components requires a reboot to complete its installation.
`/reboot_message` *"reboot message"*	This argument displays the specified reboot message on remote consoles connected to the server you want to reboot. You must use this argument with the `/reboot` option, or the argument is ignored.
`/reboot_delay` *timeout_in_seconds*	This argument delays the reboot of the server for the length of time specified by the *timeout_in_seconds* variable. You must use this argument with the `/reboot` option, or the argument is ignored. Acceptable values are between 15 and 3600. The default timeout value is 15 seconds for Microsoft® Windows® and 60 seconds for Linux. In Linux, the Reboot Delay time is converted from seconds to minutes. For Linux, any value under a full minute, 59 seconds or less, rounds to the next minute.
`/reboot_always`	If the following conditions are met, then this argument forces the server to reboot: • The `/reboot_always` option is selected or given as a command line argument. • All components selected for installation are successfully installed.

Command line argument	Description
/s[ilent]	This argument causes the installation to run silently with no GUI or console output. All data writes to the log file. Any generated prompts use the default option and continue the installation without user input. If a component requires input before installation (such as configuration information), then the component installation fails, and an error message writes to the log file. Failed dependencies are not reported to the user when using the /s[ilent] argument. To check for failed dependencies, remove the /s[ilent] argument, reissue the command line, and then the HP Smart Update Manager GUI appears.
/c[omponent] *<component to install>* or *<component1_to_install>* *<component2_to_install>*	This argument specifies the components to install. Components to install can be specified with or without the /c[omponent] argument. If using the /c[omponent] argument, only one component can be specified with the argument. However, multiple /c arguments and components can be specified on the same line. If the /c[omponent] argument is not used, multiple components can be specified at the same time, but the components must be separated by a blank and listed after all the arguments on the command line. The components are installed in the order provided unless dependencies between components require installation in a different order. If so, the utility changes the installation order based on the component dependencies to ensure the successful installation of as many components as possible. Multiple components and bundles can be specified on the same command line. When mixing components and bundles on the command line, the filter switches control what components and bundles are installed.
/group *"group_name"*	This argument specifies an already defined group name in the HP Smart Update Manager GUI.
/b[undle] *<bundlename>* or *<bundle1_to_install>* *<bundle2_to_install>*	This argument specifies the bundles to install. Bundles to install can be specified with or without the /b[undle] argument. If using the /b[undle] argument, only one bundle can be specified with the argument. However, multiple /b arguments and bundles can be specified on the same line. If the /b[undle] argument is not used, multiple bundles can be specified at the same time, but the bundles need to be separated by a blank and listed after all the arguments on the command line. Multiple components and bundles can be specified on the same command line. When mixing components and bundles on the command line, the filter switches control what components and bundles are installed.
/allow_update_to_bundle	This argument is a filter switch and enables the user to install newer versions of components defined in a PSP or firmware bundle. This argument enables these components to replace the older versions of the same component that might have shipped with the bundles.
/allow_non_bundle_components	This argument is a filter switch and enables the user to install components that are not included in the bundle but reside in the directory with the components in the bundle.
/use_latest	This argument is a filter switch for use with bundles. The argument enables you to use the latest version of the bundle when multiple versions of bundles are listed on the command line. If there are no bundles specified on the command line, and multiple bundles are in the directory, the /use_latest argument allows HP Smart Update Manager to use the bundle with the latest version for installation.
/use_location *"file_share"*	This argument specifies a directory or file share that contains the PSP and components for use with HP Smart Update Manager. The "file_share" format

Command line argument	Description
	must be a mapped file share and not in Universal Naming Convention (UNC) format. If you do not specify this argument, the directory containing hpsum.exe or HP Smart Update Manager is used by default. This populates the Directory box on the Source Selection screen. The logged-in account must have access to this location. The `/user` and `/passwd` arguments do not have any effect when attempting to access the file share. You can use those arguments only when connecting to a target system.
`/use_web`	This argument specifies that the check box for Check ftp.hp.com on the Source Selection screen is to be selected. This allows components to be retrieved from hp.com and to be used in the list of possible updates.
`/use_d[ownloaded]`	This argument specifies that the check box for Include components previously downloaded from HP.com on the Source Selection screen is to be selected. This allows those previously downloaded components to be included in the list of possible updates.
`/tpmbypass` or `/ignore_tpm`	These arguments specify that if a TPM is enabled, the warning message must be ignored and component installation is allowed to continue.
`/use_snmp`	This argument specifies that components, which use SNMP protocol, are available to be selected for installation. These components are available for selection by default. When the `/use_snmp` argument is used, and the `/use_wmi` argument is not, the WMI components are optional.
`/use_wmi`	This argument specifies that components, which use WMI protocol, are available to be selected for installation. These components are optional by default and will not be installed unless this argument is used. When the `/use_wmi` argument is used, and the `/use_snmp` argument is not, the SNMP components are optional.
`/romonly`	This argument is a filter switch and enables the user to see only the firmware components needed for installation. When using this filter switch, you must exit, and then restart HP Smart Update Manager to return to an unfiltered state. Do not use the `/romonly` argument with the `/softwareonly` argument.
`/softwareonly`	This argument is a filter switch and allows the user to see only the software components needed for installation. When using this filter switch, you must exit, and then restart HP Smart Update Manager to return to an unfiltered state. Do not use the `/softwareonly` argument with the `/romonly` argument.
`/dryrun`	This argument simulates the installation for a test run. Nothing is installed.
`/continue_on_error` *<error>*	This argument causes the installation to continue and ignore errors. Valid values are *<error>*=ServerNotFound, *<error>*=BadPassword and *<error>*= FailedDependencies. The ServerNotFound option can be used to bypass inactive or unavailable remote hosts when deploying firmware or software to multiple remote hosts at the same time. FailedDependencies can be used to ignore any failed dependencies and proceed with the ones that are ready to be installed.
`/override_existing_ connection`	This argument defines the behavior when a remote target has an existing HP Smart Update Manager session in progress. This argument overrides the session in progress and reinitializes the installation framework on the remote host.
`/express_install`	This argument starts express install (for local host only). The HP Smart Update Manager performs discovery, install, or exit without user interaction. The user

Command line argument	Description
	can cancel or terminate HP Smart Update Manager.
`/user <username> or /username <username>`	This argument enables you to log in to HP BladeSystem c-Class Onboard Administrator with your user ID.
`/psswd <password>`	This argument enables you to use the password for the user ID specified in the `/user` parameter. The password is used to log in to remote hosts and HP BladeSystem c-Class Onboard Administrators.
`/current_credential`	This argument enables the credentials of the local host to be used as the credentials to access the targets instead of providing the username and password explicitly for each target. The assumption is that the current credentials are valid for the targets being accessed. (Applies to Windows® operating systems only.)
`/target "netAddress"`	This argument is the IP address or the DNS name of a HP BladeSystem c-Class Onboard Administrator or remote host. When two Onboard Administrators are in an enclosure, this argument should be the active Onboard Administrator. When specifying the IP address, you can use either the IPv4 or IPv6 format.
`/logdir "path"`	This argument enables you to redirect the output from HP Smart Update Manager or the HP BladeSystem c-Class Onboard Administrator flash utility to a different directory than the default location. For Windows® components, the default location is *%SYSTEMDRIVE%\CPQSYSTEM\hp\log<netAddress>* and the redirected location is *<path>\hp\log\<netAddress>*. For Linux components, the default location is */var/hp/log/<netAddress>* and the redirected location is *<path>/hp/log/<netAddress>*.
`/v[erbose]` or `/veryv[erbose]`	These arguments enable you to set the verbosity level for the HP Smart Update Manager execution log file, hpsum_execution_log_<date>_<time>.log. Using one of these arguments increases the level of detail that is retained in the log file. The default value is normal verbosity.
`/report`	This argument generates a report listing, a target summary, and how the components in the repository affect the target (For example, whether each component applies to the target or not). The report name is of the format, HPSUM_ Report_<date>_<time>.html. By default, it is located in the present working directory where HP Smart Update Manager is initiated from. If that location is write-protected, the report can be found in the same directory as the HP Smart Update Manager log files.
`/inventory_report`	This argument generates a report listing of the components in the specified repository. The report name is of the format, HPSUM_Inventory_Report_<date>_<time>.html. By default, it is located in the present working directory where HPSUM is initiated from. If that location is write-protected, the report can be found in the same directory as the HP Smart Update Manager log files.
`/inputfile "filename"`	This argument allows you to script the deployment of firmware and software to multiple remote systems at one time. For details of the file format and commands, see the Creating HP Smart Update Manager input files (on page 54) section.

Component configuration for Windows components only

To configure components without using the HP Smart Update Manager GUI, issue the command, `hpsum_config` *<component_to_configure>*. This command presents the same configuration screens seen in the HP Smart Update Manager GUI. You must run this command from a CD or other read-only media, or the component cannot be configured. Configuration for a given component only needs to be executed once. The configuration is stored within the component and is propagated to all target servers when deployed through HP Smart Update Manager GUI or command line. To change the configuration, rerun `hpsum_config` against the component and a new configuration writes out. If a component does not need configuration, the `hpsum_config` command returns to the console.

To configure components to be deployed on all editions of the Windows Server® 2008 with the Server Core option, you must access the system as a remote host using HP Smart Update Manager running on a system with a supported Windows® operating system, and then configure the components before deployment.

Command line examples

The following command line parameter examples can be executed within these environments:

- Windows® PSPs:
  - ProLiant Support Pack for Microsoft® Windows Server™ 2003 v7.90 (`BP000323.xml`)
  - ProLiant Support Pack for Microsoft® Windows Server™ 2003 v7.80 (`BP000315.xml`)
- Firmware:
  - System ROM
  - Smart Array controller
  - Hard drives
  - iLO
- Software—later version of:
  - HP Insight Diagnostics Online Edition for Windows Server™ 2003 (`cp008097.exe`)
  - HP System Management Homepage for Windows® (`cp008257.exe`)
- HP Smart Update Manager
  - Defined groups: Management Servers—Three servers (Management Server1, Management Server2, Management Server3)

Example 1:

This command line input deploys the latest PSP and firmware components:

```
hpsum /use_latest /allow_non_bundle_components /silent
```

Results: All the software components from the 7.90 PSP and firmware components, which HP Smart Update Manager determined needed to be installed, were installed.

Example 2:

Either of the following command line inputs can deploy the previous version of the PSP only and force all the components to be installed:

- `hpsum /f:bundle /softwareonly BP000315.xml`

- `hpsum /b BP000315.xml /f:bundle /softwareonly`

Results: All the software components from the 7.80 PSP, which HP Smart Update Manager determined needed to be installed, were installed. No firmware was installed.

Example 3:

This command line input deploys firmware:

`hpsum /romonly`

Results: All the firmware components, which HP Smart Update Manager determined needed to be installed, were installed. No software was installed.

Example 4:

Either of the following command line inputs can deploy two software components:

- `hpsum /f:software cp008097.exe cp008257.exe`
- `hpsum /c cp008097.exe /c cp008257.exe /f:software`

Results: The two components were installed. No firmware or other software was installed.

Example 5:

Either of the following command line inputs can deploy the latest PSP, later versions of components in the bundle, and firmware to three remote hosts and force all components to be installed:

- `hpsum /group "Management Servers" /current_credential /use_latest /allow_update_to_bundle /allow_non_bundle_components /force:all /override_existing_connection /continue_on_error ServerNotFound /silent /logdir "Management_Server_Files"`
- `hpsum /target "Management Server1" /target "Management Server2" /target "Management Server3" /user administrator /passwd letmein /use_latest /allow_update_to_bundle /allow_non_bundle_components /force:all /override_existing_connection /continue_on_error ServerNotFound /silent /logdir "Management_Server_Files"`

Results: All the firmware components, software components from the 7.90 PSP, `cp008097.exe`, and `cp008257.exe` were installed on Management Server1, Management Server2, and Management Server3.

HP Smart Update Manager return codes

HP Smart Update Manager has consolidated return codes from Linux and Windows® components into a new, enhanced return code mapping. These return codes determine the status of the component installation. You can also use return codes in a script to control the execution of the script and determine any required branching.

In Linux, the negative return codes are reported. These return codes are determined by subtracting the negative value from 256.

To view the installation log file locations, see "Viewing the installation results (on page 30)."

Return code	Value	Linux	Windows	Text
SUCCESS_NO_REBOOT	0	0	0	The installation was successful.

Return code	Value	Linux	Windows	Text
SUCCESS_REBOOT	1	1	1	The installation was successful, but a reboot is required.
SUCCESS_NOT_REQUIRED	3	3	3	The component was current or not required.
FAILURE_GENERAL	-1	255	255	A general failure occurred. See the error log for details.
FAILURE_BAD_PARM	-2	254	254	A bad input parameter was encountered.
FAILURE_COMPONENT_FAILED	-3	253	253	The installation of the component failed.

Windows smart component return codes

Error level	Meaning
0	The smart component failed to install. For more details, see the log file.
1	The smart component installed successfully.
2	The smart component installed successfully, but the system must be restarted.
3	The installation was not attempted because the required hardware is not present, the software is current, or there is nothing to install.

Linux smart component return codes

Single target servers:

Error level	Meaning
0	The smart component installed successfully.
1	The smart component installed successfully, but the system must be restarted.
2	The installation was not attempted because the required hardware is not present, the software is current, or there is nothing to install.
3	The smart component failed to install. For more details, see the log file.

Multi-target servers:

Error level	Meaning
0	The installation of the deliverable is successful. No reboot is required.
1	The installation of the deliverable is successful. Reboot is required for the deliverable to be enabled.
2	The installation was not attempted because the version to be installed matches the version already installed.

Error level	Meaning
3	The installation was not attempted because of one of the following: • The version to be installed is older than the version already installed. • The supported hardware is not present, not enabled, or in a state that an installation could not be attempted. • The smart component does not support the environment. • There is nothing for the component to accomplish.
4	If the component is installing to a remote target, such as Onboard Administrator or other network-based deployment, this return code indicates that the target cannot be found.
5	The installation was canceled by a user before anything could be installed.
6	The installer cannot execute because of an unmet dependency or installation tool failure.
7	The actual installation operation (not the installation tool) failed.

Creating HP Smart Update Manager input files

The HP Smart Update Manager input file functionality enables network administrators to leverage this capability to script multiple targets or groups within a single operation. Currently, there is a limit of 29 total targets for an installation with HP Smart Update Manager. The input file functionality can be leveraged to streamline even further the updates for workgroup-sized groups of servers and targets. To protect your credentials, use a secure server or a management console.

To create an input file, use Microsoft® Notepad. All section headers and trailers [END] must match. Failure to use the SILENT=YES option causes the GUI mode to be used but the information provided enables you to skip screens where information has already been provided. The DRYRUN=YES option can be used to do dry runs of installations to ensure the scripts are working without deploying the firmware updates that may be needed on each target. Remove the "DRYRUN=YES" option to perform the updates.

For parameters that can take list values, list separator can be commas, semicolons or spaces.

Examples of the HP Smart Update Manager input file:

REBOOTALLOWED = YES

REBOOTREQUIRED = NO

REBOOTMESSAGE = "Server is going down for a reboot"

REBOOTDELAY = 15

COMPONENTSLIST = cp001234.exe, cp001235.exe

BUNDLESLIST = bp001234.xml

ALLOWUPDATEBUNDLE = YES

SKIPTARGET = NO

IGNOREERRORS = ServerNotFound, FailedDependencies

SOURCEPATH = c:\pkgsource1

USELATEST = YES

SILENT = YES

OPTIONS = /f:rom

[TARGETS]

HOST = schinta1

HOST = schinta2

UID = root

PWD = root123

HOST = 234.567.765.432

[END]

Example 1: The two targets are passed to be updated. The targets do not necessarily have to be OAs. They can be any target supported by HP Smart Update Manager.

```
DRYRUN = YES
SILENT = YES

[TARGETS]
  HOST = BL465C-01
  HOST = 192.168.1.2
[END]
```

Example 2: A host is passed along with the user ID and password to use.

```
DRYRUN = YES
SILENT = YES

[TARGETS]
  HOST=BL685cG6
  UID = Bigboss2
  PWD = password
[END]
```

NOTE: The credentials can be left out of the file for greater security and passed on the command line to HP Smart Update Manager. The only limitation of this is that the userID and credentials must be the same on all.

When the file has been created, to use it with HP Smart Update Manager, add it as the inputfile <filename> parameter to a normal HP Smart Update Manager command line. For example, if the name of the input file is hpsum.in, the command line syntax is hpsum –inputfile hpsum.in. Full paths can be added to the input file location if it is not stored in the same location as the HP Smart Update Manager executables. The <filename> field may be enclosed in double quotes to allow for paths with spaces. Also, the input file itself may contain the same flags on the command line. The usual command line flags may still be used with the -inputfile flag, and takes precedence over any given input file.

Input file format and rules

The input file is divided into two sections:

- Configuration

  The configuration section starts from the beginning of the file and proceeds until the first target section is encountered. This section consists of a number of settings parameters and their values. Each configuration setting must appear on a fresh line in the file along with its value. Comments start with a # character at the beginning of the line. Only one # is allowed on any line.

- Target

  You can provide remote host targets to HP Smart Update Manager. This section can repeat any number of times in the input file, providing a way to organize targets in related sets.

  The section starts with a special header "TARGETS" enclosed in a pair of square brackets:

  ```
  [TARGETS]
  ```

  Targets section ends with the special string "END" enclosed in a pair of brackets:

  ```
  [END]
  ```

  The keyword TARGETS can be suffixed with an optional arbitrary string. This enables you to tag the purpose of the TARGETS section. Other than the visible difference in the header, the contents of such a section are not treated any differently. For example,

  ```
  [TARGETS_WIN2003]
  ...
  [END]
  ```

  - Credentials: The TARGETS section allows the targets to be grouped according to the credentials needed for logging in remotely. Each TARGETS section must have a set of login credentials, which applies to all targets in that section. If you want to use the current host's login credentials to log into one or more remote targets, you can do so by setting the variable USECURRENTCREDENTIAL to YES. Login credentials for one or more hosts can be supplied using the variables UID and PWD. If given at the beginning of a TARGETS section, both variables must be used. If given in the middle of a TARGETS section, one or the other can be used to override the selected variable and continue using the active value for the remaining variable.
  - Remote Target: A remote target can be specified using the variable HOST. Possible values are a DNS Name or an IP address.

File encoding

To allow for the inclusion of double-byte characters, the input file is in UTF-8 format.

Error reporting

If errors are encountered in the input file, HP Smart Update Manager exits with a return value of -2 (bad parameter). The details of the location and nature of the error are recorded in hpsum_execution_log_<date>_<time>.raw.

Input file parameters

Parameter	Description	Possible Values
`/silent`	This argument causes the installation to run silently with no GUI or console output. All data is written to the log file.	YES, NO

Parameter	Description	Possible Values
	Any generated prompts use the default option and continue the installation without user input. If a component requires input before installation (such as configuration information), then the component installation fails (unless the IGNOREERRORS = "Failedependencies" parameter is supplied), and an error message is written to the log file.	
/forceall	This argument forces both firmware and software components.	YES, NO
/forcerom	This argument forces updates to firmware components.	YES, NO
/forcesoftware	This argument forces updates to software components.	YES, NO
/forcebundle	This argument enables you to override or downgrade an existing installation of components in the selected bundle.	YES, NO
/downgrade	This argument enables you to downgrade to an earlier version of firmware for multi-target devices such as hard drives and array controllers. (Applies to firmware only.)	YES, NO
/rewrite	This argument enables you to rewrite the same version of firmware only for multi-target devices such as hard drives and array controllers. (Applies to firmware only.)	YES, NO
/rebootallowed	This argument enables you to reboot if required.	YES, NO
/rebootmessage	This argument enables you to create a message to be displayed prior to rebooting.	Any string
/rebootdelay	This argument enables you to delay before rebooting.	Time in seconds
/componentslist	This argument enables you to limit the list of components to be updated.	Component names with file extensions (.exe and .scexe)
/bundleslist	This argument enables you to limit the list of bundle xml	Bundle file names

Parameter	Description	Possible Values
	files to be filtered on.	
/allowupdatebundle	This argument is a filter switch and enables you to install newer versions of components defined in a PSP or firmware bundle. This argument enables these components to replace the older versions of the same component that might have shipped with the bundles.	YES, NO
/skiptarget	This argument defines the behavior when a remote target has an existing HP Smart Update Manager session in progress. This argument allows you to skip the host if there is already an existing HP Smart Update Manager session. A NO overrides the existing session.	YES, NO
/ignoreerrors	This argument causes the installation to continue and ignore errors. Valid values are ServerNotFound, BadPassword and FailedDependencies. The ServerNotFound option can be used to bypass inactive or unavailable remote hosts when deploying firmware or software to multiple remote hosts at the same time. FailedDependencies can be used to ignore any failed dependencies and proceed with the ones that are ready to be installed.	ServerNotFound, BadPassword, FailedDependencies
/sourcepath	This argument can be used to provide a single local repository path. This creates an inventory from the given path instead of the local or default repository.	Directory path
/uselatest	This argument is a filter switch for use with bundles. The argument enables you to use the latest version of the bundle when multiple versions of bundles are listed on the command line. If there are no bundles specified on	YES, NO

Parameter	Description	Possible Values
	the command line, and multiple bundles are in the directory, this parameter allows HP Smart Update Manager to use the bundle with the latest version for installation.	
/dryrun	This argument simulates the installation for a test run. Nothing is installed.	YES, NO
/options	This parameter can be used to specify the HP Smart Update Manager CLI options inside the input file and this will override the configuration settings. Parameters can be separated by a semi-colon, comma or a space.	All CLI switches For example, OPTIONS = /f:rom,/silent
/usesnmp	This argument specifies that components, which use SNMP protocol, are available to be selected for installation. These components are available for selection by default. When the /usesnmp argument is used, and the /usewmi argument is not, the WMI components are optional.	YES, NO
/usewmi	This argument specifies that components, which use WMI protocol, are available to be selected for installation. These components are optional by default and will not be installed unless this argument is used. When the /usewmi argument is used, and the /usesnmp argument is not, the SNMP components are optional.	YES, NO
/romonly	This argument is a filter switch and allows the user to see only the firmware components needed for installation. Do not use the /romonly argument with the /softwareonly argument.	YES, NO
/softwareonly	This argument is a filter switch and allows the user to	YES, NO

Parameter	Description	Possible Values
	see only the software components needed for installation. Do not use the `/softwareonly` argument with the `/romonly` argument.	
`/usecurrentcredential`	This argument enables the credentials of the local host to be used as the credentials to access the targets instead of providing the username and password explicitly for each target. The assumption is that the current credentials are valid for the targets being accessed. (Applies to Windows® operating systems only.)	YES, NO
`/webupdateneeded`	This argument enables you to instruct HP Smart Update Manager to include the components from HP.com in the list of possible updates.	YES, NO
`/useproxyserver`	This argument enables the inclusion of a proxy server (and port number) to access ftp.hp.com.	String value For example, 11.22.33.44:80
`/useproxyscript`	This argument enables the inclusion of a proxy script to access ftp.hp.com.	Web URL For example, autoproxy.com
`/deleteinputfile`	This argument enables you to instruct HP Smart Update Manager to delete the input file after it has been read in.	YES, NO (default)
`/onfaileddependency`	This argument instructs HP Smart Update Manager how to proceed when a component has a failed dependency. The default of OmitHost causes the host to be put in a failure state and no install is attempted on it. OmitComponent deselects the affected component(s) and proceeds with any updates that do not have dependency failures. Force attempts all updates, even if they have dependency failures.	OmitHost (default), OmitComponent, Force

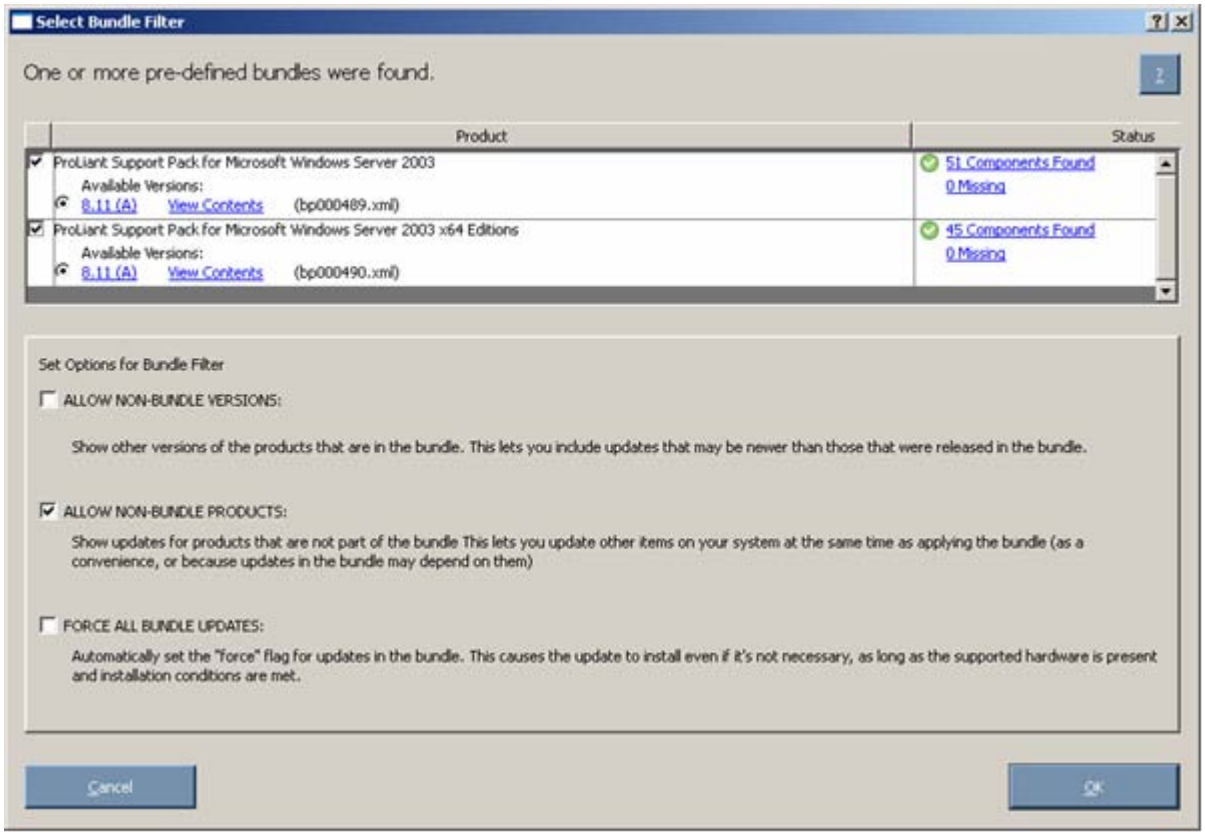
Advanced topics

Deploying firmware and software simultaneously

HP Smart Update Manager utility enables you to deploy firmware and software components simultaneously. Only Windows® online deployments support deploying firmware and software components from Windows® PSPs and HP BladeSystem online bundles simultaneously. The latest Microsoft® Windows® PSP, bundles, and firmware components must be in the same directory and the cp*.exe file added to the repository to deploy simultaneously. With the ability to get components from ftp.hp.com, you can deploy software and firmware components without using bundles.

NOTE: HP Smart Update Manager is compatible with various types of HP bundles.

To deploy firmware and software components from Windows® PSPs and server blade bundles simultaneously, run the HP Smart Update Manager. On the Select Bundle Filter screen, select the bundle, and then select the **ALLOW NON-BUNDLE PRODUCTS** option.



To proceed with the deployment process, click **OK.** The Select Items to be Installed ("Selecting components to install" on page 22) screen appears with the appropriate firmware and software components.

For more information on the PSPs, see the *HP ProLiant Support Pack User Guide*.

Server virtualization detection and support

HP Smart Update Manager, running in the context of a Windows® PSP, supports server virtualization that runs on a Windows® host. However, HP Smart Update Manager, running in the context of a Windows® PSP, does not run on a VMware host or on a guest operating system environment regardless of what host hypervisor you use.

HP Smart Update Manager, running in the context of the Firmware Maintenance CD, does not support server virtualization that runs on a Windows® or Linux host and blocks attempts to install firmware from a guest or child virtual machine. The server virtualization does not run on a VMware host or on a guest operating system environment regardless of which host hypervisor you use. The Firmware Maintenance CD does not boot to a guest operating system environment.

Configuring IPv6 networks with HP Smart Update Manager

Starting with HP Smart Update Manager version 3.2.0, you can deploy to remote targets in IPv6-based networks for Windows® and Linux target servers. Using HP Smart Update Manager with IPv6 networks presents challenges for IT administrators.

For Windows®-based servers, to communicate with remote target servers, HP Smart Update Manager uses either existing credentials or user-provided user name and password to connect to the admin$ share. This share is an automatic share provided by Windows Server®. After HP Smart Update Manager connects to the admin$ share, it copies a small service to the target server for the duration of the installation. After this service starts, HP Smart Update Manager uses this service to communicate between the local and remote target server. During this process, HP Smart Update Manager opens ports in the Windows® firewall to enable HP Smart Update Manager to use SOAP calls over SSL to pass data among local and remote systems. These ports are defined in Allowing ports in HP Smart Update Manager ("Enabling ports in HP Smart Update Manager" on page 75). After the installation is completed or canceled, HP Smart Update Manager stops the remote service, removes it from the target server, closes the port on the Windows® firewall, and then releases the share to the target server admin$ share.

For Linux-based servers, to communicate to remote target servers, HP Smart Update Manager starts by using the user-provided user name and password to create a SSH connection to the target server. After the HP Smart Update Manager connects, copies a small service to the target server for the duration of the installation. After this service starts, HP Smart Update Manager uses this service to communicate between the local and remote target server. During this process, HP Smart Update Manager opens ports in the iptables firewall to enable HP Smart Update Manager to use SOAP calls over SSL to pass data between the local and remote systems. These ports are defined in Allowing ports in HP Smart Update Manager ("Enabling ports in HP Smart Update Manager" on page 75). When the installation is completed or canceled, HP Smart Update Manager stops the remote service, removes it from the target server, closes the port in the iptables firewall, and then closes the SSH connection to the target server.

Configuring IPv6 for Windows Server 2003

For information on setting up a Windows Server® 2003 operating system within an IPv6 network, see the online Microsoft® Technet article Step-by-Step Guide for Setting Up IPv6 in a Test Lab (http://www.microsoft.com/downloads/details.aspx?FamilyID=fd7e1354-3a3b-43fd-955f-11edd39551d7&displaylang=en).

Before using HP Smart Update Manager to deploy software and firmware updates to remote Windows Server® 2003 servers, you must add a registry entry to enable file sharing connections over IPv6 networks. To make the registry entry:

1. Start the Registry Editor (`Regedt32.exe`).
2. Locate and click the following key in the registry:

   ```
   HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters
   ```

3. On the Edit menu, click **Add Value.**
4. Add the following registry value:

   Value name: `DisableStrictNameChecking`

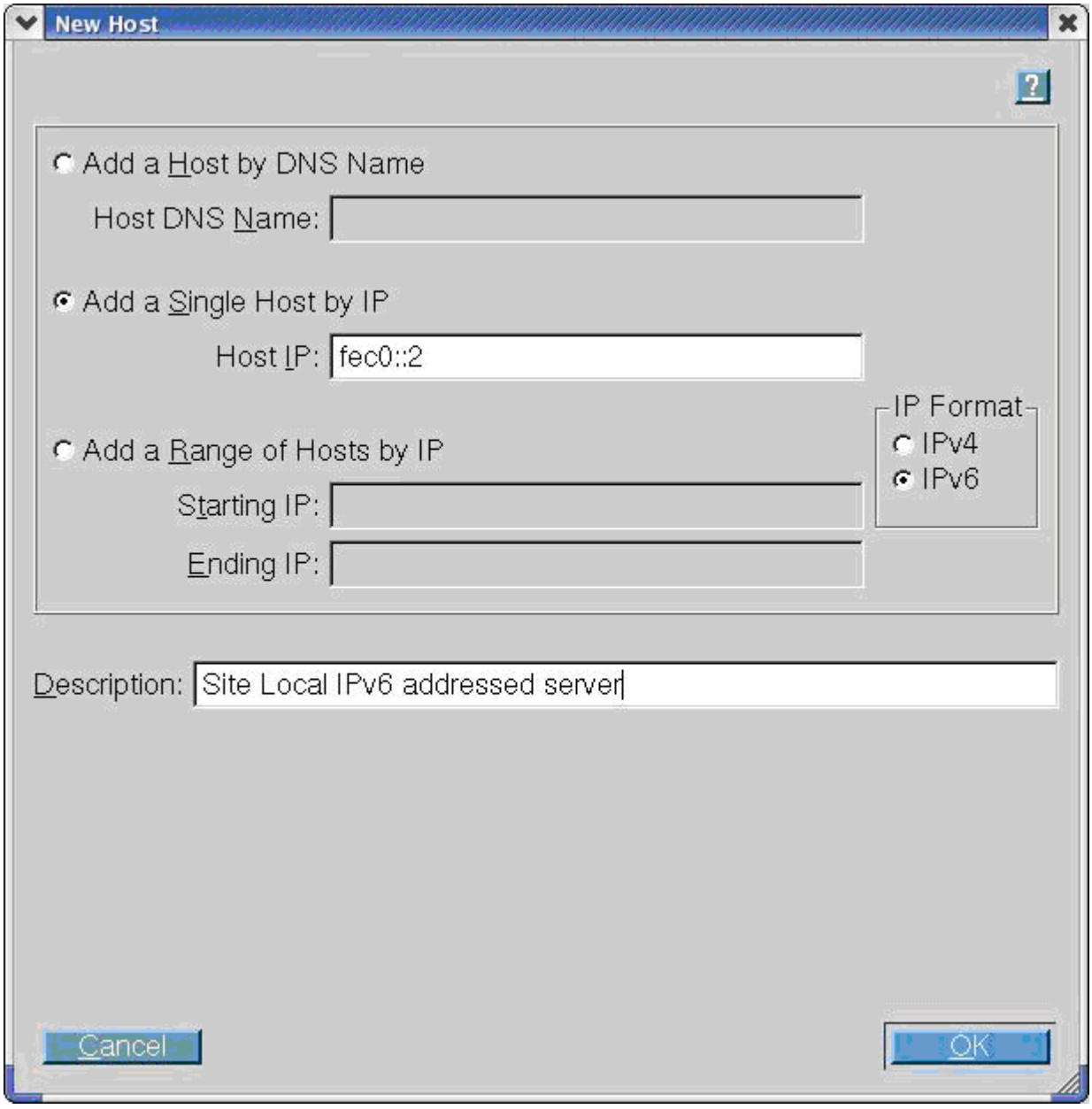
   Data type: `REG_DWORD`

   Radix: `Decimal`

   Value: 1
5. Quit the Registry Editor.

For more information about these steps, see the Microsoft® Knowledge Base Item 281308 on the Microsoft® website (http://www.microsoft.com).

IPv6 addresses can be passed to HP Smart Update Manager in command line arguments or using the HP Smart Update Manager user interface. In the HP Smart Update Manager user interface, you can add a remote host on an IPv6 network by either entering the DNS name of the IPv6 target server or by selecting the IPv6 address button and entering the IPv6 address. HP Smart Update Manager supports both the short-name and full IPv6 notation. You do not need to add the optional interface number when you enter the address.



If you cannot connect to the target server or receive a `Discovery failed` message when executing HP Smart Update Manager in an IPv6 environment, see the troubleshooting section ("Troubleshooting HP Smart Update Manager in IPv6 networks" on page 79).

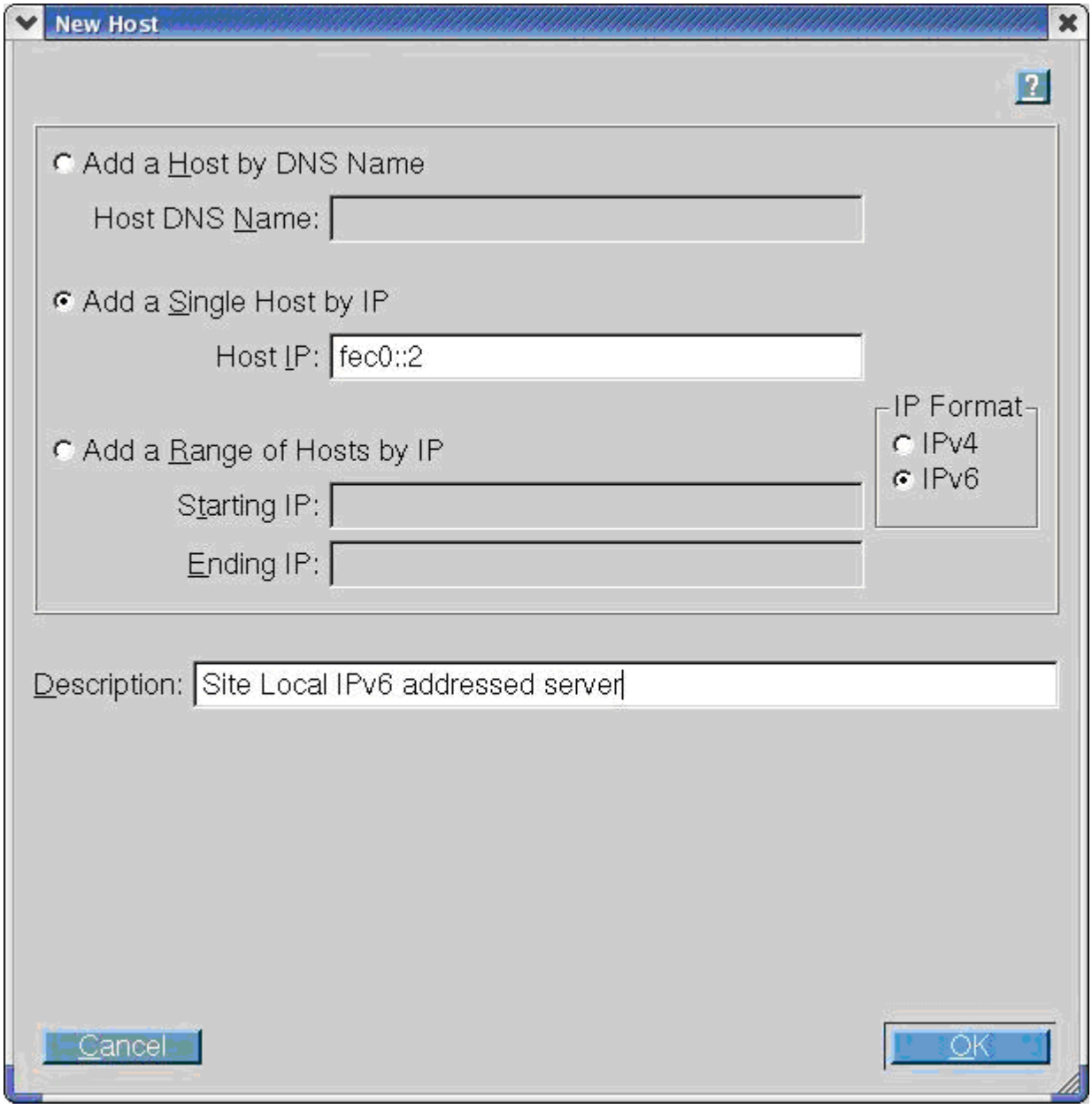
After you connect to the target server, all other HP Smart Update Manager functions work identically. Log files for IPv6 hosts are stored with all other HP Smart Update Manager files in the \CPQSYSTEM\hp\log\<ip_address> directory.

Configuring IPv6 for Windows Server 2008

HP Smart Update Manager provides the most robust support for remote deployment when using Windows Vista® as a client to Windows Server® 2008-based servers. Using HP Smart Update Manager in this environment enables you to use all the capabilities of IPv6 including link-local, site-local, and global IP addresses for both local and remote target servers. Windows Vista®, when used as a client to run HP Smart Update Manager to remote Windows Server® 2008 operating systems or as a target operating system on HP Workstation server blades, provides the infrastructure that supports full IPv6 deployment of software and firmware updates from HP Smart Update Manager.

NOTE: Windows® XP clients are not supported in IPv6 networks for HP Smart Update Manager deployment.

IPv6 addresses can be passed to HP Smart Update Manager in command line arguments or using the HP Smart Update Manager user interface. In the HP Smart Update Manager user interface, you can add a remote host on an IPv6 network by either entering the DNS name of the IPv6 target server or by selecting the IPv6 address button and entering the IPv6 address. HP Smart Update Manager supports both the short-name and full IPv6 notation. You do not need to add the optional interface number when you enter the address.



If you cannot connect to the target server or receive a Discovery failed message when executing HP Smart Update Manager in an IPv6 environment, see the troubleshooting section ("Troubleshooting HP Smart Update Manager in IPv6 networks" on page 79).

After you connect to the target server, all other HP Smart Update Manager functions work identically. Log files for IPv6 hosts are stored with all other HP Smart Update Manager files in the \CPQSYSTEM\hp\log\<ip_address> directory.

Limitations of IPv6 for Windows Server 2003 and Windows Server 2008

Windows Server® 2003 requires site-local addresses to provide the necessary file-sharing capabilities needed by HP Smart Update Manager. This means that link-local and global IPv6 addresses are not supported as remote targets with HP Smart Update Manager.

Windows Server® 2008 or Windows® environments do not have any known limitations to using HP Smart Update Manager.

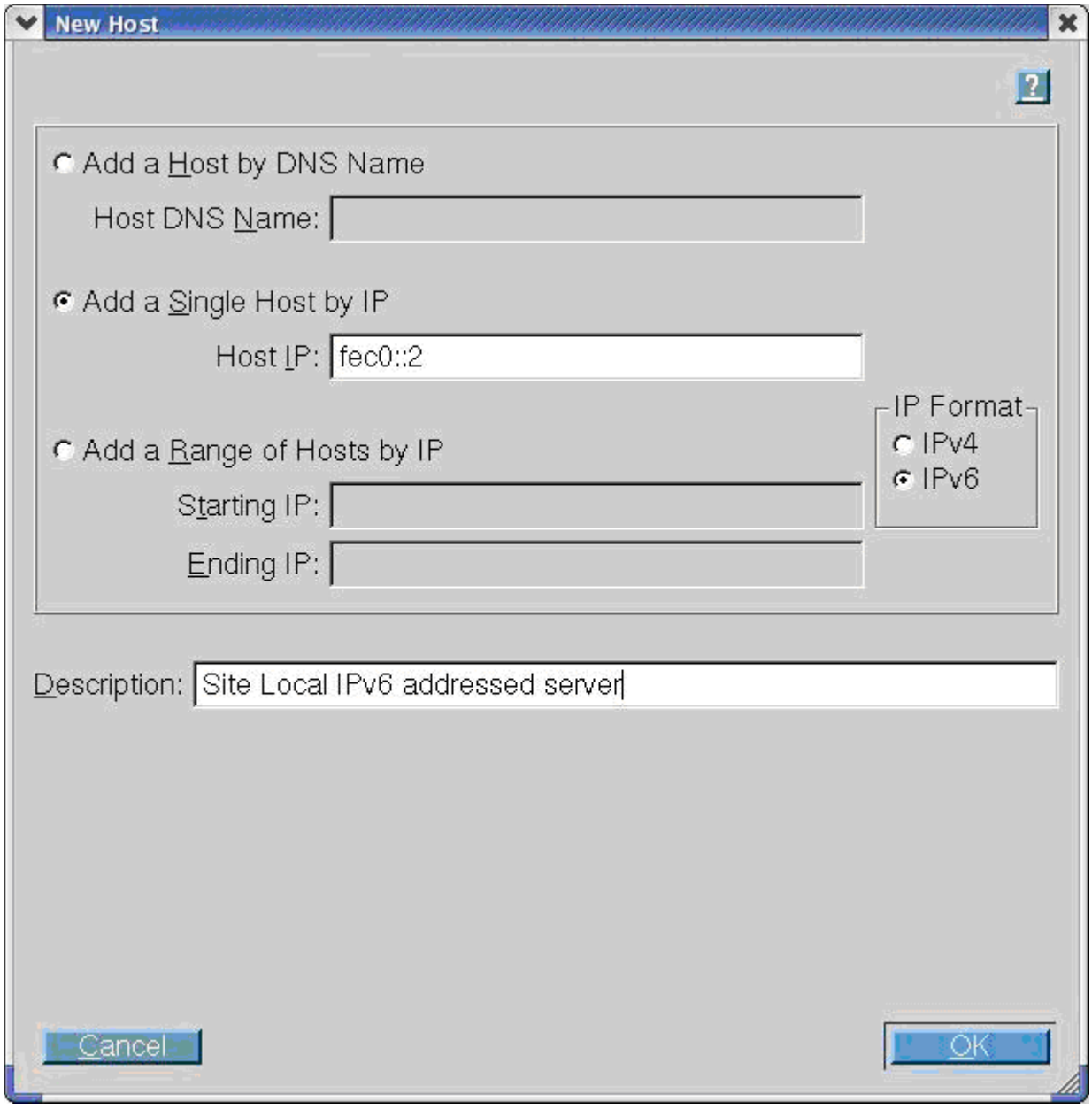
NOTE: Windows® XP clients are not supported in IPv6 networks for HP Smart Update Manager deployment.

Configuring IPv6 for Linux

HP Smart Update Manager leverages the IPv6 capabilities of Linux as provided by the Red Hat Enterprise Linux and Novell SUSE Linux Enterprise Server products. Using HP Smart Update Manager in this environment enables you to use all the capabilities of IPv6 including link-local, site-local, and global IP addresses for both local and remote target servers. Remote target servers must have the iptables-ipv6 RPM installed before targeting them from HP Smart Update Manager. Failure to install the iptables-ipv6 RPM prevents HP Smart Update Manager from opening the communications port needed to send data to the initiating Linux workstation. You can disable the Linux firewall to allow HP Smart Update Manager to work, but the Linux server becomes vulnerable to attack.

For information on how to setup IPv6 in a Linux environment, please see the Linux IPv6 How-To (http://www.linux.org/docs/ldp/howto/Linux+IPv6-HOWTO/index.html).

IPv6 addresses can be passed to HP Smart Update Manager in command line arguments or using the HP Smart Update Manager user interface. In the HP Smart Update Manager user interface, you can add a remote host on an IPv6 network by either entering the DNS name of the IPv6 target server or by selecting the IPv6 address button and entering the IPv6 address. HP Smart Update Manager supports both the short-name and full IPv6 notation. You do not need to add the optional interface number when you enter the address.



If you cannot connect to the target server or receive a Discovery failed message when executing HP Smart Update Manager in an IPv6 environment, see the troubleshooting section ("Troubleshooting HP Smart Update Manager in IPv6 networks" on page 79).

After you connect to the target server, all other HP Smart Update Manager functions work identically. Log files for IPv6 hosts are stored with all other HP Smart Update Manager files in the /var/hp/log/<ip_address> directories.

Limitations of IPv6 for Linux

The only current limitation of HP Smart Update Manager in a Linux IPv6 environment is that all remote target Linux-based servers must have the iptables-ipv6 rpm file installed. You can find the file on the distribution media for both Red Hat Enterprise Linux and Novell SUSE Linux Enterprise Server operating systems. HP Smart Update Manager uses this file to open a port in the IPv6 firewall to communicate with the Linux system that runs HP Smart Update Manager. Failure to install iptables-ipv6 results in HP Smart Update Manager reporting a discovery failure unless you disable the firewall.

Troubleshooting

Recovering from a failed ROM upgrade

Recovering from a failed system ROM upgrade

Use redundant ROM or ROMPaq to recover from a system ROM upgrade failure.

Redundant ROM recovery

When you flash the system ROM, ROMPaq writes over the backup ROM and saves the current ROM as a backup, enabling you to switch easily to the alternate ROM version if the new ROM becomes corrupted for any reason. This feature protects the existing ROM version, even if you experience a power failure while flashing the ROM.

When the server boots, the server detects if the current ROM is corrupt. If a corrupt ROM is detected, then the system boots from the backup ROM and sends an alert through POST that the ROM is corrupt.

To access the redundant ROM through RBSU:

1. Power up your desktop. A prompt appears in the upper right corner of the screen.
2. Access RBSU by pressing F9.
3. Select **Advanced Options.**
4. Select **ROM Selection.**
5. Select **Switch to Backup ROM.**
6. Press the **Enter** key.
7. To exit the current menu, press the **Esc** key, or to exit RBSU, press the **F10** key. The server restarts.

If RBSU is inaccessible, then you can switch ROM images by changing the switch settings on the system configuration switch. For more information, see your server documentation.

If both ROM images are corrupt, use ROMPaq recovery.

ROMPaq recovery

The Disaster Recovery feature supports systems that do not support the Redundant ROM feature. Disaster Recovery only applies to platforms with nonredundant system ROM. If both the up-to-date and backup versions of the ROM are corrupt, then perform ROMPaq Disaster Recovery procedures:

1. On another server, download and save the ROMPaq image to the hard drive from the HP website (http://www.hp.com).
2. Execute the ROMPaq image to create the ROMPaq disk.
3. Switch to the server with the corrupted ROM.
4. Power down the server.
5. Insert the ROMPaq disk.

6. Power up the server.

   The server generates one long beep and two short beeps to indicate that it is in disaster recovery mode. If the disk is not in the correct drive, then the system continues to beep until a valid ROMPaq disk is inserted.

   The ROMPaq disk flashes both system ROM images. If successful, a sequence of ascending audible beeps is generated. If unsuccessful, a sequence of descending audible beeps is generated, and you must repeat the disaster recovery process.
7. Power down the server.
8. Remove the ROMPaq disk.
9. Power up the server.

To manually set the server for ROMPaq disaster recovery:

1. Power down the server.
2. Remove the access panel.
3. Set the system maintenance switch positions for disaster recovery. Switch positions are server-specific; see the server documentation for information about the correct settings for your server.
4. Insert a ROMPaq diskette with the latest system ROM from the Firmware Maintenance CD or the HP website (http://www.hp.com/support).
5. Install the access panel.
6. Power up the server.
7. Allow the system to boot completely.
8. Repeat steps 1 and 2.
9. Reset the system maintenance switch positions to their original settings.
10. Repeat steps 5 and 6.

Recovering from a failed option ROM upgrade

To recover from an option ROM upgrade failure, use the recovery method that is appropriate to the specific option.

Array controller ROMs

Array controllers support Recovery ROM, which is a redundancy feature that ensures continuous system availability by providing a backup ROM. During the flash process, a new version of the firmware can be flashed to the ROM while the controller maintains the last known version of the firmware. If the firmware becomes corrupt, the controller reverts back to the redundant version of the firmware and continues operating.

NOTE: Storage option ROMs cannot be downgraded with ROMPaq because ROMPaqs have been retired as a delivery method for storage options.

Lights-Out management ROMs

To perform disaster recovery for RILOE II, iLO, and iLO 2, see the documentation for your particular Lights-Out management product on the Remote management website (http://www.hp.com/servers/lights-out).

Recovering from an installation failure

Collecting trace directories

HP Smart Update Manager generates a set of debug trace logs located in the %TEMP%\hp_sum directory on Windows systems and \tmp\hp_sum on Linux systems. These files contain internal process and debug information, which can be useful in determining HP Smart Update Manager failures.

> **NOTE:** To break out to a Linux console while booted to the Firmware Maintenance CD, press **Ctrl Alt d b x.** Each key (d, b, x) is hit in succession. This command allows you to collect logs from the \tmp\hp_sum directory.

Examine the OpMan.trace, IPScout.trace, OSScout.trace, InstallClient.log, and InstallManager.log trace files to determine the cause of the failure. These files provide the following information.

Trace files	Function
OpMan.trace	Provides operations trace of the overall installation process.
IPScout.trace	Provides the information on whether the remote target might be contacted and the type of target found (iLO, server, VC, OA).
OSScout.trace	Provides the details of the connection setup and is responsible for cleaning up after an installation and initiating a reboot, if needed and selected by the user, on the target system.
InstallClient.log	Provides the details of the execution of the individual components, including the command line parameters, used to launch the components and the component return code before it is converted to HP Smart Update Manager return codes.
InstallManager.log	Provides the interaction between the Operations Manager and the remote installation client. Any failure in network communications is reported in this file and surfaced as an Installation Failed message for the affected component and potentially all components that follow the failing component.
discagent.trace	Provides the details of the execution of the discovery agent on either the local system during a local installation or the remote target server. If a discovery tool fails, it is reported to this trace file and surfaced as a Discovery Failed message.
discmanager.trace	Provides the interaction between the Operations Manager and the remote discovery client. If a discovery tool fails, it is reported to this trace file and surfaced as a Discovery Failed message.

It is possible to look in the OpMan.trace file and see which component was winnowed from the installation set and which ones were added. Normally, components are winnowed if:

- They do not support installation on the given OS
- The hardware they are designed for is not discovered to be present in the server
- The component is not for the type of target selected
- The component does not report itself capable of being deployed to a given target
- The component cannot be deployed in either the online or offline environment HP Smart Update Manager detects it is running in
- The component is for a particular class (p-Class or c-Class) of BladeSystem enclosure and the component does not find that class of enclosure.

The following is an example of the output trace in the OpMan.trace on how to determine if a component was prevented from being shown on the Select Items to Install screen or being deployed from the silent console mode. In the example, the binary image files 0.bin and 1.bin (which represented iLO firmware files), components cp011301.exe and cp011500.exe, and the HP BladeSystem Firmware Update Bundle for Windows represented by bundle file bp000648.xml were added to the installation set. All the other components were removed for various reasons.

```
InstallSet.cpp[212]: Winnow--Adding FileName 0.bin
InstallSet.cpp[212]: Winnow--Adding FileName 1.bin
InstallSet.cpp[222]: Winnow--Removing FileName 2.bin
InstallSet.cpp[212]: Winnow--Adding FileName cp011301.exe
InstallSet.cpp[222]: Winnow--Removing FileName cp011321.exe
InstallSet.cpp[222]: Winnow--Removing FileName cp011489.exe
InstallSet.cpp[222]: Winnow--Removing FileName cp011497.exe
InstallSet.cpp[212]: Winnow--Adding FileName cp011500.exe
InstallSet.cpp[222]: Winnow--Removing FileName cp011504.exe
InstallSet.cpp[222]: Winnow--Removing FileName cp011505.exe
InstallSet.cpp[222]: Winnow--Removing FileName cp011550.exe
InstallSet.cpp[222]: Winnow--Removing FileName cp011560.exe
InstallSet.cpp[242]: Target 0: Added Bundle bp000648.xml
```

Recovering from a discovery failure

Troubleshooting connection errors

If you are receiving an HPSUM Connection Error or Discovery Failed messages, follow these main troubleshooting tips.

- Ensure your workstation does not have an existing connection to the ADMIN$ share on the target IP address. If it does, it prevents HP Smart Update Manager from connecting to the remote server's share because Windows only allows one connection from a client to a server's share. This can be checked by entering net use at a command prompt. If there is an existing share to the target IP address \admin$ share, delete it and try the installation again.
- Ensure that the target IP address server's admin$ share is accessible. Validate the target server can be accessed by entering net use x: \\<ip_address_or_dns_name>\admin$ for the target server's IP address or DNS name. When the connection is validated, ensure that it is deleted by entering net use x: /d at command prompt.
- Ensure the user ID being used to connect to the target IP address server is part of the administrator's group. If it is not, HP Smart Update Manager blocks installation to the target.
- Ensure WMI is enabled and running on all Windows target servers.
- For Linux, ensure the SSH port is not blocked.
- In some rare cases, external storage enclosures may cause HP Smart Update Manager to report a discovery failure. To resolve this problem, disconnect the external storage until the firmware updates are completed.

- For Linux, ensure that the target server can be contacted through SSH and that the scp command is available to securely send files to the target server.
- Ensure the firewall ports on any routers in the network as documented in the Enabling ports in HP Smart Update Manager section of this document.
- The Symantec End Point Protection product (SEP) blocks HP Smart Update Manager ability to communicate with remote targets if the Network Threat Analysis feature is enabled. Disable this feature while HP Smart Update Manager is in use on the workstation.
- Examine the OpMan.trace, IPScout.trace, OSScout.trace, discagent.trace and discmanager.trace files to determine the cause of the failure. For more information, see Collecting trace directories.

Recovering from a loss of Linux remote functionality

Configuring firewall settings

When the `Unable to Access Host` message appears, the target firewall is enabled. By default, the target firewall is enabled in Linux.

To recover remote Linux functionality, the target and host firewall must be disabled or reconfigured to allow IP traffic through the ports needed by HP Smart Update Manager to deploy firmware. For a list of the ports that need to be configured in the firewall, see Allowing ports in HP Smart Update Manager ("Enabling ports in HP Smart Update Manager" on page 75).

Recovering from a blocked program on Microsoft Windows

Configuring Windows firewall settings

The Windows® Security Alert appears when a program is blocked from accepting connections from the Internet or a network.



To set the rules for the Windows® Firewall and Security Policy, click **Unblock,** and then set your firewall settings to the following:

1. Click **Start>Control Panel>Administrative Tools>Windows Firewall with Advanced Security>Inbound Rules>Remote Administration (NP-IN).**
2. Select **Enabled,** and then select **Allow the connections.**

For Direct to iLO support, you must enable ping.

Enabling ports in HP Smart Update Manager

The ports that HP Smart Update Manager uses cannot be configured. When HP Smart Update Manager port initiates communications to remote targets, it uses several well-known ports depending on the operating system. For Windows®, it uses ports 138 and 445 to connect to remote targets (equivalent to remote and file print share functionality). For Linux, HP Smart Update Manager uses port 22 (SSH) to start the communications with the remote target.

HP Smart Update Manager uses defined ports to communicate between the remote target and the workstation where HP Smart Update Manager is executing. When you run HP Smart Update Manager, it uses the administrator/root privileges to dynamically register the port with the default Windows® and Linux firewalls for the length of the application execution, then closes and deregisters the port. All communications are over a SOAP server using SSL with additional functionality to prevent man-in-the-middle, packet spoofing, packet replay, and other attacks. The randomness of the port helps prevent port

scanning software from denying service to the application. The SOAP server is deployed on the remote target using the initial ports described above (ports 138, 445, and 22) and then allocates another independent port as documented below for its communications back to the workstation where HP Smart Update Manager is running. During shutdown of HP Smart Update Manager, the SOAP server is shutdown and removed from the target server, leaving the log files.

To deploy software to remote targets on their secure networks using HP Smart Update Manager, the following ports are used.

For Windows®

Ports	Description
Ports 445 and 137/138/139 (Port 137 is used only if you are using NetBIOS naming service.)	These ports are needed to connect to the remote ADMIN$ share on target servers. These are the standard ports Windows® servers use to connect to remote file shares. If you can connect remotely to a remote Windows® file share on the target server, then you have the right ports open.
Ports 60000-60007	Random ports are used in this range to pass messages back and forth between the local and remote systems via SSL. These ports are used on the system running HP Smart Update Manager to send data to the target server. Several internal processes within HP Smart Update Manager automatically use the port from 60000 when no other application uses it. If there is a port conflict, the manager uses the next available one. There is no guarantee that the upper limit is 60007 as it is dependent on how many target devices are selected for installation.
Ports 61000-61007	These ports are used from the target server back to the system running HP Smart Update Manager. The same mechanism is used by the remote access code as the 60000 ports, with the first trial port as 61000. There is no guarantee that the upper limit is 61007 when a conflict occurs. For the case of ipv4-only and one NIC, the lowest available one is used by HP Smart Update Manager to pass information between processes on the local workstation where HP Smart Update Manager is executed, and the next available one is used to receive messages from remote servers.
Port 62286	This port is the default for some internal communications. It is the listening on the remote side if there is no conflict. If a conflict occurs, the next available one is used.
Ports 80 or 63000-63005	The logs are passed to the target and the logs are retrieved via an internal secure web server that uses port 80 if it is available or a random port between 63000 and 63005, if it is not. This support allows updates of the iLO firmware without the need to access the host server and allows servers running VMware or other virtualization platforms to update their iLO without the need to reboot their server or migrate their virtual machines to other servers.

For Linux

Port	Description
Port 22	This port is establishes a connection to the remote Linux server via SSH.

Ports 60000-60007	Random ports are used in this range to pass messages back and forth between the local and remote systems via SSL. These ports are used on the system running HP Smart Update Manager to send data to the target server. Several internal processes within HP Smart Update Manager automatically use the port from 60000 when no other application uses it. If there is a port conflict, the manager uses the next available one. There is no guarantee that the upper limit is 60007 as it is dependent on how many target devices are selected for installation.
Ports 61000-61007	These ports are used from the target server back to the system running HP Smart Update Manager. The same mechanism is used by the remote access code as the 60000 ports, with the first trial port as 61000. There is no guarantee that the upper limit is 61007 when a conflict occurs. For the case of ipv4-only and one NIC, the lowest available one is used by HP Smart Update Manager to pass information between processes on the local workstation where HP Smart Update Manager is executed, and the next available one is used to receive messages from remote servers.
Port 62286	This port is the default for some internal communications. It is used for listening on the remote side if there is no conflict. If a conflict occurs, the next available one is used.
Ports 80 or 63000-63005	The logs are passed to the target and the logs are retrieved via an internal secure web server that uses port 80 if it is available or a random port between 63000 and 63005, if it is not. This support allows updates of the iLO firmware without the need to access the host server and allows servers running VMware or other virtualization platforms to update their iLO without the need to reboot their server or migrate their virtual machines to other servers.

Recovering from operating system limitations when using a Japanese character set

Displaying the user-specified reboot message using a Japanese character set when running on a Linux operating system

You might specify a message to appear prior to shutting down the system during a reboot operation. When using a Japanese character set and running on a Japanese version of a Linux operating system, the message does not appear properly.

Rebooting with the user-specified reboot message using a Japanese character set when running on a Windows operating system

You might specify a message to appear prior to shutting down the system during a reboot operation. When using a Japanese character set and running on a Japanese version of a Windows® operating

system, the message causes the reboot not to occur automatically. For a successful reboot, you must select the **Exit** button.

Recovering from Fatal Error - application will exit message

Running in a directory path containing double-byte characters

When running in a directory path containing double-byte characters, the HP Smart Update Manager encounters a fatal error while trying to initialize.



The HP Smart Update Manager cannot be run in directories containing double-byte characters in the path name. Paths can be created with double-byte characters when using certain versions of the operating system, such as Japanese or Chinese.

Recovering from a missing reboot message when running on SUSE LINUX Enterprise Server 9

Running HP Smart Update Manager on SUSE LINUX Enterprise Server 9

You can specify a reboot message that appears before a server reboots after a successful installation of firmware or software. However, when running HP Smart Update Manager on SUSE LINUX Enterprise Server 9, the reboot message does not appear because there is no access to the console when using SUSE LINUX Enterprise Server 9. This error is not unique to HP Smart Update Manager, and it is an operating system limitation.

NOTE: Beginning with the Firmware Maintenance CD v8.50, HP Smart Update Manager no longer runs on SUSE Enterprise Linux 9.

Recovering a lost HP Smart Update Manager connection

Mounting the Firmware Maintenance CD on virtual media

When either iLO and NIC firmware are updated, the HP Smart Update Manager connection is lost and cannot install components. If an access error exists, HP Smart Update Manager cancels the installation.

Troubleshooting HP Smart Update Manager in IPv6 networks

If HP Smart Update Manager cannot connect to the remote server, you might receive a Discovery Failed error. Discovery failures can be caused by third-party storage, failure to access the remote target server, and an inability to access system resources. For IPv6 networks, host discovery failures can be caused by the incorrect configuration of the IPv6 network.

Troubleshooting HP Smart Update Manager in IPv6 Windows Server 2003 environment

To validate that the IPv6 network is configured correctly for HP Smart Update Manager support, you must verify the following based on your operating system version.

- Validate that the addresses are site-local. Site-local addresses normally start with "FEC0:". Global and link-local IPv6 addresses are not supported when the remote target is Windows Server® 2003.
- Validate that you can ping the remote target server. With Windows® operating systems, you can still use the ping command to ping IPv6 addresses: ping <ipv6 address>.
- Ensure you can ping the IPv6 loopback address: ping ::1.
- Use the DNS hostname instead of IPv6 address to ensure the address is correct.
- Ensure you have installed the IPv6 protocol. It is not installed by default in Windows Server® 2003. Be sure to reboot the server after installing the protocol to ensure addresses are properly obtained.
- Verify that you can connect to the admin$ share using the credentials within HP Smart Update Manager by issuing the following command at a console prompt:

  ```
  net use * \\<ipv6-address>.ipv6-literal.net\admin$ /user:<username>
  net use * \\fec0::2.ipv6-literal.net\admin$ /user:administrator
  ```

  You might need to provide the password if you are using a user name that is not the same as you used to log in to the local system. All network shares require the use of the .ipv6-literal.net name string to be properly configured by Windows®.

  NOTE: You do not need to use the .ipv6-literal.net suffix when entering IPv6 address into the HP Smart Update Manager user interface or when passing IPv6 address using command line parameters to HP Smart Update Manager.

  After you validate that you can access the admin$ share on the remote target server, HP Smart Update Manager works unless other network or hardware issues exist.

- Ensure you have made the registry change on remote target servers as mentioned in the HP Smart Update Manager Usage in a Windows Server® 2003 IPv6 environment ("Configuring IPv6 for Windows Server 2003" on page 62).
- Move back to an IPv4 network address to ensure HP Smart Update Manager properly finds the remote target server without any issues.

You can always copy HP Smart Update Manager to the target servers and execute using the local installation method.

Troubleshooting HP Smart Update Manager in IPv6 Windows Server 2008 environment

To validate that the IPv6 network is configured correctly for HP Smart Update Manager support, you must verify the following based on your operating system version.

- Validate that you can ping the remote target server. With Windows® operating systems, you can use the ping command to ping IPv6 addresses: ping <ipv6 address>.
- Ensure you can ping the IPv6 loopback address: ping ::1.
- Use the DNS hostname instead of IPv6 address to ensure the address is correct.
- Verify that you can connect to the admin$ share using the credentials within HP Smart Update Manager by issuing the following command at a console prompt:

  ```
  net use * \\<ipv6-address>.ipv6-literal.net\admin$ /user:<username>
  net use * \\fec0::2.ipv6-literal.net\admin$ /user:administrator
  ```

  You might need to provide the password if you use a user name that is different from the one you used to log in to the local system. All network shares require the use of the .ipv6-literal.net name string to be properly configured by Windows®.

  After you validate you can access the admin$ share on the remote target server, HP Smart Update Manager works unless there are other network or hardware issues.

Troubleshooting HP Smart Update Manager in IPv6 Red Hat and Novell SUSE-based Linux environments

- Verify that you can establish an ssh connection to the remote target server using the credentials within HP Smart Update Manager by issuing the following command at a console prompt:

  ```
  ssh <ipv6 address>
  ssh 2101:db8:0:1::9
  ```

  You must enter the root password for the target Linux server at the console to complete the IPv6 connection.
- Validate that you can ping the remote target server. In Linux, you need to use the ping6 command to ping IPv6 addresses: ping6 <ipv6 address>.
- Ensure you can ping the IPv6 loopback address: ping6 ::1.
- Use the DNS hostname instead of IPv6 address to ensure the address is correct.

- Use `ipconfig` to validate you have IPv6 addresses assigned to your NICs. For more information about troubleshooting your configuration, see the Linux IPv6 How-To (http://www.linux.org/docs/ldp/howto/Linux+IPv6-HOWTO/index.html).
- For more information about setting up and troubleshooting IPv6 networks, see Getting Around IPv6 by Carla Schroder (http://www.enterprisenetworkingplanet.com/netsp/article.php/3634596).
- Move back to an IPv4 network address to ensure HP Smart Update Manager properly finds the remote target server without any issues.
- HP Smart Update Manager can always be copied to the target servers and executed using the local installation method.

Technical support

Reference documentation

To download the ProLiant Firmware Maintenance and other CDs, see the SmartStart download website (http://www.hp.com/go/ssdownloads).

For general information on management products, refer to the ProLiant Essentials website (http://www.hp.com/servers/proliantessentials).

For information about support for updating SATA hard drives in a Modular Smart Array 20/50/60/70 storage enclosure connected to a ProLiant server using a Smart Array controller, see the HP StorageWorks Modular Smart Arrays website (http://www.hp.com/go/msa) for the support matrix.

For information about operating systems supported by ProLiant servers, refer to the operating system support matrices (http://www.hp.com/go/supportos).

For information about firmware support, refer to the ProLiant Firmware Maintenance CD Matrix (http://www.hp.com/servers/smartstart/supportmatrices).

Operating system information

For information about Microsoft® Windows® operating systems, refer to the Microsoft® website (http://www.microsoft.com).

For information about Linux operating systems, refer to one of the following websites:

- Red Hat Linux (http://www.redhat.com)
- SUSE LINUX (http://www.novell.com/linux)

HP contact information

For the name of the nearest HP authorized reseller:

- See the Contact HP worldwide (in English) webpage (http://welcome.hp.com/country/us/en/wwcontact.html).

For HP technical support:

- In the United States, for contact options see the Contact HP United States webpage (http://welcome.hp.com/country/us/en/contact_us.html). To contact HP by phone:
  - Call 1-800-HP-INVENT (1-800-474-6836). This service is available 24 hours a day, 7 days a week. For continuous quality improvement, calls may be recorded or monitored.
  - If you have purchased a Care Pack (service upgrade), call 1-800-633-3600. For more information about Care Packs, refer to the HP website (http://www.hp.com/hps).
- In other locations, see the Contact HP worldwide (in English) webpage (http://welcome.hp.com/country/us/en/wwcontact.html).

Acronyms and abbreviations

GUI

graphical user interface

HBA

host bus adapter

HPSUM

HP Smart Update Manager

I/O

input/output

iLO

Integrated Lights-Out

iLO 2

Integrated Lights-Out 2

NIC

network interface controller

POST

Power-On Self Test

PSP

ProLiant Support Pack

RBSU

ROM-Based Setup Utility

RILOE II

Remote Insight Lights-Out Edition II

SAN

storage area network

SAS

serial attached SCSI

SCSI

small computer system interface

SOAP

Simple Object Access Protocol

SSH

Secure Shell

SSL

Secure Sockets Layer

WMI

Windows Management Instrumentation

Index

A

adding groups 37
adding hosts 33
advanced topics 61
Allow Downgrades 28
Allow Rewrites 28
Allow Shared Devices 28
arguments 46
array controllers 8, 22
audience assumptions 5
authorized reseller 82

B

BladeSystem firmware 7
blocked HP Smart Update Manager, recovering from 75

C

command line arguments 46
command line examples 51
command line interface, using 46
command line syntax 46
command line tools 15
command syntax 46
component configuration, Windows 51
component selection pane 25
component status 22, 42
components, adding new 11
components, deploying 8, 15
components, installation 22, 32, 42
components, selecting to install on multiple hosts 42
configuring firewall settings 74, 75
controllers, array 8
credentials 32, 40

D

deleting groups 37
deleting hosts 33
deploying components 8, 15
deploying firmware and software simultaneously 61
deployment methods 8
deployment scenarios 15
deployment to multiple remote hosts 16
deployment, graphical 15, 16
deployment, offline 9
deployment, online 9
deployment, scripted 15, 16, 46
disaster recovery 70
Disaster Recovery, ROMPaq 70
documentation 82
double-byte characters 56, 78
downgrading firmware 28
download permission 19
drive key 8

E

editing groups 37
editing hosts 33
end user license agreement (EULA) 9
entering credentials 40
error code 52
error reports 56
EULA (end user license agreement) 9
examples 51

F

failed dependencies 46
Failed Dependencies screen 25
features, new 6
file encoding 56
firewall settings, configuring 74, 75
firmware and software deployment, simultaneous 61
Firmware Maintenance CD 5, 8, 9, 15
force install 28
format and rules, inut files 55

G

graphical deployment 15, 16
groups 32, 37
GUI, using for multiple-host installations 32

H

hard drive space 5

hard drives 11
host field 22, 42
hosts 32, 33, 40
HP Onboard Administrator for HP c-Class BladeSystem 8
HP Smart Update Manager GUI 17
HP Smart Update Manager overview 5
HP website 8, 11, 17, 82
hpsum_detail_log.txt log 30
hpsum_log.txt log 30

I

input files 54, 55
installation host 20
installation log 30
installation options 22, 25, 28
Installation Progress 28
installation status 30, 44
installation, selecting components for multiple hosts 42
installing multiple hosts using GUI 32
introduction 5
Inventory Progress screen 32
IPv6 network configurations 62
IPv6, troubleshooting 79, 80

K

keyboard support 17

L

Lights-Out Management ROM flash components 8
Lights-Out Management ROMs 8, 71
limitations, Linux IPv6 environment 69
limitations, Windows Server IPv6 environment 67
Linux IPv6 environment 67
Linux remote functionality, recovering 74
Linux smart components, return codes 53
local host, graphical deployment 15, 16
local host, scripted deployment 15, 16
location, to check for updates 17
log files 30

M

managing groups 37
managing hosts 33
memory 5
minimum requirements 5
multiple hosts 32, 42
multiple remote hosts, deployment 15, 16
multiple-host installations 32

N

new features 6
NIC firmware 8, 22, 28

O

offline deployment 9
Onboard Administrator 8
online deployment 9
operating systems 82
options, deployment 8
options, installation 22, 25, 28
options, reboot 25
overview, Firmware Maintenance CD 5
overview, HP Smart Update Manager 5
overwriting firmware 28
format and rules, inut files 55

P

packages 5
parameters 46, 56
ports, enabling in HP Smart Update Manager 75
ProLiant Essentials Foundation Pack 8
proxy settings 17

R

Reboot Delay 25
Reboot Options 25
reboot settings 22, 25
recovering from a failed option ROM upgrade 71
recovering from a failed system ROM upgrade 70
redundant ROM 70
references 82
remote functionality, recovering 74
remote hosts 16, 32
remote hosts, deployment to multiple 16
requirements, minimum 5
return codes 52
return codes, Linux smart components 53
return codes, Windows smart components 53
rewriting firmware 28
ROM recovery, redundant 70
ROM redundancy 70
ROM upgrade behavior 28
ROM upgrade, recovering from failed option 71
ROM upgrade, recovering from failed system 70

ROM, array controller 71
ROM, Lights-Out management 8, 71
ROM, storage 71
ROMPaq Disaster Recovery 70

S

SAS hard drive 8
scenarios, deployment 15
scripted deployment 16, 46
selecting an installation host 20
selecting components to install 22, 42
selections for single host 42, 44
server host pane 42
server virtualization detection and support 62
settings, reboot 25
shared storage, updating ROMs for 28
SLES (SUSE Linux Enterprise Server) 78
software and firmware deployment, simultaneous 61
source selections 17
status, component 22, 42
status, installation 30, 44
status, system 42
support 82
SUSE Linux Enterprise Server (SLES) 78
syntax 46
system status field 22, 24, 42

T

technical support 82
TPM (Trusted Platform Module) 5, 11, 13, 40
trace logs 72
troubleshooting 70
Trusted Platform Module (TPM) 5, 11, 13, 40

U

USB drive key 8, 9, 11
using the GUI 32

V

View Failed Dependencies 25

W

web, pulling from 17
website, HP 17, 82
Windows Management Instrumentation (WMI) 5
Windows Server 2003 IPv6 environment 62
Windows Server 2008 IPv6 environment 65
Windows smart components, return codes 53
WMI (Windows Management Instrumentation) 5