Hewlett Packard
Enterprise

# SUM Best Practices Implementation Guide

**Abstract**

This document describes the best practices for performing a firmware and software update for your server environment with SUM. This document is intended for individuals who perform updates and understand the configuration and operations of Microsoft Windows, Windows Server, Linux, smart components, and the risk of data loss from performing updates.

Part Number: 613178–007a
Published: 1 2017
Edition: 2

# Contents

# Introduction to SUM Best Practices

Updating firmware, software, and drivers is crucial for maintaining servers, enclosures, and other infrastructure systems within an enterprise. This document describes the best practices for using SUM, SPP, and other tools to update ProLiant and Integrity, Moonshot product firmware, software, and drivers, including:

- Information to help identify a firmware maintenance strategy
- Determining which firmware to update
- Selecting the appropriate tools to perform firmware updates
- Considering the process dependencies
- Guidance for performing firmware updates

**NOTE:**

Not all update tools and procedures work for all servers.

The update strategies in this guide are intended to minimize downtime and provide the least intrusive method of updating the OA, VC, iLO, Ethernet, servers, and other components in your environment.

## Explanation of SUM guides

These guides are written to help you create strategies for using SUM with update packages.

- *SUM Best Practices Planning Guide*

  –Provides an outline for creating a firmware update plan to follow before updating your server environment.
- *SUM Best Practices Implementation Guide*

  –Provides examples for implementing an update.

You can find these guides on the SUM Information Library at **http://www.hpe.com/info/sum-docs**.

# Using SUM

## Minimum requirements for SUM

For more information about the minimum requirements for SUM, see the *Smart Update Manager Release Notes* at **http://www.hpe.com/support/SUM-RN-en**.

## SUM execution modes

SUM provides the following modes of execution for users: GUI, command-line, Input file, interactive command-line, and Linux RPM deployment script.

For details on the GUI, interactive CLI, and RPM modes see the *Smart Update Manager User Guide* at **http://www.hpe.com/support/SUM-UG-en**.

## SUM Deployment modes

The following key terms apply when using SUM to deploy updates:

| Term | Definition |
|---|---|
| Local | The installation runs on the physical hardware you are updating. For example, running a utility on a server to update the server's system ROM. |
| Remote | The installation runs on one system, but updates other physical targets. For example, updating the OA or Integrity server firmware across a network. |

*Table Continued*

| Term | Definition |
|---|---|
| Online | The installation occurs while the host processor is running in the normal server environment. For example, if the server runs Microsoft Windows Server 2008, the update occurs under this environment. The update does not require you to boot to a special environment to update the firmware. You might need to reboot the target to activate the firmware. |
| Offline | In offline mode, the SUM boots a small Linux kernel and enables updates to occur on a single server.<br>• Only updates the local system<br>• Only uses a single repository<br>**NOTE:**<br>Some features of SUM that require the regular local host operating systems are not supported in offline mode.<br>**NOTE:**<br>Offline deployment for Scalable Update groups slightly differs from this offline mode. SUM can remotely deploy offline updates to Scalable Update groups. SUM powers down the Scalable Update group nodes and deploys updates. |

These terms can be used in combination to designate the type of environment required for updates to occur, such as local-online or remote-online.

Offline mode does not support all functions SUM can perform in online mode, including:

- Network functionality
- Configuring components
- Using baselines outside the location running SUM
- Associated nodes
- Updating remote nodes

# SUM CLI mode and Input files

The SUM CLI and Input file modes allow you to deploy updates from a baseline to the local and remote nodes. In CLI mode, add all parameters in one command line to execute the entire sequence on multiple nodes without any user interaction. This method requires the `silent` command. You can update one or more nodes using this method.

Use Input file mode to add all parameters to a text file, and then call SUM using the `inputfile` parameter with the text file name as the parameter. This method requires the `silent` parameter. Using the Input file method allows you to provide a larger number of nodes to update.

The SUM CLI and Input file modes are process-oriented tools. SUM finishes the command, and then it does not save the settings or results. If you want to perform a few steps and save the work for later, use the GUI or interactive CLI mode.

| CLI Mode | Number of nodes | Scripting strengths |
|---|---|---|
| CLI | 1-45 | Use one command to issue all instructions to the nodes. |
| Input file | 1-45 | • Create a file that includes all information for baselines and nodes.<br>• Save files for future use.<br>• Review potential typographical errors before running the script. |

# SUM special considerations

## Disabling BitLocker to permit firmware updates (Windows only)

To allow firmware updates, temporarily disable BitLocker support:

**Procedure**

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 windows, and then start the firmware update.

To enable advanced startup options:

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

The following table describes TPM detection scenarios that you might encounter.

| Scenario | Result |
|---|---|
| TPM is detected and enabled, using GUI mode, and a system ROM must be updated. | SUM displays a warning message indicating that it detected TPM. SUM offers an option to **Ignore Warnings**. You can only deploy the updates if you select **Ignore Warnings**. |
| TPM is detected and enabled, using CLI or Input file mode, the `/tpmbypass` switch is not given, and firmware must be applied to the server. GUI mode does not support `/tpmbypass`. | No 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. |

*Table Continued*

| Scenario | Result |
|---|---|
| TPM is detected and enabled with Option ROM Measuring, using GUI mode, and a system ROM must be updated. | A warning message appears. After selecting **OK**, you can continue. The installation is not canceled. |
| TPM is detected and enabled with Option ROM Measuring, using CLI or Input file mode, the `/tpmbypass` switch is not given, and any firmware updated must be applied to the server. | No 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. |
| TPM is detected and enabled, using CLI or Input file mode, the installation occurs, and the `/tpmbypass` switch is supplied. | The installation occurs. |

In the SUM GUI, you can disable TPM on the Deploy screen. You can also disable TPM in CLI or interactive CLI mode.

## HPE Integrity servers running OpenVMS or Non-Stop

SUM interacts only with the management interface on Integrity systems running OpenVMS or NonStop operating systems. SUM provides enclosure and platform firmware updates. You must manually update I/O card firmware using the EFI packages method on these systems.

## Using Linux root credentials

If you run SUM from a Linux system and you have not logged into the system as a root user, you can still update targets from the CLI or GUI if you use Linux root credentials. In SUM GUI mode, you can enter the Linux root credentials on the Enter Credentials screen when you select targets. In CLI mode, use the sudo commands available for command lines. For more information about the prerequisites on using root credentials, see the *Smart Update Manager User Guide* or *Smart Update Manager CLI Guide*, depending on which mode you are using: **http://www.hpe.com/info/sum-docs**.

## SUM network ports used

SUM requires that certain network ports are available. If you lock down network ports, make sure that the ports listed in the network port tables are open so that SUM works correctly when connecting to remote node servers and hosts. If you are unable to unlock these network ports, you must run SUM locally and update network-based hosts through their web interfaces (for example, the OA, iLO, and VC modules).

**NOTE:**

Use the `open_firewall` parameter for SUM to automatically open the required firewall ports on the local host and any remote servers.

Updates for most node types require network traffic in both directions between the server running SUM and the node. The server running SUM creates a local HTTP server, which is used to serve firmware binaries to the node and to communicate node status. The remote node issues HTTP requests and posts status updates to the server running SUM during the update process. If there is a routing problem or firewall blocking traffic back from the remote node to the system running SUM, firmware updates might be blocked, status updates blocked or delayed, or both.

After creating the initial communication binds to one of the available ports, SUM traffic can move to a dedicated high-number port number (greater than 1024). This frees up the initial port for new requests.

| **System running SUM** | **Target node type** | **Inventory phase** | | | **Deployment phase** | | |
|---|---|---|---|---|---|---|---|
| | | To target | From target (SUM 7.2.1 and earlier) | From target (SUM 7.3.0 and later) | To target | From target (SUM 7.2.1 and earlier) | From target (SUM 7.3.0 and later) |
| Windows | Windows | 445, 135, 137, 138, 139 | 63001, 63002 | None | 445, 135, 137, 138, 139 | 63001, 63002 | None |
| Windows or Linux | Linux | 22 | 63001, 63002 | None | 22 | 63001, 63002 | None |
| Windows or Linux | HP-UX | 22, 63002 | 63001, 63002 | 63001, 63002 | 22 | 63001, 63002 | 63001, 63002 |
| Windows or Linux | VMware | 443, 5989 | 63001, 63002 | 63001, 63002 | 443, 5989 | 63001, 63002 | 63001, 63002 |
| Windows or Linux | OA | 22, (80), 443 | None | None | 22, (80), 443 | None | None |
| Windows or Linux | iLO, VC, FC switch, SAS switch, Moonshot, Superdome 2/X | 22, (80), 443 | VC components: 63001, 63002 | None | 22, (80), 443 | 63001, 63002 | 63001, 63002 |

SUM uses port 63002 to communicate between the `hpsum_binary` and `hpsum_service` applications on both Windows and Linux systems. If ports are listed in both columns, SUM communicates bidirectionally.

**NOTE:**

Windows to Windows traffic uses WMI, a standard DCOM-In port 135 and Async-in and WMI-in.

Issue the commands `/port` and `/ssl_port` to change from ports 63001 and 63002 if there are firewall conflicts. Use `--open_firewall` to open the HTTP and HTTPS ports used by SUM for external access. Open these ports for remote node functionality and for remote browser access. For example:

```
hpsum /port 80 /ssl_port 443
```

You can issue the command `/ftp_port` to assign which port to use for FTP service. By default the FTP port is disabled. Use the command to enable the service.

## Changing the port address in the `.ini` file

You can change the network ports SUM uses by editing the `sum.ini` file or using the `/port` or `/ssl_port` CLI parameters. For more information on using SUM CLI mode, see *Smart Update Manager CLI Guide*.

The following commonly used alternate network ports are:

### Procedure

1. `port=63001` edit to `port=80`.
2. `ssl_port=63002` edit to `ssl_port=443`.

# Downloading the server updates

## Downloading an SPP

**Procedure**

1. Open a web browser and go to the SPP website at **http://www.hpe.com/servers/spp/download**.
2. On the **Download** tab, click **SPP ISO Image**.
3. On the Drivers & software page, click **Obtain software**.

   **NOTE:**

   SPP downloads require an active warranty, HPE Care Pack, or support agreement linked to your HPE Passport.
4. Click **Documentation** to view the documentation for the latest SPP release.

## Custom SPP downloads overview

On the SPP downloads page, you can generate a custom SPP that includes only the components you select. Use filters to select the components you want to view. You can then select components that apply to your environment. The SPP website generates an SPP for you that you can download and might be smaller than the entire SPP.

## Downloading the HPE Integrity firmware bundle

**Procedure**

1. Open a web browser and go to the Integrity website at **http://www.hpe.com/info/integrity**.
2. Click **Support and Drivers**.
3. Click **Drivers & Software**.
4. Enter your product model and then click **Search**.
5. Click your product.
6. Click the operating system your product uses.
7. Click **Download** for the firmware bundle you want to use.

   **NOTE:**

   You can download Integrity release sets from the BladeSystem Release Sets for Integrity website at: **http://www.hpe.com/info/smartupdate/integrity**.

## Downloading the HPE Moonshot Component Pack

**Procedure**

1. Open a web browser and go to the Moonshot website at **http://www.hpe.com/info/Moonshot/download**.
2. Follow the instructions to download the Moonshot file.
3. Click **Documentation** to view the documentation for the latest release.
4. On the **Download** tab, click **Full Component Pack**.
5. Follow the instructions to download the file.

# Downloading the latest version of SUM

**Procedure**

1. Open a web browser and go to the SUM website at **http://www.hpe.com/servers/sum**.
2. Click **Download**.
3. Select the version of SUM you want.
4. Click **Download**.

# Deploying server firmware

## Updating server firmware overview

The following list is an overview of the update instructions for all environments.

**Procedure**

1. Download the updates, for example SPP or Integrity bundle. For more information, see **Downloading the server updates**.

   **NOTE:**

   The SPP and Integrity bundles include a version of SUM that can deploy the updates in the bundle. You can download the latest version of SUM from the website **http://www.hpe.com/servers/sum**.

2. SUM allows you to use the entire update package, or create custom baselines with selected components from the update package. Custom baselines can include only components that apply to your environment. Create environmental baselines and backup plans for your environment. This allows you to save a backup of the firmware, software, and drivers on each server if you need to deploy the updates again.
3. Create a test lab or test server to represent your network environment.
4. Use SUM to generate installed component versions and available updates reports for your nodes.
5. Update one server for your lab environment or a test server. Allow it to run for 72 hours to verify that no problems exist before updating the remaining targets in your environment.
6. Verify that all updates installed correctly. Use the Gather Logs utility after exiting SUM.
7. If needed, troubleshoot problems.

## Creating a custom baseline in SUM

SUM 7.0.0 and later includes a function that allows you to easily create a baseline of components from your update repositories. You can create baselines based on operating system, node, and update criticality. This allows you to create a new update baseline that includes only updates for a specific server, or set of servers. For more information on using SUM to create a baseline, see the *Smart Update Manager User Guide*.

## Installation scenarios using SUM

### Updating one or more servers in a single location

**Procedure**

1. Download your updates. For more information, see **Downloading the server updates**.
2. Unpack the download, mount the files, or copy them to a USB key.
3. Use automatic mode or interactive mode from the SPP. For more information about implementing the firmware, see **Implementing firmware** on page 17.

### Updating HPE Integrity enclosures

When you update an entire enclosure, use SUM in a single session to update OA, VC, and iLO nodes at one time, and then update HP-UX nodes. The update procedure is normally the same for c-Class and Superdome 2 enclosures:

SUM 6.x and later update instructions

**Procedure**

1. Start with servers powered on and running HP-UX.
2. Launch SUM, and add Integrity bundles as baselines to the Baseline Library. For more information on adding repositories in SUM, see the *Smart Update Manager Online Help* or *Smart Update Manager User Guide*.
3. Add the HP-UX servers as nodes.
4. Add the OA, VC, and other nodes.
   a. In c-Class systems, all installed blades and VC are discovered as associated targets.
   b. In Superdome 2/X systems, all partitions are discovered, although this is not visible until the Review/Install screen. Partitions are managed as part of the single enclosure target.
5. Enter user credentials for all nodes.
6. Select a baseline for each node.
7. Inventory the nodes.
8. Set the reboot options for the node.
9. Generate the updates to be installed report.
10. Deploy the updates from the OA node. SUM sequences the OA, VC, and then associated iLO nodes.
11. Deploy the updates for the HP-UX nodes.
12. After SUM finishes the updates, and the targets have rebooted, you can continue with other updates not controlled by SUM.
    a. On non-HP-UX systems, EFI packages can be used for updating I/O cards.
    b. You can install HP-UX software and driver patches.

## Updating server firmware for distributed corporate environments

**Procedure**

1. Download your updates. For more information, see **Downloading the server updates**.
2. Gather IP addresses for the OA, VC, iLO, and at least one NIC in each target.
3. Run a VCSU health check for all VC modules to make sure the VCs are in a good health state and you can apply updates to them.
4. Generate reports in SUM for the gathered OA, VC, iLO, and server IP addresses. SUM builds a report of the currently installed firmware versions, and required updates. The report does not generate information for offline targets or components.
5. Update your servers and other nodes. If the nodes are in a c-Class enclosure, see the *SUM Best Practices Planning Guide* for information about the installation order. To download the guide, see the information library website at **http://www.hpe.com/info/sum-docs**.

   You have multiple options for staging the server updates, if you want to apply offline updates:

   - Burn multiple DVDs or create multiple USB keys. Send the physical media to each remote location and use the automatic update mode of the SPP.
   - Set up PXE or iLO Virtual Media to boot the SPP.
   - Copy the ISO contents to one staging computer, and then write a script to install it locally on all servers.
   - For ProLiant G7 servers and earlier, use the `SmartStart Scripting Toolkit`. For ProLiant Gen8 servers and later, use the `Scripting Toolkit`.
   - Install updates on each server individually across a network.
   - Copy the SPP to one computer at the remote location using a network share (Windows) or NFS mount (Linux), and then write scripts to install updates on remote targets.

- Copy the SPP and use iLO Virtual Media to boot each remote system to the SPP and have the automatic mode update the servers.
- Copy the files from the `\hp\swpackages` directory on the SPP to the remote servers and use SUM directly using the silent, express, or GUI mode.

**NOTE:**

If you are copying to a server that is used to perform the update, and that server needs to be updated, update the server separately.

- Use PXE boot to move the SPP over the network.
- For online updates run from a central management station or server, you can update all servers, iLO, OA, and VC in an enclosure from one SUM session.

**NOTE:**

To minimize issues with system resources and network traffic, see the Scaling SUM updates in your environment section in the *Smart Update Manager User Guide*.

## Updating server firmware for large enterprises

If the targets are in a c-Class enclosure, see the *SUM Best Practices Planning Guide*. To download the guide, see the information library website at **http://www.hpe.com/info/sum-docs**.

### Procedure

1. Download your updates. For more information, see **Downloading the server updates**.
2. Collect the IP addresses for the OA, VC, iLO, and at least one NIC for each server you want to update.

   **NOTE:**

   You can minimize the number of IP addresses you need by gathering the IP addresses of a server HP-UX IP address (for Integrity servers) or OA IP address (for ProLiant and Integrity servers). When you add these as nodes to SUM, SUM automatically discovers the associated iLO, server, and VC targets.

3. Run VCSU health check for all OAs and VC modules. Make sure they are in a state that allows firmware updates to proceed. For more information about health statuses, see **VC firmware update overview** on page 30.
4. Use SUM to generate reports to get details on what firmware, software, and driver versions are currently installed, and what updates are available.

   You have multiple options for staging the server updates, to apply offline updates:

   - Set up PXE or iLO Virtual environment to boot the SPP.
   - Copy the SPP or Integrity bundle contents to one staging computer, and then write a script to install it on all local servers.
   - For ProLiant G7 servers and earlier, use the `SmartStart Scripting Toolkit`. For ProLiant Gen8 servers and later, use the `Scripting Toolkit`.
   - Script deployment of firmware using SUM, Microsoft SCCM in Windows, and YUM or the Software Delivery Repository for Linux.
   - Copy the SPP, or Integrity bundle, to one computer at the remote location using network share (Windows) or NFS mount (Linux), and then write a script to install it on the remote targets.
   - Use the SPP via iLO Virtual Media to boot each remote system to the ISO and have the automatic mode update the servers.

**NOTE:**

Update the iLO independently before performing other updates.

- Copy the files from the `\hp\swpackages` directory on the SPP to the remote servers and execute SUM directly using silent, express, or GUI mode.
- Insert a USB key containing an SPP or Integrity bundle into the OA USB port and use the OA web interface to boot each server in an enclosure.

**NOTE:**

You can also stage the SPP on a web server.

- For online updates run from a central management station or server, you can update all servers, iLO, OA, and VC in an enclosure from one SUM session.

## Updating mixed HPE ProLiant and HPE Integrity environments

To update an environment with both ProLiant and Integrity servers:

### Procedure

1. Review the support matrix. Be sure to use OA and VC versions supported by both ProLiant and Integrity servers. For more information, see the BladeSystem Release Sets for Mixed ProLiant and Integrity website at **http://h18004.www1.hpe.com/products/servers/firmware/mixed-release-sets.html**.
2. Download the latest SPP version and Integrity Smart Update Firmware bundles.
3. Extract the SPP and Integrity Smart Update Firmware bundles to separate directories. Do not place more than one bundle or SPP in a directory.
4. Launch SUM and on the Baseline Library screen, add the baselines.

   **NOTE:**

   The SPP and Integrity bundles include a copy of SUM that will deploy the components in that SPP or bundle. A newer version of SUM might be available. You can download the latest version of SUM at **http://www.hpe.com/servers/sum-download**.
5. Perform your updates. Be sure you do not update the OA or VC to a version not listed in the support matrix.

# Implementing firmware

## Updating ProLiant servers overview

You have multiple options for updating firmware, software, and drivers in online mode. Your environment, the size of the maintenance window, and the level of automation you need determine the best method of updating. You can use the following scenarios to update firmware and drivers for VMware, Windows, and Linux servers. Some operating systems, such as Solaris, require you to use the offline mode to update your servers.

**NOTE:**

For information on the updates available and whether they are online or offline updates, see the *SPP Release Notes*.

### Procedure

1. Download the SPP. For more information, see **Downloading the server updates**.

**NOTE:**

SPP includes a version of SUM that deploys the SPP. If you want the latest version of SUM, download it from: **http://www.hpe.com/servers/sum**.

2. Mount the SPP ISO.
3. You can copy the files to a local drive, or burn them to a USB key. Use the `USB Key Utility` to transfer the SPP to a USB key. For more information, see the documentation provided with the `USB Key Creator Utility`.
4. Before deploying firmware on a server, use the following best practices to ensure successful updates.
   - Test your setup in a lab environment before updating production servers.
   - If you do not have access to a test lab, pick one server and update it. Let the updated server run for a few days, and if everything continues to work properly, update other servers starting with small groups of similar servers.
   - Make sure you are within the SPP support window. If problems occur, it is best to be working on the most current release with support.
   - If you are setting up a new server, update the firmware before installing the operating system. This ensures that any firmware issues with the operating system installation have been addressed.
   - Always ensure you have a backup of the server in case the firmware update fails.
   - Always reboot the server after server-based driver or firmware upgrades. This allows the server to activate new firmware.
5. Run SUM to perform your updates. For more information, see the *Smart Update Manager User Guide*, available on the Information Library at **http://www.hpe.com/info/sum-docs**.

**NOTE:**

To activate the updates, reboot the server after all firmware updates have completed successfully.

## Updating enclosure firmware

### Procedure

1. Download your updates. For more information, see **Downloading the server updates**.
2. Gather information about the servers and targets you want to update.
   a. Gather IP addresses for the OA, VC, iLO, and at least one NIC in each server.

      **NOTE:**

      You can minimize the number of IP addresses you need by gathering the IP addresses of a server HP-UX IP address (for Integrity servers) or OA IP address (for ProLiant and Integrity servers). When you add these as targets to SUM, SUM automatically discovers the associated iLO, server, and VC targets.

   b. Run a VCSU health check for all VC modules to make sure the VCs are in a good health state and you can apply updates.
   c. Generate reports with SUM for the gathered OA, VC, iLO, and server IP addresses. SUM generates a report of the currently installed firmware versions, and updates required. The report does not generate information for offline targets or components.
3. Schedule a phased update approach. You might have to perform partial updates to the enclosure if you cannot update all servers at once. Even if you perform partial updates, maintain the installation order.
4. Perform the update.
5. Review the results and log files to ensure the updates completed correctly.
6. Use SUM to generate a report of the current firmware. Use this as a record of what you installed. If there are problems after the update, you can use this report along with the reports you generated earlier to troubleshoot.

# Updating firmware and drivers online for VMware vSphere 5 and later

Use the following instructions to enable VMware vSphere 5 and later on servers to work with SUM version 7.1.0 and later.

SUM supports online firmware and driver updates on ProLiant servers running VMware vSphere 5 in remote deployment mode. SUM requires the Insight Management WBEM Providers installed and running on the server to perform inventory and updates. After the Insight Management WBEM Providers are installed and running, launch SUM on a Windows or Linux host, select the VMware ESXi host as a remote target or node, and then apply the updates.

For more information on updating VMware-based ProLiant servers, see *Best practices for updating VMware-based ProLiant server firmware and drivers* at **https://www.hpe.com/h20195/V2/GetDocument.aspx?docname=4AA5-0247ENW**.

## Downloading the VMware vSphere 5 offline WBEM bundle

The following must be true to update a VMware vSphere 5 or later target:

- The target must be running VMware vSphere 5 or later.
- The target must be active on the network so SUM can detect it.
- You are not attempting to run SUM on the VMware vSphere 5 or later target. You cannot run SUM on a VMware ESXi host.
- You are executing SUM on a Windows or Linux host.
- The VMware server must be running hp-smx-provider-500.03.01.2–434156 or later. You can get the bundle from one of the following locations:
    - Version 1.3.5 or later of the Insight Management WBEM Provider offline bundle. You can download the bundle from the Online Depot at **http://vibsdepot.hpe.com/**.
    - The providers are included in version 5.25 or later of the Custom image for vSphere 5.0, Version 5.32 or later of the Custom Image for vSphere 5.1 or any version of the Custom Image ISO for vSphere 5.5 or later. You can download the Custom Image ISO from the Custom VMware ESXi Image for ProLiant Servers website at **http://www.hpe.com/info/esxidownload**.

## Installing offline bundles on a VMware vSphere 5 host

You can install the offline bundle from VMware vCenter Update Manager as a patch. For more information and instructions, see *Deploying and updating VMware vSphere 5 on ProLiant Servers* at: **https://www.hpe.com/h20195/V2/GetDocument.aspx?docname=4AA4-7994ENW**.

You can install:

- The offline bundle from VMware Update Manager.
- VMware vSphere Command-Line Interface on a Microsoft Windows or Linux system.

For information about importing or installing the vSphere CLI 5.0, see the *VMware vSphere Command-Line Interface Installation and Reference Guide*.

### Procedure

1. Power off any virtual machines that are running on the host and place the host into maintenance mode.
2. Transfer the offline bundle onto the vSphere 5 host local path, or extract it onto an online depot.
3. Install the bundle on the vSphere 5 host using one of the following methods:
    - **Install remotely from client, with offline bundle contents on an online depot**

```
esxcli -s <server> -u root -p mypassword software vib install -d <depotURL/
bundle-index.xml>
```

- **Install remotely from client, with offline bundle on vSphere 5 host**

  ```
  <server> -u root -p mypassword software vib install -d <ESXi local
  path><bundle.zip>
  ```

- **Install from vSphere 5 host, with offline bundle on vSphere 5 host**

  ```
  esxcli software vib install -d <ESXi local path><bundle.zip>
  ```

4. After the bundle is installed, reboot the ESXi host to activate the updates.
5. If you want to verify that the vibs on the bundle were installed, type: `esxcli -s <server> -u root -p mypassword software vib list`.

## Updating an Integrity server online

You can use SUM to update platform and I/O card firmware on Integrity servers.

### Updating a rack-mount or c-Class blade

**Procedure**

1. **NOTE:**

   Update OA, VC, and iLO firmware in one SUM session, and update I/O firmware on HP-UX in a separate SUM session.

1. Select the baselines which contain the updates.

   **NOTE:**

   The default baseline is the directory where SUM is running. For more information about using SUM, see the *Smart Update Manager User Guide* or *Smart Update Manager Online Help*.

2. Enter the IP address and credentials for the OA.

   **NOTE:**

   SUM will find the associated iLO and VC nodes.

3. Enter the user credentials for the associated VC nodes and assign a baseline (SUM 6.x).
4. On the Review/Install Updates or Nodes overview screen, generate an Updates to be Installed report.
5. Set the reboot options.

   **NOTE:**

   Set the Integrity iLO target reboot settings to `If Needed` or `Always` to ensure full activation of the firmware update.

6. Click **Install** to start the update immediately, or click **Schedule Update** to schedule the update. If you schedule an update, click **Install** after you create the schedule to have the updates start at the specified time.
7. After completing the updates to the iLO, OA, and VC, exit SUM.
8. After the servers boot, make sure they are running HP-UX.
9. Start a new SUM session.
10. On the Select Targets screen, enter the IP address and root credentials for each HP-UX operating system instance.
11. Repeat steps 4–6.

12. Continue with other updates after SUM finishes updating the targets and the targets have rebooted.

    **NOTE:**

    On non-HP-UX systems, use EFI packages to update I/O cards.

## Updating a single Superdome 2/X nPartition

You can update one or more nPartitions or unassigned blades in a Superdome 2 enclosure in an SUM session. By default, SUM updates the entire enclosure, but you can manually select to update a subset of the enclosure. For example, if you are running two nPartitions in one Superdome 2 enclosure, you can update only one nPartition at a time.

### Procedure

1. Make sure the server is powered on and running HP-UX.
2. Select the repositories which contain the updates.

    **NOTE:**

    The default repository is the directory where SUM is running. For more information about using SUM, see the *Smart Update Manager User Guide* or *Smart Update Manager Online Help*.

3. Enter the IP address and administrator credentials for the OA target.

    **NOTE:**

    SUM discovers all of the associated nPartitions and include that information in the Select Devices section for the OA target. You can choose to update a single nPartition.

4. On the Review/Install Updates screen (SUM 5.x), or Deploy screen (HPE 6.x), choose the nPartitions you want to update, and select the reboot options available on the View Devices screen from the Select Components screen.

    **NOTE:**

    If you want to update only one nPartition, clear the targets you do not want to update on the Select Devices screen , which you can access from Select Components.

5. SUM will make sure there are no conflicts after the update finishes. If SUM finds issues, it will display them.
6. Run the Updates to be Installed report.
7. Start or schedule the update.
8. After SUM finishes the updates, and the nPartition has rebooted, you can perform other updates.
9. After completing the updates to the iLO, OA, and VC, exit SUM.
10. After the servers complete booting up, make sure they are running HP-UX.
11. Start a new SUM session.
12. On the Select Targets screen, enter the IP address and root credentials for each HP-UX operating system instance.

# Updating firmware in offline automatic mode on ProLiant servers

Use the following instructions to update the firmware on a server using the SPP.

**Procedure**

1. Download the SPP. For more information, see **Downloading the server updates**.
2. Copy the ISO image file to a USB key, and then insert it into the USB port on your server.
3. Browse to the OA web interface, and log in by using the OA administrator credentials.
4. Click **Device Bays** to display a summary of all blades in the enclosure.
5. Select the check box beside each server you want to update.
6. Click **DVD**, and then click **Connect to spp.*.iso** from the pull-down menu. In this example, the * signifies the version, date, and pass number of the SPP that you downloaded.
7. Select the check box next to each blade that needs to be updated. During the DVD connection step, the blades are not selected.
8. Click **Virtual Power**, and then click **Momentary Press**. After confirming the message on the blades, the blades will power down if they were already powered on. If the blades were powered off, they will power on. Make sure all blades are powered off before you proceed.

   **NOTE: Momentary Press**

   brings down any operating system that is running on the blade, as long as ACPI support has not been disabled in the operating system.

9. When you boot to the SPP, all feedback is provided through the UID lights. While the update process is running, the UID light flashes. 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 operating system can be installed or the server can be restarted to its previous operating system.
   - If the UID light is solid, a firmware update failure has occurred requiring attention. You can either plug in the KVM dongle or use iLO Remote Console support to browse into the affected server to determine the cause of the failure. The SPP loads the error log into a `vi` editor window for review.

     Resolve the issue causing the failure before installing or restarting the operating system to prevent issues that could affect server operation.

   **NOTE:**

   The server automatically reboots after the SPP finishes installing updates.

   As an alternative, the SPP can be burned to a physical DVD and placed in an external DVD drive connected to the KVM dongle for the individual blade that must be updated.

   For information on how to script updates of the SPP, see **Scripting firmware updates for multiple enclosures, including the OA, VC, and server blades**.

## Updating in offline interactive mode for HPE ProLiant servers

**NOTE:**

For information on how to add components to an existing tool, see the Creating a custom baseline or ISO section of the *SUM Best Practices Planning Guide*.

Insert the USB key into the server and press a key within 30 seconds after booting the system. If you wait longer than 30 seconds, the updates begin automatically.

The SPP supports both online and offline installations. Because of the limitations of some types of firmware, it might be necessary to update firmware in both the online and offline environments to ensure that all relevant firmware are updated correctly.

**NOTE:**

If you need to update VC firmware, the firmware smart components must be downloaded off the web and added to contents of the SPP. OA and VC firmware components can only be updated online.

## Updating server firmware online

- Place the SPP onto a USB key, and insert the USB key into the OA USB ports on the c3000 Enclosure and c7000 Enclosure.
- Insert a USB key containing the SPP image created by using the USB Key Creator for Windows utility into the SUV cable attached to the physical blade that you want to update, if the blade server supports the SUV cable connection. For Windows, use a USB key.

### iLO Virtual Media overview

The iLO Virtual Media can be connected through the OA interface to a given server, through the iLO Virtual Media applet, or remotely through RIBCL scripts.

In Windows, the iLO Virtual Media shows up as the next available drive letter.

In Linux, the iLO Virtual Media must be mounted:

- `mount /dev/sda /mnt/floppy -t vfat` to mount a virtual floppy
- `mount /dev/sda1 /mnt/keydrive` to mount a virtual USB key drive

**IMPORTANT:**

Copy the files locally if you are updating the NIC firmware, even if you are accessing files through a Windows network file share or Linux NFS `mountpoint`. Failure to copy the files locally can cause all firmware updates after the NIC firmware update to fail because of loss of network connectivity related to the update.

After the files are available locally on the server selected to update, change to the `\hp\swpackages` directory or the file share location to begin the update. For more information, see **Using SUM** on page 6.

## Updating firmware offline (ProLiant servers only)

**Procedure**

1. Download the SPP. For more information, see **Downloading the server updates**.
2. To extract the SPP ISO image, open Windows Explorer, double-click on the ZIP file, and then copy the ISO image to a directory on a USB key or network hard drive.

   For Linux users, unzip the extracted file: `unzip spp.<version>.zip`.
3. Insert the USB key into the USB port on the front of a C3000 Enclosure or on the back of a C7000 Enclosure.
4. In a web browser, open the BladeSystem OA web interface, and log in with the OA administrator credentials.
5. Click **Device Bays** to pull up a summary of all blades in the enclosure.
6. Select the check box beside each blade that you want to update.
7. Click **DVD**, and then click **Connect to spp*.iso** in the pull-down menu where the * signifies the version, date, and pass number of the SPP file that you downloaded.
8. Select the check box next to each blade that you want to update if the blades were not selected during the DVD connection step.

9. Click **Virtual Power**, and then click **Momentary Press**. After confirming the message on the blades, the blades power off if they were already on. If the blades were powered off, they will power on. Make sure all blades are off before you proceed.
10. Use the remote console to browse into each blade, and begin the installation. For more information, see **Using SUM** on page 6.

    Some screens, such as the Source Selection and Select Installation Hosts, are not displayed in offline mode.

    **NOTE:**

    The iLO firmware must be deselected if the SPP is executed in offline mode to prevent errors that might occur when the iLO firmware is updated and the iLO virtual media and remote console is reset. Update the iLO firmware online first using SUM in online mode through the operating system or through the iLO Network Management Port.

    Reboot the server once the firmware updates have completed successfully to activate all software.

    You can burn the SPP to a physical DVD and place it in an external DVD drive connected to the SUV cable for the individual blade that must be updated.

## Updating the OA firmware using SUM

**Procedure**

1. Download the SPP or Integrity Smart Update bundle. For more information, see **Downloading the server updates**.
2. Mount the SPP ISO or extract the Integrity Smart Update bundle.
   - **a.** SPP
     - Mount the ISO.
     - In Linux, untar/unzip the spp.<version>.zip file:

       ```
       tar zxvf spp.<version>.zip
       ```
   - **b.** Integrity Smart Update bundle
     - In Windows, double-click the `.exe` file.
     - In Linux, double-click the `.tar.gz` file.
3. Begin the update using SUM. For more information, see **Using SUM**.

   Ensure the target device IP address or DNS name is in the information for the Active OA management NIC port. During the OA firmware update process, the Standby OA firmware is updated first, and then the active OA firmware. If the VC configuration is 1.34 or later, downtime does not affect server lades or traffic through any VC modules. After the firmware is updated, the OA experiences a brief downtime as the firmware activates. This downtime does not affect any server blades or traffic through any VC module. If the VC firmware version is earlier than 1.34, a network fabric downtime of up to 10 minutes can occur while the firmware activates.

**NOTE:**

The firmware update process for both OAs should take about 6-8 minutes. An individual OA firmware update should take approximately 4-6 minutes.

If the OA firmware is updated independently of other components of the OA firmware version being deployed, make sure you are using a support OA version. For more information, see the SPP website at **http://www.hpe.com/servers/spp**.

Multiple OAs can be updated simultaneously to speed up the process.

If you are using VC modules in your enclosure, run VCSU health check before updating the OA firmware.

## Scripting firmware updates for multiple enclosures, including the OA, VC, and server blades

Because there are many different processes you can use to script firmware deployments, this scenario focuses on leveraging existing tools for this functionality. This scenario uses SPP and Integrity Smart Update bundle through SUM to update the OA firmware, the VCSU to update the VC firmware, and the SPP to update all server blade firmware.

For information on the correct order for updating OA and VC firmware, see **OA SPP installation order overview**.

**NOTE:**

The following instructions focus on the effort needed to update firmware, assuming the VC firmware is at least at 1.34 or later. If the VC firmware is earlier than 1.34, the setup is still the same but in the installation sequence, the steps for the VC firmware update and the OA firmware update should be reversed.

Because there is no single tool available for updating all firmware in the BladeSystem infrastructure at once; updates require a multi-step process.

### Procedure

1. Download the SPP and Integrity Smart Update bundle. For more information, see **Downloading the server updates**.
2. Set up either Microsoft IIS or Apache web servers.
3. Validate that the iLO Advanced License is installed on each blade.
4. Update the iLO license for multiple servers to the iLO Advanced License if needed.
5. Obtain the iLO firmware version to confirm iLO firmware is at least at 1.50 or later to support the automation process.
6. Script the deployment of the OA firmware update process by using SPP or Integrity Smart Update Firmware bundle and SUM.
7. Script the deployment of the VC firmware update process by using SPP or Integrity Smart Update Firmware bundle and SUM.
8. Script the deployment of SPP through the iLO Virtual Media support.
9. Script the development of Integrity Smart Update bundles to iLO and HP-UX servers by using SUM.

## Using a PXE server to deploy updates

Use these steps to set up a PXE server on a Linux system.

### Procedure

1. Install the following packages:

- `tftp-server`
- `dhcp`
- `httpd`
- `syslinux`

2. Set up a DNS server on your network.

   **NOTE:**

   While a DNS server is not required, best practice is to set one up.

3. Activate `TFTP` within `XINETD`.
   - Change `disable=yes` to `disable=no` in `/ect/xinet.d/tftp`.
   - Restart `XINETD`.
4. Set up the PXE server to use a static IP:
   a. Create the file `/ect/sysconfig/network-scripts/ifcfg-eth0.static`
   b. Set the contents to the file as:

   ```
   DEVICE=eth0

   BOOTPROTO=STATIC

   ONBOOT=no

   TYPE=Ethernet

   IPADDR=<IP>

   NETMASK=<IPMASK>

   GATEWAY=<GATEWAYIP>
   ```
5. Set up the PXE boot environment:
   a. Copy `initrd.img` and `vmlinuz` from the `/system` directory of the SPP ISO to `/tftpboot` directory of the PXE system.
   b. Copy `pxelinux.0` (PXE boot Linux kernel) to the `/tftpboot` directory.
   c. Ensure the files copied to `/tftpboot` are world readable.
6. Configure `PXELINUX`
   a. Create directory `/tftpboot/pxelinux.cfg`.
   b. Create files representing the hex value of the static IP address in the `/tftpboot/pxelinux.cfg` directory. For example, if the static IP address used is 192.168.0.254, the hex value is C0A800FE and the files to be created would be:
      - `C`
      - `C0`
      - `C0A`
      - `C0A8`
      - `C0A80`
      - `C0A800`
      - `C0A800F`
      - `C0A800FE`

   c. Create a zero-sized file (using touch) representing the MAC address of the NIC of the boot PXE boot client (pre-pended with 01 and replacing ‘:’ with ‘-‘) in the `/tftpboot/pxelinux.cfg` directory. For example, if the NIC MAC address were 00:01:02:03:04:05, a file name would be 01-00-01-02-03-04-05.
7. Create a default `pxelinux` configuration.
   a. Create a file name default in the `/tftpboot/pxelinux.cfg` directory.
   b. Set the contents of the default file to:

```
prompt 1
default Linux
timeout 100
label Linux
kernel vmlinux
append initrd=initrd.img ramdisk_size=9216 noapic acpi=off
```

8. Copy the entire contents of the SPP ISO to a directory named `/tftpboot/SPP*`, where “” represents the version of the SPP.
9. Add the following to `/ect/httpd/conf/httpd/conf` where “*” represents the version of the SPP.

```
<Directory /tftpboot/SPP*>
Options Indexes
AllowOverride None
</Directory>
Alias /linux /tftpboot/SPP*
```

10. Start the `dhcpd` and apache services and activate `tftp`.

```
service dhcpd start
service xinetd restart
service httpd start
```

11. PXE boot the servers to begin the update process.

## Updating HPE Moonshot nodes

### Procedure

1. Download the HPE Moonshot Component Pack. For more information, see **Downloading the HPE Moonshot Component Pack** on page 12.
2. Unpack the file in an empty directory.
3. Launch SUM and follow the instructions in the Moonshot Component Pack Update Guide available on the Information Library at **http://www.hpe.com/info/moonshot/docs**.

# Deploying individual server firmware types

Use SPP as your source for update tools and firmware, software, and driver components. Use Integrity Smart Update Firmware bundles as your source for firmware updates. Only deploy individual components if there is a hot fix that resolves an issue you are experiencing. The following sections discuss reminders and tips for specific types of firmware. Unless otherwise specified, use SUM from the SPP or Integrity bundle to perform an update.

## System ROM update overview

System ROM firmware is staged and not immediately activated upon update. This means that the firmware is written to the physical ROM chip in the server but will not be activated until the server is rebooted. While it is recommended that you reboot as soon as possible to activate new firmware, there is no harm in leaving the System ROM image deployed and rebooting the server during a later maintenance window. System ROM firmware can be updated in either online or offline mode.

## iLO firmware update overview

iLO firmware is activated immediately upon update of the iLO by an automatic reset. This reset disconnects any virtual media devices and remote consoles through the iLO. This reset normally takes less than a minute and does not affect the operating system or any running applications. The server does not need to be rebooted to activate the iLO firmware. iLO firmware can be updated in either online or offline mode.

## NIC firmware update overview

To update NIC firmware, use the SPP or Integrity Smart Update Firmware bundle. The corresponding operating system-specific NIC driver must be previously installed in online mode. You can obtain a NIC driver by using the one available in the SPP or Integrity Smart Update Firmware bundle. After the driver is in place, use SUM to update the firmware. You can update the NIC firmware in either online or offline mode.

In special cases, different firmware can be preloaded on the adapter for a Broadcom NIC, depending on the functionality of the adapter. An example of this is the NC373i Multifunction Gigabit Server Adapter and the NC373m Multifunction Gigabit Server Adapter. The adapter is released in two forms. One form includes iSCSI support and the version is in the 1.x.x range. The same adapter is also available without iSCSI support and has firmware version in the 4.x.x range. The NIC firmware component is intelligent enough to only load the appropriate firmware on the adapter. Due to the different functionality that the different types of firmware enable, it is important to use the NIC firmware components and SUM to deploy NIC firmware and not attempt to update the firmware directly as this could cause loss of functionality.

**NOTE:**

If updating from a version older than the 4.6.16.0 version of the Broadcom 1 Gb NIC driver, it is first necessary to update to the 4.6.16.0 version before continuing to later versions. More information about this can be obtained from the customer advisory on the advisory website at **http://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay/?docId=c01684544**.

## CNA firmware overview

CNAs combine the functionality of fiber channel and NICs onto a single adapter. CNAs behave the same as Fibre Channel adapters. You can update CNAs in either offline or online mode.

# Emulex, QLogic, and Brocade Fibre Channel HBA firmware

Using SPP 2012.01.0 or later, you can update FC HBA and CNA firmware online in supported Windows and Linux environments.

**NOTE:**

Integrity Smart Update bundles that include I/O card firmware allow you to update these targets online.

# Power Management Controller firmware update overview

Power Management Controller firmware controls the power subsystem of the servers.

- An iLO driver must be loaded.
- OA firmware must be at level 2.41 or later for dynamic power capping to function properly.

# Smart Array Controller firmware update overview

The controller firmware updates are staged until the next reboot of the server. Once the server is rebooted, the new version of the controller firmware is activated. Updating the Smart Array controller firmware requires the installation of the Smart Array driver for the given OS and architecture in use. For offline mode, this driver is loaded automatically. Use SUM provided with SPP or Integrity bundle to update the Smart Array controller firmware. Smart Array controller firmware can be updated in either online or offline mode.

# SAS and SATA hard drive firmware update overview

You can install SAS and SATA hard drives behind both Smart Array controllers and non-Smart Array controllers. The requirements differ depending on whether you are using a Smart Array controller or a non-Smart Array controller. Use SPP as a source for the firmware.

## Behind a Smart Array controller requirements

Any version of the driver meets the requirements to update the SAS or SATA hard drive firmware.

## Behind a non-Smart Array controller requirements

The SPP, or SPP-related hot fixes, and Integrity bundles provide non-Smart Array controller components that SUM supports.

# Tape firmware update overview

To successfully update the tape firmware:

- Load an appropriate driver for the controller.
- Make sure there is a tape in the drive, failure to do so could cause the update to fail.

# OA firmware update overview

Use SPP or Integrity Smart Update Firmware bundle as the source for your OA updates.

The following are requirements for updating OA firmware:

- You must connect a workstation to the same network as the OA network port, or connect through a router for network access to the OA.
- You must have OA administrator credentials. Other types of OA credentials do not allow firmware updates.
- The OA firmware can only be updated online. You cannot boot to the SPP.

Execute SUM from a workstation or server running any supported version of a Windows or Linux operating system. You can execute SUM, add the IP address or DNS name of the OA network port as a remote host, and SUM will automatically detect the target is an OA and only allow the OA firmware to be available for selection.

## OA SPP installation order overview

This installation order is recommended for most updates to help minimize downtime and issues. See the SPP Release Notes and SPP Component Notes for known issues that require updates that differ from the recommended order. The documents are available at **http://www.hpe.com/info/spp/documentation**.

- **Without an operating system** - Update:
  1. OA
  2. iLO
  3. VC
  4. All other nodes
- **With an operating system** - Update:
  1. OA
  2. Blades and iLO
  3. VC

# VC firmware update overview

You can use the following to update VC firmware:

- SUM - Use SUM to update the firmware if this is a new system.
- HPE OneView - Use HPE OneView to update the firmware if the system is managed by HPE OneView.
- VCSU - Use VCSU if this system is an existing installation with no operating system.

The following are dependencies you must meet to update VC firmware:

- Connect a workstation to the same network as the VC management port, or on a network through a router.
- Have both the OA and VC administrator credentials.
- The VCSU uses information from the OA in updating the VC firmware; it requires both sets of credentials.
- The VC firmware can only be updated online. You cannot boot to the SPP to perform this update.

The VCSU provides a command-line scriptable method to update the VC firmware. It also contains logic that minimizes any network and fabric outages caused by the update process under certain VC configurations. In some cases, the VCSU can eliminate all outages during the firmware update process if correct redundancy has been installed. VCSU must be executed from a Windows or Linux (requires version 1.40 or later of VCSU) workstation or server.

You can use SUM to update the VC firmware in a Virtual Connect domain. Use VCSU to update the VC firmware in the following cases:

- **Unhealthy state**

  —SUM reports a module as unhealthy during discovery on the Select Targets screen.
- **Force the same version**

  —SUM does not allow you to force rewrite the same firmware version.
- **Downgrade VCM**

  —SUM does not allow you to force downgrade VC firmware.
- **Non-redundant configuration**

  —If SUM detects that the VC module is non-redundant, it will not allow you to perform any updates. This prevents an accidental server outage.

- **Not part of a domain**

  —SUM alerts you if the VC module is not part of a domain. SUM requires the VC module to be part of a domain to perform discovery.
- **Change activation order**

  —If you want to change the activation order, insert time delay for VC modules, or choose other non-default options.
- **The VC domain is managed by VCEM**

  —If the VC module is in a domain that is managed by VCEM, you need to put the VC domain into maintenance mode. After enabling maintenance mode in VCEM, rescan the VC module in SUM and continue with the update. After the update finishes, use VCEM to bring the domain out of maintenance mode. For more information, see the Virtual Connect documentation at **http://www.hpe.com/info/virtualconnect/docs**.

**IMPORTANT:**

If the VC configuration is not redundant or if the VC firmware version is earlier than version 1.34, a network fabric downtime of up to 10 minutes can occur while the firmware is being activated. This affects all servers in the enclosure and prevents network access until the VC firmware is activated.

**NOTE:**

Because of the possibility of NIC fabric downtime during a VC firmware installation, update the VC from a workstation outside the enclosure to ensure continuous network access to the firmware update utilities.

## VC installation order

For more information on the proper installation order for the VC firmware, see **OA SPP installation order overview** on page 30.

# 3Gb and 6Gb SAS BL Switch firmware update

Use VSM to update the 3GB and 6GB SAS BL Switch firmware.

# Updating firmware on a RHEL server

### Procedure

1. Log in to the Support Center and generate a token to validate download permissions.
2. Add the Firmware Pack for ProLiant as an additional yum repo:

   ```
   /etc/yum.repos.d/fwpp.repo
   ```
3. Install SUM:

   ```
   yum install hpsum
   ```
4. Download and unpack appropriate firmware RPMs:

   ```
   yum install $(hpsum requires)
   ```
5. Deploy the recommended updates:

   ```
   hpsum upgrade
   ```

   Or, to skip the prompt:

   ```
   hpsum -y upgrade
   ```

# HPE Moonshot firmware update

The Moonshot Component Pack provides firmware updates for Moonshot nodes. You can use SUM version 6.5.0 or later to update Moonshot nodes.

# Deploy updates to iLO Federation groups using SUM

You can use the SUM GUI to deploy updates to iLO Federation groups through one node, called the Interface iLO. SUM can deploy updates to a group in online or offline mode. If you use offline mode, make sure that you have an ISO file that SUM can use to deploy the updates after it takes the group members offline. For more information, see the *Smart Update Manager User Guide*.

# Server firmware update FAQs

The following sections provide typical questions and answers about firmware updates. Over time, some of the answers might change, so be sure to see the most recent edition of this document for the most current information about firmware deployment best practices.

## Server firmware update FAQs

**What tools should I use to update the various firmware types?**

The recommended tools for updating firmware are SUM, HPE OneView, and VCSU. Use VCSU in specific update conditions. For more information, see **VC firmware update overview** on page 30. Firmware updates are released as part of the SPP, Integrity Smart Update Firmware bundles, and Moonshot Component Pack.

**Why must I always upgrade to the latest individual firmware and driver components?**

- SPP

  You do not have to update your server environment with every SPP release. The SPP is supported for one year. Hot fixes are updates considered important enough to release outside of the SPP cycle. A Customer Advisory is assigned to each hot fix. Hot fixes are then added to the next SPP release. If a hot fix does not affect your server environment, there is no need to install it immediately. You can wait until you update your environment. For more information about SPP, see the SPP website at **http://www.hpe.com/servers/spp**.
- Integrity Firmware bundles

  Update to the latest Integrity Firmware bundle to make sure you have the latest updates and bug fixes.

## SUM firmware FAQs

This section contains questions that are directly related to SUM and its use in the firmware environment.

**How does SUM work when applied to an entire chassis; for example, does it update each blade, iLO, and so on, sequentially or in parallel?**

SUM performs dependency checking on targets, which ensures that all dependencies are met before an installation begins. The SUM discovery process also detects the required updates for targets, and allows SUM to perform updates in the correct order.

**Should I use SUM, SIM, or HPE OneView?**

- Use SUM if you have enough system resources to process the updates in GUI or inputfile mode. SUM consumes resources based on the number of baselines you use and the number of nodes you update.
- Use SIM if you have more than nodes than the suggested number of nodes for SUM.
- Use HPE OneView to update firmware if the node is managed by HPE OneView.

SUM works with non-server-based targets, such as the OA and VC, which the VCA cannot update. The SIM and HPE OneView version control infrastructure have been designed to leverage SUM as the deployment mechanism to remove the requirement of an agent on each target and allows SIM and HPE

OneView to support firmware deployment to network-based devices such as the OA and VC.

**What about administrators who have invested time to understand SIM and, specifically, VC?**

The SUM technology was incorporated into SIM starting in the SIM 6.0 release as a new method of deploying software and firmware. This will still allow administrators who have invested in the VCRM to leverage that investment but will allow users to update firmware on one year after SUM provides equivalent functionality compared to what is available today. Currently, the SUM equivalent functionality to all features of Version Control will not be completed for several releases. Plenty of advance notice will be given to administrators to allow them to plan and implement any changes needed to support the new SIM version control infrastructure. In most cases, the only change needed will be to remove the Version Control Agent from the servers after validating the new SIM version control infrastructure works in their environment. VCRM servers can still be leveraged, but are not required to support this new version control infrastructure.

**Where do I obtain the *Smart Update Manager User Guide*?**

You can find the HP Smart Update Manager User Guide on the Smart Update Manager Information Library at **http://www.hpe.com/info/sum-docs**.

**How can I leverage the SUM pull-from-web functionality when my data center cannot be connected to the internet for security reasons?**

1. Connect the host system to a network with an internet connection.
2. Launch SUM.
3. Add a baseline by selecting the **from hpe.com** function.
4. After SUM downloads the updates and inventories the baseline, shut down SUM and disconnect the computer from the network with internet connectivity.
5. Connect the computer to the secure network.
6. Launch SUM and then deploy updates.

**Does the SUM CLI allow creation of a group from a file with a list of IP addresses or DNS names when the file is presented as a file name that is given as a CLI command-line parameter?**

SUM can accept an input file for the IP addresses and user credentials. The `USECURRENTCREDENTIAL` option can be used with the CLI for Windows only as current credentials are not available for Linux users. For more information on how to use this in your firmware deployments, see **SUM special considerations**.

**What is the purpose of the dryrun scripting option?**

What is the purpose of the dryrun scripting option? Its primary purpose is to test scripts called from the CLI approach to SUM. The dryrun feature in SUM is activated by using the `/dryrun` or `--dryrun` switch, which causes SUM to bypass the actual calling of the firmware smart components during installation and return SUCCESS. This mode is useful for validating when the targets are available, that credentials are valid, and that all of the network interfaces and ports are available for a successful firmware deployment.

**NOTE:**

SUM 6.x does not support the `DRYRUN` option.

**When using the SPP to upgrade an entire c7000 Enclosure and all of its constituents, including**

- Can I simply give the SUM tool the OA IP address?
- Is the tool able to upgrade all of the components inside the chassis because the OA can automatically identify the addresses of the iLOs and modules?

**the OAs, server blades, iLOs, and switch modules:**

- Do I have to manually add IP addresses of the blades, iLOs, modules, and so on, into the SUM GUI interface, thereby creating my own group, which is, in effect, the enclosure and all of its contents?
- Must I always manually add the host OS IP address that upgrades the blade server BIOS because the OA cannot identify what it is?

SUM updates all server firmware in online mode. SUM updates the OA through the OA interface, not through the NIC interface. The SPP and Integrity bundles provide the firmware versions that you use to update the server firmware.

You need to provide the IP address or DNS name for G7 and earlier targets that you want to update. SUM detects the OA host servers list on targets, and if you added servers to the OA host servers list, SUM will ask if you want to add the target.

If you are using a Gen8 or Gen9 server that is running AMS, you do not need to provide an IP address.

# BladeSystem firmware-related FAQs

This section contains questions directly related to blade firmware updates.

**Can SIM use the SPP as a VCRM custom baseline?**

Yes, it can be used by dropping the downloaded and expanded bundle into the VCRM directory and running a rescan on this directory from the Systems Management Homepage for the VCRM. For information on additional support for the SIM 7.0 release, see SIM and Version Control Agent.

**NOTE:**

VCRM 7.0.0 and later is required to support the SPP.

**What is the recommended tool for determining the currently-deployed BladeSystem enclosure firmware versions?**

Using SUM, you can generate either an HTML, CSV, XML formatted report file detailing the repository contents, target firmware, target installable details, and failed dependencies.

**NOTE:**

Not all reports are available on all GUI screens. If a report is not available, SUM grays out the report option.

**What are the dependencies between the SPP firmware and drivers?**

System software (for example, drivers and services) dependencies for firmware updates are very generic in that a driver needs to be loaded so the device can be discovered, version checked, and so on.

**Can we upgrade each component directly to the latest version or do we need intermediate revision steps?**

Almost all components can be upgraded to the latest firmware revision without issue. The only component that requires an interim revision is for OA firmware updates from 1.x firmware revisions to 2.x versions. For more information, see the following support documents:

- Customer Advisory: OA - Upgrading Firmware From Version 1.x to Version 2.25 (or Later) Will Not Be Successful: **http://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay/?docId=c01597033**
- Link to earlier versions of the OA firmware: **http://www.hpe.com/info/oa**

**NOTE:**

If updating from a version older than the 4.6.16.0 version of the Broadcom 1 Gb NIC driver, it is first necessary to update to the 4.6.16.0 version before continuing to later versions. More information about this can be obtained from the customer advisory on the advisory website at **http://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay/?docId=c01684544**.

**Can I update my Blades HBA and CNA firmware online?**

Yes, starting with SPP version 2012.02.0 and SUM 5.0.1, HBA and CNA firmware updates can be performed while online.

**How do I manage my Ethernet Blade interconnect switch updates?**

You must use the vendor tools to update the blade interconnect switch modules.

**Are there any guidelines for downgrading firmware?**

There are several limitations about downgrading firmware. If necessary, firmware downgrades should only be attempted on a component-by-component basis. Do not downgrade components unless absolutely necessary.

**Can you upgrade versions of HBA and CNA firmware without being concerned about going through an interim version to facilitate the upgrade?**

There are no generational skipping requirements for Fibre Channel HBAs. You can upgrade from one firmware and boot BIOS version to another without any intermediate steps.

**NOTE:**

You need to perform an offline update to get to the HBA and CNA firmware versions included in the SPP version 2011.09.0 or later before you can update the HBA and CNA firmware online starting with 2012.02.0 or later.

**Can I roll-back the individual changes on a per-server or per-chassis basis?**

There is no uninstall/reverse functionality, although it is possible to force older components to overwrite newer ones if a reference set of the presently installed versions is created. Do not downgrade components unless absolutely necessary.

**IMPORTANT:**

If you do decide to downgrade a component, do not downgrade more than one firmware version. For example, do not downgrade from version 6.5 to 4.0. Downgrading more than one firmware version risks incompatibilities between the downgraded firmware and other hardware. You will need to download the component you want to downgrade manually, it will not be included as part of the latest SPP or Integrity bundle.

**How often should we upgrade firmware?**

Update your ProLiant firmware once per year to keep your firmware up-to-date with the latest updates.

**How does the firmware version affect our support status?**

The SPP version is supported for 12 months. In some cases, it may extend the support period beyond a year, so always consult the *Service Pack for ProLiant Release Notes*. For more information, see the SPP website at **http://www.hpe.com/servers/spp**.

**NOTE:**

Generally, you can tell when your support period ends by the version number of the release. For example, if you have installed the content of SPP 2011.09.0, your support period should end the last day of September, 2012 based on version 2011=year, 09= month, 0=release ID number.

# SPP FAQs

**How do I add updated components to the SPP?**

For more information about adding components, see the *SUM Best Practices Planning Guide*.

**What order of update should be followed when updating a blade enclosure?**

For information on how to update a blade enclosure using the SPP, see **OA SPP installation order overview** on page 30.

# Mixed ProLiant and Integrity environments FAQs

**Can I update a mixed ProLiant and Integrity environment at the same time?**

Yes. For more information on updating a mixed environment, see **Updating mixed HPE ProLiant and HPE Integrity environments** on page 17.

# Troubleshooting

## Troubleshooting SUM failure on Windows hosts due to McAfee firewalls

### Symptom

McAfee firewalls block SUM traffic.

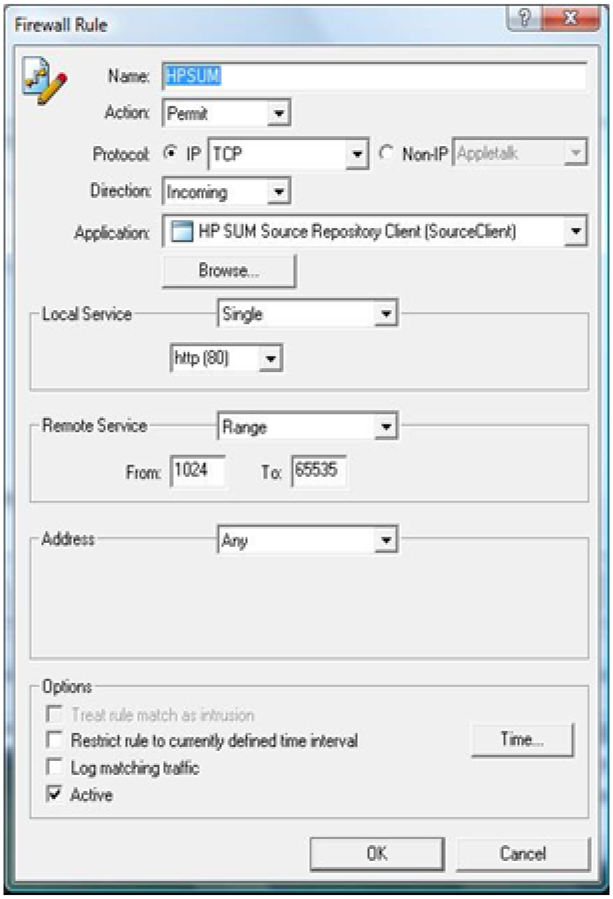
### Action

### Procedure

1. Enable the port traffic associated with the SUM application:
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 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.



Name: HPSUM

Action: Permit

Protocol: ● IP TCP ○ Non-IP Appletalk

Direction: Incoming

Application: HP SUM Source Repository Client (SourceClient)

Local Service: Single

http (80)

Remote Service: Range

From: 1024 To: 65535

Address: Any

Options

□ Treat rule match as intrusion

□ Restrict rule to currently defined time interval

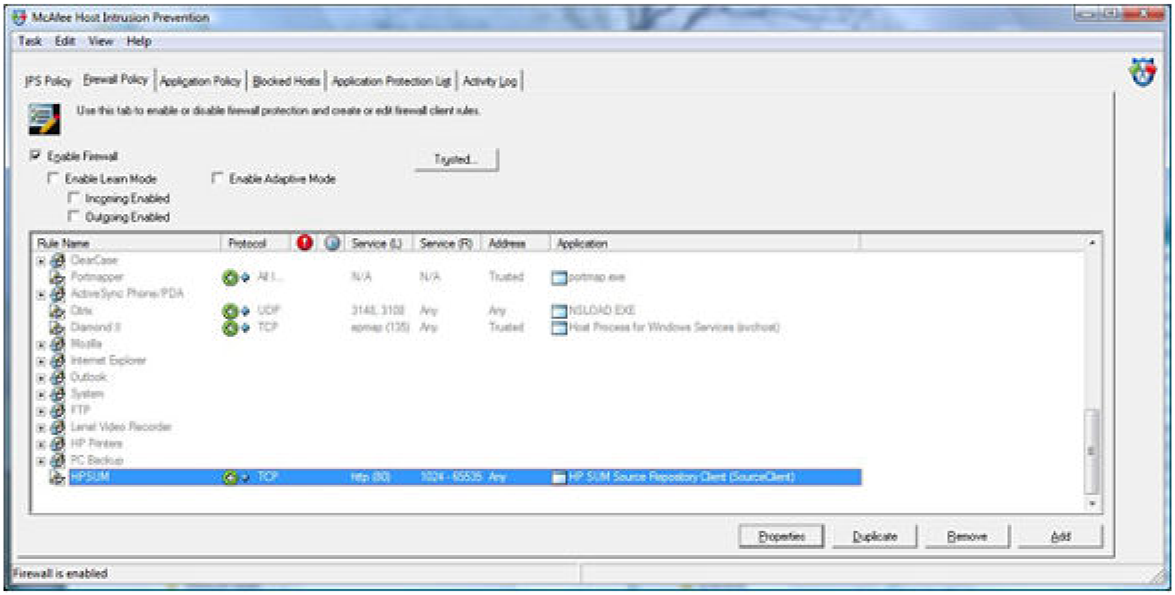
□ Log matching traffic

☑ Active

**NOTE:**

SUM 6.x uses port 63002.

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



Use this tab to enable or disable firewall protection and create or edit firewall client rules.

☑ Enable Firewall

□ Enable Learn Mode

□ Incoming Enabled

□ Outgoing Enabled

□ Enable Adaptive Mode

| Rule Name | Protocol | Service (L) | Service (R) | Address | Application |
|---|---|---|---|---|---|
| ClearCase | | | | | |
| Portmapper | All I... | N/A | N/A | Trusted | portmap.exe |
| ActiveSync Phone/PDA | | | | | |
| Citrix | UDP | 3148, 3108 | Any | Any | NSLOAD.EXE |
| Diamond II | TCP | epmap (135) | Any | Trusted | Host Process for Windows Services (svchost) |
| Mozilla | | | | | |
| Internet Explorer | | | | | |
| Outlook | | | | | |
| System | | | | | |
| FTP | | | | | |
| Lenel Video Recorder | | | | | |
| HP Printers | | | | | |
| PC Backup | | | | | |
| HPSUM | TCP | http (80) | 1024 - 65535 | Any | HP SUM Source Repository Client (SourceClient) |

Firewall is enabled

# Troubleshooting SUM connection errors

### Symptom

Use these tips to troubleshoot SUM connection errors:

- Ensure your workstation does not have an existing connection to the ADMIN$ share on the target IP address. If it does, it prevents 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 Administrators or Linux root equivalent group. If it is not, SUM blocks installation to the target.
- Ensure WMI is enabled and running on all Windows target servers.
- For Windows target servers, enter the user name in `DOMAIN\USER` format, where `<user>` is the administrative user name, and `<domain>` is either the NETBIOS computer name or the Active Directory domain name for this user account..
- For Linux, ensure the SSH port is not blocked by a firewall.
- 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 are open on any routers in the network. For more information, see **SUM network ports used**.
- The Symantec Endpoint Protection product blocks SUMs ability to communicate with remote targets if the Network Threat Analysis feature is enabled. Disable this feature while SUM is in use on the workstation.
- Examine the trace directories for connection problems. For more information, see **Collecting SUM trace directories** on page 40.
- Ensure the server has a valid serial number.

# Collecting SUM trace directories

### Cause

If you need to contact Hewlett Packard Enterprise for support with an issue, run the GatherLogs utility. GatherLogs is in the same directory as SUM.

SUM generates a set of debug trace logs that contain internal process and debug information which can be useful in determining SUM failures. Trace directories are stored in the `/tmp/ HPSUM` (Linux) and `%temp%\HPSUM` Windows) directories. SUM creates trace directories for each function and node that SUM updates.

SUM includes a utility named `GatherLogs.bat` (Windows) or `Gatherlogs.sh` (Linux) to create a compressed .zip (Windows) or tar.gz (Linux) file with all the logs. If you need to review the log files, you can run this utility to gather all the logs in one file.

### Action

### Procedure

1. If you are running SUM in offline mode, use the following instructions to collect trace directories and logs.
1. Launch SUM in offline mode.
2. Launch the command prompt from the SUM GUI by pressing `CTRL-ALT-D-B-X`.

**NOTE:**

After approximately 30 seconds, the command prompt appears over the SUM GUI window.

3. Change the directory to the one running SUM. For example, `cd /mnt/bootdevice/SPP2014100/hp/swpackages`.
4. Type `./gatherlogs.sh` to collect the SUM logs. All logs are collected in a `.tar.gz` file in the directory where you placed SUM or in a temp directory if the SUM directory is read-only. The log file is named `HPSUM_Logs_$(datetime).tar`.
5. Place the logs on a removable media if you want to view them on another computer.

**NOTE:**

If the log files appear corrupt, use a different extraction application. Some extraction applications might cause errors.

| Logs | Windows Directory | Linux Directory |
|---|---|---|
| User level logs | `C:\cpqsystem\hp\log` | `/var/hp/log` |
| Debug logs | `%temp%\HPSUM` | `/tmp/HPSUM` |
| Local copy of SUM binaries when needed* | `%temp%\localhpsum` | `/tmp/localhpsum` |
| Remote node files | `admin$\temp\HPSUM` | `/tmp/HPSUM` |

*SUM 6.3.0 and later makes a local copy of binaries and support files when SUM is launched from a network mounted share or read-only location. This allows SUM uninterrupted access during updates.

**NOTE:**

If you do not find logs in the locations listed above on Linux systems, check the directory `/var/cpq/Component.log`.

You can save the log files to a USB key if you have one inserted in a USB port.

a. Launch SUM in offline mode.
b. Launch the command prompt from the SUM GUI by pressing `CTRL-ALT-D-B-X`.

# Troubleshooting failed iLO firmware updates

### Action

### Procedure

1. Follow these steps to recover from a failed firmware update using the Drive Key Boot Utility.
1. Copy the iLO offline flash component to your USB drive key.
2. Verify that the iLO security override switch is set to disabled.
3. Boot the USB drive key containing the iLO flash component.

**NOTE:**

For more information on creating a USB Key, see the SUM Best Practices Planning Guide.

4. After the first screen displays, switch to text console by pressing the `Ctrl+Alt+F1` keys.
5. Switch to the directory where the flash component is stored by entering `cd`.

6. Enter `/mnt/usb/components/` at the # prompt.
7. Remove the loaded iLO driver by entering the following commands:
   - `/ect/init.d/hp-snmp-agents stop`
   - `/ect/init.d/hp-ilo stop`
   - `/ect/init.d/hpasm stop`
8. Run the component by using the --direct option. For example: `./CP00xxxx.scexe --direct`.
9. Enter `y` at the **Continue (Y/N)?** prompt.
10. After programming is successfully completed, set the security override switch to `Enabled`, and reboot the server.

    In some instances, after an iLO or PowerPIC firmware update, a server shows a red X in the OA web interface, and the server is unable to power on. Several causes for this condition are possible. The following items list three possible ways to recover from this scenario once it has been confirmed that all iLO, System ROM, OA, and Power Management Controller firmware has been updated.

    When a blade is first inserted into an enclosure, the Power Management Controller calculates the amount of power needed to power up the server. This value is then requested from the OA. With Power Management Controller 0.7 firmware, the value is incorrectly calculated, which causes the request to the OA to reach the maximum value. This usually occurs at around 500 watts instead of the normal range of 100-200 watts for a given blade server. When too many servers request the maximum value, the OA becomes over-allocated and prevents some blades from powering up. Even after the power management controller is updated, there are instances when the incorrect values in NVRAM for the blade server persists. If this occurs, try the following solutions.

### Action

### Procedure

1. **Reset the blade**

1. Remove the blade and re-insert it.
2. If this does not work, reset the NVRAM.

### Action

### Procedure

1. **Clear the NVRAM**

1. Power off the blade.
2. Remove the blade from the enclosure.
3. Open the blade cover, locate the Configuration Reset switch, and set it to on.
4. Re-insert the blade into the enclosure.
5. Allow the blade to power up, and wait until it prompts you to reset the Configuration Reset switch to off.
6. Power off the blade again.
7. Remove the blade from the enclosure.
8. Open the blade cover, locate the Configuration Reset switch, and reset it to off.
9. Re-insert the blade into the enclosure.

   Allow the blade to power up and go through initial configuration. At this point, the blade can be flashed to the latest firmware version (the fans return to a normal state, along with power allocation to the blade).

**NOTE:**

Resetting the configuration causes any RBSU settings to return to default. After following this set of instructions, it might be necessary to reset the RBSU settings after updating the PowerPIC firmware to the latest version.

If clearing the NVRAM does not clear the problem, it might be necessary to reset the iLO.

### Action

### Procedure

1. **Reset the iLO**
1. Power off the blade.
2. Remove the blade from the enclosure.
3. Open the blade cover and look at the pin chart sticker. Determine the jumpers that will close the system maintenance switch. Set the appropriate jumper(s).
4. Re-insert the blade into the enclosure.
5. Allow the blade to power on. If the system powers on but iLO is off, turn system power off.
6. Remove the blade from the enclosure.
7. Enable System Maintenance Mode.
8. Re-insert the blade into the enclosure.
9. Allow the blade to power up, and start SPP to flash the iLO firmware.
10. Power-off the blade after the firmware updates complete.
11. Remove the blade from the enclosure.
12. Disable System Maintenance Mode on your server.
13. Remove the jumpers you set earlier.
14. Re-insert the blade into the enclosure.
15. Allow the blade to power up and go through the normal boot process.

**NOTE:**

After following this set of instructions, reset the user iLO configuration settings. Updating the iLO firmware to the latest version returns settings to default and user configuration settings must be reset.

# Troubleshooting issues related to Integrity servers

## Failed to download component or HTTP access issue

### Cause

SUM requires bi-directional network communication between the target and the server running SUM to complete firmware updates. SUM might be able to perform target discovery if the communication is from the SUM server to the target, but most updates will not be able to finish without bi-directional communication. SUM launches an HTTP server on the system running SUM to provide the bi-directional communication. If the firewall blocks the network communication, the logs usually indicate an issue with HTTP retrieval of the firmware binary.

For more information on disabling McAfee firewalls, see **Troubleshooting SUM failure on Windows hosts due to McAfee firewalls** on page 38. For information on disabling other firewalls, see the documentation accompanying that software.

**NOTE:**

SUM 6.x supports the options `/port` and `/ssl_port`. Use these commands to avoid conflicts with firewalls.

## Pending system firmware updates

On Integrity rack-mount and c-Class systems, system firmware is part of the platform firmware update by the iLO management interface. If the rack-mount or iLO management interface system is powered on when you try to update it, the system firmware cannot be immediately programmed into the flash memory because the memory is in use. iLO stages the software firmware image and performs the update when you power down the system. The update takes approximately 6 minutes, and then you can power the system back on.

When SUM performs a system update that includes system firmware, you can choose to upload and reboot to activate the system, or upload the firmware, but not activate it. If you choose to let SUM reboot and activate the system, SUM issues an operating system shutdown request, monitors the system firmware programming, and then issues a request to power on the system.

If you do not allow SUM to reboot the system to activate the system firmware, the update is staged pending system reboot. If you attempt to update the system firmware before the reboot activates the pending firmware, iLO prevents the update. SUM prompts you to either activate or cancel the staged firmware. After you make this decision, you can install the latest firmware update.

If you start a new SUM session and add a system with a pending system firmware update, SUM gives you options on how to proceed.

- **Leave the system for manual reboot to activate**: This option prevents you from updating the system until after you reboot the system to activate the update.
- **Let SUM shut down the OS and let activation happen**: This option allows SUM to power down the system, monitor the system firmware installation, and then power the system up. You can proceed with the new updates.
- **Let SUM cancel the pending update**: SUM cancels the pending update, and the operating system does not reboot. After SUM cancels the pending update, you can continue with new platform firmware updates.

  **NOTE:**

  Hewlett Packard Enterprise does not recommend canceling pending system firmware updates. iLO and system firmware are designed to be installed in pairs. If you cancel a pending update, you might leave the system in an unstable state when the system reboots.

**NOTE:**

On Superdome 2 nPartitions, you can install but not activate partition firmware. Superdome 2 enclosures allow you to apply updates when partition firmware is pending activation.

## Checking for pending system firmware manually

To manually check for pending system firmware, use the iLO GUI or CLI.

### Procedure

1. From the iLO GUI, select **Status Summary** and then click **FW Revisions** tab. The table displays any pending firmware version.
2. From the iLO CLI command menu, type `sr`. The table displays any pending firmware version.

## Activating pending system firmware manually

You can manually activate pending system firmware by powering down the system. The following commands remove DC power from the main server, but the AC standby power remains on. To activate pending firmware:

### Procedure

- From the iLO GUI, click the **Power Management** tab.
- From the iLO CLI command menu, type `pc -off`.
- From HP-UX, type **shutdown -h**.

**NOTE:**

The commands shutdown -r and reboot do not power down the server. These commands result in HP-UX stopping, but the pending update does not activate.

## Canceling pending system firmware manually

### Procedure

- If you need to manually cancel a pending system firmware update, use the iLO CLI command menu. Type `fw - cancel`.

**NOTE:**

Canceling a pending system firmware update might leave the system with incompatible iLO and system firmware images. If you cancel a pending system firmware, you should perform a full platform firmware update immediately.

## Firmware mismatch on multi-blade servers/nPartitions

On Integrity multi-blade servers, you might have a mismatch in firmware between blades after you replace, upgrade, or re-configure a blade. If there is a mismatch between blades, you cannot boot the server. To correct a mismatch, use SUM to update firmware. When SUM finishes the updates, all blades will be at the same firmware level.

If SUM identifies a blade firmware mismatch that prevents booting a system during target discovery, SUM forces the installation to the currently available version of the firmware. This might result in a downgrade of one or more blades.

When SUM identifies a firmware mismatch, it displays an error message in the target status area. You can find the details of the firmware mismatch on the Select Components screen.

- On c-Class servers, SUM displays a mismatch link listed for installed firmware. You can click the link to view the firmware versions on each blade.
- On Superdome 2 servers, go to the Select Devices screen. Click the **Mismatch** link to view the versions..

## Enclosure-level firmware mismatch situations

Components other than blades might have mismatching firmware versions in an enclosure. During discovery, SUM can identify these mismatches and provide a link to view the details on the Review/Install Updates screen.

## I/O card driver version dependency failure

To install I/O card firmware on HP-UX, the firmware components require a minimum driver version. A `Dependency failure` error message appears in the target status area. Click the link to view a description of the failure, including the minimum required version. Before you can update the I/O card with SUM, you must update to the minimum version using tools outside of SUM.

# Support and other resources

## Websites

**General websites**

| | |
|---|---|
| **Hewlett Packard Enterprise Information Library** | **www.hpe.com/info/EIL** |
| **Smart Update Manager** | **www.hpe.com/servers/sum** |
| **Smart Update Manager Downloads** | **www.hpe.com/servers/sum-download** |
| **Smart Update Manager Information Library** | **www.hpe.com/info/sum-docs** |
| **Smart Update Tools** | **www.hpe.com/servers/sut** |
| **Smart Update Tools Information Library** | **www.hpe.com/info/sut-docs** |
| **Service Pack for ProLiant** | **www.hpe.com/servers/spp** |
| **Service Pack for ProLiant documentation** | **www.hpe.com/info/spp/documentation** |
| **Service Pack for ProLiant downloads** | **www.hpe.com/servers/spp/download** |
| **Service Pack for ProLiant custom downloads** | **www.hpe.com/servers/spp/custom** |
| **HPE SDR site** | **downloads.linux.hpe.com** |

For additional websites, see **Support and other resources**.

## Support and other resources

### Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:

  **http://www.hpe.com/assistance**
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:

  **http://www.hpe.com/support/hpesc**

**Information to collect**

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

# Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates:

| | |
|---|---|
| **Hewlett Packard Enterprise Support Center** | **www.hpe.com/support/hpesc** |
| **Hewlett Packard Enterprise Support Center: Software downloads** | **www.hpe.com/support/downloads** |
| **Software Depot** | **www.hpe.com/support/softwaredepot** |

- To subscribe to eNewsletters and alerts:

  **www.hpe.com/support/e-updates**
- To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:

  **www.hpe.com/support/AccessToSupportMaterials**

**IMPORTANT:**

Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HP Passport set up with relevant entitlements.

# Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website:

**http://www.hpe.com/support/selfrepair**

# Remote support

Remote support is available with supported devices as part of your warranty or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product's service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

If your product includes additional remote support details, use search to locate that information.

### Remote support and Proactive Care information

| | |
|---|---|
| **HPE Get Connected** | **www.hpe.com/services/getconnected** |
| **HPE Proactive Care services** | **www.hpe.com/services/proactivecare** |
| **HPE Proactive Care service: Supported products list** | **www.hpe.com/services/proactivecaresupportedproducts** |
| **HPE Proactive Care advanced service: Supported products list** | **www.hpe.com/services/proactivecareadvancedsupportedproducts** |

### Proactive Care customer information

| | |
|---|---|
| **Proactive Care central** | **www.hpe.com/services/proactivecarecentral** |

| | |
|---|---|
| **Proactive Care service activation** | **www.hpe.com/services/proactivecarecentralgetstarted** |

## Warranty information

To view the warranty for your product, see the *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products* document, available at the Hewlett Packard Enterprise Support Center:

**www.hpe.com/support/Safety-Compliance-EnterpriseProducts**

### Additional warranty information

| | |
|---|---|
| **HPE ProLiant and x86 Servers and Options** | **www.hpe.com/support/ProLiantServers-Warranties** |
| **HPE Enterprise Servers** | **www.hpe.com/support/EnterpriseServers-Warranties** |
| **HPE Storage Products** | **www.hpe.com/support/Storage-Warranties** |
| **HPE Networking Products** | **www.hpe.com/support/Networking-Warranties** |

## Regulatory information

To view the regulatory information for your product, view the *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products*, available at the Hewlett Packard Enterprise Support Center:

**www.hpe.com/support/Safety-Compliance-EnterpriseProducts**

### Additional regulatory information

Hewlett Packard Enterprise is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements such as REACH (Regulation EC No 1907/2006 of the European Parliament and the Council). A chemical information report for this product can be found at:

**www.hpe.com/info/reach**

For Hewlett Packard Enterprise product environmental and safety information and compliance data, including RoHS and REACH, see:

**www.hpe.com/info/ecodata**

For Hewlett Packard Enterprise environmental information, including company programs, product recycling, and energy efficiency, see:

**www.hpe.com/info/environment**

## Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (**docsfeedback@hpe.com**). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.

# Acronyms and abbreviations

| **CNA** | Converged Network Adaptor |
|---|---|
| **CPLD** | Complex Programmable Logic Device |
| **DHCP** | Dynamic Host Configuration Protocol |
| **DNS** | domain name system |
| **EFM** | Enclosure Firmware Management |
| **HBA** | host bus adapter |
| **HPE SIM** | HPE Systems Insight Manager |
| **iLO** | Integrated Lights-Out |
| **ISO** | International Organization for Standardization |
| **KVM** | keyboard, video, monitor |
| **MSA** | Modular Smart Array |
| **NVRAM** | non-volatile random access memory |
| **OA** | Onboard Administrator |
| **PXE** | Preboot Execution Environment |
| **PXE BOOT** | Preboot eXecution Environment Enable/Disable utility |
| **RIBCL** | Remote Insight Board Command Language |
| **RPM** | Red Hat Package Manager |
| **SAS** | serial attached SCSI |
| **SATA** | serial ATA |
| **SCCM** | System Center Configuration Manager |
| **SCP** | secure copy |
| **SOAP** | Simple Object Access Protocol |
| **SPP** | Service Pack for ProLiant |
| **SUV** | serial, USB, video |
| **TPM** | Trusted Platform Module |
| **UID** | unit identification light |
| **USB** | universal serial bus |
| **VC** | Virtual Connect |
| **VCA** | Version Control Agent |
| **VCRM** | Version Control Repository Manager |
| **VCSU** | Virtual Connect Support Utility |
| **VM** | Virtual Machine |
| **VSM** | Virtual SAS Manager |

*Table Continued*

| | |
|---|---|
| **WBEM** | Web Based Enterprise Management |
| **WMI** | Windows Management Instrumentation |