

HP ProLiant Firmware Maintenance CD User Guide



Part Number 447788-007
February 2009 (Seventh 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
Obtaining the HP ProLiant Firmware Maintenance CD.....	6
Deployment options	6
Online deployment	7
Offline deployment	7
HP USB key utility	8
Deployment of components not on Firmware Maintenance CD	8
Trusted Platform Module.....	8
TPM scenarios.....	9
Firmware Maintenance CD powered by HP Smart Update Manager	10
Deployment scenarios	10
Graphical deployment on a local host.....	11
Scripted deployment on a local host	11
Deployment to multiple remote hosts.....	11
Keyboard support.....	12
First time execution	12
Selecting an installation host for the first time	14
Selecting components to install for the first time	15
Local host installations using the GUI	15
Selecting an installation host	16
Selecting components to install	17
Viewing the installation results.....	25
Multiple-host installations using the GUI.....	27
Selecting remote hosts or groups	27
Selecting components to install on multiple hosts.....	36
Viewing the installation results for multiple hosts	38
Scripted deployment	40
Command line interface	40
Command line syntax	40
Command line arguments	40
Component configuration for Windows components only	44
Command line examples	44
HP Smart Update Manager return codes	45
Advanced topics.....	48
Deploying firmware and software simultaneously.....	48
Server virtualization detection and support	49
Configuring IPv6 networks with HP Smart Update Manager.....	49
Configuring IPv6 for Windows Server 2003	49
Configuring IPv6 for Windows Server 2008	52
Configuring IPv6 for Linux.....	54
Troubleshooting	57

Recovering from a failed ROM upgrade.....	57
Recovering from a failed system ROM upgrade.....	57
Recovering from a failed option ROM upgrade.....	58
Recovering from an installation failure.....	59
Collecting trace directories.....	59
Recovering from a loss of Linux remote functionality.....	59
Configuring firewall settings.....	59
Recovering from a blocked program on Microsoft Windows.....	60
Configuring Windows firewall settings.....	60
Enabling ports in HP Smart Update Manager.....	60
Recovering from operating system limitations when using a Japanese character set.....	62
Displaying the user-specified reboot message using a Japanese character set when running on a Linux operating system.....	62
Rebooting with the user-specified reboot message using a Japanese character set when running on a Windows operating system.....	62
Recovering from Fatal Error - application will exit message.....	63
Running in a directory path containing double-byte characters.....	63
Recovering from a missing reboot message when running on SUSE LINUX Enterprise Server 9.....	63
Running HP Smart Update Manager on SUSE LINUX Enterprise Server 9.....	63
Recovering a lost HP Smart Update Manager connection.....	63
Mounting the Firmware Maintenance CD on virtual media.....	63
Troubleshooting HP Smart Update Manager in IPv6 networks.....	64
Troubleshooting HP Smart Update Manager in IPv6 Windows Server 2003 environment.....	64
Troubleshooting HP Smart Update Manager in IPv6 Windows Server 2008 environment.....	65
Troubleshooting HP Smart Update Manager in IPv6 Red Hat and Novell SUSE-based Linux environments.....	65
Technical support.....	66
Reference documentation.....	66
Operating system information.....	66
HP contact information.....	66
Acronyms and abbreviations.....	67
Index.....	69

Introduction

HP ProLiant Firmware Maintenance CD overview

The HP ProLiant Firmware Maintenance CD provides a collection of firmware for your ProLiant servers and options. Beginning with the Firmware Maintenance CD 7.50, the HP Smart Update Manager utility enables you to deploy firmware components from a single, easy-to-use interface that is supported in both Microsoft® Windows® and Linux environments. This utility enables legacy support of existing firmware components while simplifying the firmware deployment process. The CD also provides installation logic and version control that check for dependencies, installing only the correct updates for optimal system configuration.

To deploy the Firmware Maintenance CD contents, see "Online deployment (on page 7)" and "Offline deployment (on page 7)."



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.

Minimum requirements

To successfully deploy HP Smart Update Manager on target systems based on a Microsoft® 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



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

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	<p>HP Smart Update Manager supports online deployments of all ROM flash components for both Windows® and Linux including:</p> <ul style="list-style-type: none"> • HP Onboard Administrator for HP c-Class BladeSystem • System hard-drive (SAS and SATA) • Array-controller • Lights-Out Management ROM flash components

NOTE: The Onboard Administrator is 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	<p>HP Smart Update Manager supports offline deployments of all ROM flash components including:</p> <ul style="list-style-type: none"> • 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`
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 15)" or "Multiple-host installations using the GUI (on page 27)."

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 15)" or "Multiple-host installations using the GUI (on page 27)."

HP USB key utility

The HP USB Key Utility is a Windows® application that 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.

To make a bootable CD fro Windows users:

1. Download the USB Key Utility Smart Component to a directory on your hard drive, and then switch to that directory. The downloaded file is a self-extracting executable with a filename based on the USB Key Utility Smart Component Number.
2. From that drive and directory, execute the downloaded file.

Deployment of components not on Firmware Maintenance CD

If you have components not on the Firmware Maintenance CD, you can add new components to HP Smart Update Manager. To deploy software and firmware components 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 8), or copy the \compaq\swpackages directory to the hard dive, and then remove the read-only bit.

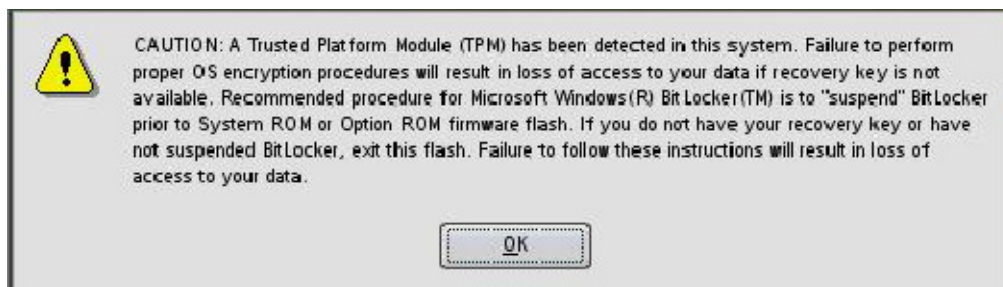
Trusted Platform Module

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.



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
- Red Hat Enterprise Linux 4
- Red Hat Enterprise Linux 5
- SUSE Linux Enterprise Server 9
- SUSE Linux Enterprise Server 10 x86

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

Scenario	Description
Graphical deployment on a local host	Use this scenario when you: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• Are not familiar with command line tools.• Are deploying components on one or more remote hosts.• Do not require scripting.

Scenario	Description
Scripted deployment to a remote host	Use this scenario when you: <ul style="list-style-type: none"> • Are familiar with command line tools. • Are deploying components on one or more hosts. • Must perform a customized, scripted deployment to one or more host systems.

Graphical deployment on a local host

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

To deploy components to a local host using the 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 and are available in the same directory as the HP Smart Update Manager.

For information about performing the deployment using the GUI, see "Local host installations using the GUI (on page 15)."

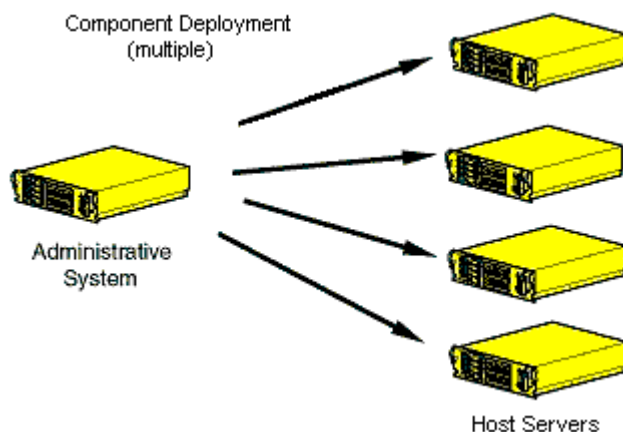
Scripted deployment on a local host

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 and are available in the same directory as the HP Smart Update Manager.
3. Create a script to customize the deployment. See "Scripted deployment (on page 40)" 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, 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 and are available in the same directory as the HP Smart Update Manager.

For more information about performing the deployment using the graphical interface, see "Multiple-host installations using the GUI (on page 27)."

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 and are available in the same directory as the HP Smart Update Manager.
3. Create a script to customize the deployment. For more information, see "Scripted deployment (on page 40)."
4. Execute the script.

Keyboard support

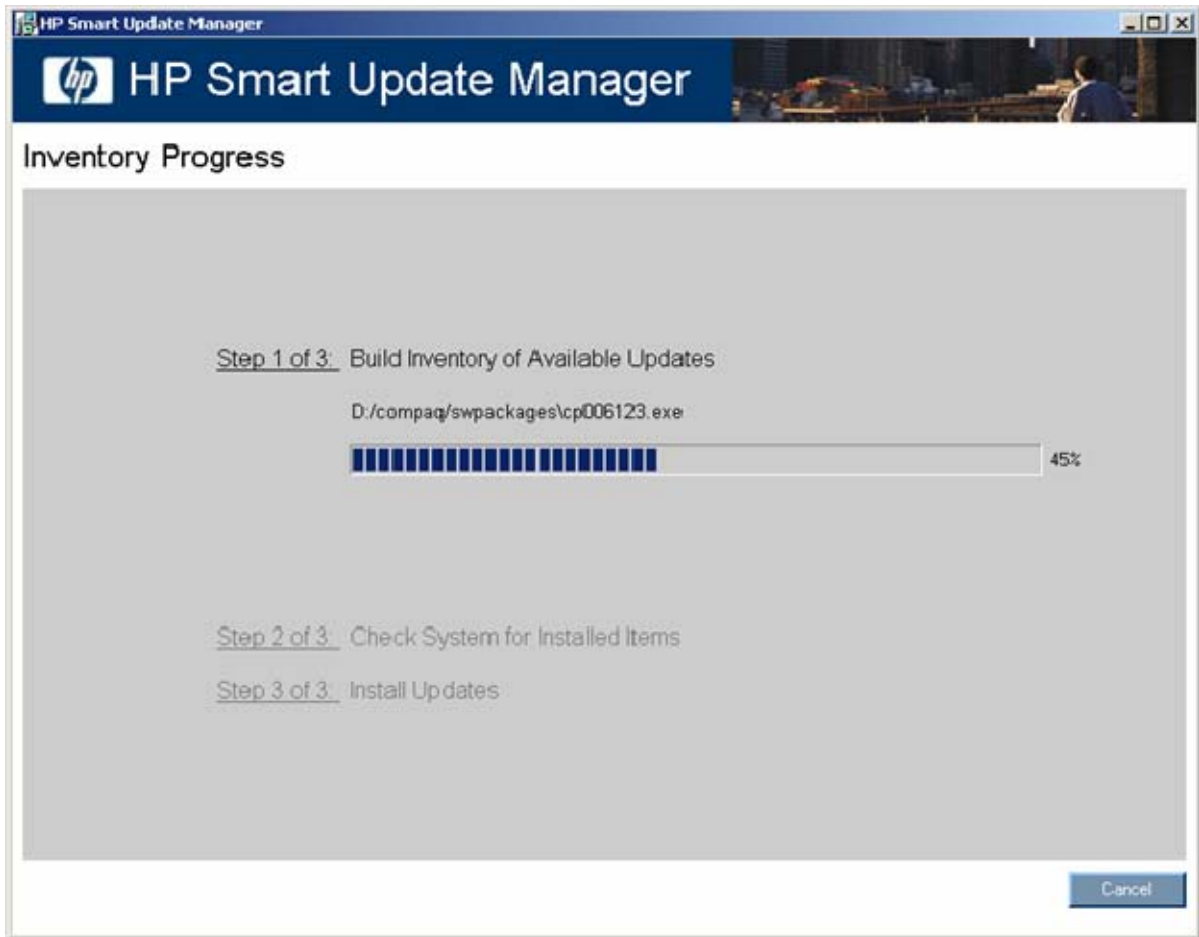
The HP Smart Update Manager graphical user interface has accelerator keys that enable you to manage and control common tasks quickly. To ensure proper navigation, the following are a few reminders.

- 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.

First time execution

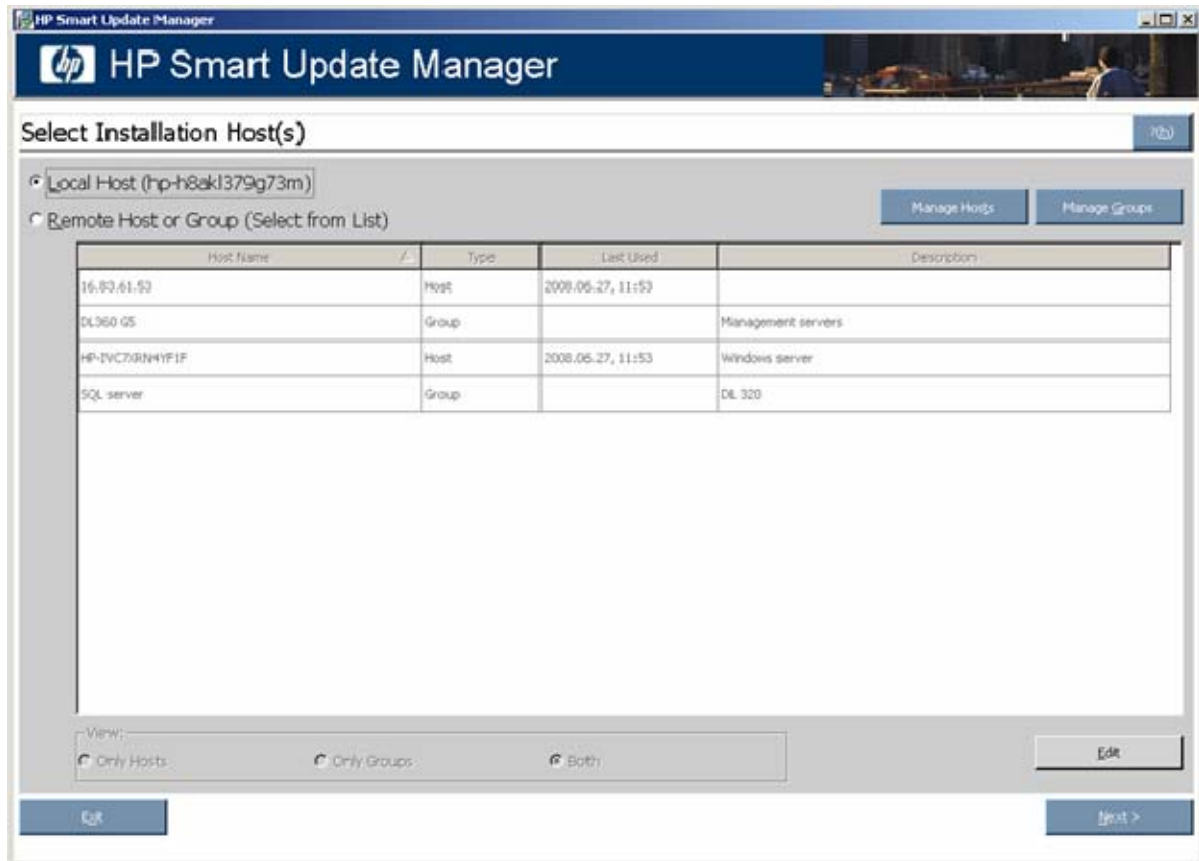
The HP Smart Update Manager provides an easy-to-use graphical interface that enables you to deploy and maintain firmware components. To access the HP Smart Update Manager, see "Deployment Options (on page 6)."

The Inventory Progress screen appears while the HP Smart Update Manager builds an inventory of available updates. After checking the system for installed items, HP Smart Update Manager installs the updates.



Selecting an installation host for the first time

The Select Installation Host(s) screen appears when the inventory process ("First time execution" on page 12) is complete.

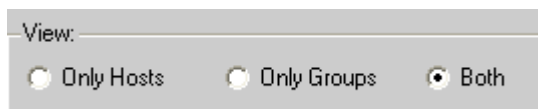


The Select Installation Host(s) screen enables you to choose a host for component installation. By default, the first time you run HP Smart Update Manager on a particular system, the only host available is the local host. However, you can also select remote hosts as your targets. For more information about using the graphical interface for multiple remote deployments, see "Multiple-host installations using the GUI (on page 27)."

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:

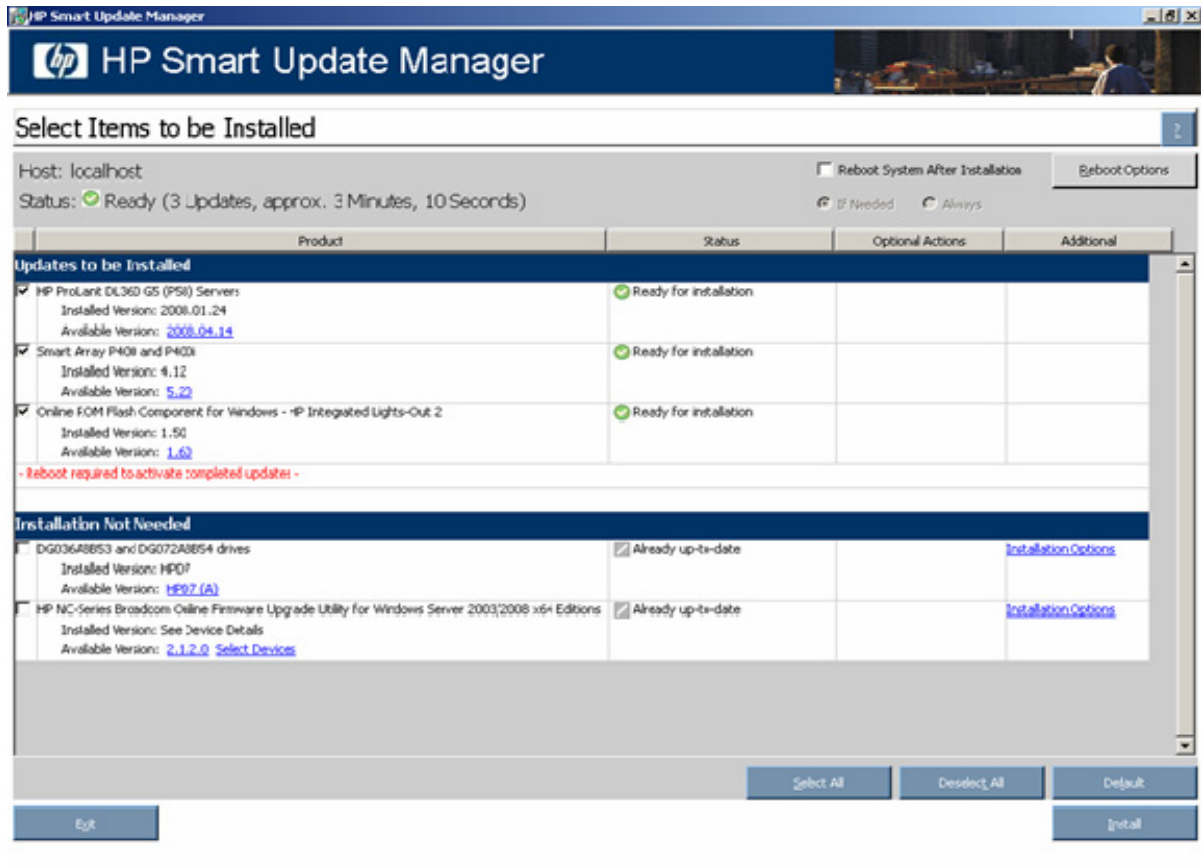
- Manage Hosts—Enables you to add, edit, and delete hosts.

- 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. The Select Items to be Installed screen appears.

Selecting components to install for the first time

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.



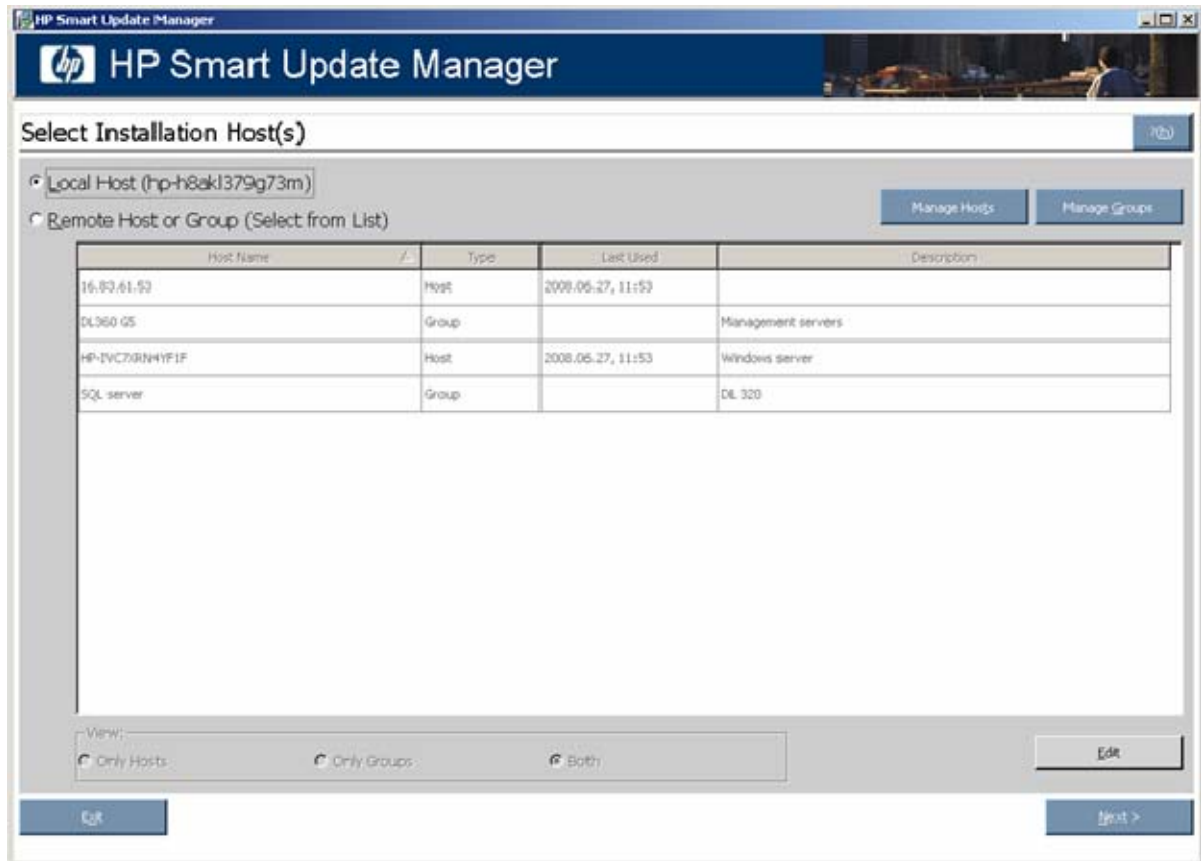
For more information about the Select Items to be Installed screen and its sections, see "Selecting components to install (on page 17)."

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 easily deploy components on a local host by using the Smart Update Manager GUI.

Selecting an installation host

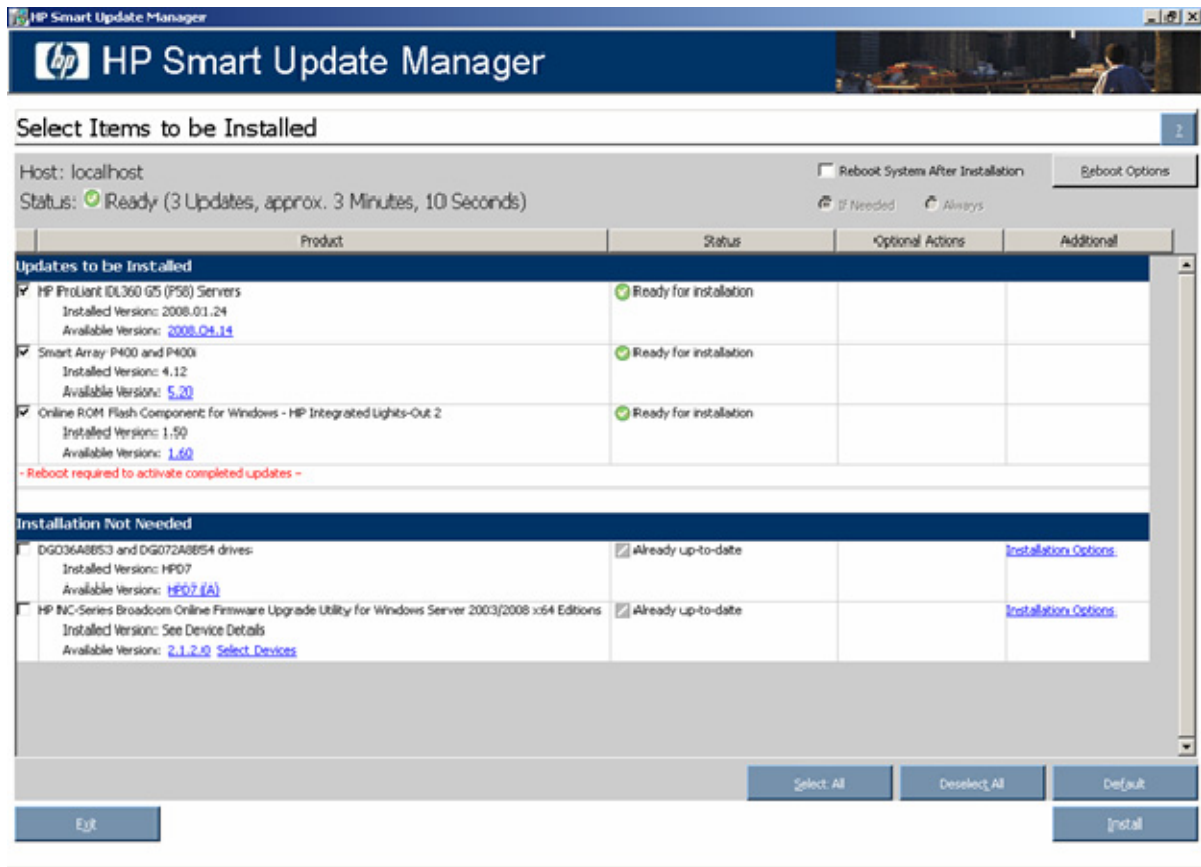
To continue with the deployment process using a local host, select a host from the Select Installation Host(s) screen, and click **Next**.



The Discovery Progress screen appears while the HP Smart Update Manager checks the local system to see which items are already installed.

Selecting components to install

When the discovery process ("Selecting an installation host" on page 16) is complete, the Select Items to be Installed screen appears.



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.
- 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—Deselects 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.

NOTE: HP Smart Update Manager does not support supplemental update for self-discovered components. If you need to add additional components to the Firmware CD, the Firmware CD must be migrated to a USB key and the new components added to the \compaq\swpackages directory. For information on how to create the USB key version of the Firmware CD, see HP USB key utility (on page 8).

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.

Deselected By User			
<input type="checkbox"/>	HP Insight Management Agents for Windows Server 2003 Installed Version: None Available Version: 7.80.0.0	<input checked="" type="checkbox"/> Deselected by User	
<input type="checkbox"/>	HP Virus Throttle for Windows Server 2003 Installed Version: None Available Version: 8.60.0.0	<input checked="" type="checkbox"/> Deselected by User	
<input type="checkbox"/>	HP Version Control Agent for Windows Installed Version: None Available Version: 2.1.8.780	<input checked="" type="checkbox"/> Deselected by User	

- 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**.

Installation Not Needed			
<input type="checkbox"/>	Smart Array P600 Installed Version: 1.52 Available Version: 1.52 (A)	<input checked="" type="checkbox"/> Already up-to-date	Installation Options
<input type="checkbox"/>	HP ProLiant DL380 G4 (P51) Installed Version: 2006.04.26 Available Version: 2006.04.26 (B)	<input checked="" type="checkbox"/> Already up-to-date	Installation Options
<input type="checkbox"/>	HP Network Configuration Utility for Windows Server 2003 Installed Version: 8.70.0.0 Available Versions: <input type="radio"/> 8.70.0.0 <input type="radio"/> 8.60.0.0	<input checked="" type="checkbox"/> Already up-to-date	Installation Options

- Excluded by Filtering—The components in this section were excluded through your filtering options. You can use the Select Bundle Filter option to change the exclusion on a single target. For multiple targets, this must be repeated on each additional target.

Excluded by Filtering			
<input type="checkbox"/>	Smart Array P600 Installed Version: 1.52 Available Version: 1.52 (A)	<input checked="" type="checkbox"/> Deselected by User	
<input type="checkbox"/>	Smart Array 641/642 Installed Version: 2.76 Available Version: 2.80 (A)	<input checked="" type="checkbox"/> Deselected by User	
<input type="checkbox"/>	HP ProLiant DL380 G4 (P51) Installed Version: 2006.04.26 Available Version: 2006.04.26 (B)	<input checked="" type="checkbox"/> Deselected by User	

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

Updates to be Installed			
<input checked="" type="checkbox"/>	Smart Array 641/642 Installed Version: 2.76 Available Version: 2.80 (A)	<input checked="" type="checkbox"/> Ready for installation	
<input checked="" type="checkbox"/>	HP Virus Throttle for Windows Server 2003 Installed Version: None Available Version: 8.80.0.0	<input checked="" type="checkbox"/> Ready for installation	
<input checked="" type="checkbox"/>	HP Insight Management Agents for Windows Server 2003 Installed Version: None Available Versions: 7.90.0.0 7.80.0.0	<input type="checkbox"/> Failed Dependencies View Failed Dependencies	<input checked="" type="checkbox"/> Configurable Configure Now

- 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.

Optional Updates			
<input type="checkbox"/>	HP Insight Management WBEM Providers Installed Version: None Available Version: 2.1.0.0		

- 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.


No Device Driver Installed			
<input type="checkbox"/>	HP Integrated Lights-Out 2 Installed Version: None Available Version: 1.43	<input checked="" type="checkbox"/> No supported devices	

Status field

Status: None Selected

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
<input checked="" type="checkbox"/>	Ready	All selected components are ready to be installed.
<input checked="" type="checkbox"/>	Already up-to-date	No component installation is required.
<input checked="" type="checkbox"/>	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.

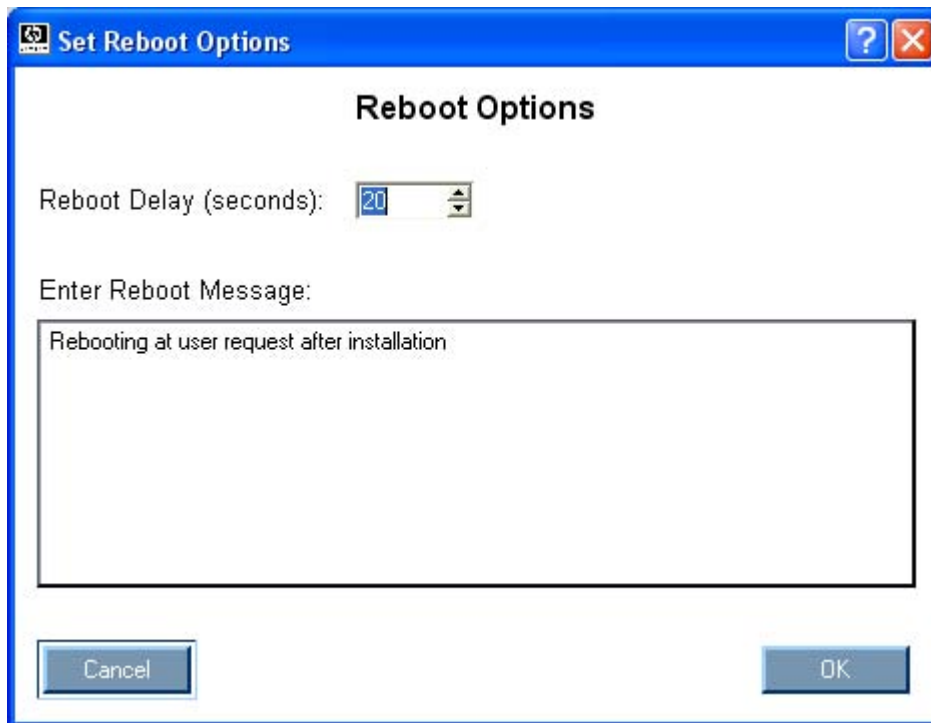


To instruct the system to reboot after updates are installed:

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.

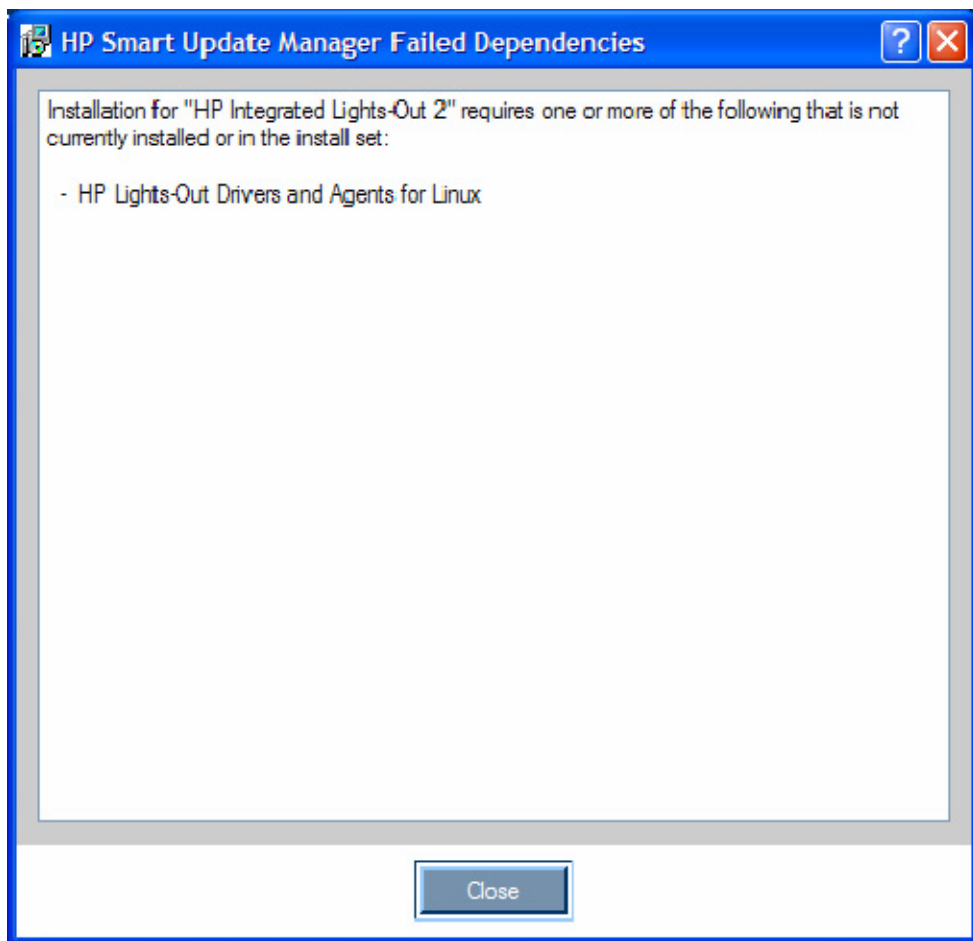
The component selection pane is divided into the following columns:

- **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 .

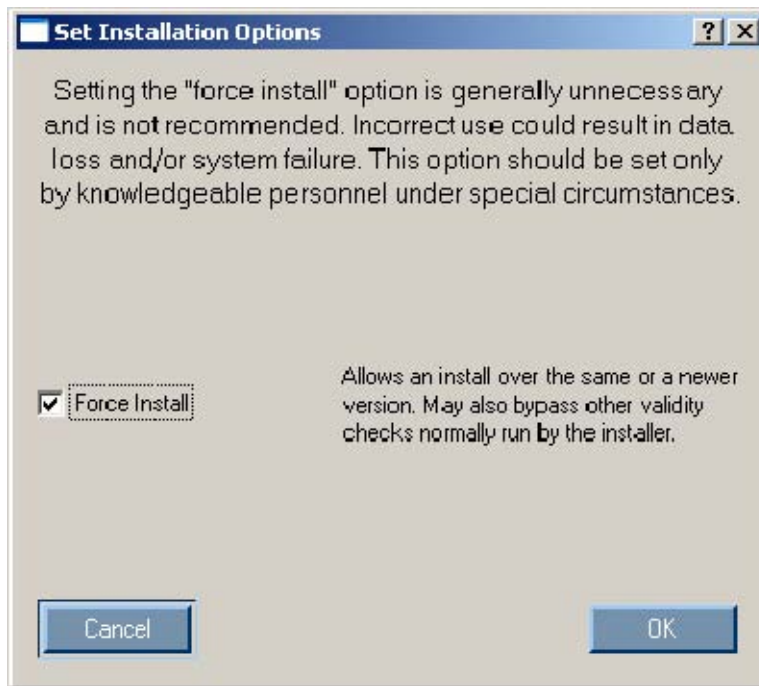
- **Optional Actions**—Reserved for future use.
- **Additional**—Contains the installation options and additional information for the components.

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.



- 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.



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.

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.

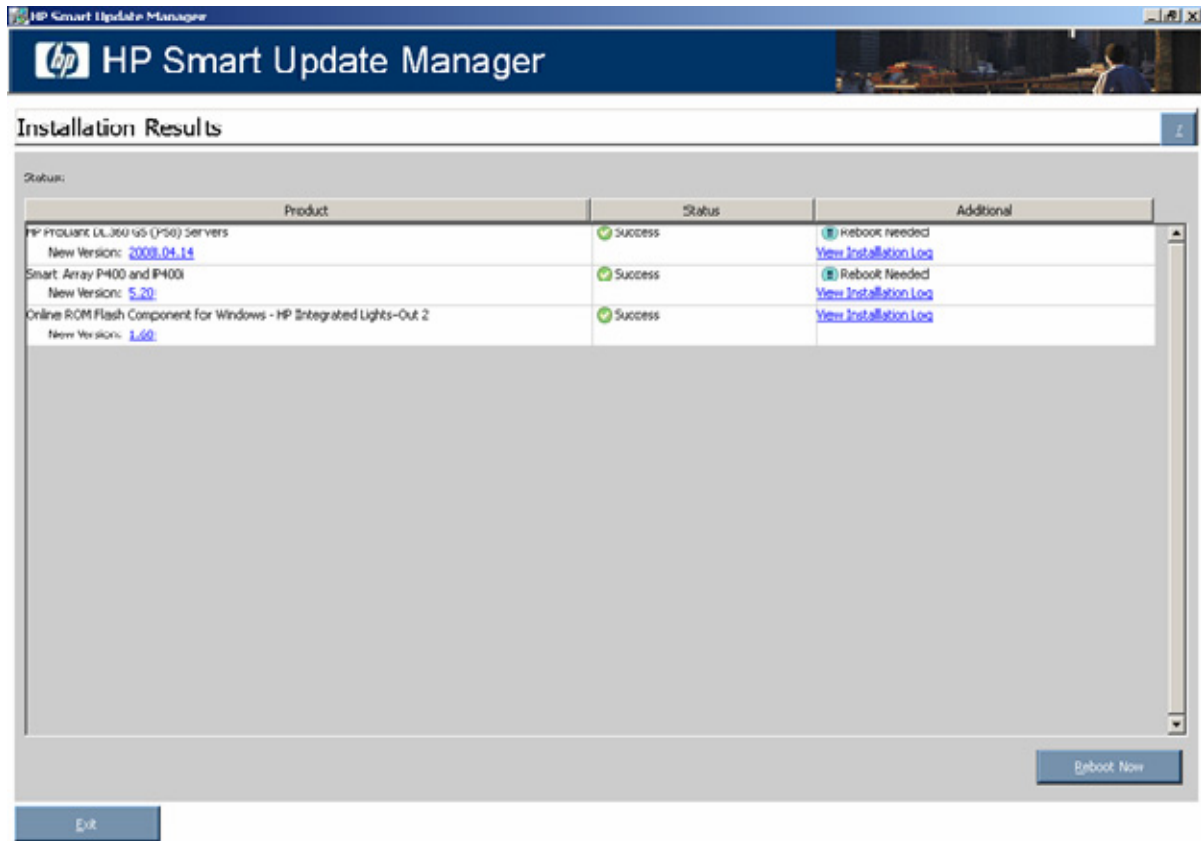
	Default	Allow downgrades	Allow rewrites
Firmware upgrade v3.05	No change	3.05	3.10
Firmware upgrade v3.10	No change	No change	3.10

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:

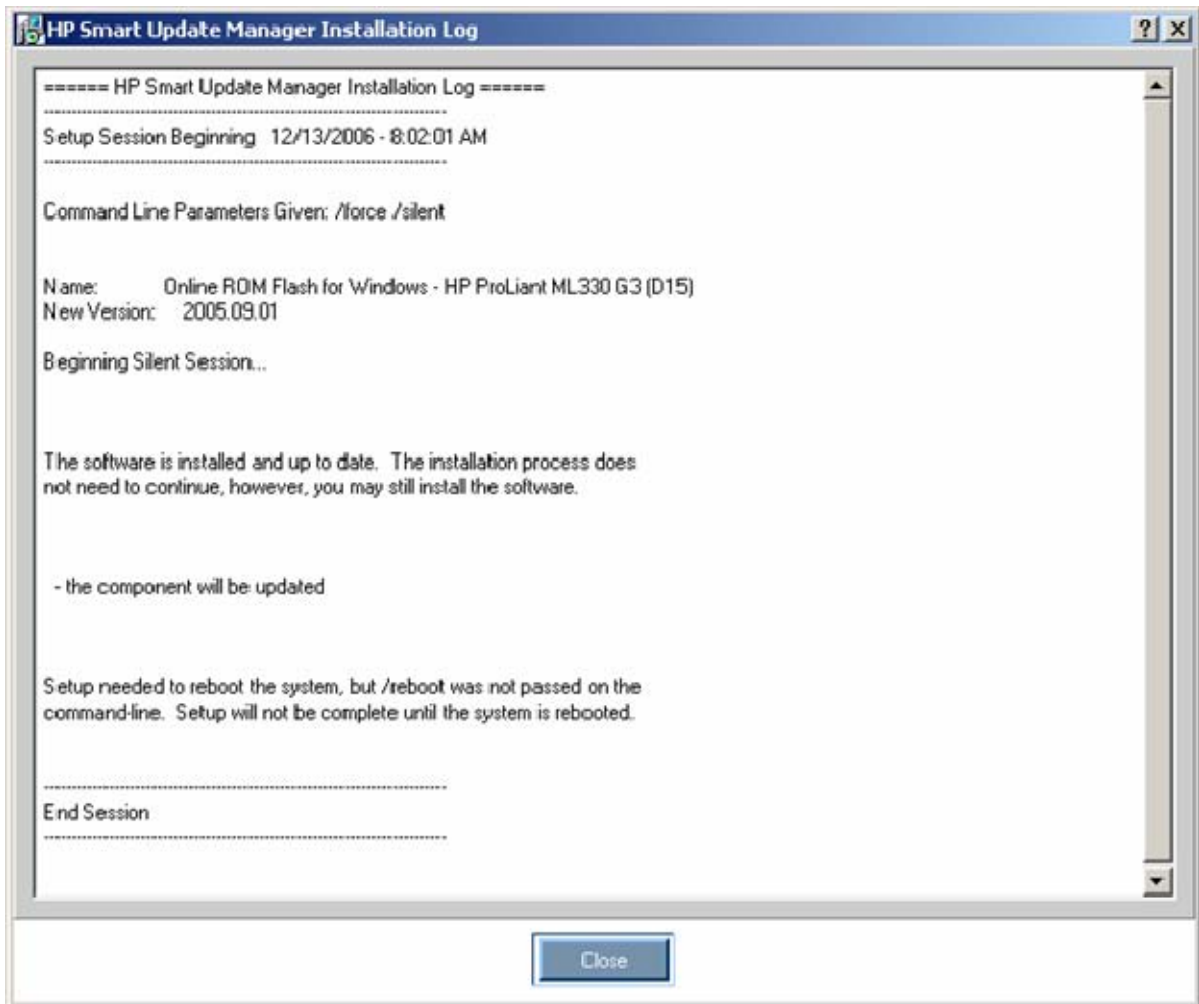
- **Product**—Specifies the name of the installed component. To see the component version history, click the version number.
- **Status**—Specifies the installation status of the component.

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®, 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, 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.

Multiple-host installations using the GUI

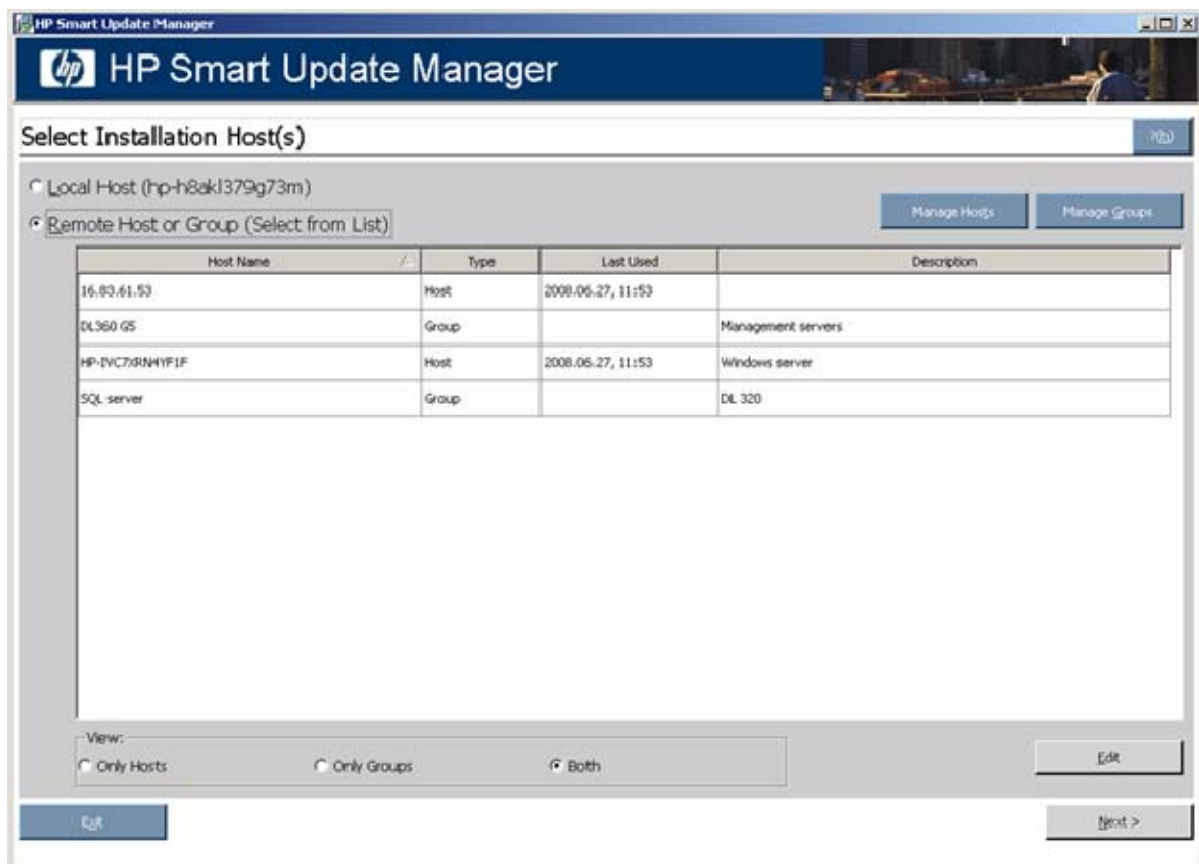
HP Smart Update Manager provides an easy-to-use graphical interface that enables you to deploy and maintain firmware components. To access HP Smart Update Manager, see "Deployment options (on page 6)."

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. Hosts include servers, Onboard Administrators, iLO, and iLO 2.

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 28)." To add groups, see "Managing groups (on page 31)."

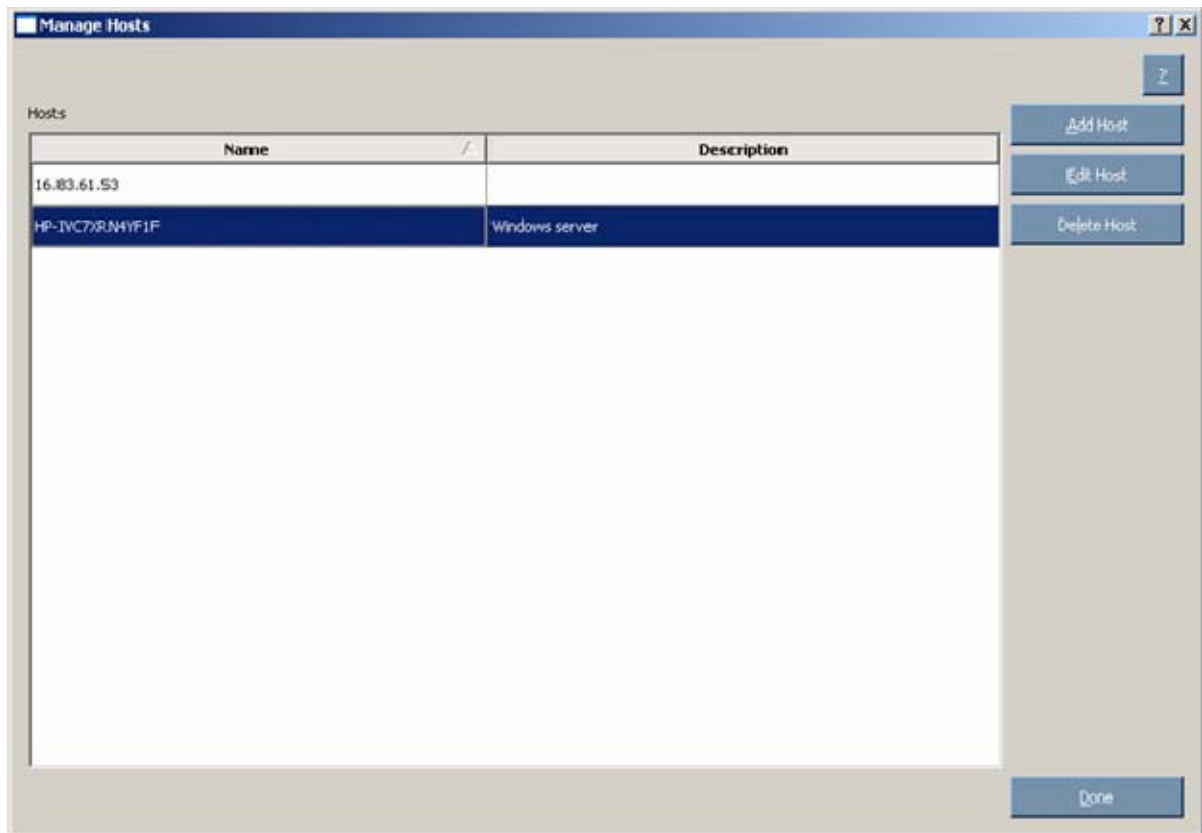
To continue with the deployment process:

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 34).
4. Click **OK** to proceed, as described in [Selecting components to install on multiple hosts](#) (on page 36).
5. When the installation is complete, the Installations results for multiple hosts screen ("[Viewing the installation results for multiple hosts](#)" on page 38) appears.

Managing hosts

To add, edit, or delete hosts, click the **Manage Hosts** button. The Manage Hosts screen appears. Hosts include servers, Onboard Administrators, iLO, and iLO 2.

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.



To add a host:

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

The screenshot shows the 'New Host' dialog box with the following fields and options:

- Add a Host by DNS Name
Host DNS Name:
- Add a Single Host by IP
Host IP: IP Format: IPv4 IPv6
- Add a Range of Hosts by IP
Starting IP:
Ending IP:
- Description:

Buttons: Cancel, OK

2. Select the method to add a host from the following:
 - o Enter the DNS name of the host you want to add.
 - o Enter the IP address of the host you want to add.
 - o 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.

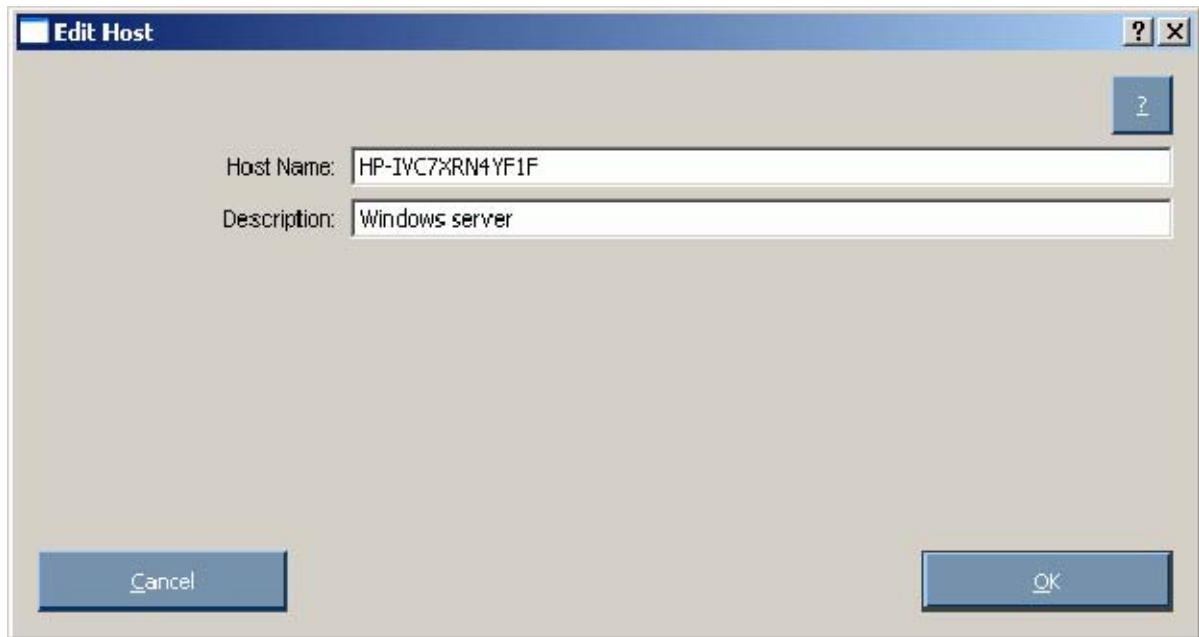
NOTE: When adding hosts using either IP address option, you can select from the IP format options: IPv4 or IPv6. The IPv4 format is the default option since it is the current Internet protocol. The IPv6 format is the next generation Internet protocol.

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.

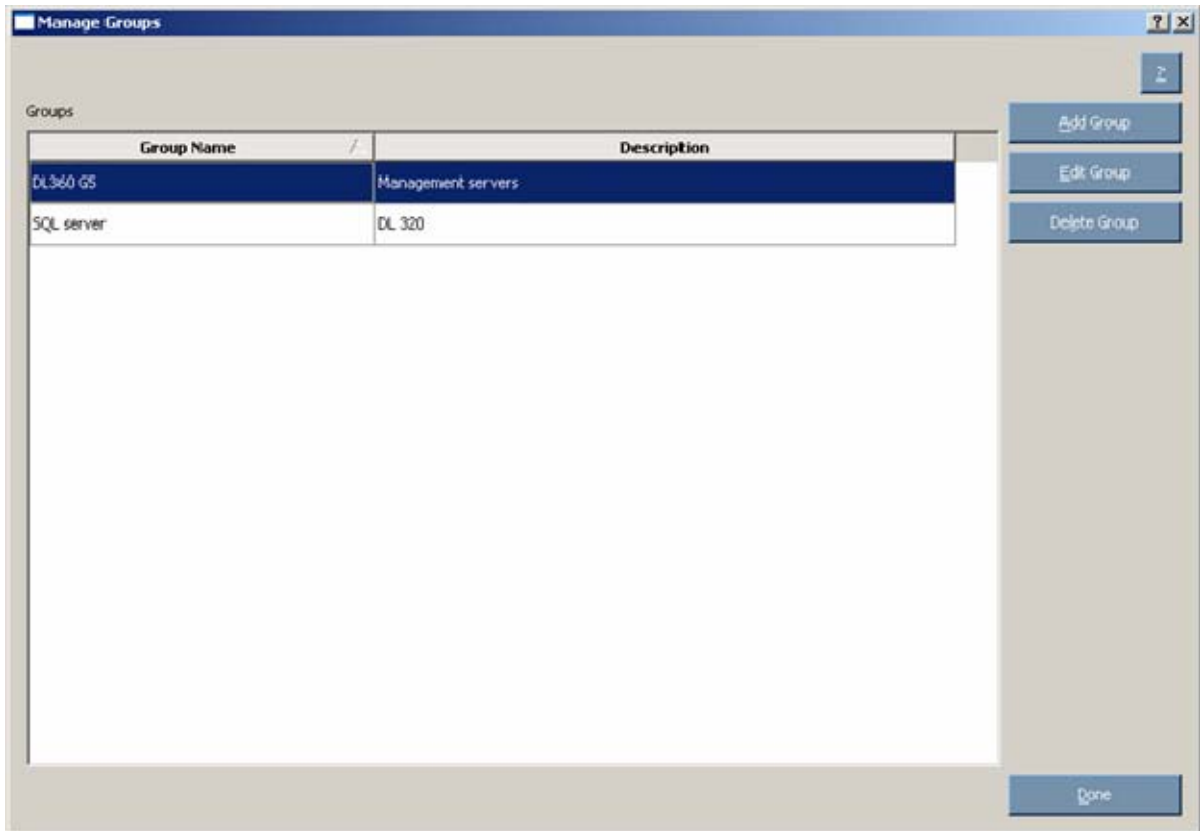
3. Click **OK**.

To delete a host:

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

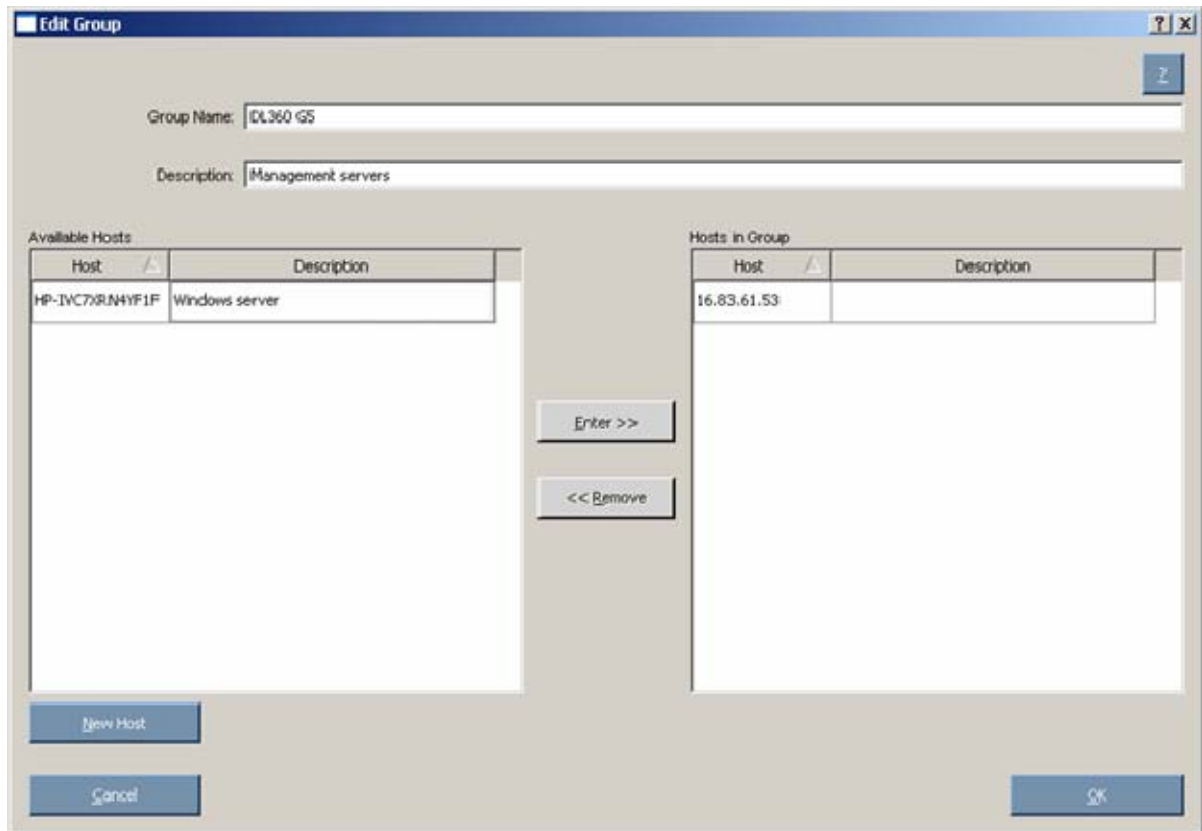
Managing groups

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.

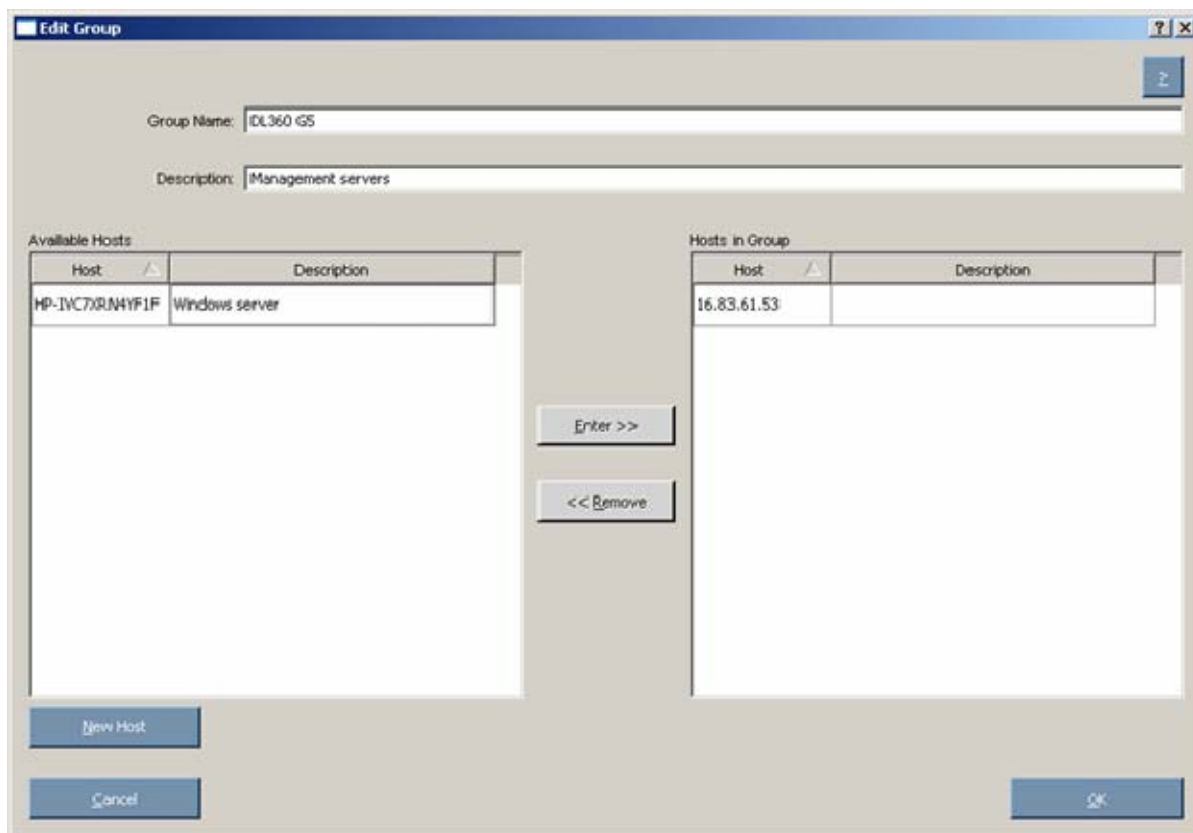


2. Enter a group name.
3. Enter an optional user-defined description given to the group to be added.
4. Select the hosts to be added to the group from the Available Hosts pane. You can add new hosts from this screen by clicking the **New Host** button. For more information on adding hosts, see "Managing hosts (on page 28)."
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.



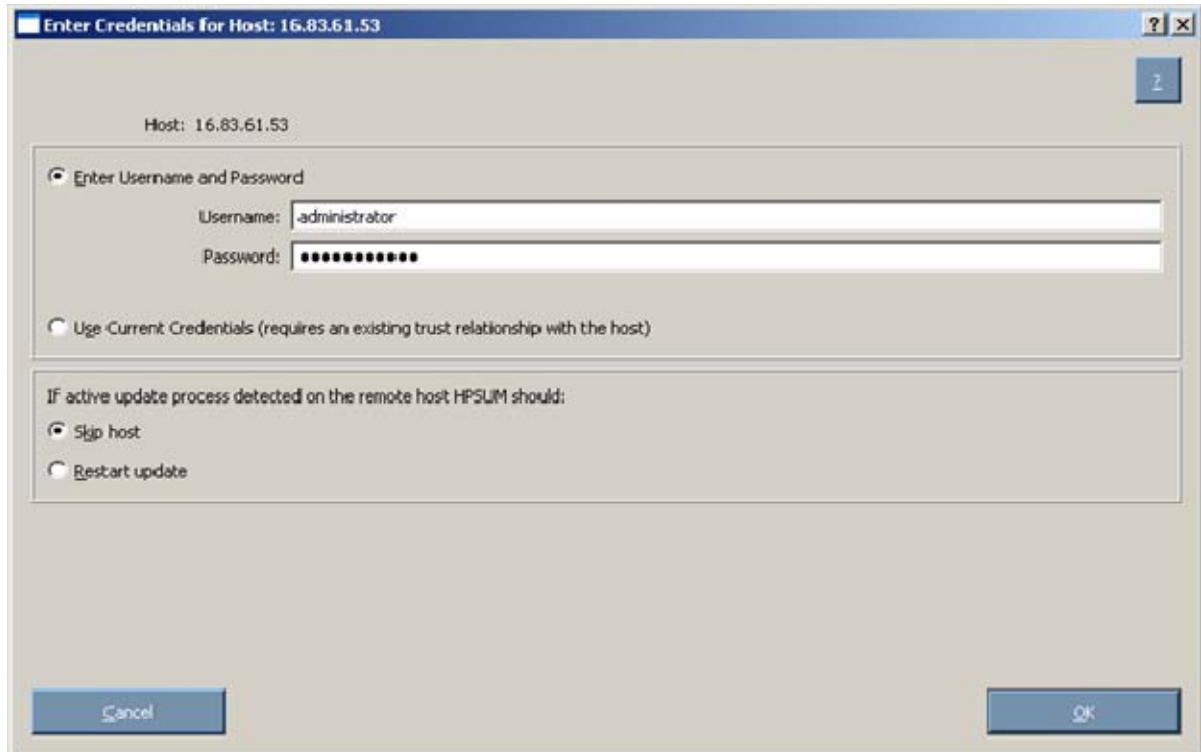
2. Edit the group name as needed.
3. Edit the optional user-defined description given to the host as needed.
4. Click the **Enter** and **Remove** buttons to add or remove hosts as needed.
5. Click **OK**.

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.



The screenshot shows a dialog box titled "Enter Credentials for Host: 16.83.61.53". The host IP address "16.83.61.53" is displayed at the top. Below this, there are two main sections. The first section is titled "Enter Username and Password" and is selected with a radio button. It contains two input fields: "Username:" with the text "administrator" and "Password:" with a series of black dots. The second section is titled "Use Current Credentials (requires an existing trust relationship with the host)" and is not selected. Below this, there is a section titled "IF active update process detected on the remote host HPSUM should:". It contains two radio buttons: "Skip host" (selected) and "Restart update". At the bottom of the dialog, there are two buttons: "Cancel" on the left and "OK" on the right.

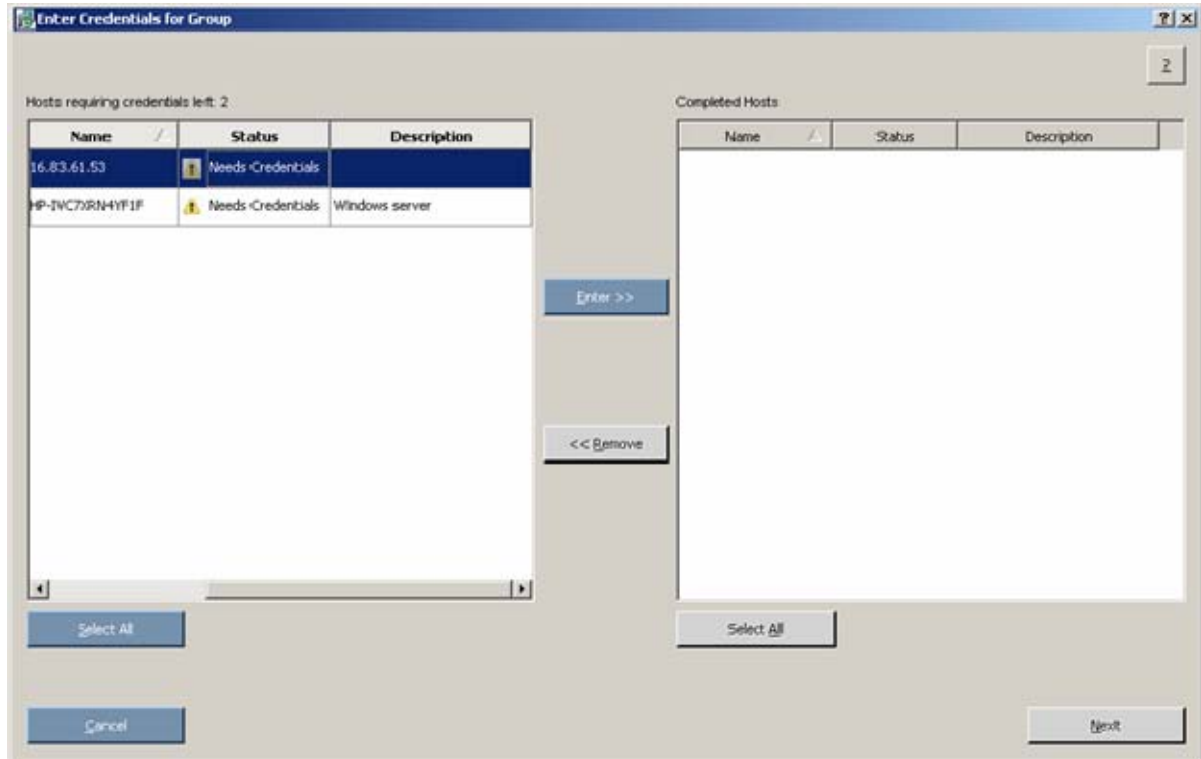
To enter the credentials for the host, choose one of the following:

- 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.

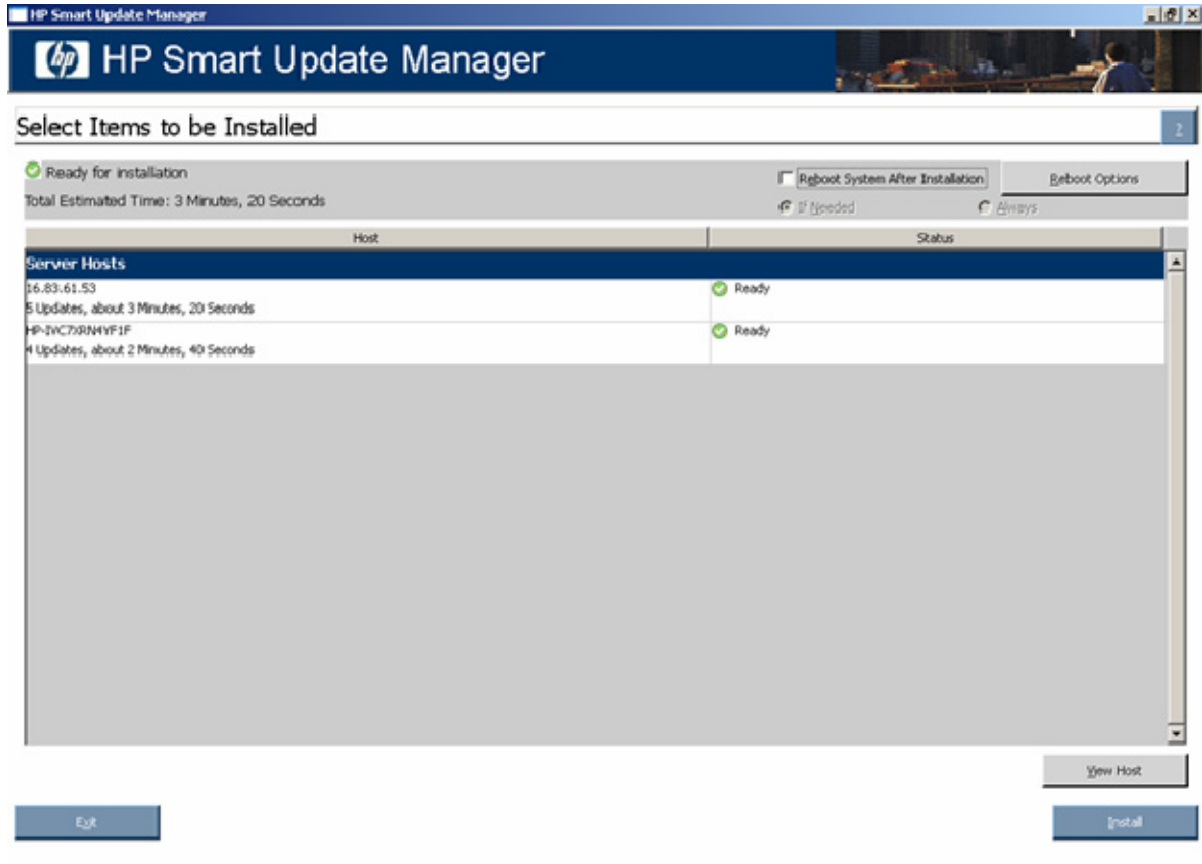
To enter the credentials for the host:

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 8).

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:

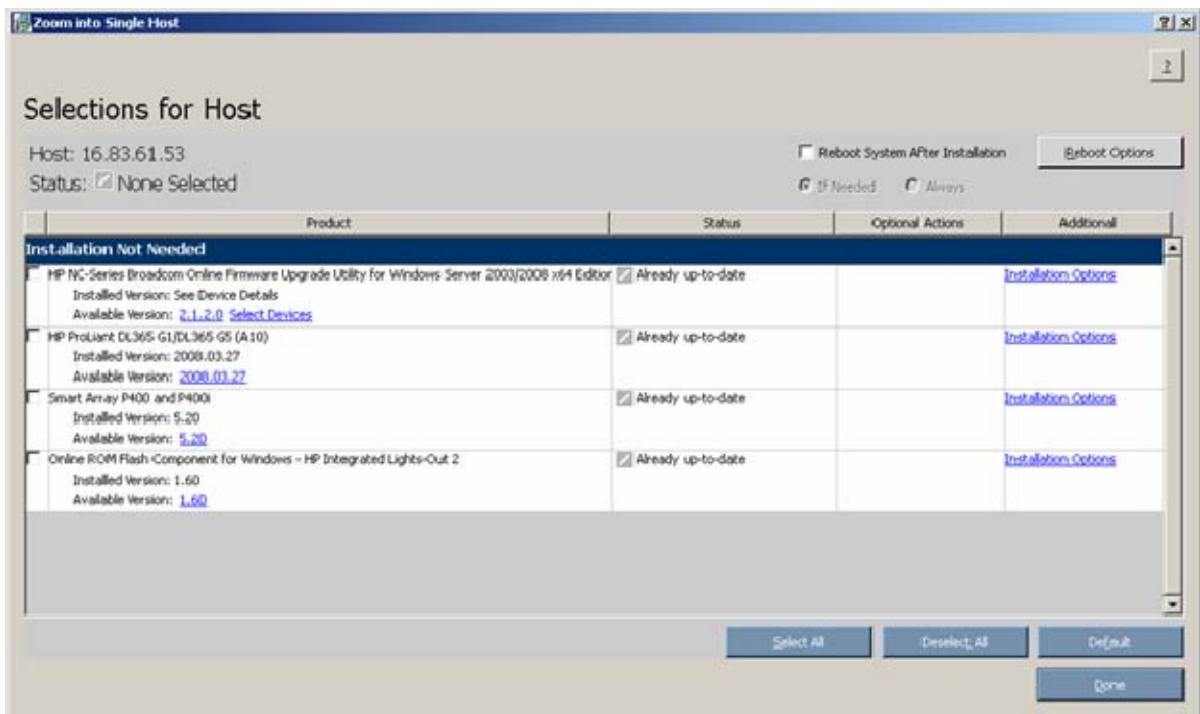
- Host—Specifies the name of the system, number of updates available, and the estimated time for the installation.
- Status—Specifies the status of the host.

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.

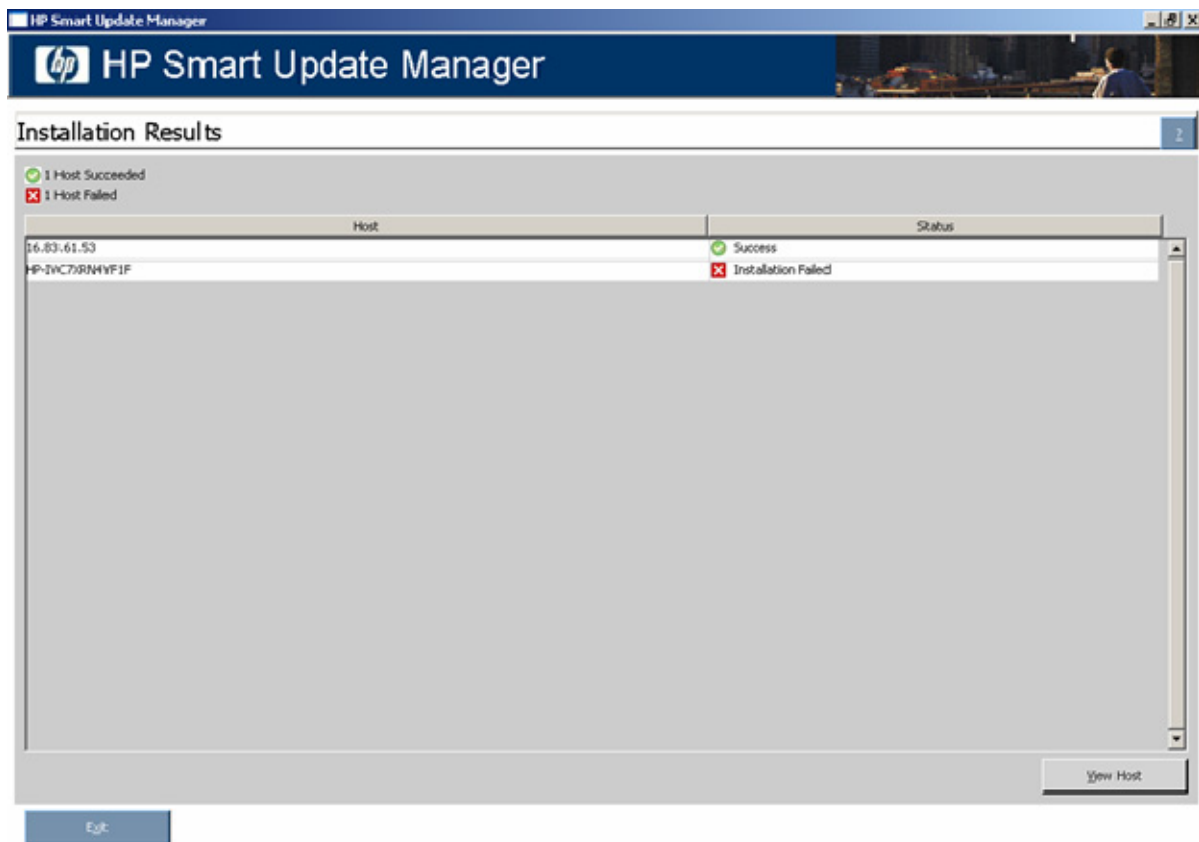


To set single-host selections, proceed as described in "Selecting Components to Install (on page 17)."

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:

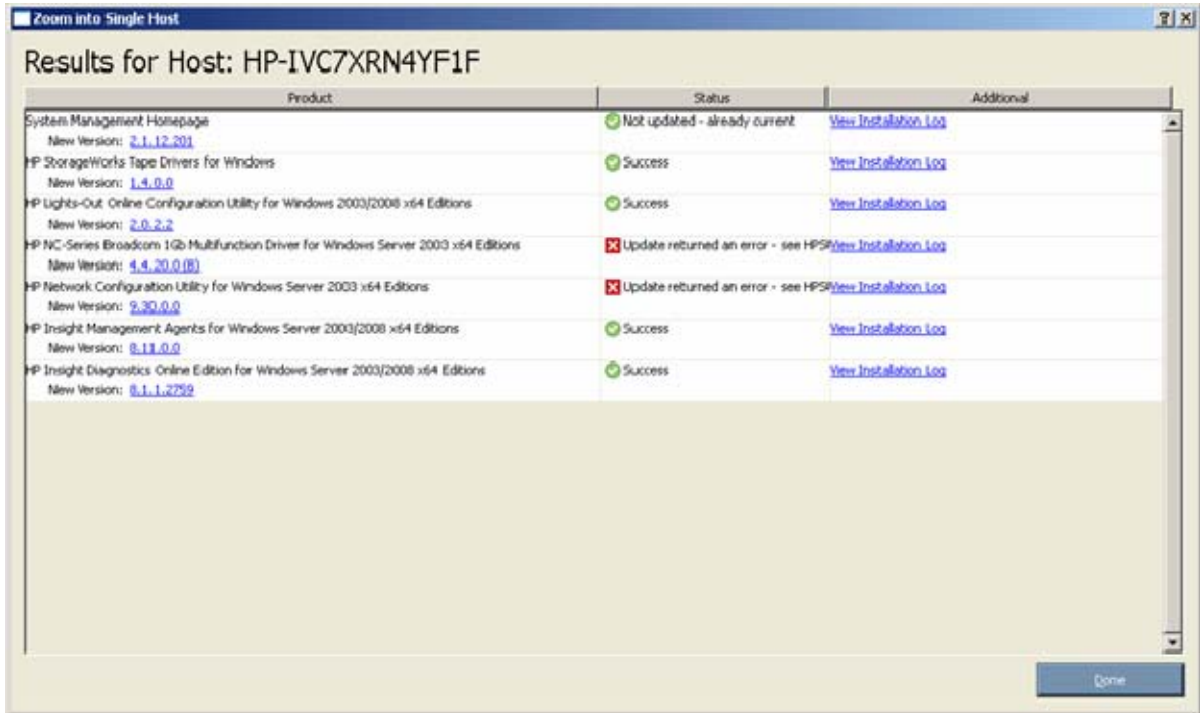
- Host—Specifies the IP address or DNS name of the host.
- Status—Specifies the overall installation status of the components on the remote host.

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 25)."

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_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> ...]
```

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.

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.

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.

Command line argument	Description
<code>/f[orce]:rom</code>	This argument enables you to override or downgrade the existing installation of the selected firmware components. (Applies to firmware only.)
<code>/f[orce]:software</code>	This argument enables you to override or downgrade the existing installation of the selected software components.
<code>/f[orce]:all</code>	This argument enables you to override or downgrade the existing installation of the selected software components, firmware components, and bundles.
<code>/g</code> or <code>/downgrade</code>	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.)
<code>/e</code> or <code>/rewrite</code>	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.)
<code>/m[utual]</code>	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 <code>/m</code> option is not passed, then the component installation fails. (Applies to firmware only.)
<code>/r[eboot]</code>	If the following conditions are met, then this argument causes the server (or host server in a remote installation) to reboot: <ul style="list-style-type: none"> • The <code>/reboot</code> 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.
<code>/reboot_message</code> <code>"reboot message"</code>	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 <code>/reboot</code> option, or the argument is ignored.
<code>/reboot_delay</code> <code>timeout_in_seconds</code>	This argument delays the reboot of the server for the length of time specified by the <code>timeout_in_seconds</code> variable. You must use this argument with the <code>/reboot</code> 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.
<code>/reboot_always</code>	If the following conditions are met, then this argument forces the server to reboot: <ul style="list-style-type: none"> • The <code>/reboot_always</code> option is selected or given as a command line argument. • All components selected for installation are successfully installed.
<code>/s[ilent]</code>	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 <code>/s[ilent]</code> argument. To check for failed dependencies, remove the <code>/s[ilent]</code> argument, reissue the command line, and then the HP Smart Update Manager GUI appears.

Command line argument	Description
<pre>/c[omponent] <component to install> or <component1_to_install> <component2_to_install></pre>	<p>This argument specifies the components to install. Components to install can be specified with or without the <code>/c[omponent]</code> argument. If using the <code>/c[omponent]</code> argument, only one component can be specified with the argument. However, multiple <code>/c</code> arguments and components can be specified on the same line. If the <code>/c[omponent]</code> 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.</p>
<pre>/group "group_name"</pre>	<p>This argument specifies an already defined group name in the HP Smart Update Manager GUI.</p>
<pre>/b[undle] <bundle name> or <bundle1_to_install> <bundle2_to_install></pre>	<p>This argument specifies the bundles to install. Bundles to install can be specified with or without the <code>/b[undle]</code> argument. If using the <code>/b[undle]</code> argument, only one bundle can be specified with the argument. However, multiple <code>/b</code> arguments and bundles can be specified on the same line. If the <code>/b[undle]</code> 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.</p>
<pre>/allow_update_to_bundle</pre>	<p>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.</p>
<pre>/allow_non_bundle_components</pre>	<p>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.</p>
<pre>/use_latest</pre>	<p>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 <code>/use_latest</code> argument allows HP Smart Update Manager to use the bundle with the latest version for installation.</p>
<pre>/use_location "file_share"</pre>	<p>This argument specifies a directory or file share that contains the PSP and components for use with HP Smart Update Manager. If you do not specify this argument, the directory containing <code>hpsum.exe</code> or HP Smart Update Manager is used by default. The logged-in account must have access to this location. The <code>/user</code> and <code>/passwd</code> 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.</p>
<pre>/use_snmp</pre>	<p>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 <code>/use_snmp</code> argument is used, and the <code>/use_wmi</code> argument is not, the WMI components are optional.</p>

Command line argument	Description
<code>/use_wmi</code>	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 <code>/use_wmi</code> argument is used, and the <code>/use_snmp</code> argument is not, the SNMP components are optional.
<code>/romonly</code>	This argument is a filter switch and allows 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 <code>/romonly</code> argument with the <code>/softwareonly</code> argument.
<code>/softwareonly</code>	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 <code>/softwareonly</code> argument with the <code>/romonly</code> argument.
<code>/dryrun</code>	This argument simulates the installation for a test run. Nothing is installed.
<code>/continue_on_error</code> <code><error></code>	This argument causes the installation to continue and ignore errors. Valid values are <code><error>=ServerNotFound</code> and <code><error>=BadPassword</code> . The <code>ServerNotFound</code> option can be used to bypass inactive or unavailable remote hosts when deploying firmware or software to multiple remote hosts at the same time.
<code>/override_existing_connection</code>	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.
<code>/express_install</code>	This argument starts express install (for local host only). The HP Smart Update Manager performs discovery, install, or exit without user interaction. The user can cancel or terminate HP Smart Update Manager.
<code>/user <username></code> or <code>/username <username></code>	This argument enables you to log in to HP BladeSystem c-Class Onboard Administrator with your user ID.
<code>/passwd <password></code>	This argument enables you to use the password for the user ID specified in the <code>/user</code> parameter. The password is used to log in to remote hosts and HP BladeSystem c-Class Onboard Administrators.
<code>/current_credential</code>	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.)
<code>/target "netAddress"</code>	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.
<code>/logdir "path"</code>	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 <code>%SYSTEMDRIVE%\CPQSYSTEM\hp\log<netAddress></code> and the redirected location is <code><path>\hp\log\<netAddress></code> . For Linux components, the default location is <code>/var/hp/log/<netAddress></code> and the redirected location is <code><path>/hp/log/<netAddress></code> .

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 25)."

Return code	Value	Linux	Windows	Text
SUCCESS_NO_REBOOT	0	0	0	The installation was successful.
SUCCESS_REBOOT	1	1	1	The installation was successful, but a reboot is required.

Return code	Value	Linux	Windows	Text
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.
3	The installation was not attempted because of one of the following: <ul style="list-style-type: none"> • 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.

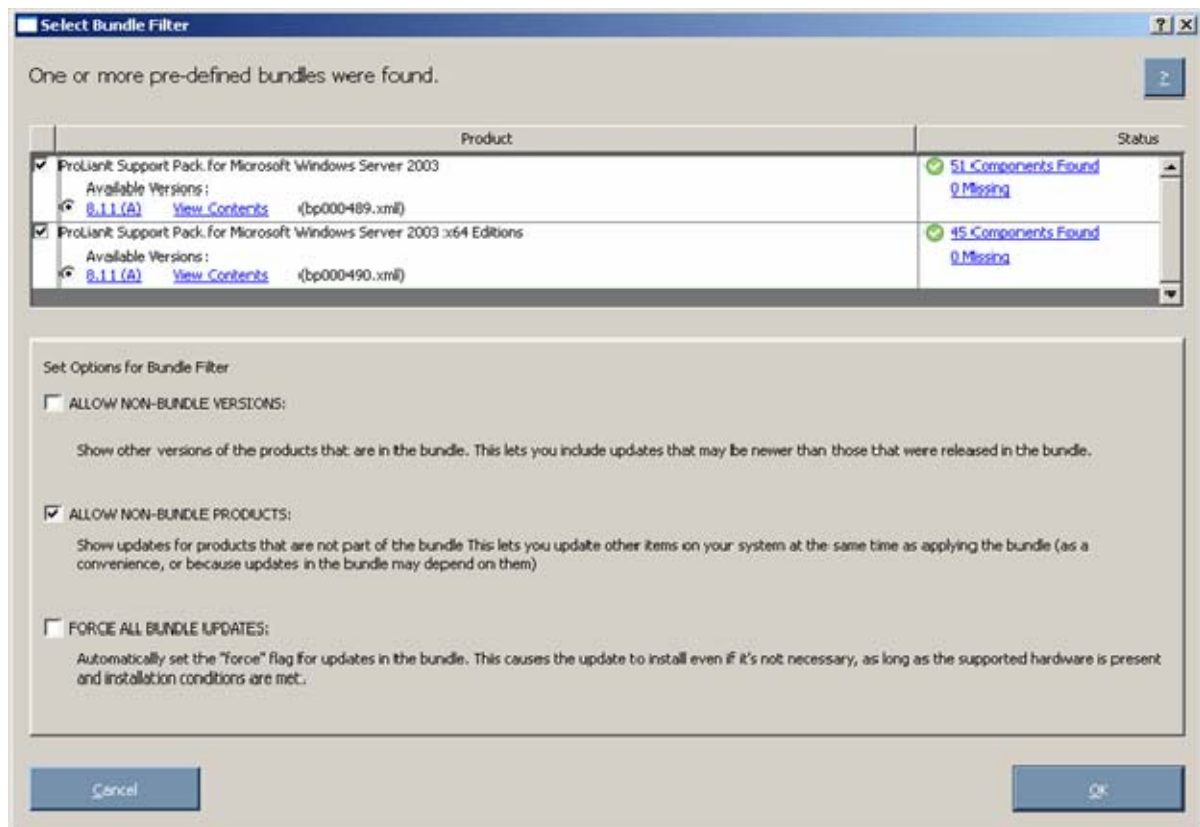
Error level	Meaning
5	The installation was canceled by a user before anything could be installed.
6	The installer cannot execute because of an unmet dependency or installation tool failure.
7	The actual installation operation (not the installation tool) failed.

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 server blade bundles simultaneously. The latest Microsoft® Windows® PSP, bundles, and firmware components must be in the same directory and the cp*.exe and/or cp*.scexe files added to the repository to deploy simultaneously.

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 17) 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

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 60). 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 60). 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.

The screenshot shows a 'New Host' dialog box with the following fields and options:

- Add a Host by DNS Name
Host DNS Name:
- Add a Single Host by IP
Host IP:
- Add a Range of Hosts by IP
Starting IP:
Ending IP:

IP Format:
 IPv4
 IPv6

Description:

Buttons: Cancel, OK

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 64).

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.

The screenshot shows a 'New Host' dialog box with the following fields and options:

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

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 64).

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\ 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.

The screenshot shows a 'New Host' dialog box with the following fields and options:

- Add a Host by DNS Name
Host DNS Name:
- Add a Single Host by IP
Host IP:
- Add a Range of Hosts by IP
Starting IP:
Ending IP:

IP Format:
 IPv4
 IPv6

Description:

Buttons: Cancel, OK

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 64).

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, insert the Firmware Maintenance CD. The Firmware Maintenance CD interface appears.
2. Read the End-User License Agreement. To continue, click **Agree**. The Firmware Maintenance CD interface reappears.
3. Click the **Firmware Update** tab.
4. Click **Browse Firmware CD**.

5. Download and save the ROMPaq image to the hard drive from the HP website (<http://www.hp.com>).
6. Execute the ROMPaq image to create the ROMPaq disk.
7. Switch to the server with the corrupted ROM.
8. Power down the server.
9. Insert the ROMPaq disk.
10. 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.

11. Power down the server.
12. Remove the ROMPaq disk.
13. 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. These files contain internal process and debug information. To resolve this issue, collect these 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 60).

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	<p>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.</p> <p>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.</p>
Ports 61000-61007	<p>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.</p>
Port 62286	<p>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.</p>
Ports 80 or 63000-63005	<p>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.</p>

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

The user can specify a reboot message that will appear 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 will 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.

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®. For more information about accessing IPv6, see the Microsoft® Knowledge Base article (<http://support.microsoft.com/kb/944007>).

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 49).
- 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®. For more information about accessing IPv6, see the Microsoft® Knowledge Base article (<http://support.microsoft.com/kb/944007>).

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 31
- adding hosts 28
- advanced topics 48
- Allow Downgrades 23
- Allow Rewrites 23
- Allow Shared Devices 23
- arguments 40
- array controllers 6, 17
- audience assumptions 5
- authorized reseller 66

B

- blocked HP Smart Update Manager, recovering from 60

C

- command line arguments 40
- command line examples 44
- command line interface, using 40
- command line syntax 40
- command line tools 10
- command syntax 40
- component configuration, Windows 44
- component selection pane 21
- component status 17, 36
- components, adding new 8
- components, deploying 6, 10
- components, installation 15, 17, 27
- components, selecting to install on multiple hosts 36
- configuring firewall settings 59, 60
- controllers, array 6
- credentials 27, 34

D

- deleting groups 31
- deleting hosts 28
- deploying components 6, 10
- deploying firmware and software simultaneously 48
- deployment methods 6
- deployment scenarios 10

- deployment to multiple remote hosts 11
- deployment, graphical 10, 11
- deployment, offline 7
- deployment, online 7
- deployment, scripted 10, 11, 40
- disaster recovery 57
- Disaster Recovery, ROMPaq 57
- documentation 66
- double-byte characters 63
- downgrading firmware 23
- drive key 6

E

- editing groups 31
- editing hosts 28
- end user license agreement (EULA) 7
- entering credentials 34
- error code 45
- EULA (end user license agreement) 7
- examples 44
- execution, first time 12

F

- failed dependencies 40
- Failed Dependencies screen 21
- firewall settings, configuring 59, 60
- firmware and software deployment, simultaneous 48
- Firmware Maintenance CD 5, 6, 7, 10
- first time execution 12
- force install 23

G

- graphical deployment 10, 11
- groups 27, 31
- GUI, using for multiple-host installations 27

H

- hard drive space 5
- host field 17, 36
- hosts 27, 28, 34
- HP Onboard Administrator for HP c-Class BladeSystem 6

HP Smart Update Manager GUI 15
HP Smart Update Manager overview 5
HP website 6, 8, 66
hpsum_detail_log.txt log 25
hpsum_log.txt log 25

I

installation host 12, 14
installation log 25
installation options 17, 21, 23
Installation Progress 23
installation status 25, 38
installation, selecting components for multiple hosts 36
installing multiple hosts using GUI 27
introduction 5
Inventory Progress screen 27
IPv6 network configurations 49
IPv6, troubleshooting 64, 65

K

keyboard support 12

L

Lights-Out Management ROM flash components 6
Lights-Out Management ROMs 6, 59
limitations, Linux IPv6 environment 56
limitations, Windows Server IPv6 environment 54
Linux IPv6 environment 54
Linux remote functionality, recovering 59
Linux smart components, return codes 46
local host installations 14
local host, graphical deployment 10, 11
local host, scripted deployment 10, 11
log files 25

M

managing groups 31
managing hosts 28
memory 5
minimum requirements 5
multiple hosts 27, 36
multiple remote hosts, deployment 10, 11
multiple-host installations 27

N

NIC firmware 6, 17, 23

O

offline deployment 7
Onboard Administrator 6
online deployment 7
operating systems 66
options, deployment 6
options, installation 17, 21, 23
options, reboot 20
overview, Firmware Maintenance CD 5
overview, HP Smart Update Manager 5
overwriting firmware 23

P

packages 5
parameters 40
ports, enabling in HP Smart Update Manager 60
ProLiant Essentials Foundation Pack 6

R

Reboot Delay 20
Reboot Options 20
reboot settings 17, 20
recovering from a failed option ROM upgrade 58
recovering from a failed system ROM upgrade 57
redundant ROM 57
references 66
remote functionality, recovering 59
remote hosts 11, 27
remote hosts, deployment to multiple 11
requirements, minimum 5
return codes 45
return codes, Linux smart components 46
return codes, Windows smart components 46
rewriting firmware 23
ROM recovery, redundant 57
ROM redundancy 57
ROM upgrade behavior 23
ROM upgrade, recovering from failed option 58
ROM upgrade, recovering from failed system 57
ROM, array controller 58
ROM, Lights-Out management 6, 59
ROM, storage 58
ROMPaq Disaster Recovery 57

S

SAS hard drive 6
scenarios, deployment 10
scripted deployment 11, 40

- selecting an installation host 16
- selecting an installation host, first time 14
- selecting components to install 17, 36
- selecting components to install, first time 15
- selections for single host 36, 38
- server host pane 36
- server virtualization detection and support 49
- settings, reboot 20
- shared storage, updating ROMs for 23
- SLES (SUSE Linux Enterprise Server) 63
- software and firmware deployment, simultaneous 48
- status, component 17, 36
- status, installation 25, 38
- status, system 36
- support 66
- SUSE Linux Enterprise Server (SLES) 63
- syntax 40
- system status field 17, 19, 36

T

- technical support 66
- TPM (Trusted Platform Module) 5, 8, 34
- trace logs 59
- troubleshooting 57
- Trusted Platform Module (TPM) 5, 8, 34

U

- USB drive key 6, 7, 8
- using the GUI 27

V

- View Failed Dependencies 21

W

- Windows Management Instrumentation (WMI) 5
- Windows Server 2003 IPv6 environment 49
- Windows Server 2008 IPv6 environment 52
- Windows smart components, return codes 46
- WMI (Windows Management Instrumentation) 5