Managing Firmware through UCSM

Download and Manage Firmware in Cisco UCS Manager

Firmware Image Management

Cisco delivers all firmware updates to Cisco UCS components in bundles of images. Each image represents an individual firmware package specific to one hardware component. For example: IOM image, Cisco UCS Manager image, and so on.Cisco UCS firmware updates are available to be downloaded to fabric interconnects in a Cisco UCS domain in the following bundles:

Cisco UCS Infrastructure Software Bundle

Cisco UCS Manager Release 4.0 and later releases contain four separate infrastructure bundles:

These bundles include firmware images that are required to update the following components:

- Cisco UCS Manager software
- Kernel and system firmware for the fabric interconnects
- I/O module firmware

Note Cisco UCS 6400 Series Fabric Interconnects and Cisco UCS 6500 Series Fabric Interconnects do not have separate kickstart and system images.

Note The UCS infrastructure bundle for one platform cannot be used to activate another platform. For example, the infrastructure bundle for the UCS 6300 Series Fabric Interconnect cannot be used to activate the Cisco UCS 6400 Series Fabric Interconnect and Cisco UCS 6500 Series Fabric Interconnects.

Cisco UCS B-Series Blade Server Software Bundle

This bundle includes the following firmware images that are required to update the firmware for the blade servers in a Cisco UCS domain. In addition to the bundles created for a release, these bundles can also be released between infrastructure bundles to enable Cisco UCS Manager to support a blade server that is not included in the most recent infrastructure bundle.

- CIMC firmware
- BIOS firmware
- Adapter firmware
- Board controller firmware
- Third-party firmware images required by the new server

Cisco UCS C-Series Rack-Mount UCS-Managed Server Software Bundle

This bundle includes the following firmware images that are required to update components on rack-mount servers that have been integrated with and are managed by Cisco UCS Manager:

- CIMC firmware
- BIOS firmware
- Adapter firmware
- Storage controller firmware

Note You cannot use this bundle for standalone C-series servers. The firmware management system in those servers cannot interpret the header required by Cisco UCS Manager. For information on how to upgrade standalone C-series servers, see the C-series configuration guides.

Cisco also provides release notes, which you can obtain on the same website from which you obtained the bundles.

Caution Ensure that before starting the auto-install process, you capture the data according to Verification that the Data Path is Ready.

- Before acknowledging the pending activity during auto-install, it is important to confirm that all the subordinate VIF paths are rebuilt.
- Ensure that you monitor the UCS VIF paths only from the CLI and not from the faults within the UCS Manager GUI.
- If you fail to monitor the UCS VIF paths, it may result in partial or complete "All Paths Down" state.

We recommend that you follow the guidelines prior to any processes that require reboot of both Fabric Interconnects.

Firmware Image Headers

Every firmware image has a header, which includes the following:

- Checksum
- Version information
- Compatibility information that the system can use to verify the compatibility of component images and any dependencies

Firmware Image Catalog

Cisco UCS Manager maintains an inventory of all available images. The image catalog contains a list of images and packages. A package is a read-only object that is created when it is downloaded. It does not occupy disk space and represents a list or collection of images that were unpacked as part of the package download. When an individual image is downloaded, the package name remains the same as the image name.

Cisco UCS Manager provides you with two views of the catalog of firmware images and their contents that have been downloaded to the fabric interconnect:

Packages

This view provides you with a read-only representation of the firmware bundles that have been downloaded onto the fabric interconnect. This view is sorted by image, not by the contents of the image. For packages, you can use this view to see which component images are in each downloaded firmware bundle.

Images

The images view lists the component images available on the system. You cannot use this view to see complete firmware bundles or to group the images by bundle. The information available about each component image includes the name of the component, the image size, the image version, and the vendor and model of the component.

You can use this view to identify the firmware updates available for each component. You can also use this view to delete obsolete and unneeded images. After all the images in the package have been deleted, Cisco UCS Manager deletes the package itself.

Tip Cisco UCS Manager stores the images in bootflash on the fabric interconnect. In a cluster system, space usage in bootflash on both fabric interconnects is the same, because all images are synchronized between them. Faults are raised when the bootflash partition exceeds 70 percent and total used space exceeds 90 percent. If Cisco UCS Manager generates such a fault, delete obsolete images to free up space.

Obtaining Software Bundles from Cisco

Before you begin

Determine which of the following software bundles you need in order to update the Cisco UCS domain:

- Cisco UCS Infrastructure Software Bundle for Cisco UCS 6500 Series Fabric Interconnects, Cisco UCS 6400 Series Fabric Interconnects, 6300 Series Fabric Interconnects and 6324 Fabric Interconnects—Required for all Cisco UCS domains.

- Cisco UCS B-Series Blade Server Software Bundle—Required for all Cisco UCS domains that include blade servers.
- Cisco UCS C-Series Rack-Mount UCS-Managed Server Software Bundle—Only required for Cisco UCS domains that include integrated rack-mount servers. This bundle contains firmware to enable Cisco UCS Manager to manage those servers and is not applicable to standalone C-Series rack-mount servers.

Procedure

Step 1 In a web browser, navigate to Cisco.com.

Step 2 Under **Support**, click **All Downloads**.

Step 3 In the center pane, click **Servers - Unified Computing**.

Step 4 If prompted, enter your Cisco.com username and password to log in.

Step 5 In the right pane, click the link for the software bundles you require, as follows:

Bundle	Navigation Path
Cisco UCS Infrastructure Software Bundle for Cisco UCS 6500 Series Fabric Interconnects, Cisco UCS 6400 Series Fabric Interconnects, 6300 Series Fabric Interconnects, and 6324 Fabric Interconnects	Click **UCS Infrastructure and UCS Manager Software** > **Unified Computing System (UCS) Infrastructure Software Bundle**.
Cisco UCS B-Series Blade Server Software Bundle	Click **UCS B-Series Blade Server Software** > **Unified Computing System (UCS) Server Software Bundle**.
Cisco UCS C-Series Rack-Mount UCS-Managed Server Software Bundle	Click **UCS C-Series Rack-Mount UCS-Managed Server Software** > **Unified Computing System (UCS) Server Software Bundle**.

Tip The Unified Computing System (UCS) Documentation Roadmap Bundle, which is accessible through these paths, is a downloadable ISO image of all Cisco UCS documentation.

Step 6 On the first page from which you download a software bundle, click the **Release Notes** link to download the latest version of the Release Notes.

Step 7 For each software bundle that you want to download, do the following:

a) Click the link for the latest release 4.0 software bundle.

The release number is followed by a number and a letter in parentheses. The number identifies the maintenance release level, and the letter differentiates between patches of that maintenance release. For more information about what is in each maintenance release and patch, see the latest version of the Release Notes.

b) Click one of the following buttons and follow the instructions provided:

- **Download Now**—Allows you to download the software bundle immediately.
- **Add to Cart**—Adds the software bundle to your cart to be downloaded at a later time.

c) Follow the prompts to complete your download of the software bundle(s).

Step 8 Read the Release Notes before upgrading your Cisco UCS domain.

What to do next

Download the software bundles to the fabric interconnect.

Downloading Firmware Images to the Fabric Interconnect from a Remote Location

Note In a cluster setup, the image file for the firmware bundle is downloaded to both fabric interconnects, regardless of which fabric interconnect is used to initiate the download. Cisco UCS Manager maintains all firmware packages and images in both fabric interconnects in sync. If one fabric interconnect is down, the download finishes successfully. The images are synced to the other fabric interconnect when it comes back online.

Before you begin

Obtain the required firmware bundles from Cisco.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Click the **Equipment** node.

Step 3 In the **Work** pane, click the **Firmware Management** tab.

Step 4 Click the **Installed Firmware** tab.

Step 5 Click **Download Firmware**.

Step 6 In the **Download Firmware** dialog box, click the **Remote File System** radio button in the **Location of the Image File** field and fill in the following fields:

Name	Description
Protocol field	The protocol to use when communicating with the remote server. This can be one of the following: • **FTP** • **TFTP** **Note** The TFTP file size limitation is 32 MB. Because firmware bundles can be much larger, Cisco recommends that you do not choose TFTP for firmware downloads. • **SCP** • **SFTP** • **USB A**—The USB drive inserted into fabric interconnect A. • **USB B**—The USB drive inserted into fabric interconnect B. **Note** USB A and USB B are applicable only for Cisco UCS 6324 (UCS Mini) and Cisco UCS 6300 Series fabric interconnects. For Cisco UCS 6300 Series fabric interconnects, only the first of the two ports is detected.
Server field	If the file came from a remote server, this is the IP address or hostname of the remote server on which the files resides. If the file came from a local source, this field displays "local". **Note** If you use a hostname rather than an IPv4 or IPv6 address, you must configure a DNS server. If the Cisco UCS domain is not registered with Cisco UCS Central or DNS management is set to local, configure a DNS server in Cisco UCS Manager. If the Cisco UCS domain is registered with Cisco UCS Central and DNS management is set to global, configure a DNS server in Cisco UCS Central.
Filename field	The name of the firmware file.
Path field	The absolute path to the file on the remote server. If you use SCP, the absolute path is always required. If you use any other protocol, you may not need to specify a remote path if the file resides in the default download folder. For details about how your file server is configured, contact your system administrator.
User field	The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP.
Password field	The password for the remote server username. This field does not apply if the protocol is TFTP.

Step 7 Click **OK**.

Cisco UCS Manager GUI begins downloading the firmware bundle to the fabric interconnect.

Step 8 (Optional) Monitor the status of the download on the **Download Tasks** tab.

Note If Cisco UCS Manager reports that the bootflash is out of space, delete obsolete bundles on the **Packages** tab to free up space. To view the available space in bootflash, navigate to the fabric interconnect, click **Equipment**, and expand the **Local Storage Information** area on the **General** tab.

Step 9 Repeat this task until all the required firmware bundles have been downloaded to the fabric interconnect.

What to do next

After the image file for the firmware bundles download completes, update the firmware on the endpoints.

Downloading Firmware Images to the Fabric Interconnect from the Local File System

Note In a cluster setup, the image file for the firmware bundle is downloaded to both fabric interconnects, regardless of which fabric interconnect is used to initiate the download. Cisco UCS Manager maintains all firmware packages and images in both fabric interconnects in sync. If one fabric interconnect is down, the download finishes successfully. The images are synced to the other fabric interconnect when it comes back online.

Before you begin

Obtain the required firmware bundles from Cisco.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Click the **Equipment** node.

Step 3 In the **Work** pane, click the **Firmware Management** tab.

Step 4 Click the **Installed Firmware** tab.

Step 5 Click **Download Firmware**.

Step 6 In the **Download Firmware** dialog box, click the **Local File System** radio button in the **Location of the Image File** field.

Step 7 In the **Filename** field, type the full path and name of the image file.

If you do not know the exact path to the folder where the firmware image file is located, click **Browse** and navigate to the file.

Note For the HTML5 GUI in Cisco UCS Mini, click **Choose File** to locate the firmware image file.

Step 8 Click **OK**.

Cisco UCS Manager GUI begins downloading the firmware bundle to the fabric interconnect.

Step 9 (Optional) Monitor the status of the firmware bundle download on the **Download Tasks** tab.

Note If Cisco UCS Manager reports that the bootflash is out of space, delete obsolete bundles on the **Packages** tab to free up space. To view the available space in bootflash, navigate to the fabric interconnect on the **Equipment** tab and expand the **Local Storage Information** area on the **General** tab.

Step 10 Repeat this task until all the required firmware bundles have been downloaded to the fabric interconnect.

What to do next

After the image file for the firmware bundles download completes, update the firmware on the endpoints.

Canceling an Image Download

You can cancel the download task for an image only while it is in progress. After the image has downloaded, deleting the download task does not delete the image that was downloaded. You cannot cancel the FSM related to the image download task.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand the **Equipment** node.

Step 3 In the **Work** pane, click the **Firmware Management** tab.

Step 4 On the **Download Tasks** tab, right-click the task you want to cancel and select **Delete**.

Determining the Contents of a Firmware Package

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Click the **Equipment** node.

Step 3 In the **Work** pane, click the **Firmware Management** tab.

Step 4 On the **Packages** subtab, click the + icon next to a package to view its contents.

Step 5 To take a snapshot of the package contents, do the following:

a) Highlight the rows that include the image name and its contents.

b) Right-click and choose **Copy**.

c) Paste the contents of your clipboard into a text file or other document.

Checking Conformance of the Contents of a Firmware Package

You can use the Check Conformance feature to verify that all your components are running the correct firmware version for the bundle selected. This should not be used before a firmware upgrade is performed, but after the upgrade is completed.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Click the **Equipment** node.

Step 3 In the **Work** pane, click the **Firmware Management** tab.

Step 4 In the **Packages** subtab, select the package that you want to check for conformance.

Step 5 Click **Check Conformance**.

Step 6 In the dialog box that appears, the **Message** column describes whether each component is in conformance with the firmware package.

Checking the Available Space on a Fabric Interconnect

If an image download fails, check whether the bootflash on the fabric interconnect or fabric interconnects in the Cisco UCS has sufficient available space.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Fabric Interconnects**.

Step 3 Click the fabric interconnect on which you want to check the available space.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 Expand the **Local Storage Information** area.

When you download a firmware image bundle, a fabric interconnect needs at least twice as much available space as the size of the firmware image bundle. If the bootflash does not have sufficient space, delete the obsolete firmware, core files, and tech support files from the fabric interconnect.

Firmware Upgrades through Auto Install

Auto Install enables you to upgrade a Cisco UCS domain to the firmware versions contained in a single package in the following stages:

- Install Infrastructure Firmware—Uses the Cisco UCS Infrastructure Software Bundle to upgrade the infrastructure components, such as the fabric interconnects, the I/O modules, and Cisco UCS Manager. Firmware Image Management, on page 1, provides details about the available infrastructure software bundles in Cisco UCS Manager Release 4.0. Recommended Process for Upgrading Infrastructure Firmware

Through Auto Install, on page 13, details the process that Cisco recommends for automatically installing infrastructure firmware.

- Install Chassis Firmware—Uses the Cisco UCS C-Series Rack-Mount UCS-Managed Server Software Bundle to upgrade the chassis components.
- Install Server Firmware—Uses the Cisco UCS B-Series Blade Server Software Bundle to upgrade all blade servers in the Cisco UCS domain; the Cisco UCS C-Series Rack-Mount UCS-Managed Server Software Bundle to upgrade all rack servers.

These stages are independent and can be run or scheduled to run at different times.

You can use Auto Install to upgrade the infrastructure components to one version of Cisco UCS and upgrade the chassis and server components to a different version.

Note You cannot use Auto Install to upgrade either the infrastructure or the servers in a Cisco UCS domain if Cisco UCS Manager in that domain is at a release prior to Cisco UCS 2.1(1). However, after you upgrade Cisco UCS Manager to Release 2.1(1) or greater, you can use Auto Install to upgrade the remaining components in a Cisco UCS domain that is at the minimum required firmware level. For more information, see Cautions, and Guidelines for Upgrading with Auto Install.

In Cisco UCS Manager Releases 3.1(1l), 3.1(2b), 3.1(2c), and 3.1(2e), activating the Cisco UCS Manager software through Auto Install fails if the power policy is configured with **Redundancy** set to **Grid** and **Power Capping** set to **No Cap**. In Cisco UCS Manager releases earlier than Cisco UCS Manager Release 3.1(2b) and later than 3.1(2e), activating the Cisco UCS Manager software through Auto Install no longer fails based on the configured power policy.

Direct Upgrade After Auto Install

During Auto Install, the startup version of the default infrastructure pack is configured. To successfully complete a direct upgrade or activation of Cisco UCS Manager, Fabric Interconnects, and IOMs after Auto Install, ensure that the startup version is cleared before starting direct upgrade or activation. If the startup version of the default infrastructure pack is configured, you cannot directly upgrade or activate Cisco UCS Manager, Fabric Interconnects, and IOMs. Clearing the Startup Version of the Default Infrastructure Pack and the Service Pack, on page 20, provides detailed steps for clearing the startup version.

Automatic Internal Backup

Note Beginning with release 4.2(3d), Cisco UCS Manager introduces **Password Encryption Key** to enhance security for backup configuration files.

If you do not set **Password Encryption Key**, then **Automatic Internal Backup** also fails. For more information on how to set **Password Encryption Key**, see *Setting Password Encryption Key for Locally Authenticated Users* section in Cisco UCS Manager Administration Management Guide for your release.

While the Infrastructure firmware is being upgraded, an automatic full state backup file is created. Cisco UCS Manager Release 2.2(4) introduced two new backup stages that are visible in the FSM status. These are:

1. **InternalBackup**—Backs up the configuration.
2. **PollInternalBackup**—Waits for the backup to complete.

After the backup is successfully completed, the backup file, named as "bkp.*timestamp*.tgz", is stored within the `/workspace/backup` directory of both the fabric interconnects. This location contains only the latest backup file.

If the backup fails, a minor fault stating "**internal backup failed**" is logged. This fault is not logged in case of downgrade to a release prior to Cisco UCS Manager Release 2.2(4).

Before restoring the configuration for a fabric interconnect from this backup file, copy it from the fabric interconnect to a file server by using the **copy** command from local-mgmt.

This example shows how to copy the automatic internal backup file to a file server:

```
UCS-A# connect local-mgmt
UCS-A (local-mgmt) # copy workspace:/backup/bkp.1429690478.tgz
scp://builds@10.190.120.2://home/builds/
```

Prepare for Firmware Install

You can use Auto Install to upgrade a Cisco UCS domain to the firmware versions contained in a single package. Auto Install provides the ability to install firmware in three independent phases—Install Infrastructure Firmware, Install Chassis Firmware, and Install Server Firmware. During Auto Install, the firmware for some endpoints such as the IOMs, adapters, BIOS and CIMC are first updated and then activated.

Updating the firmware on an endpoint involves staging the firmware image to the backup partition on an endpoint. The update phase does not require or cause reboot of the endpoint. During activation, you set the firmware in the backup partition as the active firmware version on the endpoint. Activation can require or cause the reboot of an endpoint. Therefore, the time taken to complete the Auto Install process includes the time required to do the following:

- Update or stage firmware to the backup partition of all endpoints

Note This process takes most of the time spent to complete Auto Install.

- Activate firmware on all the endpoints
- Reboot all applicable endpoints

Cisco UCS Manager Release 3.2(3) introduces the ability to update or stage the firmware of infrastructure, server components, and S3260 chassis simultaneously, and keep it independent of the activation process. Because staging firmware does not involve rebooting any endpoints, this ability allows you to stage the firmware on all endpoints without waiting for a maintenance window. Consequently, the time taken to complete the Auto Install process no longer includes the time taken to stage firmware to the backup partition of all endpoints. You can, thus, significantly reduce the downtime required for maintenance.

If you stage the firmware using this feature before performing Auto Install, you can skip backup updates and proceed with firmware activation and endpoint reboots. If you do not stage the firmware on the endpoints through this feature, you can continue to use Auto Install to update and activate the components. The ability

to stage firmware to the backup partition of endpoints does not change the legacy ability of Auto Install to update and activate the firmware of components.

Install Infrastructure Firmware

Install Infrastructure Firmware upgrades all infrastructure components in a Cisco UCS domain, including Cisco UCS Manager, and all fabric interconnects and I/O modules. All components are upgraded to the firmware version included in the selected Cisco UCS Infrastructure Software Bundle.

Install Infrastructure Firmware does not support a partial upgrade to only some infrastructure components in a Cisco UCS domain domain.

You can schedule an infrastructure upgrade for a specific time to accommodate a maintenance window. However, if an infrastructure upgrade is already in progress, you cannot schedule another infrastructure upgrade. You must wait until the current upgrade is complete before scheduling the next one.

Note You can cancel an infrastructure firmware upgrade if it is scheduled to occur at a future time. However, you cannot cancel an infrastructure firmware upgrade after the upgrade has begun.

Install Server Firmware

Install Server Firmware uses host firmware packages to upgrade all servers and their components in a Cisco UCS domain. All servers whose service profiles include the selected host firmware packages are upgraded to the firmware versions in the selected software bundles, as follows:

- Cisco UCS B-Series Blade Server Software Bundle for all blade servers in the chassis.
- Cisco UCS C-Series Rack-Mount UCS-Managed Server Software Bundle for all rack-mount servers that are integrated into the Cisco UCS domain.

Note You cannot cancel a server firmware upgrade process after you complete the configuration in the **Install Server Firmware** wizard. Cisco UCS Manager applies the changes immediately. However, the timing of the actual reboot of servers occurs depends upon the maintenance policy in the service profile associated with the server.

Required Order of Steps for Auto Install

If you want to upgrade all components in a Cisco UCS domain to the same package version, you must run the stages of Auto Install in the following order:

1. Install Infrastructure Firmware
2. Install Server Firmware

This order enables you to schedule the server firmware upgrades during a different maintenance window than the infrastructure firmware upgrade.

Recommended Process for Upgrading Infrastructure Firmware Through Auto Install

Cisco recommends the following process for upgrading infrastructure firmware through Auto Install:

1. Stage the software and prepare for upgrade:
   a. Create All Configuration and Full-State backup files. Creating an All Configuration Backup File, and Creating a Full State Backup File, provide detailed information.
   b. Download firmware packages. Downloading Firmware Images to the Fabric Interconnect from a Remote Location, on page 5, and Downloading Firmware Images to the Fabric Interconnect from the Local File System, on page 7, provide detailed information.
   c. Stage the Infrastructure firmware if using Cisco UCS Manager Release 3.2(3) or later releases. Preparing for Firmware Install, on page 14, provides detailed information about staging the infrastructure firmware.

Note Although this step is optional, it is also recommended.

   d. Disable Smart Call Home. Disabling Smart Call Home, provides detailed information about disabling Smart Call Home.

2. Prepare for fabric upgrade:
   a. Verify Cisco UCS Manager faults and resolve the service -impacting faults. Viewing UCS Manager Faults, provides detailed information about verifying faults.
   b. Verify High Availability status and identify the secondary fabric interconnect. Verifying the High Availability Status and Roles of a Cluster Configuration, provides detailed information.
   c. Configure the default maintenance policy. Configuring the Default Maintenance Policy, provides detailed information. You can also click **Play** on this video (http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/configure_the_default_maintenance_policy.html) to watch how to configure the default maintenance policy as **User Ack**.
   d. Verify that VLAN and FCOE IDs do not overlap.
   e. Disable the management interface. Disabling the Management Interface, provides detailed information about disabling the management interface for the secondary fabric interconnect.
   f. Verify that all paths are working. Verification that the Data Path is Ready, provides detailed information.

3. Upgrade infrastructure firmware through Auto Install. Upgrading the Infrastructure Firmware with Auto Install, on page 15, provides detailed information. You can also click **Play** on this video (http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/upgrade_the_infrastructure_firmware_with_auto_install.html) to watch how to upgrade infrastructure firmware with Auto Install.

Note If you staged the infrastructure firmware by using **Prepare for Firmware Install**, this step will only involve an activate with reboot, if reboot is required.

4. Verify High Availability status in cluster.
5. Verify that all paths are working.
6. Verify new faults. Viewing Faults Generated During the Upgrade of a Fabric Interconnect provides detailed information.
7. Acknowledge activation of the primary fabric. Acknowledging the Reboot of the Primary Fabric Interconnect, on page 18, provides detailed information. You can also click **Play** on this video (http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/acknowledge_pending_reboot_of_the_primary_fabric_interconnect.html) to watch how to acknowledge the reboot of the primary fabric interconnect.
8. Verify new faults.

Preparing for Firmware Install

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Click the **Equipment** node.

Step 3 In the **Work** pane, click the **Firmware Management** tab.

Step 4 In the **Work** pane, click the **Firmware Auto Install** tab.

Step 5 In the **Actions** area, click **Prepare for Firmware Install**.

Step 6 On the **Select Package Versions** page of the **Prepare for Firmware Install** wizard, do the following:

a) To update the infrastructure components in the Cisco UCS domain, choose the software bundle to which you want to upgrade from the **New Version** drop-down list in the **A-Series Infrastructure Firmware** area.

b) To update the blade servers in the Cisco UCS domain, choose the software bundle to which you want to upgrade from the **New Version** drop-down list in the **B-Series Blade Server Firmware** area.

c) To update the rack-mount servers and S3260 chassis in the Cisco UCS domain, choose the software bundle to which you want to upgrade from the **New Version** drop-down list in the **C-Series Chassis/Rack-Mount Server Firmware** area.

If the Cisco UCS domain includes both blade servers and rack servers, we recommend that you choose a new firmware version for the B-Series blade servers and C-Series rack-mount servers in the **Select Package Versions** page and upgrade all servers in the domain.

Note If you update the default host firmware package, you might cause the upgrade of firmware on unassociated servers and on servers with associated service profiles that do not include a host firmware package. This firmware upgrade may cause the reboot of those servers according to the maintenance policy defined in the service profile.

d) Click **Next**.

Step 7 On the **Select Firmware Packages** page of the **Prepare for Firmware Install** wizard, do the following:

a) Expand the node for each organization that contains a firmware package you want to update with the selected software.

b) Check the check box next to the name of each firmware package that you want to update.

This step modifies all the selected infra, host and chassis firmware packages with the new version of firmware.

c) Click **Next**.

Step 8 On the **Firmware Package Dependencies** page of the **Prepare for Firmware Install** wizard, do the following:

a) Expand the node for each host firmware package listed in the table.

b) Review the list of service or chassis profiles that include the host or chassis firmware package.

c) If desired, click a link in one of the following columns:

- **Host/Chassis Pack DN** column—Opens the navigator for the host or chassis firmware package.
- **Service/Chassis Profile DN** column—Opens the navigator for the service or chassis profile.

d) Do one of the following:

- To change one or more of the selected firmware packages, click **Prev**.
- If you are satisfied that you have selected the appropriate firmware packages and want to review the impact of the firmware updates on the endpoints, click **Next**.
- To start the firmware update immediately, click **Update**.

Step 9 On the **Endpoints Summary** page of the **Prepare for Firmware Install** wizard, do the following:

a) Click the appropriate check boxes to filter the results in the **UCS Firmware Pack Endpoints** table.

You can filter the results by the type of endpoint.

b) Review the list of impacted endpoints.

c) Do one of the following:

- If you want to change one or more of the selected firmware packages, click **Prev**.
- If you are satisfied that you have selected the appropriate firmware packages and want to start the server upgrade, click **Update**.

Upgrading the Infrastructure Firmware with Auto Install

The **Firmware Auto Install** tab is not available if the Cisco UCS Manager GUI is at a release lower than 2.1(1).

Note You cannot use Auto Install to upgrade either the infrastructure or the servers in a Cisco UCS domain if Cisco UCS Manager in that domain is at a release prior to Cisco UCS Manager 2.1(1). However, after you upgrade Cisco UCS Manager to Release 2.1(1) or greater, you can use Auto Install to upgrade the remaining components in a Cisco UCS domain that is at the minimum required firmware level. For more information, see Cautions, and Guidelines for Upgrading with Auto Install, and the appropriate Cisco UCS upgrade guide.

Beginning with Cisco UCS Manager Release 3.1(3), you can use Auto Install to install a service pack on Cisco UCS Manager and both fabric interconnects. You can apply a service pack on a base infrastructure pack, but you cannot install the service pack independently.

You can install a compatible service pack through Auto Install without upgrading the infrastructure pack. This will trigger service pack installation on both fabric interconnects. Certain service pack installations may require the fabric interconnects to be reloaded.

Auto Install of infrastructure firmware using a service pack is supported only when all the infrastructure components are at Cisco UCS Manager Release 3.1(3) or later releases.

Before you begin

- Complete all prerequisites listed in Prerequisites for Upgrading and Downgrading Firmware.
- Stage the Infrastructure firmware if using Cisco UCS Manager Release 3.2(3) or later releases. Preparing for Firmware Install, on page 14, provides detailed information about staging the infrastructure firmware.

Note Although this is optional, it is also recommended.

If your Cisco UCS domain does not use an NTP server to set the time, make sure that the clocks on the primary and secondary fabric interconnects are in sync. You can do this by configuring an NTP server in Cisco UCS Manager or by syncing the time manually.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Click the **Equipment** node.

Step 3 In the **Work** pane, click the **Firmware Management** tab.

Step 4 In the **Work** pane, click the **Firmware Auto Install** tab.

Step 5 In the **Actions** area, click **Install Infrastructure Firmware**.

Step 6 In the **Prerequisites** page of the **Install Infrastructure Firmware** dialog box, ensure that you address the warnings before proceeding.

Warnings are given in the following categories:

- Whether there are any current critical or major faults.
- Whether a configuration backup has been taken recently.
- Whether the management interface monitoring policy is enabled.

- Whether there is pending fabric interconnect reboot activity.
- Whether NTP is configured.

You can click the hyperlinks for each warning to address them directly. Check the checkbox for each warning that you have addressed, or check the **Ignore All** checkbox to continue without addressing the warnings.

Step 7 In the **Properties** area of the **Install Infrastructure Firmware** dialog box, complete the following fields:

Name	Description
Name field	The name of the infrastructure pack created and maintained by Cisco UCS. You cannot change the default name in this field or create a custom infrastructure pack.
Description field	A user-defined description of the infrastructure pack. This field is completed by default. However, you can enter your own description if you prefer. Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), ^ (carat), " (double quote), = (equal sign), > (greater than), < (less than), or ' (single quote).
Backup Version field	The firmware version staged through **Prepare for Firmware Install**. If the firmware version is not staged, this field is empty.
Infra Pack drop-down list	A list of the software bundles that are available for you to upgrade the firmware on the infrastructure components. If the **Infra Pack** version is different from the **Backup Version**, the downtime will include the time taken to stage and then activate the selected infra pack version. If the **Infra Pack** version is the same as the **Backup Version**, the downtime will include the time taken to activate the selected infra pack version.
Service Pack drop-down list	A list of the service pack bundles that are available for you to upgrade the firmware on the infrastructure components. You cannot directly upgrade to a service pack without selecting a base infra pack. **Note** A service pack can be applied only on its base maintenance release. For example, service pack 3.1(3)SP2 can be applied only on a 3.1(3) release. It cannot be applied on a 3.1(4) release. Setting **Service Pack** to **<not set>** removes the service pack from the firmware package.
Force check box	If checked, Cisco UCS attempts the installation even if a previous attempt to install the selected version failed or was interrupted.

Name	Description
Evacuate checkbox	If checked, Fabric Evacuation is enabled on each fabric interconnect that is being upgraded through Auto Install. Both fabric interconnects are evacuated, but not at the same time. By default, this checkbox is unchecked, and fabric evacuation is disabled.

Step 8 In the **Infrastructure Upgrade Schedule** area of the **Install Infrastructure Firmware** dialog box, do one of the following:

Option	Description
Start Time field	The date and time that the occurrence will run. Click the down arrow at the end of the field to select the date from a calendar.
Upgrade Now check box	If checked, Cisco UCS Manager ignores the **Start Time** field and upgrades the infrastructure firmware as soon as you click **OK**.

Step 9 Click **OK**.

The **Firmware Installer** field on the **Firmware Auto Install** tab displays the status of the infrastructure firmware upgrade.

Note If there is not enough space under bootflash, a warning will display and the upgrade process will stop.

What to do next

Acknowledge the reboot of the primary fabric interconnect. If you do not acknowledge that reboot, Cisco UCS Manager cannot complete the infrastructure upgrade and the upgrade remains pending indefinitely.

Certain service pack installations may require the fabric interconnects to be reloaded. In such scenarios, you must acknowledge the reboot of the primary fabric interconnect to complete the service pack installation.

Acknowledging the Reboot of the Primary Fabric Interconnect

You can use the steps detailed here, or click **Play** on this video (http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/acknowledge_pending_reboot_of_the_primary_fabric_interconnect.html) to watch how to acknowledge the reboot of the primary fabric interconnect.

Before you begin

Caution To upgrade with minimal disruption, you must confirm the following:

- Ensure that all the IOMs that are attached to the fabric interconnect are up before you acknowledge the reboot of the fabric interconnect. If all IOMs are not up, all the servers connected to the fabric interconnect will immediately be re-discovered, resulting in a major disruption.
- Ensure that both of the fabric interconnects and the service profiles are configured for failover.
- Verify that the data path has been successfully restored from the secondary fabric interconnect before you acknowledge the reboot of the primary fabric interconnect. For more information, see Verification that the Data Path is Ready.

After you upgrade the infrastructure firmware, Install Infrastructure Firmware automatically reboots the secondary fabric interconnect in a cluster configuration. However, you must acknowledge the reboot of the primary fabric interconnect. If you do not acknowledge the reboot, Install Infrastructure Firmware waits indefinitely for that acknowledgment rather than completing the upgrade.

Procedure

Step 1 On the toolbar, click **Pending Activities**.

Step 2 In the **Pending Activities** dialog box, click the **User Acknowledged Activities** tab.

Step 3 Click the **Fabric Interconnects** subtab and then click **Reboot now**.

Step 4 In the **Reboot now** dialog box that appears, click **Yes** to reboot the Fabric Interconnect and apply the pending changes.

The dialog box includes the below points and asks whether you want to continue to avoid unexpected network issues:

- Dynamic vNIC are up and running (if any).
- Ethernet and Fibre Channel data paths operating as expected.
- No unexpected faults indicating a potential error exists.

Cisco UCS Manager immediately reboots the primary fabric interconnect. You cannot stop this reboot after you click **Yes**.

Canceling an Infrastructure Firmware Upgrade

Note You can cancel an infrastructure firmware upgrade if it is scheduled to occur at a future time. However, you cannot cancel an infrastructure firmware upgrade after the upgrade has begun.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.
Step 2 Click the **Equipment** node.
Step 3 In the **Work** pane, click the **Firmware Management** tab.
Step 4 In the **Work** pane, click the **Firmware Auto Install** tab.
Step 5 In the **Actions** area, click **Install Infrastructure Firmware**.
Step 6 In the **Actions** area of the **Install Infrastructure Firmware** dialog box, click **Cancel Infrastructure Upgrade**.
Step 7 If a confirmation dialog box displays, click **Yes**.
Step 8 Click **OK**.

Clearing the Startup Version of the Default Infrastructure Pack and the Service Pack

You must clear the startup version of the default infrastructure pack and service pack before directly upgrading or activating Cisco UCS Manager, Fabric Interconnects, and IOMs.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.
Step 2 Click the **Equipment** node.
Step 3 In the **Work** pane, click the **Firmware Management** tab.
Step 4 In the **Work** pane, click the **Firmware Auto Install** tab.
Step 5 In the **Actions** area, click **Clear Startup Version**.
Step 6 In the confirmation dialog box that appears, click **Yes**.
Step 7 Click **OK**.

Upgrading the Server Firmware with Auto Install

You can perform a bulk upgrade of blade servers or rack-mount servers through this procedure.

If you staged the server firmware through **Prepare for Firmware Install**, and that backup version is the same as the selected server firmware version in this procedure, the backup version is set as the startup version.

If you did not set the backup version earlier, the selected firmware version is set as the backup version. This version is then set as the startup version.

Completing this stage will result in a reboot.

Note You cannot use Auto Install to upgrade either the infrastructure or the servers in a Cisco UCS domain if Cisco UCS Manager in that domain is at a release prior to Cisco UCS Manager 2.1(1). However, after you upgrade Cisco UCS Manager to Release 2.1(1) or greater, you can use Auto Install to upgrade the remaining components in a Cisco UCS domain that is at the minimum required firmware level. For more information, see Cautions, and Guidelines for Upgrading with Auto Install, and the appropriate Cisco UCS upgrade guide.

Note You cannot cancel a server firmware upgrade process after you complete the configuration in the **Install Server Firmware** wizard. Cisco UCS Manager applies the changes immediately. However, the timing of the actual reboot of servers occurs depends upon the maintenance policy in the service profile associated with the server.

Before you begin

- Complete all prerequisites listed in Prerequisites for Upgrading and Downgrading Firmware.
- Stage the Server firmware if using Cisco UCS Manager Release 3.2(3) or later releases. Preparing for Firmware Install, on page 14, provides detailed information about staging the server firmware.

Note Although this is optional, it is also recommended.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Click the **Equipment** node.

Step 3 In the **Work** pane, click the **Firmware Management** tab.

Step 4 In the **Work** pane, click the **Firmware Auto Install** tab.

Step 5 In the **Actions** area, click **Install Server Firmware**.

Step 6 On the **Prerequisites** page of the **Install Server Firmware** wizard, carefully review the prerequisites and guidelines listed on this page and then do one of the following:

- If you have completed all of the prerequisites, click **Next**.
- If you have not completed all of the prerequisites, click **Cancel** and complete the prerequisites before you upgrade the server firmware.

Step 7 On the **Select Package Versions** page of the **Install Server Firmware** wizard, do the following:

a) If the Cisco UCS domain contains blade servers, choose the software bundle to which you want to upgrade these servers from the **New Version** drop-down list in the **B-Series Blade Server Software** area.

b) If the Cisco UCS domain contains rack-mount servers, choose the software bundle to which you want to upgrade these servers from the **New Version** drop-down list in the **C-Series Rack-Mount Server Software** area.

If the Cisco UCS domain includes both blade servers and rack servers, we recommend that you choose a new firmware version for the B-Series blade servers and C-Series rack-mount servers in the **Select Package Versions** page and upgrade all servers in the domain.

Note If you update the default host firmware package, you might cause the upgrade of firmware on unassociated servers and on servers with associated service profiles that do not include a host firmware package. This firmware upgrade may cause the reboot of those servers according to the maintenance policy defined in the service profile.

c) To upgrade the servers to a service pack firmware version, choose the service pack to which you want to upgrade these servers from the **New Version** drop-down list in the **Service-Pack Firmware** area.
d) Click **Next**.

Step 8 On the **Select Firmware Packages** page of the **Install Server Firmware** wizard, do the following:

a) Expand the node for each organization that contains a host firmware package you want to update with the selected software.

If the firmware version for a host firmware package is staged, it appears in the **Backup Version** field along with the name of the host firmware package.

b) Check the check box next to the name of each host firmware package that you want to update.

This step updates the selected host firmware package with the new version of firmware. You must choose the host firmware packages included in the service profiles associated with all servers in the Cisco UCS domain to update all servers.

c) Click **Next**.

Step 9 On the **Host Firmware Package Dependencies** page of the **Install Server Firmware** wizard, do the following:

a) Expand the node for each host firmware package listed in the table.
b) Review the list of service profiles that include the host firmware package.
c) If desired, click a link in one of the following columns:

- **Host Pack DN** column—Opens the navigator for the host firmware package.
- **Service Profile DN** column—Opens the navigator for the service profile.

d) Do one of the following:

- If you want to change one or more of the selected host firmware packages, click **Prev**.
- If you are satisfied that you have selected the appropriate host firmware packages and want to review the impact of the server firmware upgrade on the endpoints, click **Next**.
- If you want to start the server upgrade immediately, click **Install**.

Step 10 On the **Impacted Endpoints Summary** page of the **Install Server Firmware** wizard, do the following:

a) Click the appropriate check boxes to filter the results in the **Impacted Endpoints** table.

You can filter the results by the type of endpoint and by whether the impact of the upgrade is disruptive or not.

b) Review the list of impacted endpoints.
c) If desired, click the link in the **Maintenance Policy** column to open the navigator for that policy.
d) Do one of the following:

- If you want to change one or more of the selected host firmware packages, click **Prev**.
- If you are satisfied that you have selected the appropriate host firmware packages and want to start the server upgrade, click **Install**.

Step 11 (Optional) To check on the progress of the server firmware upgrade, check the **FSM** tab for each server that you are upgrading.

The **Firmware Installer** field on the **Firmware Auto Install** tab shows only the status of an infrastructure firmware upgrade.

Firmware Upgrades through Firmware Packages in Service Profiles

You can use firmware packages in service profiles to upgrade the server and adapter firmware, including the BIOS on the server, by defining a host firmware policy and including it in the service profile associated with a server.

You cannot upgrade the firmware on an I/O module, fabric interconnect, or Cisco UCS Manager through service profiles. You must upgrade the firmware on those endpoints directly.

Host Firmware Package

This policy enables you to specify a set of firmware versions that make up the host firmware package (also known as the host firmware pack). The host firmware package includes the following firmware for server and adapter endpoints:

- **Adapter**
- **BIOS**
- **CIMC**

Note For rack mount servers, if you exclude CIMC from the host firmware pack, and upgrade or downgrade the board controller, the upgrade or downgrade may fail. This is because the CIMC firmware version and board controller firmware version may be incompatible.

- **Board Controller**
- **Flex Flash Controller**
- **GPUs**
- **FC Adapters**
- **HBA Option ROM**

- **Host NIC**
- **Host NIC Option ROM**
- **Local Disk**

Note **Local Disk** is excluded by default from the host firmware pack.

In Cisco UCS Manager Release 3.1(1), to update local disk firmware, always include the **Blade Package** in the host firmware package. The blade package contains the local disk firmware for blade and rack servers. Starting with Cisco UCS Manager Release 3.1(2), the firmware for local disk and other common endpoints is available in both the blade and rack packages.

- **PSU**
- **SAS Expander**
- **Storage Controller**
- **Storage Controller Onboard Device**
- **Storage Controller Onboard Device Cpld**
- **Storage Device Bridge**

Tip You can include more than one type of firmware in the same host firmware package. For example, a host firmware package can include both BIOS firmware and storage controller firmware or adapter firmware for two different models of adapters. However, you can only have one firmware version with the same type, vendor, and model number. The system recognizes which firmware version is required for an endpoint and ignores all other firmware versions.

You can also exclude firmware of specific components from a host firmware package either when creating a new host firmware package or when modifying an existing host firmware package. For example, if you do not want to upgrade BIOS firmware through the host firmware package, you can exclude BIOS firmware from the list of firmware package components.

Important Each host firmware package is associated with one list of excluded components, which is common across all firmware packages—Blade, and Rack. To configure a separate exclusion list for each type of firmware package, use separate host firmware packages.

The firmware package is pushed to all servers associated with service profiles that include this policy.

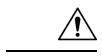
This policy ensures that the host firmware is identical on all servers associated with service profiles that use the same policy. Therefore, if you move the service profile from one server to another, the firmware versions are maintained. Also, if you change the firmware version for an endpoint in the firmware package, new versions are applied to all the affected service profiles immediately. This could cause server reboots.

You must include this policy in a service profile, and that service profile must be associated with a server for it to take effect.

This policy is not dependent upon any other policies. However, you must ensure that the appropriate firmware has been downloaded to the fabric interconnect. If the firmware image is not available when Cisco UCS Manager is associating a server with a service profile, Cisco UCS Manager ignores the firmware upgrade and completes the association.

Stages of a Firmware Upgrade through Firmware Packages in Service Profiles

You can use the host firmware package policies in service profiles to upgrade server and adapter firmware.



Caution Unless you have configured and scheduled a maintenance window, if you modify a host firmware package by adding an endpoint or changing firmware versions for an existing endpoint, Cisco UCS Manager upgrades the endpoints and reboots all servers associated with that firmware package as soon as the changes are saved, disrupting data traffic to and from the servers.

New Service Profile

For a new service profile, this upgrade takes place over the following stages:

Firmware Package Policy Creation

During this stage, you create the host firmware packages.

Service Profile Association

During this stage, you include the firmware packages in a service profile, and then associate the service profile with a server. The system pushes the selected firmware versions to the endpoints. The server must be rebooted to ensure that the endpoints are running the versions specified in the firmware package.

Existing Service Profile

For service profiles that are associated with servers, Cisco UCS Manager upgrades the firmware and reboots the server as soon as you save the changes to the firmware packages' unless you have configured and scheduled a maintenance window. If you configure and schedule a maintenance window, Cisco UCS Manager defers the upgrade and server reboot until then.

Effect of Updates to Firmware Packages in Service Profiles

To update firmware through a firmware package in a service profile, you need to update the firmware in the package. What happens after you save the changes to a firmware package depends upon how the Cisco UCS domain is configured.

The following table describes the most common options for upgrading servers with a firmware package in a service profile.

Service Profile	Maintenance Policy	Upgrade Actions
Firmware package is not included in a service profile or an updating service profile template. OR You want to upgrade the firmware without making any changes to the existing service profile or updating service profile template.	No maintenance policy	After you update the firmware package, do one of the following: • To reboot and upgrade some or all servers simultaneously, add the firmware package to one or more service profiles that are associated with servers, or to an updating service profile template. • To reboot and upgrade one server at a time, do the following for each server: 1. Create a new service profile and include the firmware package in that service profile. 2. Disassociate the server from its service profile. 3. Associate the server with the new service profile. 4. After the server has been rebooted and the firmware upgraded, disassociate the server from the new service profile and associate it with its original service profile. **Caution** If the original service profile includes a scrub policy, disassociating a service profile may result in data loss when the disk or the BIOS is scrubbed upon association with the new service profile.
The firmware package is included in one or more service profiles, and the service profiles are associated with one or more servers. OR The firmware package is included in an updating service profile template, and the service profiles created from that template are associated with one or more servers.	No maintenance policy OR A maintenance policy configured for immediate updates.	The following occurs when you update the firmware package: 1. The changes to the firmware package take effect as soon as you save them. 2. Cisco UCS verifies the model numbers and vendor against all servers associated with service profiles that include this policy. If the model numbers and vendor match a firmware version in the policy, Cisco UCS reboots the servers and updates the firmware. All servers associated with service profiles that include the firmware package are rebooted at the same time.

Service Profile	Maintenance Policy	Upgrade Actions
The firmware package is included in one or more service profiles, and the service profiles are associated with one or more servers. OR The firmware package is included in an updating service profile template, and the service profiles created from that template are associated with one or more servers.	Configured for user acknowledgment	The following occurs when you update the firmware package: 1. Cisco UCS asks you to confirm your change and advises that a user-acknowledged reboot of the servers is required. 2. Click the flashing **Pending Activities** button to select the servers you want to reboot and to apply the new firmware. 3. Cisco UCS verifies the model numbers and vendor against all servers associated with service profiles that include this policy. If the model numbers and vendor match a firmware version in the policy, Cisco UCS reboots the server and updates the firmware. A manual reboot of the servers does not cause Cisco UCS to apply the firmware package, nor does it cancel the pending activities. You must acknowledge or cancel the pending activity through the **Pending Activities** button.
The firmware package is included in one or more service profiles, and the service profiles are associated with one or more servers. OR The firmware package is included in an updating service profile template, and the service profiles created from that template are associated with one or more servers.	Configured for user acknowledgment with **On Next Boot** option	The following occurs when you update the firmware package: 1. Cisco UCS asks you to confirm your change and advises that a user-acknowledged reboot of the servers is required. 2. To reboot and to apply the new firmware, do one of the following: • Click the flashing **Pending Activities** button to select the servers you want to reboot and apply the new firmware. • Manually reboot the servers. 3. Cisco UCS verifies the model numbers and vendor against all servers associated with service profiles that include this policy. If the model numbers and vendor match a firmware version in the policy, Cisco UCS reboots the server and updates the firmware. A manual reboot of the servers causes Cisco UCS to apply the firmware package. This is enabled by the **On Next Boot** option.

Service Profile	Maintenance Policy	Upgrade Actions
The firmware package is included in one or more service profiles, and the service profiles are associated with one or more servers. OR The firmware package is included in an updating service profile template, and the service profiles created from that template are associated with one or more servers.	Configured for changes to take effect during a specific maintenance window.	The following occurs when you update the firmware package: 1. Cisco UCS asks you to confirm your change and advises that a user-acknowledged reboot of the servers is required. 2. Click the flashing **Pending Activities** button to select the servers you want to reboot and to apply the new firmware. 3. Cisco UCS verifies the model numbers and vendor against all servers associated with service profiles that include this policy. If the model numbers and vendor match a firmware version in the policy, Cisco UCS reboots the server and updates the firmware. A manual reboot of the servers does not cause Cisco UCS to apply the firmware package, nor does it cancel the scheduled maintenance activities.

Creating a Host Firmware Package

Tip You can include more than one type of firmware in the same host firmware package. For example, a host firmware package can include both BIOS firmware and storage controller firmware or adapter firmware for two different models of adapters. However, you can only have one firmware version with the same type, vendor, and model number. The system recognizes which firmware version is required for an endpoint and ignores all other firmware versions.

You can also exclude firmware of specific components from a host firmware package when creating a new host firmware package.

Important Each host firmware package is associated with one list of excluded components, which is common across all firmware packages—Blade, and Rack. To configure a separate exclusion list for each type of firmware package, use separate host firmware packages.

Before you begin

Ensure that the appropriate firmware was downloaded to the fabric interconnect.

Procedure

Step 1 In the **Navigation** pane, click **Servers**.

Step 2 Expand **Servers** > **Policies**.

Step 3 Expand the node for the organization where you want to create the policy.

If the system does not include multi tenancy, expand the **root** node.

Step 4 Right-click **Host Firmware Packages** and choose **Create Package**.

Step 5 In the **Create Host Firmware Package** dialog box, enter a unique name and description for the package.

This name can be between 1 and 32 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.

Step 6 To configure the host firmware package by selecting servers and components, select the **Simple** radio button in the **How would you like to configure the Host Firmware Package** field.

Step 7 From each drop-down list, **Blade Package**, **Rack Package**, and **Service Pack**, select the firmware package.

The images from **Service Pack** will take precedence over the images from **Blade Package** or **Rack Package**.

Step 8 In the **Excluded Components** area, check the checkboxes corresponding to the components that you want to exclude from this host firmware package.

If you do not check any component checkboxes, all the listed components are included in the host firmware package.

Step 9 To configure the host firmware package with advanced options, select the **Advanced** radio button in the **How would you like to configure the Host Firmware Package** field.

Step 10 On each subtab, do the following for each type of firmware that you want to include in the package:

a) In the **Select** column, ensure that the check boxes for the appropriate lines are checked.

b) In the **Vendor**, **Model**, and **PID** columns, verify that the information matches the servers you want to update with this package.

The model and model number (PID) must match the servers that are associated with this firmware package. If you select the wrong model or model number, Cisco UCS Manager cannot install the firmware update.

c) In the **Version** column, choose the firmware version to which you want to update the firmware.

Note Starting with Cisco UCS Manager Release 4.2(3b), UCS Manager supports the firmware management for the following NVIDIA A Series GPUs with and without Crypto-Embedded Controller (CEC):

- Nvidia A10
- Nvidia A16
- Nvidia A30
- Nvidia A40
- Nvidia A100-80GB

Example: Combined version of CEC and non-CEC separated with delimiter—94.02.5C.00.03|G133.0200.00.05|5.01||94.02.5C.00.0F|G133.0200.00.05

Step 11 When you have added all the desired firmware to the package, click **OK**.

What to do next

Include the policy in a service profile and/or template.

Updating a Host Firmware Package

If the policy is included in one or more service profiles, which do not include maintenance policies, Cisco UCS Manager updates and activates the firmware in the server and adapter with the new versions. Cisco UCS Manager reboots the server as soon as you save the host firmware package policy unless you have configured and scheduled a maintenance window.

You can also exclude firmware of specific components from a host firmware package when modifying an existing host firmware package.

Important Each host firmware package is associated with one list of excluded components, which is common across all firmware packages—Blade, and Rack. To configure a separate exclusion list for each type of firmware package, use separate host firmware packages.

Before you begin

Ensure that the appropriate firmware was downloaded to the fabric interconnect.

Procedure

Step 1 In the **Navigation** pane, click **Servers**.

Step 2 Expand **Servers** > **Policies**.

Step 3 Expand the node for the organization that includes the policy you want to update.

If the system does not include multi tenancy, expand the **root** node.

Step 4 Expand **Host Firmware Packages** and choose the policy you want to update.

Step 5 In the **Work** pane, click the **General** tab.

Step 6 On each subtab, do the following for each type of firmware that you want to include in the package:

a) In the **Select** column, ensure that the check boxes for the appropriate lines are checked.

b) In the **Vendor**, **Model**, and **PID** columns, verify that the information matches the servers you want to update with this package.

The model and model number (PID) must match the servers that are associated with this firmware package. If you select the wrong model or model number, Cisco UCS Manager cannot install the firmware update.

c) In the **Version** column, choose the firmware version to which you want to update the firmware.

Note Starting with Cisco UCS Manager Release 4.2(3b), UCS Manager supports the firmware management for the following NVIDIA A Series GPUs with and without Crypto-Embedded Controller (CEC):

- Nvidia A10
- Nvidia A16
- Nvidia A30
- Nvidia A40
- Nvidia A100-80GB

Example: Combined version of CEC and non-CEC separated with delimiter—94.02.5C.00.03|G133.0200.00.05|5.01||94.02.5C.00.0F|G133.0200.00.05

Step 7 To modify the components in the host firmware package, click **Modify Package Versions**.

The **Modify Package Versions** window appears.

Step 8 To modify the blade package, from the **Blade Package** drop-down list, select the blade package version.

Step 9 To modify the rack package, from the **Rack Package** drop-down list, select the rack package version.

Step 10 To modify the service pack, from the **Service Pack** drop-down list, select the service pack version.

To remove the service pack, select **<not set>**.

Step 11 In the **Excluded Components** area, check the checkboxes corresponding to the components that you want to exclude from this host firmware package.

If you do not check any component checkboxes, all the listed components are included in the host firmware package.

Step 12 Click **OK**.

Cisco UCS Manager verifies the model numbers and vendor against all servers associated with service profiles that include this policy. If the model numbers and vendor match a firmware version in the policy, Cisco UCS Manager updates the firmware according to the settings in the maintenance policies included in the service profiles.

Adding Firmware Packages to an Existing Service Profile

If the service profile does not include a maintenance policy and is associated with a server, Cisco UCS Manager updates and activates the firmware in the server with the new versions and reboots the server as soon as you save the changes to the service profile.

Procedure

Step 1 In the **Navigation** pane, click **Servers**.

Step 2 Expand **Servers** > **Service Profiles**.

Step 3 Expand the node for the organization that includes the service profile that you want to update.

If the system does not include multi tenancy, expand the **root** node.

Step 4 Click the service profile to which you want to add the firmware packages.

Step 5 In the **Work** pane, click the **Policies** tab.

Step 6 Click the down arrows to expand the **Firmware Policies** section.

Step 7 To add a host firmware package, select the desired policy from the **Host Firmware** drop-down list.

Step 8 Click **Save Changes**.

Firmware Automatic Synchronization

You can use the **Firmware Auto Sync Server policy** in Cisco UCS Manager to determine whether firmware versions on recently discovered servers must be upgraded or not. With this policy, you can upgrade the firmware versions of recently discovered unassociated servers to match the firmware version defined in the default host firmware pack. In addition, you can determine if the firmware upgrade process should run immediately after the server is discovered, or run at a later time.

Important The firmware automatic synchronization is dependent on the default host firmware pack. If you delete the default host firmware pack, a major fault is raised in Cisco UCS Manager. If you have configured a default host firmware pack, but not specified or configured a blade or rack server firmware in it, then a minor fault is raised. Irrespective of the severity of the fault raised, you must resolve these faults prior to setting the **Firmware Auto Sync Server policy**.

Note You cannot use the **Firmware Auto Sync Server policy** in the server that is part of a server pool.

Following are the values for the **Firmware Auto Sync Server policy**:

- **No Action**—No firmware upgrade is initiated on the server.

  This value is selected by default.

- **User Acknowledge**—Firmware on the server is not synchronized until the administrator acknowledges the upgrade in the **Pending Activities** dialog box.

You can set this policy either from the Cisco UCS Manager GUI or Cisco UCS Manager CLI. The firmware for a server is automatically triggered when the following conditions occur:

- The firmware version on a server or the endpoint on a server differs from the firmware version configured in the default host firmware pack.
- The value for the **Firmware Auto Sync Server policy** has been modified. For example, if you had initially set it as **User Ack** and you change it to **No Action**.

Important If Cisco UCS Manager is registered as a Cisco UCS domain with Cisco UCS Central, then this policy runs as a local policy. If the default host firmware pack is not defined in or is deleted from Cisco UCS Manager, then this policy will not run.

Setting the Firmware Auto-Sync Server Policy

Use this policy to determine when and how the firmware version of a recently discovered unassociated server must be updated.

If the firmware version of a specific endpoint of a server differs from the version in the default host firmware pack, the FSM state in Cisco UCS Manager displays the update status for that specific endpoint only. The firmware version of the server is not updated.

Before you begin

- You should have created a default host firmware pack prior to setting this policy.
- You should have logged in as an administrator to complete this task.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Click the **Equipment** node.

Step 3 In the **Work** pane, click the **Policies** tab.

Step 4 Click the **Global Policies** subtab.

Step 5 In the **Firmware Auto Sync Server Policy** area, select one of the following values as the **Sync State**:

- **No Action**—No firmware upgrade is initiated on the server.
- **User Acknowledge**—Firmware on the server is not synchronized until the administrator acknowledges the upgrade in the **Pending Activities** dialog box.

  This option is selected by default.

Step 6 Click **Save Changes**.

Direct Firmware Upgrade at Endpoints

If you follow the correct procedure and apply the upgrades in the correct order, a direct firmware upgrade and the activation of the new firmware version on the endpoints is minimally disruptive to traffic in a Cisco UCS domain. Recommended Process for Directly Upgrading Infrastructure Firmware at Endpoints, on page 37, details the process that Cisco recommends for upgrading infrastructure firmware on endpoints.

You can directly upgrade the firmware on the following components:

Infrastructure	UCS 5108 Chassis	UCS Rack Server	Cisco UCS S3260 Chassis

• Cisco UCS Manager
• Fabric interconnects
 	
Ensure that you upgrade Cisco UCS Manager first and then the fabric interconnects.
	• I/O modules
	• Power supply unit
	• Server:
	  • Adapter
	  • CIMC
	  • BIOS
	  • Storage controller
	  • Board controller
		• Adapter
		• CIMC
		• BIOS
		• Storage controller
		• Board controller
			• CMC
			• Chassis adapter
			• SAS expander
			• Chassis board controller
			• Server:
			  • CIMC
			  • BIOS
			  • Board controller
			  • Storage controller

For the Cisco UCS S3260 chassis, you can upgrade the CMC, chassis adapter, chassis board controller, SAS expander, and local disk firmware through the chassis firmware package in the chassis profile. *Cisco UCS S3260 Server Integration with Cisco UCS Manager, Release 4.0* provides detailed information about chassis profiles and chassis firmware packages.

You can upgrade the adapter, board controller, CIMC, and BIOS firmware through the host firmware package in the service profile. If you use a host firmware package to upgrade this firmware, you can reduce the number of times a server needs to be rebooted during the firmware upgrade process.

Important All server components must be kept at the same release level. These components are tested together for each release and a version mismatch may cause unpredictable system operation.

Stages of a Direct Firmware Upgrade

Cisco UCS Manager separates the direct upgrade process into two stages, ensuring that you can push the firmware to an endpoint while the system is running without affecting uptime on the server or other endpoints.

Update

During this stage, the system copies the selected firmware version from the primary fabric interconnect to the backup partition in the endpoint and verifies that the firmware image is not corrupt. The update process always overwrites the firmware in the backup slot.

The update stage applies only to the following endpoints in a UCS 5108 chassis:

- Adapters
- CIMCs
- I/O modules

On a Cisco UCS S3260 dense storage rack server chassis, the update stage applies only to the following endpoints:

- Chassis Management Controller (CMC)
- Shared adapter
- SAS expander
- Server:
  - BIOS
  - CIMC
  - Adapter

Caution Do not remove the hardware that contains the endpoint or perform any maintenance on it until the update process completes. If the hardware is removed or otherwise unavailable due to maintenance, the firmware update fails. This failure might corrupt the backup partition. You cannot update the firmware on an endpoint with a corrupted backup partition.

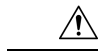
Activate

During this stage, the system sets the specified image version (normally the backup version) as the startup version and, if you do not specify **Set Startup Version Only**, immediately reboots the endpoint. When the endpoint is rebooted, the backup partition becomes the active partition, and the active partition becomes the backup partition. The firmware in the new active partition becomes the startup version and the running version.

The following endpoints only require activation because the specified firmware image already exists on the endpoint:

- Cisco UCS Manager
- Fabric interconnects
- Board controllers on those servers that support them
- On a Cisco UCS S3260 dense storage rack server chassis:
  - CMC
  - Shared adapter
  - Board controllers for chassis and server
  - SAS expander
  - Storage controller
  - BIOS
  - CIMC

When the firmware is activated, the endpoint is rebooted and the new firmware becomes the active kernel version and system version. If the endpoint cannot boot from the startup firmware, it defaults to the backup version and raises a fault.



Caution When you configure **Set Startup Version Only** for an I/O module, the I/O module is rebooted when the fabric interconnect in its data path is rebooted. If you do not configure **Set Startup Version Only** for an I/O module, the I/O module reboots and disrupts traffic. In addition, if Cisco UCS Manager detects a protocol and firmware version mismatch between the fabric interconnect and the I/O module, Cisco UCS Manager automatically updates the I/O module with the firmware version that matches the firmware in the fabric interconnect, and then activates the firmware and reboots the I/O module again.

Outage Impacts of Direct Firmware Upgrades

When you perform a direct firmware upgrade on an endpoint, you can disrupt traffic or cause an outage in one or more of the endpoints in the Cisco UCS domain.

Outage Impact of a Fabric Interconnect Firmware Upgrade

When you upgrade the firmware for a fabric interconnect, you cause the following outage impacts and disruptions:

- The fabric interconnect reboots.
- The corresponding I/O modules reboot.

Outage Impact of a Cisco UCS Manager Firmware Upgrade

A firmware upgrade to Cisco UCS Manager causes the following disruptions:

- Cisco UCS Manager GUI—All users logged in to Cisco UCS Manager GUI are logged out and their sessions ended.

  Any unsaved work in progress is lost.

- Cisco UCS Manager CLI—All users logged in through telnet are logged out and their sessions ended.

Outage Impact of an I/O Module Firmware Upgrade

When you upgrade the firmware for an I/O module, you cause the following outage impacts and disruptions:

- For a non-cluster configuration with a single fabric interconnect, data traffic is disrupted when the I/O module reboots. For a cluster configuration with two fabric interconnects, data traffic fails over to the other I/O module and the fabric interconnect in its data path.
- If you activate the new firmware as the startup version only, the I/O module reboots when the corresponding fabric interconnect is rebooted.
- If you activate the new firmware as the running and startup version, the I/O module reboots immediately.
- An I/O module can take up to 10 minutes to become available after a firmware upgrade.

Outage Impact of a CIMC Firmware Upgrade

When you upgrade the firmware for a CIMC in a server, you impact only the CIMC and internal processes. You do not interrupt server traffic. This firmware upgrade causes the following outage impacts and disruptions to the CIMC:

- Any activities being performed on the server through the KVM console and vMedia are interrupted.
- Any monitoring or IPMI polling is interrupted.

Outage Impact of an Adapter Firmware Upgrade

If you activate the firmware for an adapter and do not configure the **Set Startup Version Only** option, you cause the following outage impacts and disruptions:

- The server reboots.
- Server traffic is disrupted.

Recommended Process for Directly Upgrading Infrastructure Firmware at Endpoints

Cisco recommends the following process for directly upgrading infrastructure firmware at endpoints:

1. Stage the software and prepare for upgrade:
   a. Create All Configuration and Full-State backup files. Creating an All Configuration Backup File, and Creating a Full State Backup File, provide detailed information.
   b. Download firmware packages. Downloading Firmware Images to the Fabric Interconnect from a Remote Location, on page 5, and Downloading Firmware Images to the Fabric Interconnect from the Local File System, on page 7, provide detailed information.
   c. Disable Smart Call Home. Disabling Smart Call Home, provides detailed information.
2. Activate Cisco UCS Manager software. Activating the Cisco UCS Manager Software, on page 40, provides detailed information. You can also click **Play** on this video (http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/activate_ucsm.html) to watch how to activate Cisco UCS Manager software.
3. Update IOM firmware. Updating the Firmware on an IOM and IFM (IOM for Cisco UCS X-Series Servers), on page 43, provides detailed information. You can also click **Play** on this video (http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/update_and_activate_iom.html) to watch how to update IOM firmware.
4. Prepare for fabric upgrade:
   a. Verify UCS Manager faults and resolve the service -impacting faults. Viewing UCS Manager Faults, provides detailed information.
   b. Verify High Availability status and identify the secondary fabric interconnect. Verifying the High Availability Status and Roles of a Cluster Configuration, provides detailed information.
   c. Configure the default maintenance policy. Configuring the Default Maintenance Policy, provides detailed information. You can also click **Play** on this video (http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/configure_the_default_maintenance_policy.html) to watch how to configure the default maintenance policy as **User Ack**.
   d. Verify that VLAN and FCOE IDs do not overlap.
   e. Disable the management interface. Disabling the Management Interface, provides detailed information.

f. Activate IOM firmware. Activating the Firmware on an IOM and IFM (IOM for Cisco UCS X-Series Servers), on page 45, provides detailed information. You can also click **Play** on this video (http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/update_and_activate_iom.html) to watch how to activate IOM firmware.

5. Activate the subordinate fabric interconnect

   a. Evacuate subordinate fabric interconnect traffic. Configuring Fabric Interconnect Traffic Evacuation, provides detailed information. You can also click **Play** on this video (http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/enable_and_disable_fi_traffic_evacuation.html) to watch how to evacuate fabric interconnect traffic.

   b. Activate the subordinate fabric interconnect (FI-B) and monitor FSM. Activating the Firmware on a Subordinate Fabric Interconnect, on page 45, provides detailed information. You can also click **Play** on this video (http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/activate_the_firmware_on_a_subordinate_fabric_interconnect.html) to watch how to activate the firmware on the subordinate fabric interconnect.

   c. Verify that all paths are working. Verification that the Data Path is Ready, provides detailed information.

   d. Disable subordinate fabric interconnect traffic evacuation. Configuring Fabric Interconnect Traffic Evacuation, provides detailed information. You can also click **Play** on this video (http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/enable_and_disable_fi_traffic_evacuation.html) to watch how to disable traffic evacuation on a fabric interconnect.

   e. Verify new faults. Viewing Faults Generated During the Upgrade of a Fabric Interconnect.

6. Activate the primary fabric interconnect (FI-A)

   a. Migrate management services from the primary fabric interconnect to the secondary fabric interconnect, and change the cluster lead to the secondary fabric interconnect. Switching Over Fabric Interconnect Cluster Lead, on page 48, provides detailed information. You can also click **Play** on this video (http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/switch_over_fabric_interconnect_cluster_lead.html) to watch how to switch over the cluster lead from one fabric interconnect to another.

   b. Evacuate primary fabric interconnect traffic.

   c. Activate the primary fabric interconnect (FI-A) and monitor FSM. Activating the Firmware on a Primary Fabric Interconnect, on page 46, provides detailed information. You can also click **Play** on this video (http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/activate_the_firmware_on_a_primary_fabric_interconnect.html) to watch how to activate the firmware on a primary fabric interconnect.

   d. Verify that all paths are working.

   e. Disable primary fabric interconnect traffic evacuation.

   f. Verify new faults.

Updating the Firmware on Multiple Endpoints

You can use this procedure to update the firmware on chassis and server endpoints. Server endpoints that are part of the associated host firmware pack cannot be updated by using this procedure, and will display an error.

To update these server components using this procedure, ensure that you exclude them from the assigned host firmware pack.

Caution Do not remove the hardware that contains the endpoint or perform any maintenance on it until the update process completes. If the hardware is removed or otherwise unavailable due to maintenance, the firmware update fails. This failure might corrupt the backup partition. You cannot update the firmware on an endpoint with a corrupted backup partition.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Click the **Equipment** node.

Step 3 In the **Work** pane, click the **Firmware Management** tab.

Step 4 On the **Installed Firmware** tab, click **Update Firmware**.

Cisco UCS Manager GUI opens the **Update Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS domain. This step might take a few minutes, based on the number of chassis and servers.

Step 5 In the **Update Firmware** dialog box, do the following:

a) From the **Filter** drop-down list on the menu bar, select **ALL**.

If you want to update all endpoint firmware of a specific type, such as all adapters or server BIOS, select that type from the drop-down list.

b) In the **Select** field, do one of the following:

- To activate all endpoints to the same version, click the **Version** radio button and select the appropriate version from the **Set Version** drop-down list.
- To activate all endpoints to the firmware version included in a specific bundle, click the **Bundle** radio button and select the appropriate bundle from the **Set Bundle** drop-down list .

c) Click **OK**.

If one or more endpoints cannot be directly updated, Cisco UCS Manager displays a notification message. After you acknowledge the notification message, Cisco UCS Manager updates the firmware for all other endpoints on servers that can be directly updated.

Cisco UCS Manager copies the selected firmware image to the backup memory partition and verifies that the image is not corrupt. The image remains as the backup version until you activate it. Cisco UCS Manager begins all updates at the same time. However, some updates might complete at different times.

The update is complete when the **Update Firmware** dialog box displays **ready** in the **Update Status** column for all updated endpoints.

Step 6 (Optional) To monitor the progress of the update to a specific endpoint, right-click the endpoint and choose **Show Navigator**.

Cisco UCS Manager displays the progress in the **Update Status** area on the **General** tab. If the navigator has an **FSM** tab, you can also monitor the progress there. An entry in the **Retry #** field might not indicate that

the update failed. The retry count also includes retries that occur when Cisco UCS Manager retrieves the update status.

What to do next

Activate the firmware.

Cisco UCS Manager Firmware

Consider the following guidelines and best practices while activating firmware on the Cisco UCS Manager software:

- In a cluster configuration, Cisco UCS Manager on both fabric interconnects must run the same version.
- Cisco UCS Manager activation brings down management for a brief period. All virtual shell (VSH) connections are disconnected.
- In a cluster configuration, Cisco UCS Manager on both fabric interconnects is activated.
- A Cisco UCS Manager update does not affect server application I/O because fabric interconnects do not need to be reset.
- If Cisco UCS Manager is updated while the subordinate fabric interconnect is down, the subordinate fabric interconnect is automatically updated when it comes back up.

Upgrade Validation

Cisco UCS Manager validates the upgrade or downgrade process and displays all firmware upgrade validation failures, such as deprecated hardware, in the **Upgrade Validation** tab. If there are upgrade validation failures, the upgrade fails, and Cisco UCS Manager rolls back to the earlier version. You must resolve these faults and then use the **Force** option to continue with the upgrade.

For example, because M1 and M2 blade servers are not supported on Release 3.1(1), if you have M1 or M2 blade servers in the configuration when upgrading from Release 2.2(x) to Release 3.1(1), these will be reported as validation faults in the **Upgrade Validation** tab, and the upgrade will fail.

If you do not want Cisco UCS Manager to validate the upgrade or downgrade process, check the **Skip Validation** check box.

Activating the Cisco UCS Manager Software

You can use the steps detailed here, or click **Play** on this video (http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/activate_ucsm.html) to watch how to activate Cisco UCS Manager software.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Click the **Equipment** node.

Step 3 In the **Work** pane, click the **Firmware Management** tab.

Step 4 On the **Installed Firmware** tab, click **Activate Firmware**.

Cisco UCS Manager GUI opens the **Activate Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS domain. This step might take a few minutes, based on the number of chassis and servers.

Step 5 On the **UCS Manager** row of the **Activate Firmware** dialog box, do the following:

a) From the drop-down list in the **Startup Version** column, select the version to which you want to update the software.

b) Click **OK**.

Cisco UCS Manager disconnects all active sessions, logs out all users, and activates the software. When the upgrade is complete, you are prompted to log back in. If you are prompted to re-login immediately after being disconnected, the login will fail. You must wait until the activation of Cisco UCS Manager is completed, which takes a few minutes.

Cisco UCS Manager makes the selected version the startup version and schedules the activation to occur when the fabric interconnects are upgraded.

Activating a Service Pack for the Cisco UCS Manager Software

You can use the steps detailed here to activate a service pack for the Cisco UCS Manager software. This process will not involve upgrading or rebooting the fabric interconnects.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Click the **Equipment** node.

Step 3 In the **Work** pane, click the **Firmware Management** tab.

Step 4 On the **Installed Firmware** tab, click **Activate Firmware**.

Cisco UCS Manager GUI opens the **Activate Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS domain. This step might take a few minutes, based on the number of chassis and servers.

Step 5 From the **Filter** drop-down list on the menu bar, choose **UCS Manager**.

Step 6 On the **UCS Manager** row of the **Activate Firmware** dialog box, do the following:

a) In the **UCS Manager Service Pack** row, choose the service pack version to which you want to upgrade from the drop-down list in the **Startup Version** column.

b) Click **OK**.

Cisco UCS Manager disconnects all active sessions, logs out all users, and activates the software. When the upgrade is complete, you are prompted to log back in. If you are prompted to re-login immediately after being disconnected, the login will fail. You must wait until the activation of Cisco UCS Manager is completed, which takes a few minutes.

Removing a Service Pack from the Cisco UCS Manager Software

You can use the steps detailed here to remove a service pack from the Cisco UCS Manager software.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Click the **Equipment** node.

Step 3 In the **Work** pane, click the **Firmware Management** tab.

Step 4 On the **Installed Firmware** tab, click **Activate Firmware**.

Cisco UCS Manager GUI opens the **Activate Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS domain. This step might take a few minutes, based on the number of chassis and servers.

Step 5 From the **Filter** drop-down list on the menu bar, choose **UCS Manager**.

Step 6 In the **UCS Manager Service Pack** row of the **Activate Firmware** dialog box, choose **<not set>** as the service pack version from the drop-down list in the **Startup Version** column.

Step 7 Click **OK**.

IOM and IFM (IOM for Cisco UCS X-Series Servers) Firmware

Beginning with release 4.3(2a), Cisco UCS Manager supports Cisco UCS X9508 server chassis with Cisco UCS X-Series servers. Cisco UCS X-Series servers support Intelligent Fabric Modules (IFM), which function similarly to the Input/Output Module (IOM) in Cisco UCS B-Series servers. This guide uses the term IOM to refer both IOM and IFM.

Cisco UCS I/O modules (IOMs) bring the unified fabric into the blade server enclosure, thus providing multiple 10 Gigabit Ethernet connections between blade servers and the fabric interconnect, simplifying diagnostics, cabling, and management. IOMs extend the I/O fabric between the fabric interconnects and blade server chassis, and enable a lossless and deterministic Fibre Channel over Ethernet (FCoE) fabric to connect all blades and chassis together.

Because the IOM is similar to a distributed line card, it does not perform any switching, and is managed as an extension of the fabric interconnects. This approach removes switching from the chassis, reducing overall infrastructure complexity, and enables Cisco UCS to scale to many chassis without multiplying the number of switches needed. It allows all chassis to be managed as a single, highly available management domain.

The IOM also manages the chassis environment, which includes the power supply, fans, and blades, along with the fabric interconnect. Therefore, separate chassis management modules are not required. It fits into the back of the blade server chassis. Each blade chassis can support up to two IOMs, thus allowing increased capacity and redundancy.

Guidelines for Updating and Activating IOM Firmware

Consider the following guidelines and best practices while updating and activating firmware on IOMs:

- Each IOM stores two images—a running image and a backup image.
- The update operation replaces the backup image of an IOM with the new firmware version.
- The activate operation demotes the current startup image to a backup image. A new startup image is put in its place, and the system is configured to boot from this backup image.

- Check the **Set Startup Version Only** checkbox to set only the active image; a reset does not occur. This process can be used to upgrade multiple IOMs and then simultaneously reset them. If the fabric interconnect is updated and then activated, the fabric interconnect reboots the corresponding IOM and reduces the downtime.
- The IOM and fabric interconnect must be compatible with each other.
- If the software that runs on the fabric interconnect detects an IOM that runs an incompatible version, it performs an automatic update of the IOM to bring it to the same version as the fabric interconnect system software.

  Cisco UCS Manager raises a fault to indicate this situation. Additionally, the discovery state of IOM displays **Auto updating** while the automatic update is in progress.
- Cisco UCS Manager enables you to view the IOM firmware at the chassis level on the **Installed Firmware** tab.

You can use the steps detailed in the following sections, or click **Play** on this video (http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/update_and_activate_iom.html) to watch how to update and activate IOM firmware.

Updating the Firmware on an IOM and IFM (IOM for Cisco UCS X-Series Servers)

Caution Do not remove the hardware that contains the endpoint or perform any maintenance on it until the update process completes. If the hardware is removed or otherwise unavailable due to maintenance, the firmware update fails. This failure might corrupt the backup partition. You cannot update the firmware on an endpoint with a corrupted backup partition.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Chassis** > *Chassis Number* > **IO Modules**.

Step 3 Click the I/O module that you want to update.

Step 4 In the **General** tab, click **Update Firmware**.

Step 5 In the **Update Firmware** dialog box, do the following:

a) From the **Version** drop-down list, select the firmware version to update the endpoint.
b) Click **OK**.

Cisco UCS Manager copies the selected firmware package to the backup memory slot, where it remains until you activate it.

Step 6 (Optional) Monitor the status of the update in the **Update Status** area.

The update process can take several minutes. Do not activate the firmware until the selected firmware package displays in the **Backup Version** field in the **Firmware** area of the **General** tab.

What to do next

Activate the firmware.

Activating the Firmware on Multiple IOMs

This procedure ensures that the firmware activation for these endpoints causes minimal disruption to data traffic. If you do not activate the endpoints in the following order with the correct options configured, the endpoints may reboot and cause a temporary disruption in data traffic.

Caution Do not select **ALL** from the **Filter** drop-down list in the **Activate Firmware** dialog box to activate all endpoints simultaneously. Many firmware releases and patches have dependencies that require the endpoints to be activated in a specific order for the firmware update to succeed. This order can change depending upon the contents of the release or patch. Activating all endpoints does not guarantee that the updates occur in the required order and can disrupt communications between the endpoints, the fabric interconnects, and Cisco UCS Manager. For information about the dependencies in a specific release or patch, see the release notes provided with that release or patch.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Click the **Equipment** node.

Step 3 In the **Work** pane, click the **Firmware Management** tab.

Step 4 In the **Installed Firmware** tab, choose **Activate Firmware**.

If one or more of the selected endpoints are not configured with the required version as the backup version, that version does not display in the **Set Version** drop-down list. You must select the version from the **Startup Version** column for each individual endpoint.

Step 5 To activate the IOM firmware, do the following in the **Activate Firmware** dialog box:

a) From the **Filter** drop-down list, choose **IO Modules**.

b) From the **Set Version** drop-down list, choose the version for the current 2.0 release.

c) Check the **Ignore Compatibility Check** check box.

d) Check the **Set Startup Version Only** check box.

Important When you configure **Set Startup Version Only** for an I/O module, the I/O module is rebooted when the fabric interconnect in its data path is rebooted. If you do not configure **Set Startup Version Only** for an I/O module, the I/O module reboots and disrupts traffic. In addition, if Cisco UCS Manager detects a protocol and firmware version mismatch between the fabric interconnect and the I/O module, Cisco UCS Manager automatically updates the I/O module with the firmware version that matches the firmware in the fabric interconnect, and then activates the firmware and reboots the I/O module again.

e) Click **Apply**.

When the **Activate Status** column for all IOMs displays **pending-next-boot**, continue with Step 6.

Step 6 Click **OK**.

Activating the Firmware on an IOM and IFM (IOM for Cisco UCS X-Series Servers)

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Chassis** > *Chassis Number* > **IO Modules**.

Step 3 Select the **IO Module** node that includes the I/O module for which you want to activate the updated firmware.

Step 4 In the **General** tab, click **Activate Firmware**.

Step 5 In the **Activate Firmware** dialog box, do the following:

a) Select the appropriate version from the **Version To Be Activated** drop-down list.

If one or more of the selected endpoints are not configured with the required version as the backup version, that version does not display in the **Set Version** drop-down list. You must select the version from the **Startup Version** column for each individual endpoint.

b) If you want to set the startup version and not change the version running on the endpoint, check the **Set Startup Version Only** check box.

If you configure **Set Startup Version Only**, the activated firmware moves to the pending-next-reboot state and the endpoint is not immediately rebooted. The activated firmware does not become the running version of firmware until the endpoint reboots.

c) Click **OK**.

Fabric Interconnect Firmware

Activating the Firmware on a Subordinate Fabric Interconnect

You can use the steps detailed here, or click **Play** on this video (http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/activate_the_firmware_on_a_subordinate_fabric_interconnect.html) to watch how to activate the firmware on a subordinate fabric interconnect.

Before you begin

Determine which fabric interconnect in the cluster is the subordinate fabric interconnect.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Click the **Equipment** node.

Step 3 In the **Work** pane, click the **Firmware Management** tab.

Step 4 On the **Installed Firmware** tab, click **Activate Firmware**.

Cisco UCS Manager GUI opens the **Activate Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS domain. This step might take a few minutes, based on the number of chassis and servers.

Step 5 From the **Filter** drop-down list on the menu bar, choose **Fabric Interconnects**.

Step 6 On the row of the **Activate Firmware** dialog box for the subordinate fabric interconnect, do the following:

a) In the **Kernel** row, choose the firmware version to which you want to upgrade from the drop-down list in the **Startup Version** column.

b) In the **System** row, choose the firmware version to which you want to upgrade from the drop-down list in the **Startup Version** column.

Step 7 Click **Apply**.

Cisco UCS Manager updates and activates the firmware and reboots the fabric interconnect and any I/O module in the data path to that fabric interconnect, disrupting data traffic to and from that fabric interconnect. However, assuming the Cisco UCS domain is configured to permit traffic and port failover, data traffic fails over to the primary fabric interconnect and is not disrupted.

Step 8 Verify the high availability status of the subordinate fabric interconnect.

If the **High Availability Details** area for the fabric interconnect does not show the following values, contact Cisco Technical Support immediately. Do not continue to update the primary fabric interconnect.

Field Name	Required Value
Ready field	**Yes**
State field	**Up**

What to do next

If the high availability status of the subordinate fabric interconnect contains the required values, update and activate the primary fabric interconnect.

Activating the Firmware on a Primary Fabric Interconnect

This procedure continues directly from Activating the Firmware on a Subordinate Fabric Interconnect, on page 45, and assumes you are on the **Firmware Management** tab. You can use the steps detailed here, or click **Play** on this video (http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/activate_the_firmware_on_a_primary_fabric_interconnect.html) to watch how to activate the firmware on a primary fabric interconnect.

Before you begin

Activate the subordinate fabric interconnect.

Procedure

Step 1 On the **Installed Firmware** tab, click **Activate Firmware**.

Cisco UCS Manager GUI opens the **Activate Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS domain. This step might take a few minutes, based on the number of chassis and servers.

Step 2 From the **Filter** drop-down list on the menu bar, choose **Fabric Interconnects**.

Step 3 On the row of the **Activate Firmware** dialog box for the subordinate fabric interconnect, do the following:

a) In the **Kernel** row, choose the firmware version to which you want to upgrade from the drop-down list in the **Startup Version** column.

b) In the **System** row, choose the firmware version to which you want to upgrade from the drop-down list in the **Startup Version** column.

Step 4 Click **Apply**.

Cisco UCS Manager updates and activates the firmware and reboots the fabric interconnect and any I/O module in the data path to that fabric interconnect, disrupting data traffic to and from that fabric interconnect. However, assuming the Cisco UCS domain is configured to permit traffic and port failover, data traffic fails over to the other fabric interconnect, which becomes the primary. When it comes back up, this fabric interconnect is the subordinate fabric interconnect.

Step 5 Verify the high availability status of the fabric interconnect.

If the **High Availability Details** area for the fabric interconnect does not show the following values, contact Cisco Technical Support immediately.

Field Name	Required Value
Ready field	**Yes**
State field	**Up**

Activating the Firmware on a Non-cluster Fabric Interconnect

For a non-cluster configuration with a single fabric interconnect, you can minimize the disruption to data traffic when you perform a direct firmware upgrade of the endpoints. However, you must reboot the fabric interconnect to complete the upgrade and, therefore, cannot avoid disrupting traffic.

Tip If you ever need to recover the password to the admin account that was created when you configured the fabric interconnects for the Cisco UCS domain, you must know the running kernel version and the running system version. If you do not plan to create additional accounts, Cisco recommends that you save the path to these firmware versions in a text file so that you can access them if required.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Click the **Equipment** node.

Step 3 Expand the **Fabric Interconnects** node and click the non-cluster fabric interconnect.

Step 4 On the **General** tab, click **Activate Firmware**.

Step 5 In the **Activate Firmware** dialog box, complete the following fields:

Name	Description
Kernel Version drop-down list	Choose the version that you want to use for the kernel.
Force check box	If checked, Cisco UCS attempts the installation even if a previous attempt to install the selected version failed or was interrupted.
System Version drop-down list	Choose the version you want to use for the system.
Force check box	If checked, Cisco UCS attempts the installation even if a previous attempt to install the selected version failed or was interrupted.
Service Pack Version drop-down list	Choose the service pack version that you want to apply. **Note** A service pack can be applied only on its base maintenance release. For example, service pack 3.1(3)SP2 can be applied only on a 3.1(3) release. It cannot be applied on a 3.1(4) release. Setting **Service Pack** to **<not set>** removes the service pack from the fabric interconnect.

Step 6 Click **OK**.

Cisco UCS Manager activates the firmware and reboots the fabric interconnect and any I/O module in the data path to that fabric interconnect. For a non-cluster fabric interconnect, this disrupts all data traffic in the Cisco UCS domain.

Switching Over Fabric Interconnect Cluster Lead

This operation can only be performed in the Cisco UCS Manager CLI. You can use the steps detailed here, or click **Play** on this video (http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/switch_over_fabric_interconnect_cluster_lead.html) to watch how to switch over the cluster lead from one fabric interconnect to another.

Important During a cluster failover, the virtual IP address will be unreachable until a new primary fabric interconnect is elected.

Procedure

	Command or Action	Purpose
Step 1	(Optional) UCS-A# **show cluster state**	Displays the state of fabric interconnects in the cluster and whether the cluster is HA ready.
Step 2	UCS-A# **connect local-mgmt**	Enters local management mode for the cluster.
Step 3	UCS-A (local-mgmt) # **cluster** {**force primary** | **lead** {**a** | **b**}}	Changes the subordinate fabric interconnect to primary using one of the following commands:

	Command or Action	Purpose
		force Forces local fabric interconnect to become the primary. **lead** Makes the specified subordinate fabric interconnect the primary.

Example

The following example changes fabric interconnect B from subordinate to primary:

```
UCS-A# show cluster state
Cluster Id: 0xfc436fa8b88511e0-0xa370000573cb6c04

A: UP, PRIMARY
B: UP, SUBORDINATE

HA READY
UCS-A# connect local-mgmt
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2011, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

UCS-A(local-mgmt)# cluster lead b
UCS-A(local-mgmt)#
```

Activating a Service Pack on a Fabric Interconnect

You can use the steps detailed here to activate a service pack on a fabric interconnect.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Click the **Equipment** node.

Step 3 In the **Work** pane, click the **Firmware Management** tab.

Step 4 On the **Installed Firmware** tab, click **Activate Firmware**.

Cisco UCS Manager GUI opens the **Activate Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS domain. This step might take a few minutes, based on the number of chassis and servers.

Step 5 From the **Filter** drop-down list on the menu bar, choose **Fabric Interconnects**.

Step 6 In the **Service Pack** row of the **Activate Firmware** dialog box for the fabric interconnect, choose the service pack version to which you want to upgrade from the drop-down list in the **Startup Version** column.

Step 7 Click **OK**.

Cisco UCS Manager activates the firmware. In some cases, Cisco UCS Manager reboots the fabric interconnect, disrupting data traffic to and from that fabric interconnect.

Removing a Service Pack from a Fabric Interconnect

You can use the steps detailed here to remove a service pack from a fabric interconnect.

In some specific scenarios, such as Open SLL, removal of the service pack will lead to FI rebooting.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Click the **Equipment** node.

Step 3 In the **Work** pane, click the **Firmware Management** tab.

Step 4 On the **Installed Firmware** tab, click **Activate Firmware**.

Cisco UCS Manager GUI opens the **Activate Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS domain. This step might take a few minutes, based on the number of chassis and servers.

Step 5 From the **Filter** drop-down list on the menu bar, choose **Fabric Interconnects**.

Step 6 In the **Service Pack** row of the **Activate Firmware** dialog box for the fabric interconnect, choose **<not set>** as the service pack version from the drop-down list in the **Startup Version** column.

Step 7 Click **OK**.

Adapter Firmware

The Cisco Unified Computing System supports a broad set of converged network adapters (CNAs). CNAs eliminate the need for multiple network interface cards (NICs) and host bus adapters (HBAs) by converging LAN and SAN traffic in a single interface.

All Cisco UCS network adapters:

- Allow for the reduction of the number of required network interface cards and host bus adapters
- Are managed using Cisco UCS Manager software
- Can be used in a redundant configuration with two fabric extenders and two fabric interconnects
- Enable a "wire-once" architecture that allows cabling to be configured once, with features enabled and configured using software
- Support fibre channel multipathing

The Cisco Virtual Interface Card (VIC) delivers 256 virtual interfaces and supports Cisco VM-FEX technology. The Cisco VIC provides I/O policy coherency and visibility to enable true workload mobility in virtualized environments. The Cisco VIC is available in form factors for B-Series blade servers, and C-Series rack servers.

Updating the Firmware on an Adapter

Caution Do not remove the hardware that contains the endpoint or perform any maintenance on it until the update process completes. If the hardware is removed or otherwise unavailable due to maintenance, the firmware update fails. This failure might corrupt the backup partition. You cannot update the firmware on an endpoint with a corrupted backup partition.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Chassis** > ***Chassis Number*** > **Servers**.

Step 3 Expand the node for the server that includes the adapter you want to update.

Step 4 Expand **Adapters** and select the adapter you want to upgrade.

Step 5 In the **General** tab, click **Update Firmware**.

Step 6 In the **Update Firmware** dialog box, do the following:

a) From the **Version** drop-down list, select the firmware version to update the endpoint.

b) Click **OK**.

If one or more endpoints cannot be directly updated, Cisco UCS Manager displays a notification message. After you acknowledge the notification message, Cisco UCS Manager updates the firmware for all other endpoints on servers that can be directly updated.

Cisco UCS Manager copies the selected firmware package to the backup memory slot, where it remains until you activate it.

Step 7 (Optional) Monitor the status of the update in the **Update Status** area.

The update process can take several minutes. Do not activate the firmware until the selected firmware package displays in the **Backup Version** field in the **Firmware** area of the **General** tab.

What to do next

Activate the firmware.

Activating the Firmware on an Adapter

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Chassis** > ***Chassis Number*** > **Servers**.

Step 3 Expand the node for the server that includes the adapter for which you want to activate the updated firmware.

Step 4 Expand **Adapters** and select the adapter for which you want to activate the firmware.

Step 5 In the **General** tab, click **Activate Firmware**.

Step 6 In the **Activate Firmware** dialog box, do the following:

a) Select the appropriate version from the **Version To Be Activated** drop-down list.

If one or more of the selected endpoints are not configured with the required version as the backup version, that version does not display in the **Set Version** drop-down list. You must select the version from the **Startup Version** column for each individual endpoint.

b) If you want to set the startup version and not change the version running on the endpoint, check the **Set Startup Version Only** check box.

During a direct upgrade, you should configure **Set Startup Version Only** for an adapter. With this setting, the activated firmware moves into the pending-next-boot state, and the server is not immediately rebooted. The activated firmware does not become the running version of firmware on the adapter until the server is rebooted. You cannot configure **Set Startup Version Only** for an adapter in the host firmware package.

If a server is not associated with a service profile, the activated firmware remains in the pending-next-boot state. Cisco UCS Manager does not reboot the endpoints or activate the firmware until the server is associated with a service profile. If necessary, you can manually reboot or reset an unassociated server to activate the firmware.

c) Click **OK**.

BIOS Firmware

The Basic Input Output System (BIOS) tests and initializes the hardware components of a system and boots the operating system from a storage device. In Cisco UCS, there are several BIOS settings that control the system's behavior. You can update the BIOS firmware directly from Cisco UCS Manager.

Updating the BIOS Firmware on a Server

Caution Do not remove the hardware that contains the endpoint or perform any maintenance on it until the update process completes. If the hardware is removed or otherwise unavailable due to maintenance, the firmware update fails. This failure might corrupt the backup partition. You cannot update the firmware on an endpoint with a corrupted backup partition.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Chassis** > ***Chassis Number*** > **Servers**.

Step 3 Expand the node for the server for which you want to update the BIOS firmware.

Step 4 On the **General** tab, click the **Inventory** tab.

Step 5 Click the **Motherboard** tab.

Step 6 In the **Actions** area, click **Update Bios Firmware**.

Step 7 In the **Update Firmware** dialog box, do the following:

a) From the **Version** drop-down list, select the firmware version to update the server BIOS.
b) (Optional) If you want to update the firmware regardless of any possible incompatibilities or currently executing tasks, check the **Force** check box.
c) Click **OK**.

Cisco UCS Manager copies the selected server BIOS firmware package to the backup memory slot, where it remains until you explicitly activate it.

The update is complete when the **BIOS** area of the **Motherboard** tab displays **Ready** in the **Update Status** column for the **Backup Version**.

What to do next

Activate the firmware.

Activating the BIOS Firmware on a Server

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Chassis** > ***Chassis Number*** > **Servers**.

Step 3 Expand the node for the server for which you want to activate the updated BIOS firmware.

Step 4 On the **General** tab, click the **Inventory** tab.

Step 5 Click the **Motherboard** tab.

Step 6 In the **Actions** area, click **Activate Bios Firmware**.

Step 7 In the **Activate Firmware** dialog box, do the following:

a) Select the appropriate server BIOS version from the **Version To Be Activated** drop-down list.
b) If you want to set the start up version and not change the version running on the server, check the **Set Startup Version Only** check box.

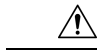
   If you configure **Set Startup Version Only**, the activated firmware moves into the pending-next-reboot state and the server is not immediately rebooted. The activated firmware does not become the running version of firmware until the server is rebooted.

c) Click **OK**.

CIMC Firmware

Cisco Integrated Management Controller (CIMC) is used for the management and monitoring of servers in Cisco UCS. CIMC provides options such as GUI, CLI, and IPMI for management and monitoring tasks. On the C-Series servers, CIMC runs on a separate chip. Thus, it is able to provide services in case of any major hardware failure or system crash. CIMC is also useful for initial configuration of the server and troubleshooting any problems in server operation. You can update the CIMC firmware directly from Cisco UCS Manager.

Updating the CIMC Firmware on a Server



Caution Do not remove the hardware that contains the endpoint or perform any maintenance on it until the update process completes. If the hardware is removed or otherwise unavailable due to maintenance, the firmware update fails. This failure might corrupt the backup partition. You cannot update the firmware on an endpoint with a corrupted backup partition.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Chassis** > ***Chassis Number*** > **Servers**.

Step 3 Expand the node for the server for which you want to update the CIMC.

Step 4 In the **General** tab, click the **Inventory** tab.

Step 5 Click the **CIMC** tab.

Step 6 In the **Actions** area, click **Update Firmware**.

Step 7 In the **Update Firmware** dialog box, do the following:

a) From the **Version** drop-down list, select the firmware version to update the endpoint.

b) Click **OK**.

Cisco UCS Manager copies the selected firmware package to the backup memory slot, where it remains until you activate it.

Step 8 (Optional) Monitor the status of the update in the **Update Status** area.

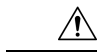
The update process can take several minutes. Do not activate the firmware until the selected firmware package displays in the **Backup Version** field in the **Firmware** area of the **General** tab.

What to do next

Activate the firmware.

Activating the CIMC Firmware on a Server

The activation of firmware for a CIMC does not disrupt data traffic. However, it will interrupt all KVM sessions and disconnect any vMedia attached to the server.



Caution Do not remove the hardware that contains the endpoint or perform any maintenance on it until the update process completes. If the hardware is removed or otherwise unavailable due to maintenance, the firmware update fails. This failure might corrupt the backup partition. You cannot update the firmware on an endpoint with a corrupted backup partition.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Chassis** > ***Chassis Number*** > **Servers**.

Step 3 Expand the node for the server that includes the CIMC for which you want to activate the updated firmware.

Step 4 On the **General** tab, click the **Inventory** tab.

Step 5 Click the **CIMC** tab.

Step 6 In the **Actions** area, click **Activate Firmware**.

Step 7 In the **Activate Firmware** dialog box, do the following:

a) Select the appropriate version from the **Version To Be Activated** drop-down list.

If one or more of the selected endpoints are not configured with the required version as the backup version, that version does not display in the **Set Version** drop-down list. You must select the version from the **Startup Version** column for each individual endpoint.

b) If you want to set the startup version and not change the version running on the endpoint, check the **Set Startup Version Only** check box.

If you configure **Set Startup Version Only**, the activated firmware moves to the pending-next-reboot state and the endpoint is not immediately rebooted. The activated firmware does not become the running version of firmware until the endpoint reboots.

c) Click **OK**.

PSU Firmware

You can update PSU firmware directly from Cisco UCS Manager.

Updating the Firmware on a PSU

Caution Do not remove the hardware that contains the endpoint or perform any maintenance on it until the update process completes. If the hardware is removed or otherwise unavailable due to maintenance, the firmware update fails. This failure might corrupt the backup partition. You cannot update the firmware on an endpoint with a corrupted backup partition.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Chassis**.

Step 3 Select the chassis for which you want to manage the PSUs.

Step 4 In the **Work** pane, click **PSUs**.

Step 5 Click the **Firmware Management** tab.

Step 6 Right-click the PSU that you want to upgrade and choose **Update Firmware**.

Step 7 In the **Update Firmware** dialog box, do the following:

a) From the **Version** drop-down list, select the firmware version to which you want to update the endpoint.

b) Click **OK**.

Cisco UCS Manager copies the selected firmware package to the backup memory slot, where it remains until you explicitly activate it.

Step 8 (Optional) Monitor the status of the update in the **Update Status** area.

The update process can take several minutes. Do not activate the firmware until the selected firmware package displays in the **Backup Version** field in the **Firmware** area of the **General** tab.

What to do next

Activate the firmware.

Activating the Firmware on a PSU

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Chassis**.

Step 3 Select the chassis for which you want to manage the PSUs.

Step 4 In the **Work** pane, click **PSUs**.

Step 5 Right-click the PSU that you want to upgrade and choose **Activate Firmware**.

Step 6 In the **General** tab, click **Activate Firmware**.

Step 7 In the **Activate Firmware** dialog box, do the following:

a) Select the appropriate version from the **Version To Be Activated** drop-down list.

If one or more of the selected endpoints are not configured with the required version as the backup version, that version does not display in the **Set Version** drop-down list. You must select the version from the **Startup Version** column for each individual endpoint.

b) If you want to set the startup version and not change the version running on the endpoint, check the **Set Startup Version Only** check box.

If you configure **Set Startup Version Only**, the activated firmware moves to the pending-next-reboot state and the endpoint is not immediately rebooted. The activated firmware does not become the running version of firmware until the endpoint reboots.

c) Click **OK**.

Board Controller Firmware

Board controllers maintain various programmable logic and power controllers for all B-Series blade servers, and C-Series rack servers. The board controller update utility enables you to make critical hardware updates.

Board controllers, introduced in Cisco UCS Manager Release 2.1(2a), allow you to make optimizations for components, such as voltage regulators, through an update to a digital controller configuration file by using the board controller update utility. Previously, updating a voltage regulator required changing physical components. These updates are at a hardware level, and are designed to be backward-compatible. Therefore, having the latest version of the board controller is always preferred.

Guidelines for Activating Cisco UCS B-Series M5 and Higher Blade Server Board Controller Firmware

The following guidelines apply to Cisco UCS B-Series M5 and higher blade-server board controller firmware:

- You never need to downgrade the board controller firmware.
- The board controller firmware version of the blade server should be the same as or later than the installed software bundle version. Leaving the board controller firmware at a later version than the version that is currently running in your existing Cisco UCS environment does not violate the software matrix or TAC supportability.
- Board controller firmware updates are backward compatible with the firmware of other components.

Guidelines for Activating Cisco UCS C-Series M5 and Higher Rack Server Board Controller Firmware

The following guidelines apply to Cisco UCS C-Series M5 and higher rack-server board controller firmware:

- The board controller firmware and the CIMC firmware must be of the same package version.
- If the activation status of the board controller displays **Pending Power Cycle** after you upgrade the board controller, a manual power cycle is required. A fault is also generated. After the power cycle is complete, the fault is cleared and the board controller activation status displays **Ready**.