HP Smart Update Firmware DVD User Guide

Abstract

This guide is intended for individuals who are familiar with the configuration and operation of Microsoft Windows, Windows Server, Windows XP, Windows Vista, smart components, and deployment of firmware and software to systems and options.

Part Number: 447788-404
March 2011
Edition: 13

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.

Contents

Introduction

HP Smart Update Firmware DVD overview

The HP Smart Update Firmware DVD provides a collection of firmware for supported HP ProLiant servers, BladeSystems, and options in an ISO image that can be used in either of the following modes:

- Offline mode (local updates only)
  - Interactive mode
  - Automatic mode
- Online mode
  - Interactive local updates
  - Interactive remote updates

The Firmware DVD also contains firmware for the BladeSystem. To deploy the Smart Update Firmware DVD contents, see "Online deployment ("Deploying components online" on page 11)" and "Offline deployment ("Deploying offline" on page 12)." In offline mode, the Smart Update Firmware DVD boots a small Linux kernel and enables firmware updates to take place on a single server using the embedded HP Smart Update Manager software. Because of the special boot environment, support for remote servers and hosts is not available. In online mode, users can leverage the autorun utility to launch HP Smart Update Manager or browse the DVD to the \hp\swpackages directory and execute firmware smart components directly.

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

△ **CAUTION:** The HP Smart Update Firmware DVD and its contents must be used only by individuals who are experienced and knowledgeable with HP SUM. Before using HP SUM to update firmware, 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 is a technology which is embedded in many HP products for installing and updating, firmware and software components on HP ProLiant and HP Integrity servers, enclosures and options. HP Smart Update Manager stores host and group information from session to session. However, usernames, passwords, and existing credentials are not stored. HP supports the current and two previous versions of the Smart Update Firmware DVD.

Minimum requirements

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

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

- A local administrative system with 512 MB of memory
- 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
- 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, the following must be available:

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

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

compat or compat-32bit or another compatibility library that provides the /usr/lib/libstdc++-libc6.2-2.so.3 file

Without this library, HP Smart Update Manager does not complete discovery and returns `Discovery Failed` messages. These libraries are not included on the SLES11 media and must be downloaded from the Internet or updated through system updates from Novell. Download the compat (for x32 installations) or compat-32bit RPM from the Novell support site or using yast2. This requires a valid subscription.

To perform Linux deployments, a root equivalent user account must be used. SSH support must be enabled and firewall opened to enable SSH communications on remote Linux servers or HP Smart Update Manager is not able to deploy updates. By default, SUSE LINUX Enterprise Server 10 and 11 block SSH support through the firewall. To enable SSH support if it has been disabled in the firewall, use the `yast2` command to open the necessary ports in the firewall. For more detailed information, see the *HP Smart Update Manager User Guide* (*http://www.hp.com/support/HP_Smart_Update_Manager_UG_en*).

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

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

Supported firmware

Firmware type	Supported by HP Smart Update Firmware DVD
ProLiant System ROM	Yes
iLO 2 firmware	Yes, local and remote
iLO 3 firmware	Yes, local and remote
Lights-Out 100 firmware	Yes
Broadcom NIC firmware	Yes
Intel NIC firmware	No
NetXen NIC firmware	Yes
Power PIC firmware	Yes
Smart Array controller firmware	Yes
SAS and SATA hard drive firmware behind Smart Array controllers	Yes
SAS and SATA hard drive firmware behind non-Smart Array controllers	No
Emulex, QLogic, and Brocade Fibre Channel Host Bus Adapter firmware	Yes, offline only
Direct attach tape drive firmware	Yes
Tape blade firmware support	Yes
Onboard Administrator firmware	Yes, online only
Virtual Connect firmware	Yes, online only
HP 3Gb SAS BL Switch firmware***	No

**The only method of flashing the MDS600 firmware in a blade environment is through the Virtual SAS Manager software.

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

Because firmware might be able to update only in online or offline mode for some components, you might have to execute the Smart Update Firmware DVD both online and offline to update all the firmware in an enclosure.

Obtaining the HP Smart Update Firmware DVD

The Smart Update Firmware DVD can be downloaded from the HP Technical Support website (http://www.hp.com/support) and HP Insight Foundation Suite for ProLiant website (http://www.hp.com/go/foundation) and is available as part of the HP Insight Foundation suite for ProLiant kit. The HP Smart Update Manager utility is available from the Smart Update Firmware DVD.

To view the release set, see the compatibility tab of the HP BladeSystem Firmware Maintenance website (http://www.hp.com/go/bladesystemupdates).

Support limitations

- Booting the Firmware DVD from iLO virtual media is only supported in offline Automatic Firmware Update mode. Users attempting to boot in this manner, might experience issues from connection timeouts, difficulties updating iLO firmware, and mouse syncing issues.
- Workstation blades are only supported for offline firmware updates.
- The 100 series servers only support offline HDD firmware updates. HDD firmware components are available in the Windows® bundle on the Firmware DVD but are meant for use with supported options.
- Virtual OS is not supported for online firmware updating but is for offline firmware updates.
- If nothing is pressed when booting in offline mode, Automatic mode is selected by default, updating the firmware.
  - If creating a Smart Update Firmware USB key for deploying in offline Automatic mode, they you must use USB Key Utility v1.5. Previous versions of the USB Key Utility might add a selection menu when booting, removing the ability to fire and forget. When using a USB Key in Autormatic firmware update mode, the Firmware DVD must be the first ISO copied to the USB Key.
  - To disable the default selection of Automatic firmware update after 30 seconds, edit the **syslinux.cfg** file located at the root of the USB Key so that the TIMEOUT setting value is 0.
- The Update attempts to install RPMs, even if not necessary.
- The Smart Update Firmware DVD on ProLiant 100 servers only supports installing firmware smart components. For installing software components, see the Easy Set-up CD documentation.

Smart Update Firmware DVD contents

Release sets and bundles

A release set is an enhanced, solutions-oriented collection of ProLiant BladeSystem firmware released on a regular basis. The full collection is tested against HP software, drivers, and PSPs to drive standardization of components to HP customers. The release set can only be applied in interactive mode and by selecting the blade system bundle. HP recommends that you not deviate from the release set firmware contents. You can monitor the compatibility page at the HP BladeSystem Firmware website (http://www.hp.com/go/bladesystemupdates) for updates to the release set.

Bundles are for ML/DL based servers and are not solution-tested and provide the same level of testing as previous iterations of the Smart Update Firmware DVD, or its predecessor, the Firmware Maintenance CD.

The following are the bundles and BladeSystem release sets included in this version of HP Smart Update Firmware DVD:

- HP Smart Update Firmware—100 Series Bundle for Linux
- HP Smart Update Firmware—100 Series Bundle for Windows®
- HP Smart Update Firmware—ML/DL/SL 300/500/700/900 Series Bundle for Linux
- HP Smart Update Firmware—ML/DL/SL 300/500/700/900 Series Bundle for Windows®
- HP Smart Update Firmware—BladeSystem Release Set 2011.05 for Linux
- HP Smart Update Firmware—BladeSystem Release Set 2011.05 for Windows®

100 series servers

Smart Update Firmware DVD supports 100 series servers and options beginning with select G6 servers. Apply firmware updates using the 100 series bundle. For special support cases, see the support limitation section of this guide.

HP Smart Update Firmware DVD powered by HP Smart Update Manager

For advanced topics on using HP Smart Update Manager containing specific cases and examples of use, see the *HP Smart Update Manager User Guide* (*http://www.hp.com/support/HP_Smart_Update_Manager_UG_en*). HP Smart Update Manager is designed for maximum flexibility and is shipped within the HP ProLiant Support Pack and HP Smart Update Firmware DVD. It provides a Graphical User Interface and a command-line, scriptable interface for deployment of firmware for single or one-to-many servers and network-based targets such as iLOs, OAs, and Virtual Connect Ethernet and Fibre Channel modules. HP SUM has an integrated hardware and software discovery engine that discovers the installed hardware, current versions of firmware in use on a target, and software versions on target servers. This prevents extraneous network traffic by only sending the components to a target host that are required. HP SUM also has logic to install updates in the correct order and ensure all

dependencies are met before deployment of a firmware update. HP SUM also contains logic to prevent version-based dependencies from derailing an installation and ensures firmware updates are handled in a manner that reduces any downtime required for the firmware update process.

HP SUM does not require an agent for remote installations as it copies a small, secure SOAP server to the target server for the duration of the installation. After the installation is complete, the SOAP server and all remote files associated with the installation except installation log files are removed. HP SUM copies the log files from the remote targets back to the system where HP SUM is executed.

The key features of HP SUM include:

- Dependency checking, which ensures appropriate install order and dependency checking between components
- Intelligent deployment only when updates are required
- Simultaneous firmware and software deployment
- Improved deployment performance
- Local or remote (one-to-many) online deployment
- Local offline deployments with the HP Smart Update Firmware DVD
- Remote offline deployment when used with the SmartStart Scripting Toolkit or iLO Virtual Media
- GUI or CLI/scriptable with extensive logging
- Remote command-line deployment

Deployment options

Host types

You can run the Smart Update Firmware DVD either online or offline.

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

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

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

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

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

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

Deploying components online

1. Choose one of the following options:
   - Insert the Smart Update Firmware DVD. The Smart Update Firmware DVD interface opens.

     NOTE: In Linux, if the autostart is not enabled, you must manually start the Smart Update Firmware DVD. Browse to the DVD contents, and select **hpsum.exe.**

   - Insert the USB drive key. Manually start the interface, and open a CLI. To access the Smart Update Firmware DVD, enter one of the following commands:
     - On Windows® operating systems, enter `\_autorun\autorun_win`

— On Linux operating systems, enter `/autorun`

NOTE: If you are using a USB drive key with multiple CD images, navigate to the appropriate CD subfolder to launch autorun for the Smart Update Firmware DVD.

2. Read the End-User License Agreement. To continue, click **Agree.** The Smart Update Firmware DVD interface appears.
3. Click the **Firmware Update** tab.
4. Click **Install Firmware.** The HP Smart Update Manager is initiated.
5. Select and install components. For more information, see the *HP Smart Update Manager User Guide* (*http://www.hp.com/support/HP_Smart_Update_Manager_UG_en*).

Deploying offline

1. Boot the server from the Smart Update Firmware DVD or a USB drive key.
2. At the menu, select either **Automatic Mode** (default) or **Interactive Mode.**
   - If **Automatic Mode** is selected or the 30 second default timer runs out, the latest firmware available on the DVD is installed. The server automatically reboots when it finishes updating. Log files is not available in this method of installation.
   - If **Interactive Mode** is selected, you must select a specific release set or bundle to apply.
3. At the prompt, select a language and keyboard.
4. Click **Continue.**
5. Read the End-User License Agreement. To continue, click **Agree.** The Smart Update Firmware DVD interface appears.
6. Click the **Firmware Update** tab.
7. Click **Install Firmware.** The HP Smart Update Manager is initiated.
8. Select and install components. For more information, see *HP Smart Update Manager User Guide* (*http://www.hp.com/support/HP_Smart_Update_Manager_UG_en*).

HP USB Key Utility

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

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

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

1. Insert your HP USB drive key.
2. Select the **HP USB Key Utility** shortcut in the HP System Tools folder.

   Follow the onscreen instructions. The HP USB Key Creator formats the USB key. Therefore, files on the key are lost. Ensure that you are using a USB key that is at least 1GB in size and does not contain any valuable files.

For Linux, the USB key can be created manually:

1. Obtain SYSLINUX 3.5 or higher from The Syslinux Project website (http://syslinux.zytor.com/index.php) and download to a Linux workstation.
2. Install the SYSLINUX RPM obtained in step 1.
3. If a directory does not already exist, create one for the USB key mountpoint.

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

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

   `mount /dev/dvdrom /dvd_mount_point` or `mount -t iso9660 firmware-<version>.iso /dvd_mount_point -o loop`
8. Change the directory to the /usb directory on the DVD:

   `dvd /dvd_mount_point/usb`
9. Execute the usbcreator.sh shell script passing in the DVD mount point and the USB mountpoint to move the Firmware DVD files to the USB key:

   `./usbcreator.sh /dvd_mount_point /usbkey`
10. If additional components must be added to the USB, copy the components into the /hp/swpackages (Linux operating systems) or the \hp\swpackages (Windows® operating systems) directory and HP Smart Update Manager picks them up automatically if the version can support the type of components added.

    NOTE: If you are using a USB drive key with multiple DVD images, navigate to the appropriate DVD subfolder and relative path seen above to copy components.
11. Unmount the DVD and the USB key. This must match the initial mount point in step 4.

    `umount /dev/dvdrom`

    `umount /dev/sda1`
12. Remove the USB key and DVD.

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

Using a hard drive

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

4. Execute HP Smart Update Manager to have the new firmware components recognized.

Deploying components not on HP Smart Update Firmware DVD

Make sure you use the correct version that is released along with the deliverable supporting the environment.

If you have components that are not on the HP Smart Update Firmware DVD that you want to deploy to a ProLiant server or option, you can include other smart components in the HP SUM environment. To deploy software and firmware components that are not on the HP Smart Update Firmware DVD:

1. Obtain the components from the HP website (http://www.hp.com).
2. Create a bootable USB key ("HP USB Key Utility" on page 12), or copy the \hp\swpackages directory to the hard drive, and then remove the read-only bit (Linux only).
3. Add the components to the \hp\swpackages directory on the USB key or to the directory on the hard drive with the components from the HP Smart Update Firmware DVD.
4. Start HP SUM.
5. On the Source Selection screen, you can specify the directory where all of the components are located as well as select the **Check ftp.hp.com (for ProLiant servers)** checkbox if you want to include the latest version of software and firmware components from the HP website (http://www.hp.com).
6. Select the checkbox for non-bundle versions, and then click **OK**.

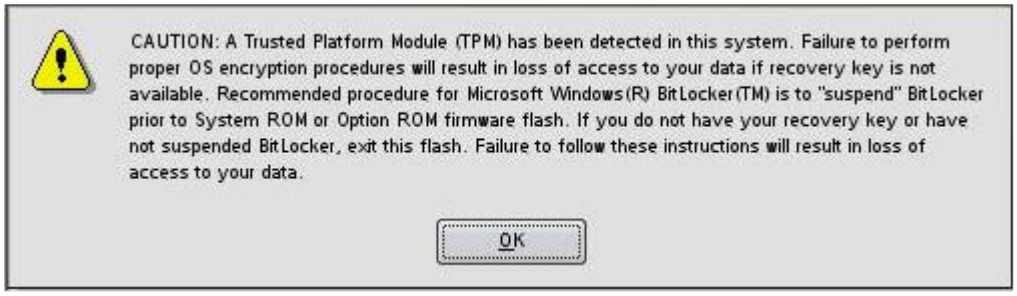
Trusted Platform Module

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

A recovery event is triggered if:

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

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



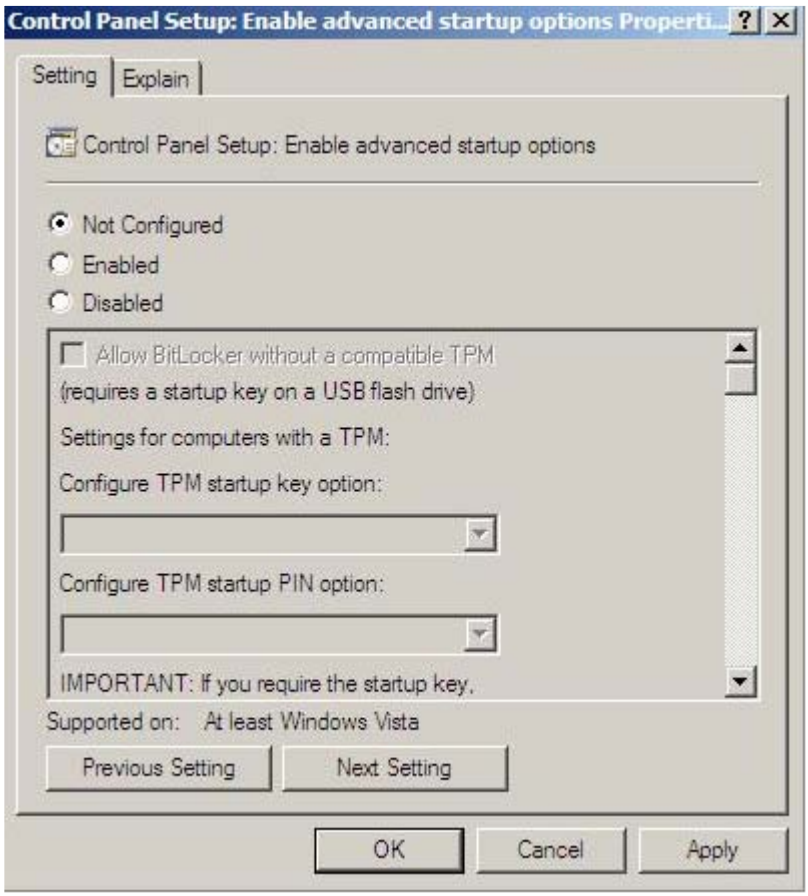
To enable firmware updates without the need to type in the TPM password on each server, the BitLocker Drive Encryption must be temporarily disabled. Disabling the BitLocker Drive Encryption keeps the hard drive data

encrypted. However, BitLocker uses a plain text decryption key that is stored on the hard drive to read the information. After the firmware updates have been completed, the BitLocker Drive Encryption can be re-enabled. Once the BitLocker Drive Encryption has been re-enabled, the plain text key is removed and BitLocker secures the drive again.

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

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

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



To enable advanced startup options, use the following command:

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

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

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

TPM scenarios

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

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

Other scenarios do not affect the normal installation procedure.

Booting a Firmware DVD over a network

This section provides instructions on booting a Firmware DVD over a network.

Prerequisites

The following is required before proceeding with the configuration:

- You must have a good working knowledge of PXE and TFTP.
- A network with a DHCP server on it.
- A TFTP server configured on the same network as the DHCP server.
- A network file server hosting the ISO images and can be accessed by a PXE booted system.
- PXELinux (http://syslinux.zytor.com/wiki/index.php/PXELINUX)

This guide assumes that you are using a Linux TFTP server and the TFTP package (http://www.kernel.org/pub/software/network/tftp). Other TFTP servers should work similarly.

Setup

Before proceeding with the configuration, ensure that your TFTP server and PXELinux configuration is setup and configured properly. To set up PXELinux:

1. Copy a Firmware DVD ISO image to the network file system, and note its location. NFS and Windows® file shares are supported.
2. For this example, the NFS and path to the ISO image used is 192.168.0.99:/path/to/fwdvd/image/FW900.iso. Test your network file system to ensure that is accessible before proceeding.
3. Copy all the files from the /system directory of the DVD to your TFTP server so that it is accessible by the TFTP software.
4. To access the /system directory of the DVD, burn and mount the ISO image, or extract it using a third-party tool.

Configuring PXELINUX

1. Using the isolinux.cfg file from the /system/ directory of the DVD as a guide, copy the labeled targets to your PXELinux configuration file. You do not need to include the entire file:

```
label sos
  MENU LABEL Automatic Firmware Update Version 9.10
  kernel hpboot_v.c32
  append vmlinuz initrd=initrd.img media=cdrom rw root=/dev/ram0
ramdisk_size=257144 init=/bin/init loglevel=3 ide=nodma ide=noraid
pnpbios=off vga=791 splash=silent showopts TYPE=AUTOMATIC
label vsos
  MENU LABEL Interactive Firmware Update Version 9.00
  kernel hpboot_v.c32
  append vmlinuz initrd=initrd.img media=cdrom rw root=/dev/ram0
ramdisk_size=257144 init=/bin/init loglevel=3 ide=nodma ide=noraid
pnpbios=off vga=791 splash=silent showopts TYPE=MANUAL
```

2. Replace the lines `kernel hpvoot_v.c32` with `kernel vmlinuz`.
3. Remove `vmlinuz` from the append line.

NOTE: The paths to files on the TFTP server are `vmlinuz` and `initrd.img`. You must modify them to include any directories or naming conventions you may have on your TFTP server.

Specifying the ISO Image Path

For the PXE booted server to find the ISO Image, you must add the ISO Image path to the append line in the PXELinux configuration file.

Add the following arguments:

```
iso1=nfs://192.168.0.99/path/to/fwdvd/image/FW900.iso
iso1mnt=/mnt/bootdevice
```

The iso1 parameter helps the PXE booted Firmware DVD locate the ISO image. The iso1mnt parameter tells the PXE booted FWDVD where the iso1 image must be mounted.

Your final configuration must be similar to the following example:

```
label sos
  MENU LABEL Automatic Firmware Update Version 9.10
  kernel vmlinuz
  append initrd=initrd.img media=cdrom rw root=/dev/ram0
ramdisk_size=257144 init=/bin/init loglevel=3 ide=nodma ide=noraid
pnpbios=off vga=791 splash=silent showopts TYPE=AUTOMATIC
iso1=nfs://192.168.0.99/path/to/fwdvd/image/FW900.iso
iso1mnt=/mnt/bootdevice
label vsos
  MENU LABEL Interactive Firmware Update Version 9.10
  kernel vmlinuz
  append initrd=initrd.img media=cdrom rw root=/dev/ram0
ramdisk_size=257144 init=/bin/init loglevel=3 ide=nodma ide=noraid
pnpbios=off vga=791 splash=silent showopts TYPE=MANUAL
iso1=nfs://192.168.0.99/path/to/fwdvd/image/FW910.iso
iso1mnt=/mnt/bootdevice
```

You can add additional ISO images by specifying the additional iso# and iso#mnt arguments, for example, `iso2=/path/to/iso2.iso iso2mnt=/mnt/iso2`.

Supported network file systems

The following network file systems are supported for use with PXE booting:

NFS:

```
iso1=nfs://192.168.0.99/path/to/fwdvd/image/FW900.iso
iso1mnt=/mnt/bootdevice
```

NFS volumes are mounted with the following options:

- -o ro
- nolock

Windows® operating systems:

```
iso1=smbfs://192.168.0.99/share/path/to/fwdvd/image/FW910.iso
iso1mnt=/mnt/bootdevice
```

Windows® operating systems with login credentials:

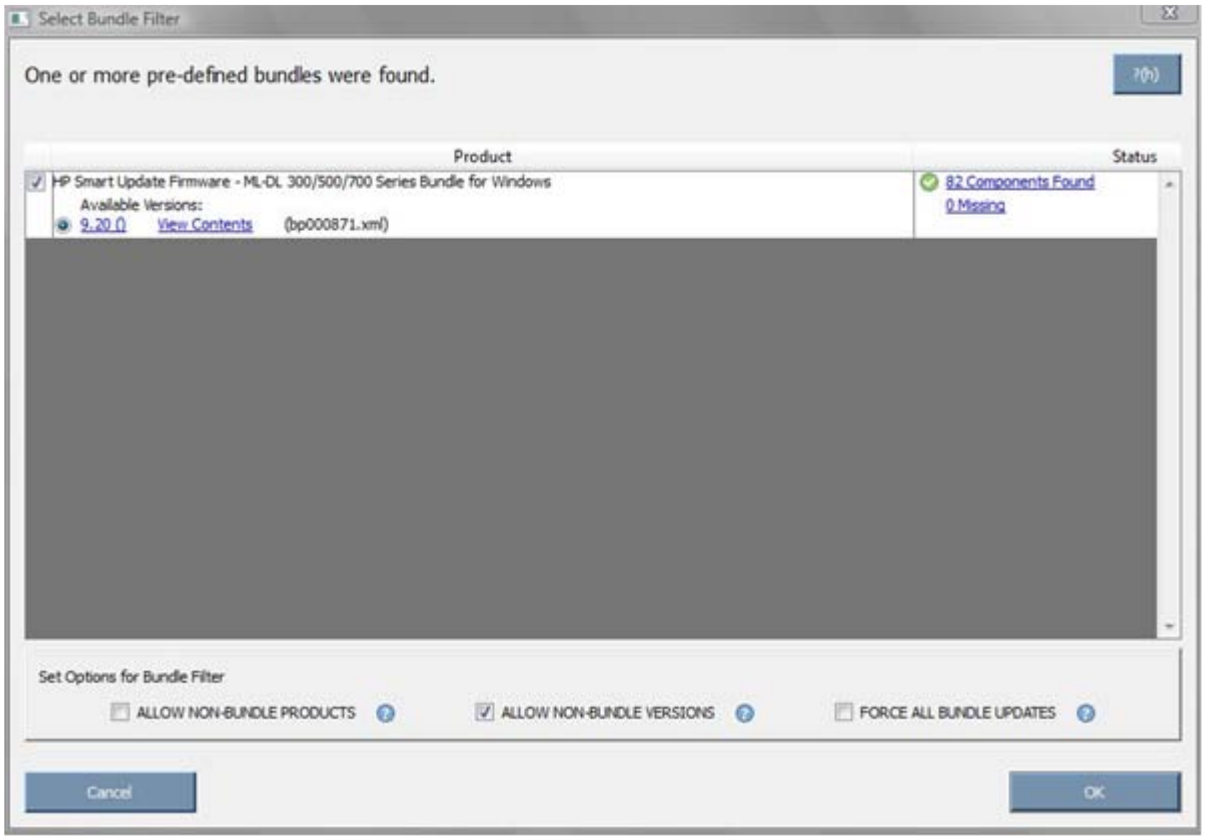
```
iso1=smbfs://user:password@192.168.0.99/share/path/to/fwdvd/image/FW910.
iso iso1mnt=/mnt/bootdevice
```

Deploying firmware and software simultaneously

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

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

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



To proceed with the deployment process, click **OK.** The Select Items to be Installed screen appears with the appropriate firmware and software components.

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

Smart Update Firmware DVD Automatic Deployment Mode

Overview

HP Smart Update DVD, in conjunction with Release Sets, provide a collection of firmware smart components that have been tested together in complex industry-like scenarios to ensure compatibility across varying firmware and software stacks. The tool is designed for users who do not have an installed operating system on their blades or who want an unattended, automated method of deploying firmware in an offline environment. Because the tool requires you to boot to it, you must take the server offline temporarily to complete the firmware update.

Automatic Mode supports the following firmware types:

- System ROM
- iLO 2
- Broadcom NIC
- Smart Array Controllers
- SAS and SATA hard drive firmware behind Smart Array Controllers
- Emulex, QLogic, and Brocade Fibre Channel Host Bus Adapters
- Tape Blade
- PowerPIC

To determine the firmware and software to update for your BladeSystem products, see the Firmware Compatibility Chart (http://www.hp.com/go/bladesystemupdates).

Offline Automatic Mode is useful for those customers who:

- Want an automated way to update a blade firmware
- Do not need to update infrastructure firmware at the same time
- Want to leverage the BladeSystem enclosure capability to load an ISO image to multiple server blades simultaneously
- Do not need feedback during the update process
- Do not need log files at the conclusion of the installation for archiving or debugging purposes
- Need to support devices that can only be updated offline
- Need to update firmware on multiple server blades simultaneously
- Need to update firmware using iLO 2's virtual media

Updating the firmware on a server

To update the firmware on a server, you have the following options:

- Updating an individual server locally (on page 21)
- Updating an individual server remotely (on page 21)
- Updating multiple servers simultaneously (on page 22)
- Updating multiple enclosures simultaneously (on page 24)

Updating an individual server locally

To update an individual server using Automatic Mode, use the c-Class SUV cable. This cable connects to the front of a blade and enables a USB CD or DVD drive to connect to a server. In this local installation, the Automatic Mode ISO image must be burned to a physical CD and placed in the USB CD or DVD drive. After you place the physical CD in the USB CD or DVD drive, you can boot the server, and Automatic Mode flashes all firmware on the server.

- If the firmware update process is completed successfully, the UID light turns off, the CD ejects, and the server reboots.
- If the firmware update process fails as indicated by the UID light being left on solid, the video can be plugged into the c-Class SUV cable, or an iLO remote console session can be initiated. Automatic Mode must have the error logged in a vi editor window to determine the cause of the firmware update failure.

NOTE: If a server does not have a front connection for the SUV-cable, they must follow the steps indicated in the Updating an individual server remotely (on page 21) section.

Updating an individual server remotely

To update an individual BladeSystem server remotely using Automatic Mode, you must download the Automatic Mode ISO image to either a hard drive or USB key.

You must attach the USB key to a workstation located on the same network as the BladeSystem server ILO Management Port.

To download the ISO image on a USB key and use the iLO Virtual Media functionality to deploy firmware updates:

1. Plug in the USB key with the Automatic Mode ISO image or use the Automatic Mode ISO image from a hard drive on a remote client computer.
2. Using Microsoft® Internet Explorer or Mozilla Firefox, browse to **ILO Management Port.**
3. Log in with your iLO administrative credentials.
4. Click the virtual media tab, and then click **Virtual Media Applet.**
5. In the Virtual CD/DVD-ROM section, click **Local Image File.**
6. Click **Browse.**
7. Locate the ISO image, and then click **Open.**
8. To connect to the ISO image, click **Connect.**

NOTE: Do not close the virtual media web page, or it might disconnect the ISO image.

9. Return to the iLO 2 webpage.
10. Click the **Power Management** tab.
11. Using the Momentary Press button, power up the server.

    NOTE: If the server is powered up, click the **Momentary Press** button to shut down the server, and then click the **Momentary Press** button again to power it back up.

12. Click **OK** when prompted to power up the server.
13. Select **Remote Console** or ensure the disconnection of the Local Image File to indicate flash is finished. A **Remote Console** session is terminated if the iLO firmware is updated during the Automatic Mode firmware update process.

Updating multiple servers simultaneously

HP recommends that you do not update more than eight servers simultaneously using the following Automatic Mode process. If you update more than eight servers simultaneously, an isolinux Disk 80 error may occur. If the isolinux Disk 80 error occurs, press any key. The server reboots to Automatic Mode, and restarts the firmware update process. If you need to update more than eight servers in an enclosure, you must execute multiple batches to complete the process.

You can use Automatic Mode to update firmware for multiple servers at once within an enclosure by using the USB port on the OA to host the Automatic Mode ISO image through the iLO Virtual Media interface to multiple servers.

To use Automatic Mode to update firmware on multiple servers in an enclosure at once:

1. To update a server blade using the Automatic Mode ISO, place it on a USB key and insert it into the USB port on the front of the c3000 Enclosure or on the rear of the C7000 Enclosure.
2. Browse to the HP BladeSystem Onboard Administrator web interface.
3. Log in using the OA administrator credentials.
4. To see the summary of all blades in the enclosure, click **Device Bays.**
5. Select each blade that needs to be updated
6. Click the **DVD** tab, and select the **Connect to bb*.iso** option in the pull down menu where the * (asterisk) signifies the version, date, and pass number of the Automatic Mode ISO file that you extracted earlier.
7. Select each blade that needs to be updated again if it was cleared during the DVD connection step.
8. Select the **Virtual Power** tab, and then select the **Momentary Press** option. After confirming the power change on the blades, the blades should power off if they were already powered on or power on if they have already been powered off. If they are powered off by clicking the **Momentary Press** option, repeat this step to power on the server blades.
9. When you boot to Automatic Mode, all feedback is provided through the UID lights. While the update process is running, the UID light blinks. Upon completion, the UID light is set to one of two states.
   - If the UID light is off, the update process is complete and the server OS can be installed or the server restarted to its previous operating system.
   - If the UID light is on solid, a firmware update failure has occurred.

10. You must either plug in the KVM dongle or use iLO Remote Console support to browse into the affected server to determine the cause of failure. Automatic Mode loads the error log into a vi editor window for review. HP recommends resolving the error before installing or restarting the operating system.

Automatic Mode might not boot with some third-party external Fibre Channel storage attached. You might need to disconnect the external storage for the duration of the update process, and reconnect it afterwards.

Updating multiple enclosures simultaneously

To update multiple enclosures simultaneously, you may use RIBCL scripts.

RIBCL scripts

RIBCL enables you to write XML scripts to configure and manage iLO 2 configuration settings, user accounts, directory settings, server settings, and HP Systems Insight Manager SSO settings. You can create your own scripts using RIBCL.

IMPORTANT: To run RIBCL scripts, you must have the iLO Advanced license.

To run the RIBCL scripts, ensure that the following prerequisites are met:

1. Apply the latest Windows® PSPs to the local host.
2. Create either an Apache or an IIS web server.
3. Copy the Automatic Mode ISO to the web server.
4. Ensure that all the iLO2 usernames and passwords match the OA username and password.
5. Install the following:

- For Windows® operating systems:
  - iLO2 Advanced license
  - OpenSSH, which you can download from OpenSSH for Windows® website (http://sourceforge.net/project/showfiles.php?group_id=103886&package_id=111688). Any SSH alternative can be used.
  - The HP Lights-Out Configuration Utility (cpqlocfg.exe), which you can download from the HP Software and Transitions website (http://h18004.www1.hp.com/support/files/lights-out/us/index.html).
- For Linux operating systems:
  - iLO2 Advanced license
  - SSLeay and IO::Socket::SSL, which can be obtained modules from Comprehensive Perl Archive Network website (http://www.cpan.org).

The following functionalities require the iLO Advanced License:

- Virtual Power—Power up, power down, or cold boot.
- Integrated Remote Console—Use any computer to gain access with Integrated Remote Console.
- Virtual Media—Use any computer DVD, CD, or USB key capability as virtual media.
- Virtual Folders—Use folders as local folders.

For more information on scripting and the syntax of the RIBCL XML, see HP Integrated Lights-Out Management Processor Scripting and Command Line Resource Guide (http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00294268/c00294268.pdf?jumpid=reg_R1002_USEN).

Sample scripts

The sample script is used to control updating firmware on blades in an enclosure. This script connects virtual media to each iLO in the enclosure. The script can either invoke the RIBCL script directly or invoke a wrapper script containing an invocation of the RIBCL script. The "for" loop at the bottom of this file contains two lines, one of which has been commented out. Comment in or out the line for the desired mode of operation.

After you have flashed the server blades, you can use the BB2.sh script to disconnect the Virtual Media by passing it the Eject_Virtual_Media.xml file as the RIBCL script to execute or Eject_Virtual_Media.sh script based on the state of the commented out lines.

```
#
# check for args
#


if [ "$TMP" == "" ]
then
  echo "Please set the TMP environment variable"
  exit
fi


usage ()
{
  echo "usage: Used to connect Virtual Media and execute a RIBCL script on each
Blade in an enclosure"
  echo "       BB1.sh <OA_ipaddress> <OA_username> <OA_password>
<script_filename>"
}


if [ "$4" = "" ]
then
  usage
  exit
fi


host=$1
user=$2
passwd=$3
script=$4


hostfile="hostlist.txt"
```

```
# If you want to use a pre-made/modified list, just comment out the if statement
# and the "show server list" line as well.
if [ -f ${TMP}/${hostfile} ]
then
  echo "removing ${TMP}/${hostfile}"
  rm -f ${TMP}/${hostfile}
fi


echo Retrieving Blade ips from OA
#
# get list of iLO ips in enclosure from OA
#
#/usr/bin/ssh $user@$host "show server list"|grep OK |awk '{print $3}' >>
${TMP}/${hostfile}
#  or do
/usr/bin/ssh $user@$host "show server list"|grep OK  >> ${TMP}/${hostfile}


#
# The for loop will loop thru the results of the above command.
# You can then invoke a RIBCL script on each ip via a wrapper shell script.
#
for ip in `awk '{print $3}' ${TMP}/${hostfile}`;
do
     echo Inserting Virtual Media on ${ip};
     ./Insert_Virtual_Media.sh ${ip} ${user} ${passwd};


     echo ${script} on [$ip];
     ./${script} ${ip} ${user} ${passwd};



done
```

Determining the success of an Automatic Mode deployment

When you boot to Automatic Mode, the UID light provides all feedback.

UID light status	Meaning
Blinking	Either a remote console is active, or the Automatic Mode is flashing

UID light status	Meaning
	firmware.
Off	The firmware update was successful.
On	At least one of the needed firmware updates failed. The remote console to the server searches for the cause of the error.

- If the UID light is off, the update process has completed, and you can install the server operating system or restore the server to its previous operating system.
- If the UID light is solid, a firmware update failure has occurred. You must either plug in the KVM dongle or use iLO Remote Console support to browse into the affected server to determine the cause of failure. Automatic Mode loads the error log into a vi editor window for review. HP recommends resolving the issue before installing or restarting the operating system. For more information on how to handle various firmware update failure scenarios, see the Troubleshooting (on page 36) section.

Special modes

Automatic Mode recognizes the following boot options at the boot prompt. The prompt is seen after the tool finishes its POST.

Boot option	Description
`console`	This option causes Automatic Mode to boot to a console prompt. All files are copied to the RAM drive. This mode can be used to add additional firmware by plugging a USB key into the c-Class SUV cable and manually mounting it or viewing the updates in console mode on a single server.
`force`	This option causes the embedded HP Smart Update Manager installation tool to force the installation of all components on the CD. This might result in an error since not all firmware can be successfully downgraded.

Advanced topics

Server virtualization detection and support

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

HP Smart Update Manager, running in the context of the Smart Update Firmware DVD, 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 Smart Update Firmware DVD 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 41). 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 41). When the installation is completed or canceled, HP Smart Update Manager stops the remote service, removes it from the target server, closes the port in the iptables firewall, and then closes the SSH connection to the target server.

Configuring IPv6 for Windows Server 2003

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

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

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

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

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

   Value name: `DisableStrictNameChecking`

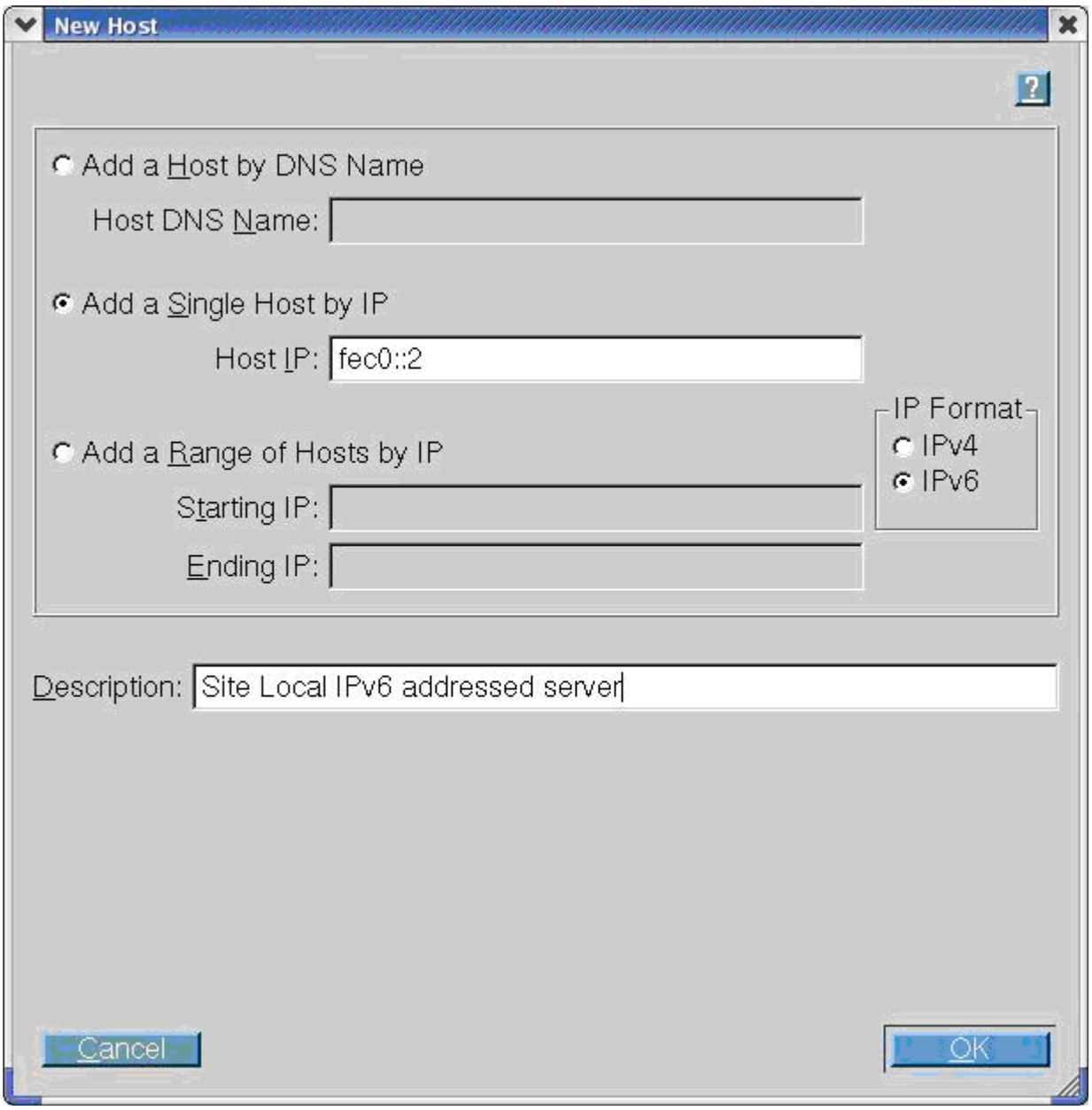
   Data type: `REG_DWORD`

   Radix: `Decimal`

   Value: 1
5. Quit the Registry Editor.

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

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



If you cannot connect to the target server or receive a `Discovery failed` message when executing HP Smart Update Manager in an IPv6 environment, see the troubleshooting section ("Troubleshooting HP Smart Update Manager in IPv6 networks" on page 45).

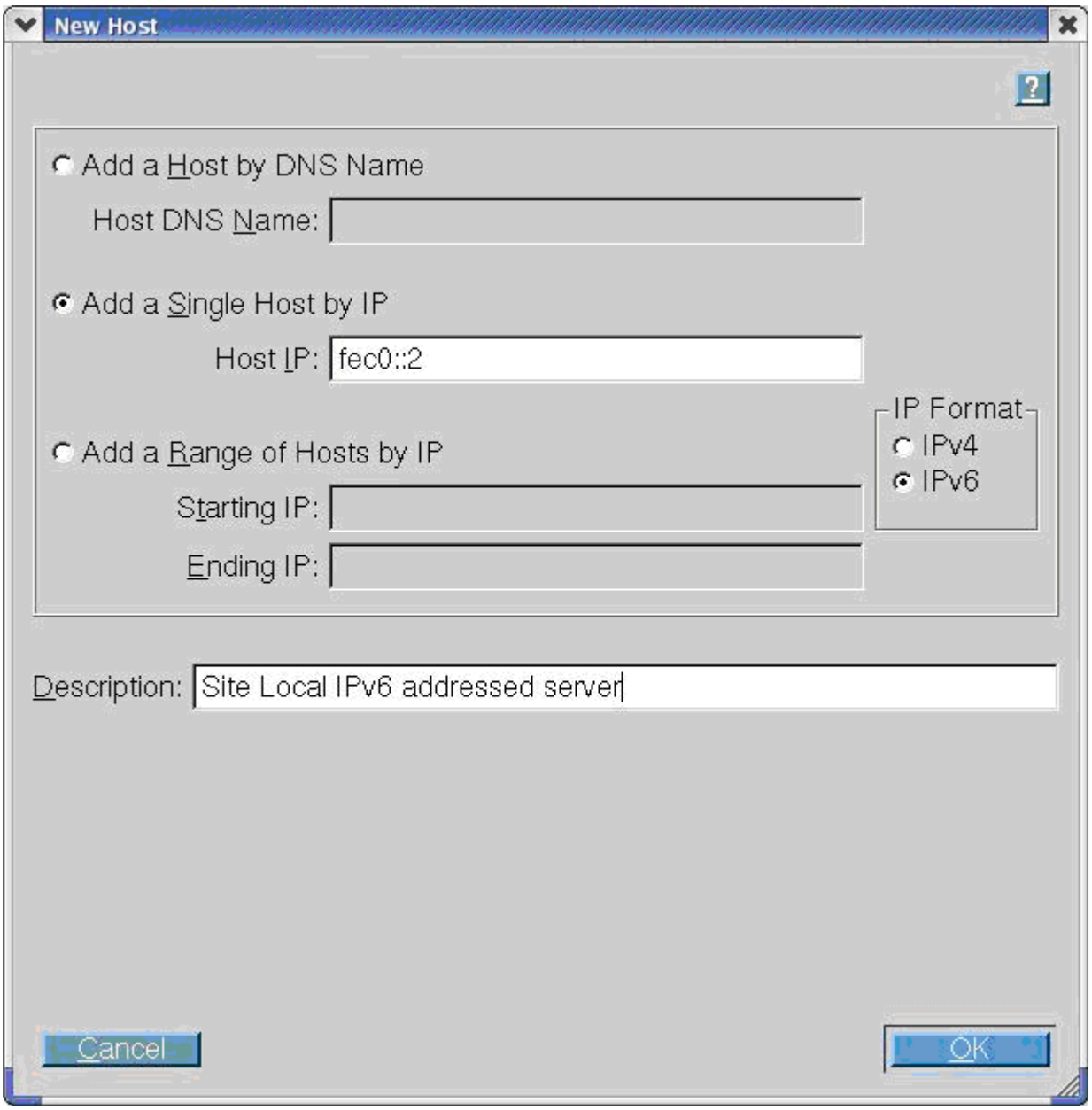
After you connect to the target server, all other HP Smart Update Manager functions work identically. Log files for IPv6 hosts are stored with all other HP Smart Update Manager files in the \CPQSYSTEM\hp\log\<ip_address> directory.

Configuring IPv6 for Windows Server 2008

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

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

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



If you cannot connect to the target server or receive a Discovery failed message when executing HP Smart Update Manager in an IPv6 environment, see the troubleshooting section ("Troubleshooting HP Smart Update Manager in IPv6 networks" on page 45).

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

Limitations of IPv6 for Windows Server 2003 and Windows Server 2008

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

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

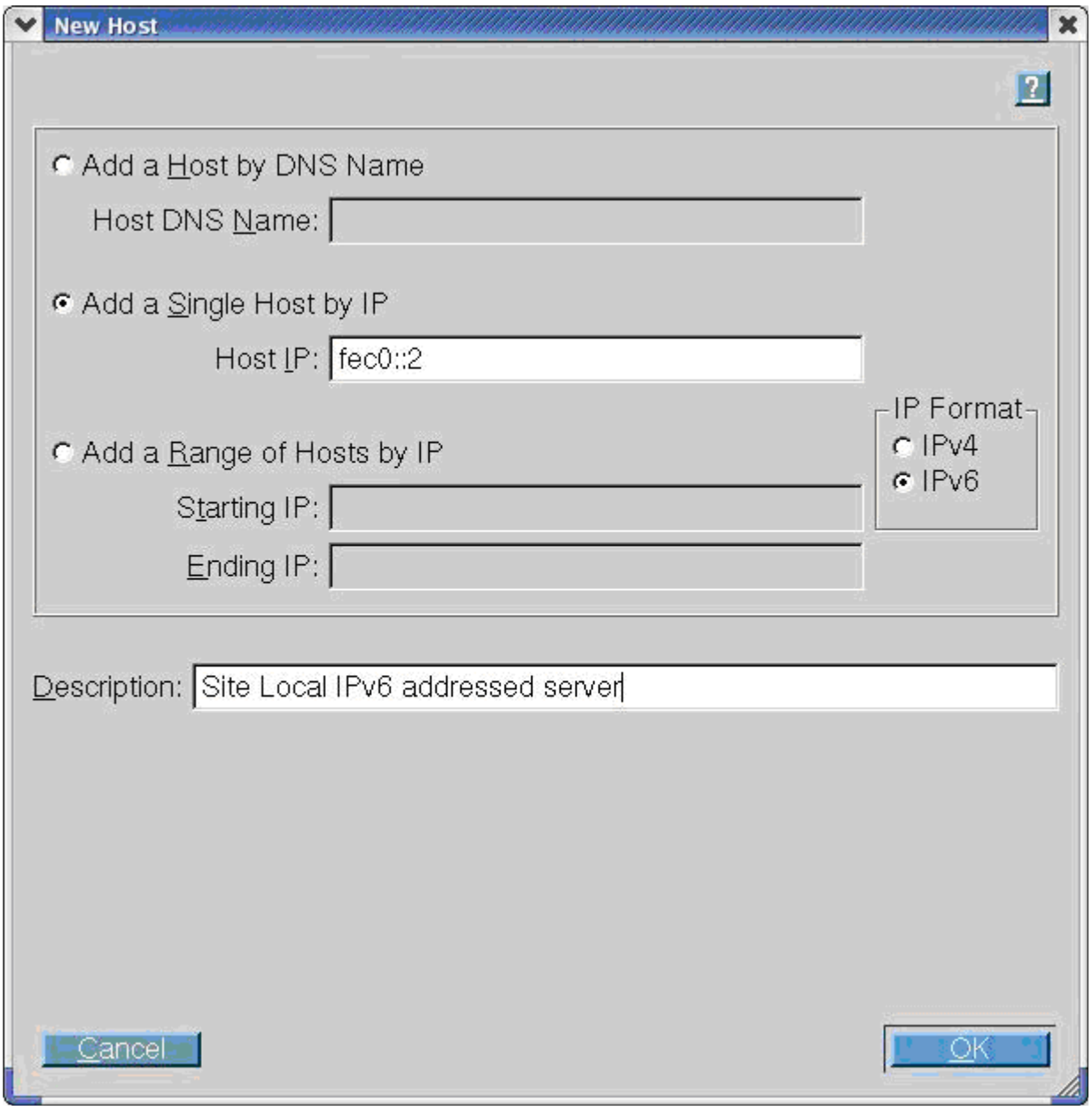
NOTE: Windows® XP clients are not supported in IPv6 networks for HP Smart Update Manager deployment.

Configuring IPv6 for Linux

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

For information on how to setup IPv6 in a Linux environment, please see the Linux IPv6 How-To (http://www.linux.com/learn/docs/ldp/592-linuxipv6-howto).

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



If you cannot connect to the target server or receive a Discovery failed message when executing HP Smart Update Manager in an IPv6 environment, see the troubleshooting section ("Troubleshooting HP Smart Update Manager in IPv6 networks" on page 45).

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

Limitations of IPv6 for Linux

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

Troubleshooting

Recovering from a failed ROM upgrade

Recovering from a failed system ROM upgrade

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

Redundant ROM recovery

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

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

To access the redundant ROM through RBSU:

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

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

If both ROM images are corrupt, use ROMPaq recovery.

ROMPaq recovery

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

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

6. Power up the server.

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

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

To manually set the server for ROMPaq disaster recovery:

1. Power down the server.
2. Remove the access panel.
3. Set the system maintenance switch positions for disaster recovery. Switch positions are server-specific.For information about the correct settings for your server, see the server documentation.
4. Insert a ROMPaq diskette with the latest system ROM from the HP Smart Update Firmware DVD or the HP website (http://www.hp.com/support (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 the 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, iLO 2, and iLO 3, see the documentation for your particular Lights-Out management product on the Remote management website (http://www.hp.com/servers/lights-out).

Recovering from an installation failure

Collecting trace directories

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

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

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

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

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

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

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

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

Recovering from a discovery failure

Troubleshooting connection errors

If you are receiving an HP SUM Connection Error or Discovery Failed messages, follow these troubleshooting tips:

- Ensure your workstation does not have an existing connection to the ADMIN$ share on the target IP address. If it does, it prevents HP SUM from connecting to the remote server's share because Windows only allows one connection from a client to a server's share. This can be verified by entering `net use` at a command prompt. If a share to the target IP address \admin$ share exists, delete it, and then attempt the installation again.
- Ensure that the target IP address server's admin$ share is accessible. Validate the target server can be accessed by entering `net use x: \\<ip_address_or_dns_name>\admin$` for the target server IP address or DNS name. When the connection is validated, ensure that it is deleted by entering `net use x: /d` at the command prompt.
- Ensure the user ID being used to connect to the target IP address server is part of the administrator's group. If it is not, HP SUM blocks installation to the target.
- Ensure WMI is enabled and running on all Windows target servers.
- For Windows target servers, enter the username in `DOMAIN\USER` format, where `<user>` is the administrative username, and `<domain>` is either the NETBIOS computer name or the AD domain name for this user account.
- For Linux, ensure the SSH port is not blocked.

- In rare cases, external storage enclosures might cause HP SUM to report a discovery failure or to hang. To resolve this issue, disconnect the external storage until the firmware updates are completed.
- For Linux, ensure that the target server can be contacted through SSH and that the `scp` command is available to securely send files to the target server.
- Ensure the firewall ports on any routers in the network as documented in the Enabling ports in HP Smart Update Manager section of this document.
- The SEP product blocks HP SUM ability to communicate with remote targets if the Network Threat Analysis feature is enabled. Disable this feature while HP SUM is in use on the workstation.
- Examine the OpMan.trace, IPScout.trace, OSScout.trace, discagent.trace, and discmanager.trace files to determine the cause of the failure. For more information, see "Collecting trace directories (on page 38)".
- Ensure the server has a valid serial number.

HP SUM hangs during discovery

If a system hang is observed during HP SUM discovery and the system is connected to external storage, in most cases disconnecting the external storage should resolve the issue.

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 41).

Recovering from a blocked program on Microsoft Windows

Configuring Windows firewall settings

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

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

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

For Direct to iLO support, you must enable ping.

Enabling ports in HP Smart Update Manager

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

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

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

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

For Windows®

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

For Linux

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

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

Recovering from operating system limitations when using a Japanese character set

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

You might specify a message to appear before the system shuts down 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 before the system shuts down 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 click **Exit**. When the message is entered using CLI, the reboot message looks corrupted since the Japanese character set is not supported in CLI.

Recovering from Fatal Error - application will exit message

Running in a directory path containing double-byte characters

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

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

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

Running HP Smart Update Manager on SUSE LINUX Enterprise Server 9

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

NOTE: HP SUM is no longer supported on SUSE Enterprise Linux 9.

Recovering a lost HP Smart Update Manager connection

HP Smart Update Firmware DVD mounted using iLO virtual media

When either iLO and NIC firmware are updated, the HP SUM connection is lost and cannot install components.

Booting the Firmware DVD from iLO virtual media is only supported in Offline Automatic Firmware Update mode. Users attempting to boot in this manner might experience issues from connection timeouts, difficulties updating iLO firmware, and mouse syncing issues. If an access error exists, HP SUM cancels the installation.

Troubleshooting HP Smart Update Manager in IPv6 networks

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

Troubleshooting HP Smart Update Manager in IPv6 Windows Server 2003 environment

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

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

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

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

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

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

- Ensure you have made the registry change on remote target servers as mentioned in the HP Smart Update Manager Usage in a Windows Server® 2003 IPv6 environment ("Configuring IPv6 for Windows Server 2003" on page 29).
- Move back to an IPv4 network address to ensure HP Smart Update Manager properly finds the remote target server without any issues.

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

Troubleshooting HP Smart Update Manager in IPv6 Windows Server 2008 environment

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

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

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

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

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

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

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

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

  You must enter the root password for the target Linux server at the console to complete the IPv6 connection.
- Validate that you can ping the remote target server. In Linux, you need to use the ping6 command to ping IPv6 addresses: ping6 <ipv6 address>.

- Ensure you can ping the IPv6 loopback address: ping6 ::1.
- Use the DNS hostname instead of IPv6 address to ensure the address is correct.
- Use `ipconfig` to validate you have IPv6 addresses assigned to your NICs. For more information about troubleshooting your configuration, see the Linux IPv6 How-To (http://www.linux.com/learn/docs/ldp/592-linuxipv6-howto).
- 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.

HP SUM found new hardware message

During the discovery progress, HP SUM might display the following pop-up message: `Found New Hardware`. This message appears because one of the self-discovery components is loading a new driver and the Windows operating systems discovers it as a new piece of hardware.

Similar pop-up messages might occur with Windows® 2008 operating systems when the **Allow Non-bundle version** option on the Select Bundle Filter screen is selected.

Non-matching systems error reported when building source Linux RPMs or installing Linux RPMs built from source

If HP SUM reports non-matching systems error when trying to build source Linux RPMs or installing Linux RPMs built from source, then the operating system on the target server does not match the operating system from which you are running HP SUM in one of the following ways:

- The distribution of the operating system does not match. For example, RHEL 4.7 and RHEL 4.8 would be a mismatch.
- The architecture of the two operating systems does not match. For example, one server might be running an operating system with x86 architecture and the other with x86_64 architecture.
- The kernel version running on the two systems does not match.

Resolution options:

1. Run HP SUM on the target server itself instead of remotely deploying HP SUM.
2. Build the driver RPM locally and take the resulting RPM file from the standard location (for example, /usr/src/redhat/RPMS/i686/<driver>.rpm) and then copy it back into the HP SUM repository. HP SUM will pick up the pre-built RPM and enable the user to deploy it anywhere they choose.

Linux component version discrepancy for source RPMs

You might observe differences in the RPM component name which might appear to be a version mismatch for the component on the Select Item to be Installed screen and the Installation Results screen. This is caused by the RPM build phase. The resulting component is actually the same version. The RPM build adds information, so it is technically the same component.

For example, if you select the component `HP NC Series Mellanox 10GBE Driver for Linux` on the Select Items to be Installed screen, it appears as `hp-minx-en-1.4.3.1-1.src.rpm` and on the Installation Results screen, it appears as `hp-minx-en-kmp-default-1.4.3.1_2.6.27.19_5-1.x86_64.rpm`.

HP SUM displays No components found in the selected repository(ies) message

The `No components found in the selected repository(ies)` error appears when at least one space is in the path name of the repository containing the components to be installed.

To resolve this issue, make sure no spaces are in the path name.

Additional/Optional Actions columns are grayed when HP SUM is maximized

If the Select Items to be Installed screen or Installation Results screen in HP SUM is maximized, the Additional column and sometimes the Optional Actions columns are grayed out.

To resolve this issue, restore the screen to the original size.

Installation of components failed with 'Update returned an error' when installing Linux RPMs

When installing any component, if the installation fails, then HP SUM displays `Update returned an error` message. To determine the installation failure, review the associated component log.

However, when installing RPMs using HP SUM you might see this error when the RPMs for more than one Linux distribution are present in a single repository and a PSP bundle from the Select Bundle Filter screen is not selected.

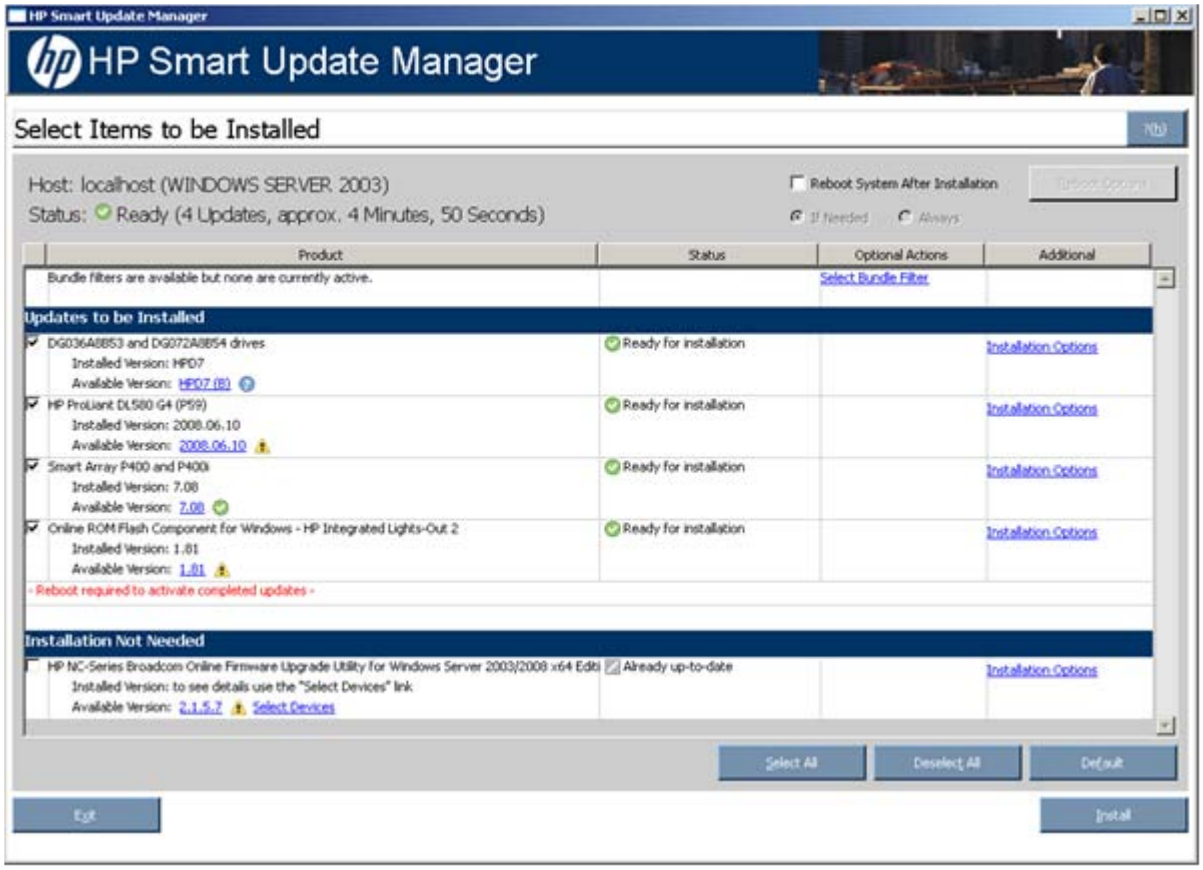
In this scenario, when multiple versions of source RPMs exist, the RPMs that are not the latest are not installed and `Update not needed` or `Not Updated-already current` messages are returned. HP SUM cannot determine which source RPMs go with which distribution because the RPMs do not contain any operating system information.

To resolve this issue, make sure to select the bundle for the OS distribution on the Select Bundle Filter screen for installation or remove the RPMs from the directory that are not applicable to the Linux distribution you are using.

Issues related to bundle filtering on the Select Items to be Installed and Select Bundle Filter screens

If you specify a bundle to use for installation when starting HP SUM (for example, hpsum /b bp000690.xml), you might experience one or more of the following:

- No bundles listed on the Select Bundle Filter screen.

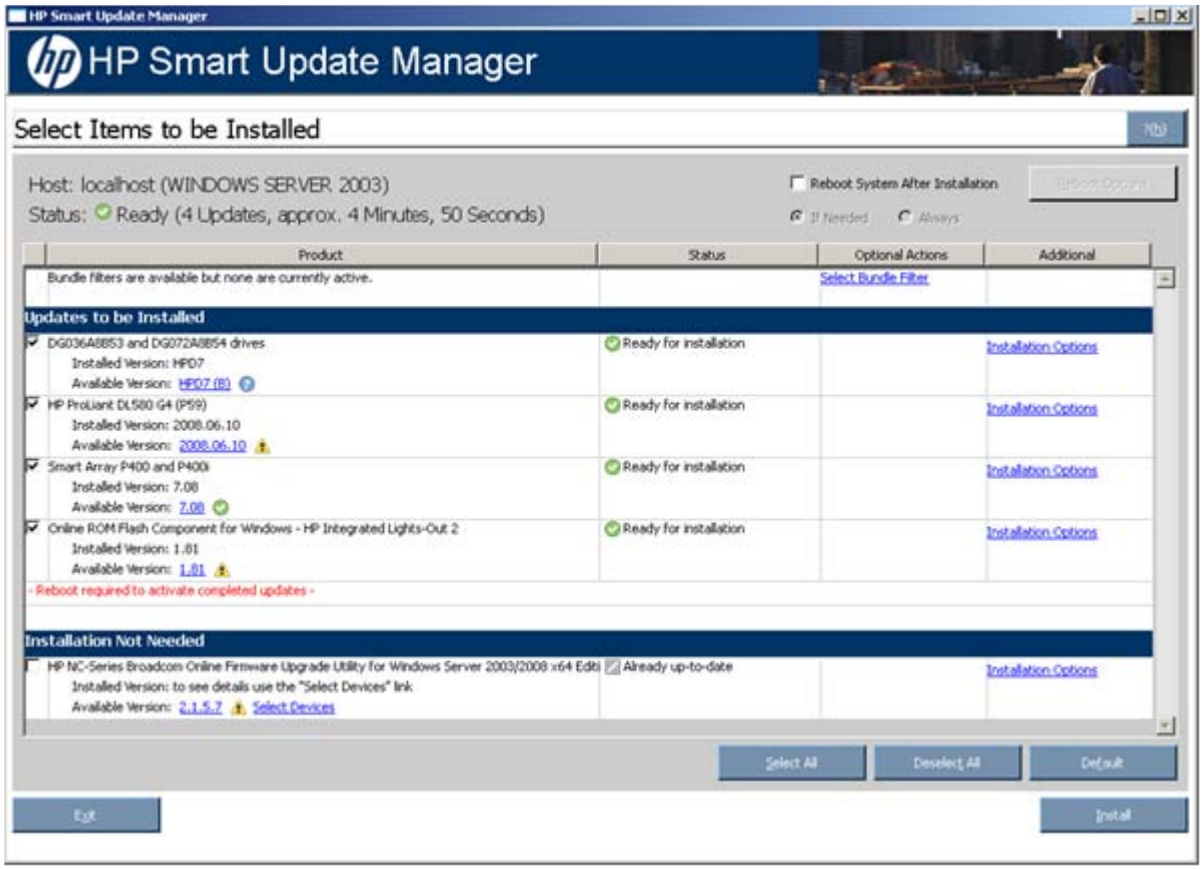


  If you specify a bundle when starting HP SUM, then the Select Bundle Filter screen is not shown and the Select Items to be Installed screen appears with the specified bundle listed as the filter. This is expected, as a bundle was preselected.

  If you then select the **Select Bundle Filter** link, then the Select Bundle Filter screen appears with no bundles available for selection. This issue occurs because HP SUM only recognizes the specified bundle and no others, even if other bundles are present in the repository. Even though this issue occurs, HP SUM is working as designed.

- No bundle being used as a filter on the Select Items to be Installed screen.

If you experience the first issue and then select **OK** on the Select Bundle Filter screen to return to the Select Items to be Installed screen, the bundle you originally specified is no longer listed as the filter. To use your bundle as the filter, you must exit and restart HP SUM.



If this issue occurs, from the GUI run HP SUM.

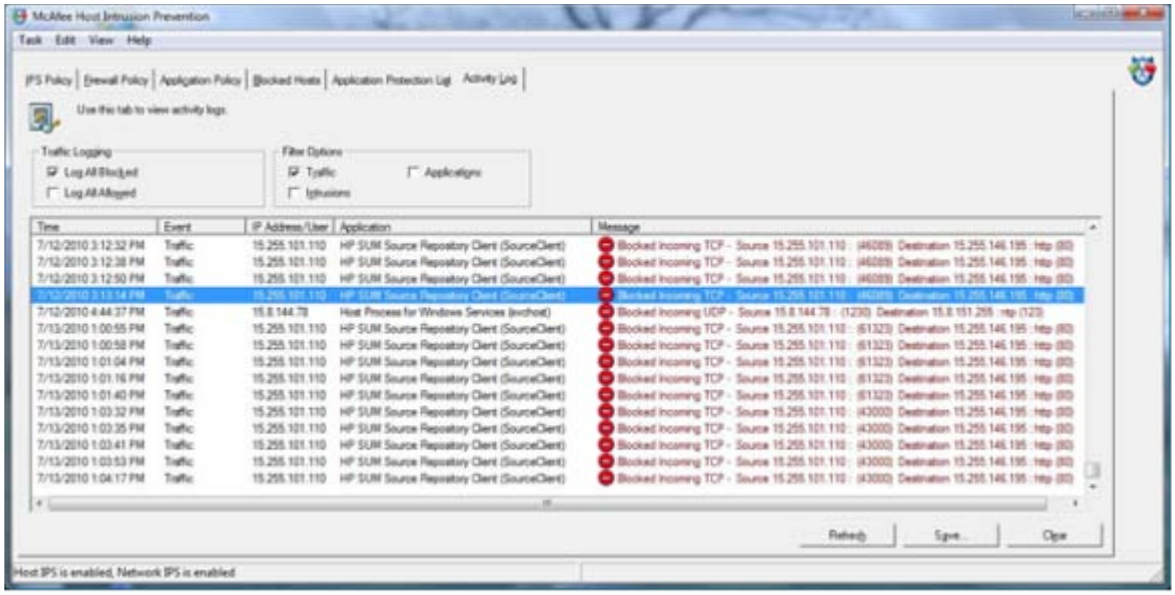
HP SUM fails on Windows Vista® due to McAfee firewalls

This is a known issue with McAfee that McAfee firewalls block HP SUM traffic.

To resolve this issue, enable the port traffic associated with the HP SUM application by performing the following steps:

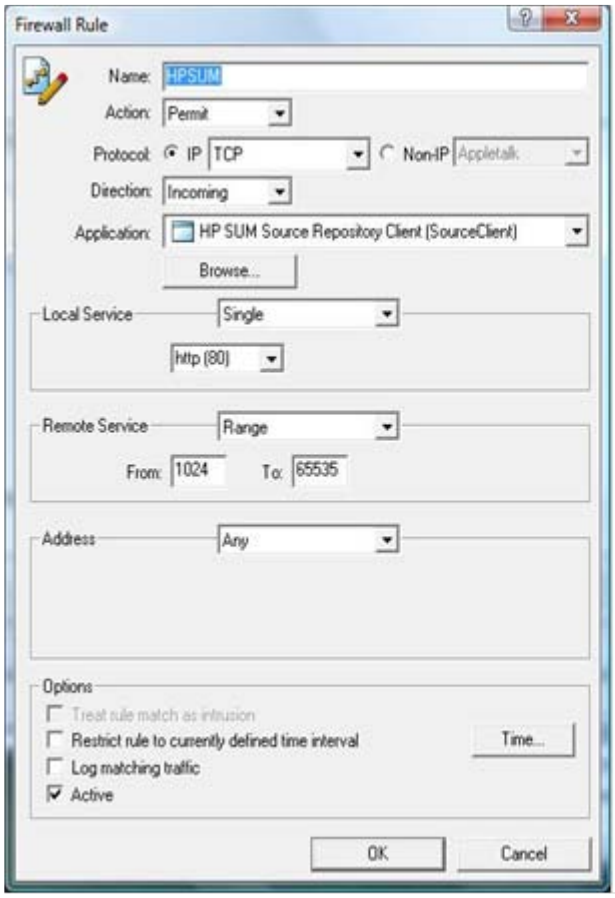
1. From the system tray, click the **McAfee** icon.
2. Select **Manage Features**.
3. Select **McAfee Host Intrusion Prevention.**
4. Select the **Activity Log** tab.

As displayed in the following image, in the Message column, notice the entry similar to the following: `Blocked Incoming TCP from the HOST (15.255.101.110) during execution of HP SUM`.

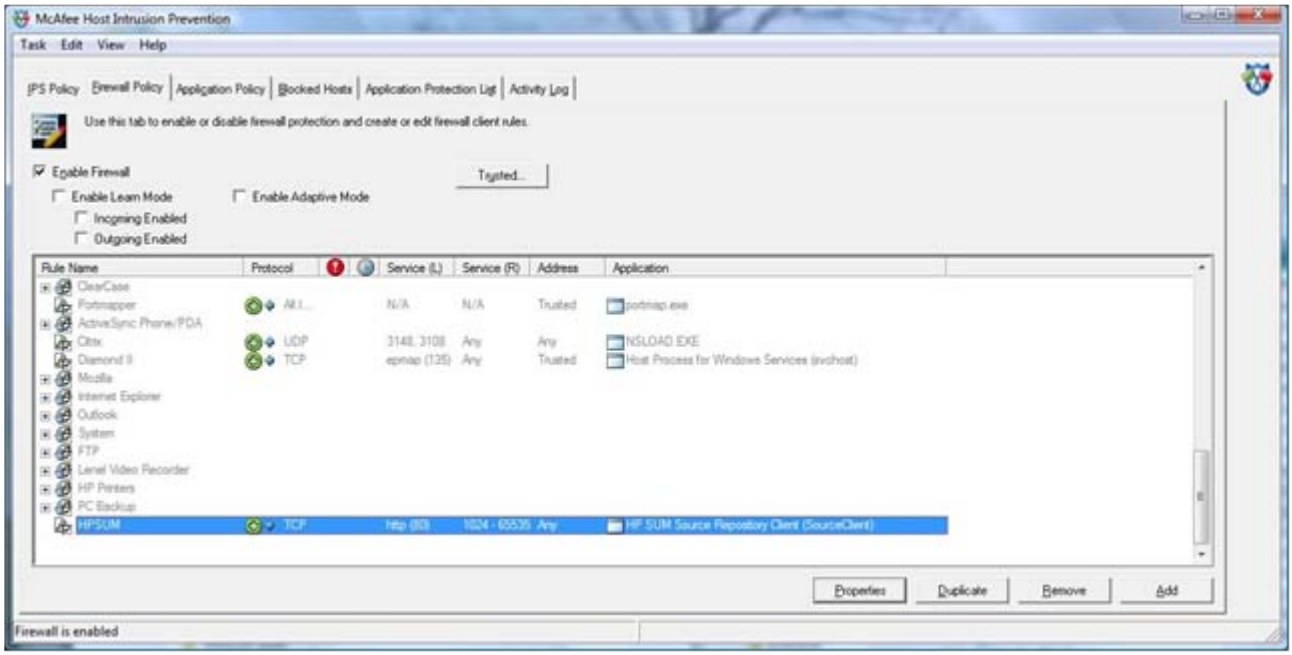


5. From the menu, select **Task>Unlock Interface**.
6. Enter the password of the McAfee user interface.
7. Select the **Firewall Policy** tab.
8. On the bottom of the screen, click **Add (Add new rule)**.

9. From the screen image, use the following settings for the new firewall rules on your system.



10. Click **OK** to ensure new firewall rules have been implemented.



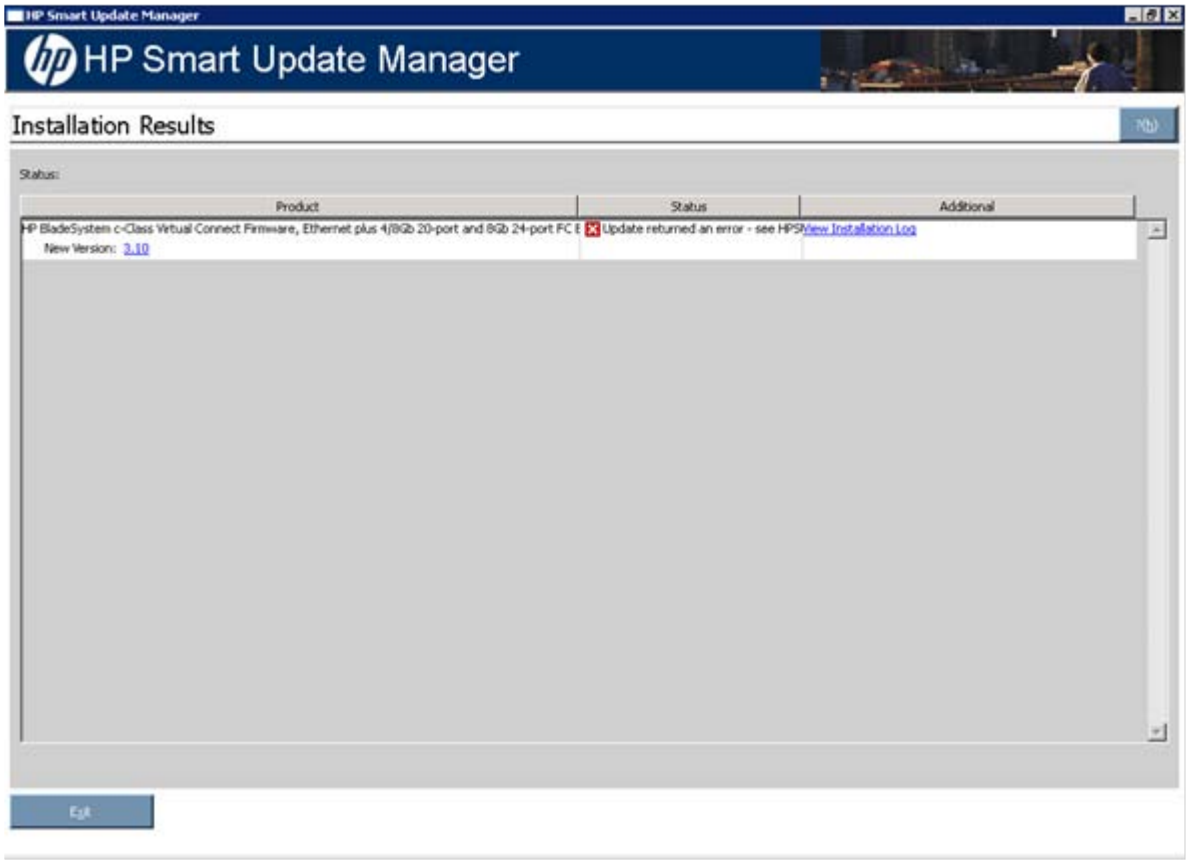
11. Restart HP SUM.

Performing these steps allows HP SUM to function, although after a period of time (ranging from minutes to hours), McAfee disables HP SUM access.

Virtual Connect firmware upgrade using HP SUM fails if VC reports an invalid or bad health state

Virtual Connect firmware can be upgraded using HP SUM only if the health state of the VC is in a good state. If the health state is `invalid` or `bad`, HP SUM does not upgrade the VC firmware.

If a VC upgrade is attempted in an invalid or bad health state, HP SUM installation fails. The details of the failure can be viewed in the installation log by clicking the **View Installation log** link in the Additional section.



Some of the VCSU Health Status `bad` states are:

- VC module is not redundant
- Cannot authenticate to OA (bad OA IP or User/Password) or to VCM (bad VCM IP or User/Password)
- Could not retrieve a list of modules in the domain or the module is empty
- For any modules, the power is not `ON`, the hardware health is not `OK`, cannot connect to module IP address, or the module role is `Unknown`
- OA version is version 3.00 or earlier, or the VLAN feature is enabled and VC modules are on a different VLAN ID than OA
- VCM Domain checkpoint is not valid
- VCM Module adjacent to the Primary VCM is not compatible with the Primary VCM

To resolve this issue, the VCSU must be used to upgrade the firmware.

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, see the Microsoft® website (http://www.microsoft.com).

For information about Linux operating systems, see 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

HDD

hard drive

HPSUM

HP Smart Update Manager

I/O

input/output

iLO

Integrated Lights-Out

iLO 2

Integrated Lights-Out 2

LO100

HP Lights-Out 100

NIC

network interface controller

POST

Power-On Self Test

PSP

ProLiant Support Pack

RBSU

ROM-Based Setup Utility

RIBCL

Remote Insight Board Command Language

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

VSM

Virtual SAS Manager

WMI

Windows Management Instrumentation

Index

S

T

U

W