Manage Firmware through Cisco UCS Manager

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 3.1 and later releases contain three 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 The UCS infrastructure bundle for one platform cannot be used to activate another platform. For example, the infrastructure bundle for the UCS 6200 Series fabric interconnect cannot be used to activate the UCS 6300 Series fabric interconnect.

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.

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 6300 Series, 6200 Series, 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 6300 Series, 6200 Series, 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 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

	Command or Action	Purpose
Step 1	UCS-A# **scope firmware**	Enters firmware mode.
Step 2	UCS-A /firmware # **download image** *URL*	Downloads the firmware bundle. Using the download path provided by Cisco, specify the URL with one of the following syntax: • **ftp:**// *server-ip-addr* / *path* • **scp:**// *username@server-ip-addr* / *path* • **sftp:**// *username@server-ip-addr* / *path* • **tftp:**// *server-ip-addr* **:** *port-num* / *path* **Note** TFTP has a file size limitation of 32 MB. Because firmware bundles can be much larger than that, we recommend that you do not select TFTP for firmware downloads. • **usbA:**/ *path* • **usbB:**/ *path* **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. **Note** If you use a hostname rather than an IP address, configure a DNS server in Cisco UCS Manager.
Step 3	Enter the password for the remote server.	The password for the remote server username. This field does not apply if the protocol is tftp.
Step 4	UCS-A /firmware # **show download-task**	Displays the status for your download task. When your image is completely downloaded, the task state changes from Downloading to Downloaded. The CLI does not automatically refresh, so you may have to enter the **show**

	Command or Action	Purpose
		download-task command multiple times until the task state displays Downloaded.
Step 5	Repeat this task until all of the firmware bundles have been downloaded to the fabric interconnect.	

Example

The following example uses SCP to download the firmware package.

```
UCS-A# scope firmware
UCS-A /firmware # download image scp://user1@192.168.10.10/images/ucs-k9-bundle.1.0.0.988.bin
OR
download image usbB:/username/ucs-k9-bundle-b-series.3.0.1a.B.bin
UCS-A /firmware # show download-task
UCS-A /firmware #
```

What to do next

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

Displaying the Firmware Package Download Status

After a firmware download operation has been started, you can check the download status to see if the package is still downloading or if it has completely downloaded.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope firmware**	Enters firmware mode.
Step 2	UCS-A /firmware # **show download-task**	Displays the status for your download task. When your image is completely downloaded, the task state changes from Downloading to Downloaded. The CLI does not automatically refresh, so you may have to enter the **show download-task** command multiple times until the task state displays Downloaded.

Example

The following example displays the download status for the firmware package. The **show download-task** command is entered multiple times until the download state indicates that the firmware package has been downloaded:

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

	Command or Action	Purpose
Step 1	UCS-A# **scope firmware**	Enters firmware mode.
Step 2	UCS-A /firmware # **delete download-task** *image_filename*	Deletes the specified image file.
Step 3	UCS-A /firmware # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example cancels an image download:

Displaying All Available Software Images on the Fabric Interconnect

This procedure is optional and displays the available software images on the fabric interconnect for all endpoints. You can also use the **show image** command in each endpoint mode to display the available software images for that endpoint.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope firmware**	Enters firmware mode.
Step 2	UCS-A /firmware # **show image**	Displays all software images downloaded onto the fabric interconnect. **Note** You must provide the software version number when directly updating an endpoint. If you intend to directly update firmware at an endpoint, note its version number in the right column.

Example

The following example displays all available software images on the fabric interconnect:

Displaying All Available Packages on the Fabric Interconnect

This procedure is optional and displays the available software packages on the fabric interconnect for all endpoints.. You can also use the **show package** command in each endpoint mode to display the available software images for that endpoint.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope firmware**	Enters firmware mode.
Step 2	UCS-A /firmware # **show package**	Displays all software packages downloaded onto the fabric interconnect. **Note** You must provide the software version number when directly updating an endpoint. If you intend to directly update firmware at an endpoint, note its version number in the right column.

Example

The following example displays all available software packages on the fabric interconnect:

Determining the Contents of a Firmware Package

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope firmware**	Enters firmware mode.
Step 2	UCS-A /firmware # **show package** *package-name* **expand**	Displays the contents of the specified firmware package.

Example

The following example displays the contents of a 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

	Command or Action	Purpose
Step 1	UCS-A# **scope fabric-interconnect** {**a** | **b**}	Enters fabric interconnect mode for the specified fabric.
Step 2	UCS-A /fabric-interconnect # **show storage** [**detail** | **expand**}	Displays the available space for the specified fabric. **Note** 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 other unneeded objects from the fabric interconnect.

Example

The following example displays the available space for a fabric interconnect:

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric-interconnect # show storage
Storage on local flash drive of fabric interconnect:
    Partition        Size (MBytes)    Used Percentage
    ---------------- ---------------- ---------------
    bootflash        8658             50
    opt              1917             2
    workspace        277              4
UCS-A /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 . Recommended Process for Upgrading Infrastructure Firmware Through Auto Install, on page 12, details the process that Cisco recommends for automatically installing infrastructure firmware.
- 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 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 17, provides detailed steps for clearing the startup version.

Automatic Internal Backup

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/
```

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:
    1. Create All Configuration and Full-State backup files. Creating an All Configuration Backup File and Configuring the Full State Backup Policy provide detailed information.
    2. Download firmware packages. Downloading Firmware Images to the Fabric Interconnect from a Remote Location, on page 4 provides detailed information.
    3. Disable Smart Call Home. Disabling Smart Call Home provides detailed information about disabling Smart Call Home.
2. Prepare for fabric upgrade:
    1. Verify Cisco UCS Manager faults and resolve the service -impacting faults.
    2. Verify High Availability status and identify the secondary fabric interconnect. Verifying the High Availability Status and Roles of a Cluster Configuration provides detailed information.
    3. Configure the default maintenance policy. Configuring the Default Maintenance Policy provides detailed information about maintenance policies and configuring the default maintenance policy to **User Ack**.
    4. Verify that VLAN and FCOE IDs do not overlap.
    5. Disable the management interface. Disabling the Management Interface provides detailed information about disabling the management interface for the secondary fabric interconnect.
    6. Verify that all paths are working. Verification that the Data Path is Ready provides detailed information.
3. Upgrade the Infrastructure Firmware with Auto Install, on page 12
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 15 provides detailed information.
8. Verify new faults.

Upgrade the Infrastructure Firmware with Auto Install

The **auto-install** scope is not available if the Cisco UCS Manager CLI 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

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

	Command or Action	Purpose
Step 1	UCS-A# **scope firmware**	Enters firmware mode.
Step 2	UCS-A /firmware # **scope auto-install**	Enters auto-install mode for infrastructure firmware upgrades.
Step 3	UCS-A /firmware/auto-install # **install infra infra-vers** *infrastructure-bundle-version* **servicepack-vers** *servicepack-bundle-version* [**starttime** *mon dd yyyy hh min sec*] [**force**] [**evacuate**] [**skipvalidation**]	Updates and activates the infrastructure firmware and the service pack bundle. You must use **starttime** to schedule the infrastructure firmware upgrade, if you do not want the upgrade to start immediately. If you use **starttime**, enter the following information to specify when you want to schedule the upgrade: • *mon*—The first three letters of the desired month, such as jan or feb. • *dd*—The number of the desired day of the month, from 1 to 31. • *yyyy*—The four numbers of the desired year, such as 2012.

	Command or Action	Purpose
		• *hh*—The hour when you want the upgrade to start, from 0 to 23. • *min*—The minute when you want the upgrade to start, from 0 to 60. • *sec*—The second when you want the upgrade to start, from 0 to 60. Use the **force** keyword to activate the firmware regardless of any possible incompatibilities or currently executing tasks. **Caution** Review the checklist that displays and ensure you have met all the requirements before you continue with the upgrade. If there is not enough space under bootflash, a warning will display and the upgrade process will stop. Use the **evacuate** keyword to enable fabric evacuation on each fabric interconnect that is being upgraded through Auto Install. Both fabric interconnects are evacuated, but not at the same time. **Note** If you enable fabric evacuation during Auto Install, and fabric evacuation was enabled manually on any of the fabric interconnects before Auto Install, fabric evacuation is disabled after Auto Install is complete.
Step 4	(Optional) UCS-A /firmware/auto-install # **install infra servicepack-vers** *servicepack-bundle-version* [**force**]	Updates and activates the service pack bundle over the existing base infrastructure pack.

Example

This example shows how to upgrade the infrastructure to the firmware in the Cisco UCS Infrastructure Software Bundle:

This example shows how to upgrade the infrastructure to the firmware in the Cisco UCS Infrastructure Software Bundle with the **evacuate** option enabled:

This example shows how to upgrade the infrastructure to a service pack version:

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

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 and cause 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

	Command or Action	Purpose
Step 1	UCS-A# **scope firmware**	Enters firmware mode.
Step 2	UCS-A /firmware # **scope auto-install**	Enters auto-install mode for infrastructure firmware upgrades.
Step 3	UCS-A /firmware/auto-install # **acknowledge primary fabric-interconnect reboot**	Acknowledges the pending reboot of the primary fabric interconnect.
Step 4	UCS-A /firmware/auto-install # **commit-buffer**	Commits the transaction to the system configuration. Cisco UCS Manager immediately reboots the primary fabric interconnect. You cannot stop this reboot after you commit the transaction.

Example

This example shows how to acknowledge the reboot of the primary fabric interconnect and commit the transaction:

```
UCS-A# scope firmware
UCS-A /firmware # scope auto-install
UCS-A /firmware/auto-install # acknowledge primary fabric-interconnect reboot
UCS-A /firmware/auto-install* # commit-buffer
UCS-A /firmware/auto-install #
```

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

	Command or Action	Purpose
Step 1	UCS-A# **scope firmware**	Enters firmware mode.
Step 2	UCS-A /firmware # **scope auto-install**	Enters auto-install mode for infrastructure firmware upgrades.
Step 3	UCS-A /firmware/auto-install # **cancel install infra**	Cancels the scheduled infrastructure firmware upgrade.
Step 4	UCS-A /firmware/auto-install # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example cancels a scheduled infrastructure firmware upgrade and commits the transaction:

```
UCS-A# scope firmware
UCS-A /firmware # scope auto-install
UCS-A /firmware/auto-install # cancel install infra
UCS-A /firmware/auto-install* # commit-buffer
UCS-A /firmware/auto-install #
```

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

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters the organization mode for the specified organization. To enter the root organization mode, enter / as the *org-name*.
Step 2	UCS-A /org # **scope fw-infra-pack** *name*	Enters the organization infrastructure firmware policy mode.
Step 3	UCS-A /org/fw-infra-pack # **set infra-bundle-version ""**	Clears the startup version of the default infrastructure pack and the service pack.
Step 4	(Optional) UCS-A /org/fw-infra-pack # **set servicepack-vers ""**	Clears the startup version of the service pack.
Step 5	UCS-A /org/fw-infra-pack* # **commit-buffer**	Commits the transaction.

Example

This example shows how to clear the startup version of the default infrastructure pack.

```
UCS-A# scope org
UCS-A /org # scope fw-infra-pack default
UCS-A /org/fw-infra-pack # set infra-bundle-version ""
UCS-A /org/fw-infra-pack* # commit-buffer
```

Viewing the Status of the FSM During An Infrastructure Firmware Upgrade

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope firmware**	Enters firmware mode.
Step 2	UCS-A /firmware # **scope auto-install**	Enters auto-install mode for infrastructure firmware upgrades.
Step 3	UCS-A /firmware/auto-install # **show fsm status expand**	Displays the status of the FSM.

Example

The following example displays the status of the FSM:

```
UCS-A /firmware/auto-install # show fsm status expand

    FSM Status:

        Affected Object: sys/fw-system/fsm
        Current FSM: Deploy
        Status: Success
        Completion Time: 2017-02-03T18:02:13.699
        Progress (%): 100

        FSM Stage:

        Order  Stage Name                                 Status       Try
        ------ ---------------------------------------- ------------ ---
        1      DeployWaitForDeploy                       Success      0
        2      DeployResolveDistributableNames           Skip         0
        3      DeployResolveDistributable                Skip         0
        4      DeployResolveImages                       Skip         0
        5      DeployDownloadImages                      Skip         0
        6      DeployCopyAllImagesToPeer                 Skip         0
        7      DeployInternalBackup                      Skip         0
        8      DeployPollInternalBackup                  Success      0
        9      DeployActivateUCSM                        Skip         0
        10     DeployPollActivateOfUCSM                  Success      0
        11     DeployUpdateIOM                           Success      0
        12     DeployPollUpdateOfIOM                     Success      0
        13     DeployActivateIOM                         Success      0
        14     DeployPollActivateOfIOM                   Success      0
        15     DeployFabEvacOnRemoteFI                   Skip         0
        16     DeployPollFabEvacOnRemoteFI               Skip         0
        17     DeployActivateRemoteFI                    Success      0
        18     DeployPollActivateOfRemoteFI              Success      0
        19     DeployFabEvacOffRemoteFI                  Skip         0
        20     DeployPollFabEvacOffRemoteFI              Skip         0
        21     DeployWaitForUserAck                      Skip         0
        22     DeployPollWaitForUserAck                  Success      0
        23     DeployFailOverToRemoteFI                  Skip         0
        24     DeployPollFailOverToRemoteFI              Skip         0
        25     DeployActivateLocalFI                     Success      0
        26     DeployPollActivateOfLocalFI               Success      0
        27     DeployActivateUCSMServicePack             Skip         0
        28     DeployPollActivateOfUCSMServicePack       Success      0
```

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 or 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.

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.

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

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 2	UCS-A org/ # **create fw-host-pack** *pack-name*	Creates a host firmware package with the specified package name and enters organization firmware host package mode.
Step 3	(Optional) UCS-A /org/fw-host-pack # **set descr** *description*	Provides a description for the host firmware package. **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any **show** command output.
Step 4	UCS-A org/fw-host-pack # **create pack-image** "*hw-vendor-name*" "*hw-model*" {**adapter** | **board-controller** | **cimc** | **graphics-card** | **host-hba** | **host-hba-optionrom** | **host-nic** | **local-disk** | **raid-controller** | **server-bios**} "*version-num*"	Creates a package image for the host firmware package and enters organization firmware host package image mode. The *hw-vendor-name* must match the full name of the vendor, and must begin and end with quotation marks. The *hw-vendor-name* and *hw-model* values are labels that help you easily identify the package image when you enter the **show image detail** command. The *version-num* value specifies the version number of the firmware being used for the package image. 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.
Step 5	UCS-A org/fw-host-pack # **create exclude-server-component** {**adapter** | **board-controller** | **cimc** | **flexflash-controller** | **graphics-card** | **host-hba** | **host-hba-optionrom** | **host-nic** | **host-nic-optionrom** | **local-disk** | **psu** | **raid-controller** | **sas-expander** | **server-bios** | **unspecified**}	Excludes the specified component from the host firmware package. **Note** By default, all components are included in the host firmware package.
Step 6	Required: UCS-A org/fw-host-pack # **delete exclude-server-component** {**adapter** | **board-controller** | **cimc** | **flexflash-controller** | **graphics-card** | **host-hba** |	Includes the specified component from the host firmware package.

	Command or Action	Purpose
	host-hba-optionrom | **host-nic** | **host-nic-optionrom** | **local-disk** | **psu** | **raid-controller** | **sas-expander** | **server-bios** | **unspecified**}	
Step 7	(Optional) UCS-A org/fw-host-pack/pack-image # **set blade-vers** *blade-version-num*	Specifies the B-Series server package image version number. Changing this number triggers firmware updates on all B-Series server components using the firmware through a service profile. Use this step only when updating a host firmware package, not when creating a package. The host firmware package can contain multiple package images. Repeat steps 4 and 5 to create additional package images for other components.
Step 8	(Optional) UCS-A org/fw-host-pack/pack-image # **set rack-vers** *rack-version-num*	Specifies the C-Series server package image version number. Changing this number triggers firmware updates on all C-Series server components using the firmware through a service profile. Use this step only when updating a host firmware package, not when creating a package. The host firmware package can contain multiple package images. Repeat steps 4 and 5 to create additional package images for other components.
Step 9	(Optional) UCS-A org/fw-host-pack/pack-image # **set servicepack-vers** *servicepack-version-num*	Specifies the service pack version number. You cannot directly upgrade to a service pack without selecting a base server pack. To remove the service pack from the host firmware package, use `""` as the service pack version number. The images from the service pack will take precedence over the images from Blade Package or Rack Package.
Step 10	UCS-A org/fw-host-pack/pack-image # **commit-buffer**	Commits the transaction. 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.

Example

The following example creates the app1 host firmware package, creates an adapter package image with version 02.00.77 firmware, and commits the transaction:

```
UCS-A# scope org
UCS-A /org # create fw-host-pack app1
UCS-A /org/fw-host-pack* # set descr "This is a host firmware package example."
UCS-A /org/fw-host-pack* # create pack-image "Cisco Systems Inc" "N20-AQ0102" adapter
"02.00.77"
UCS-A /org/fw-host-pack/pack-image* # commit-buffer
UCS-A /org/fw-host-pack/pack-image #
```

The following example excludes the server BIOS component from the app1 host firmware package, and commits the transaction:

```
UCS-A# scope org
UCS-A /org # enter fw-host-pack app1
UCS-A /org/fw-host-pack* # create exclude-server-component server-bios
UCS-A /org/fw-host-pack/exclude-server-component* # commit-buffer
UCS-A /org/fw-host-pack/exclude-server-component #
```

The following example adds a service pack to the app1 host firmware package, and commits the transaction:

```
UCS-A# scope org
UCS-A /org # scope fw-host-pack app1
UCS-A /org/fw-host-pack # set servicepack-vers 3.1(3)SP1
UCS-A /org/fw-host-pack* # commit-buffer
UCS-A /org/fw-host-pack #
```

The following example removes a service pack from the app1 host firmware package, and commits the transaction:

```
UCS-A# scope org
UCS-A /org # scope fw-host-pack app1
UCS-A /org/fw-host-pack # set servicepack-vers ""
UCS-A /org/fw-host-pack* # commit-buffer
UCS-A /org/fw-host-pack #
```

What to do next

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

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**.

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 to match with the firmware version of the default host firmware pack.

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

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the org-name.
Step 2	UCS-A /org # **scope fw-autosync-policy**	Enters the firmware auto synchronization policy mode.
Step 3	UCS-A /org/fw-autosync-policy # **set auto-sync**{*user-acknowledge* | *no-actions*}	Set one of the following values to set the policy: • **user-acknowledge**—Firmware on the server is not synchronized until the administrator acknowledges the discovered server in the **server** command mode. • **no-action**—No firmware upgrade is initiated on the server. This value is selected by default.
Step 4	UCS-A /org/fw-autosync-policy # **commit-buffer**	Commits the transaction to the system configuration.

Example

This example shows how to set the **Firmware Auto Sync Server** policy and commit the transaction to the system:

```
UCS-A # scope org
UCS-A /org # scope fw-autosync-policy
UCS-A /org/fw-autosync-policy # set auto-sync user-acknowledge
UCS-A /org/fw-autosync-policy* # commit-buffer
UCS-A /org/fw-autosync-policy #
```

What to do next

If you set the value to **user-acknowledge**, then you must acknowledge pending activity for the server for the firmware synchronization to occur.

Acknowledging the Firmware Auto Synchronization for a Server

If you have set the Firmware Auto-Sync Server policy to **User Acknowledge**, then you will have to acknowledge the pending activities for a server. If you do not acknowledge this pending activity for the server, then the firmware version of the server or the endpoints in the server are not updated to match with the firmware versions defined in the default host firmware pack.

Before you begin

- You should have logged in as an administrator to complete this task.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope chassis**	Enters the chassis command mode.
Step 2	UCS-A /chassis # **scope server** *server ID*	Enters the server command mode.
Step 3	UCS-A /chassis/server # **fw-sync** {*acknowledge* *discard*}	Acknowledges or discards the pending firmware synchronization for the server.
Step 4	UCS-A /chassis/server # **commit-buffer**	Commits the transaction to the server.

Example

This example shows how to acknowledge the pending firmware update for a server and commit the transaction:

```
UCS-A # scope chassis
UCS-A /chassis # scope server 1
UCS-A /chassis/server # fw-sync acknowledge
UCS-A /chassis/server* # commit-buffer
UCS-A /chassis/server #
```

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 35, 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* 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 standalone 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.

Outage Impacts of Direct Firmware Upgrades on M-Series Chassis and Server Endpoints

Important Cisco UCS Manager Release 3.1(2) and later releases do not support Cisco UCS M-Series Servers.

Outage Impact of a CMC Firmware Upgrade

When you upgrade the firmware for CMC in a chassis you do not cause any outage.

Outage Impact of a Shared Adapter Firmware Upgrade

If you activate the firmware for a shared adapter, you cause the following outage impacts and disruptions:

- The server reboots.
- Server traffic is disrupted.
- The storage controller reboots.

Outage Impact of a Storage Controller Firmware Upgrade

If you activate the firmware for a storage controller, you cause the following outage impacts and disruptions:

- Servers with local boot policy reboot. Servers with iSCSI boot policy do not reboot.
- Server traffic is disrupted.
- The storage controller reboots.

Outage Impact of a Board Controller Firmware Upgrade

If you activate the firmware for a board controller, you cause the following outage impacts and disruptions:

- The shared adapter reboots.
- The cartridge and server reboot.
- Server traffic is disrupted.
- The storage controller reboots.

Outage Impact of a BIOS Firmware Upgrade

A firmware upgrade to the BIOS causes the server to reboot.

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 a Board Controller Firmware Upgrade on a Server

If you activate the firmware for a board controller on a server, you cause the server to be powered off during the upgrade and powered on after the upgrade is complete.

While activating the storage controller, board controller and shared adapter firmware, it is recommended that you power down the servers. In case you do not power down the servers during activation, Cisco UCSM will attempt to power down the servers and wait for a maximum of 16 minutes. During this time, if Cisco UCSM still finds that the servers are not powered down, FSM will fail and Cisco UCSM will not power up the servers that it powered down. FSM will try to come up after 8 minutes.

If UCSM successfully powers down the servers, it will power up the associated servers, based on their desired power states, after activation is complete.

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:
    1. Create All Configuration and Full-State backup files. Creating an All Configuration Backup File and Configuring the Full State Backup Policy provide detailed information.
    2. Download firmware packages. Downloading Firmware Images to the Fabric Interconnect from a Remote Location, on page 4 provides detailed information.
    3. Disable Smart Call Home. Disabling Smart Call Home provides detailed information.
2. Activating the Cisco UCS Manager Software, on page 37
3. Update IOM firmware. Updating and Activating the Firmware on an IOM, on page 40 provides detailed information.
4. Prepare for fabric upgrade:
    1. Verify UCS Manager faults and resolve the service -impacting faults.
    2. Verify High Availability status and identify the secondary fabric interconnect. Verifying the High Availability Status and Roles of a Cluster Configuration provides detailed information.
    3. Configure the default maintenance policy. Configuring the Default Maintenance Policy provides detailed information.
    4. Verify that VLAN and FCOE IDs do not overlap.
    5. Disable the management interface. Disabling the Management Interface provides detailed information.
    6. Activate IOM firmware. Updating and Activating the Firmware on an IOM, on page 40 provides detailed information.
5. Activate the subordinate fabric interconnect

1. Evacuate subordinate fabric interconnect traffic. Stopping Traffic on a Fabric Interconnect provides detailed information.
2. Activate the subordinate fabric interconnect (FI-B) and monitor FSM. Activating the Firmware on a Fabric Interconnect, on page 42 provides detailed information.
3. Verify that all paths are working. Verification that the Data Path is Ready provides detailed information.
4. Disable subordinate fabric interconnect traffic evacuation. Restarting Traffic on a Fabric Interconnect provides detailed information.
5. Verify new faults. Viewing Faults Generated During the Upgrade of a Fabric Interconnect provides detailed information.

6. Activate the primary fabric interconnect (FI-A)
   1. 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 43 provides detailed information.
   2. Evacuate primary fabric interconnect traffic.
   3. Activate the primary fabric interconnect (FI-A) and monitor FSM. Acknowledging the Reboot of the Primary Fabric Interconnect, on page 15 provides detailed information.
   4. Verify that all paths are working.
   5. Disable primary fabric interconnect traffic evacuation. Restarting Traffic on a Fabric Interconnect provides detailed information.
   6. Verify new faults.

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

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope system**	Enters system mode.
Step 2	UCS-A /system # **show image**	Displays the available software images for Cisco UCS Manager (system).
Step 3	UCS-A /system # **activate firmware** *version-num*	Activates the selected firmware version on the system. **Note** Activating Cisco UCS Manager does not require rebooting the fabric interconnect; however, management services will briefly go down and all VSH shells will be terminated as part of the activation.
Step 4	UCS-A /system # **commit-buffer**	Commits the transaction. Cisco UCS Manager makes the selected version the startup version and schedules the activation to occur when the fabric interconnects are upgraded.

Example

The following example upgrades Cisco UCS Manager and commits the transaction:

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

	Command or Action	Purpose
Step 1	UCS-A# **scope firmware**	
Step 2	UCS-A /firmware # **show image type** mgmt-service-pack	Displays the available software images for Cisco UCS Manager (system).

	Command or Action	Purpose
Step 3	UCS-A /firmware # **exit**	
Step 4	UCS-A# **scope system**	Enters system mode.
Step 5	UCS-A /system # **activate service-pack** *version-num* **module security**	Activates the selected service -pack version on the system. 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.
Step 6	UCS-A /system # **commit-buffer**	Commits the transaction.
Step 7	(Optional) UCS-A /system # **show version**	Shows a summary of the firmware versions, including the service pack version, on the system.

Example

The following example upgrades Cisco UCS Manager to version 3.1(3)SP2 and commits the transaction:

```
UCS-A# scope firmware
UCS-A# /firmware # show image type mgmt-service-pack
Name                                       Type                 Version
------------------------------------------ -------------------- -------
ucs-manager-k9.service-pack.3.1.3.SP1.gbin    Mgmt Service Pack    3.1(3)SP1
ucs-manager-k9.service-pack.3.1.3.SP2.gbin    Mgmt Service Pack    3.1(3)SP2
ucs-manager-k9.service-pack.3.1.4.SP1.gbin    Mgmt Service Pack    3.1(4)SP1
UCS-A# /firmware # exit
UCS-A# scope system
UCS-A# /system # activate service-pack 3.1(3)SP2 module security
As part of activation, all cli sessions will be terminated.
Continue with activation? (yes/no) yes
UCS-A# /system* # commit-buffer
UCS-A# /system # show version
UCSM:
    Running-Vers: 3.1(2.172a)
    Package-Vers: 3.1(2.173)A
    Activate-Status: Ready

UCSM Service Pack:
    Running-Vers: 3.1(3)SP2
    Running-Modules: security
    Package-Vers:
    Activate-Status: Ready


UCS-A# /system #
```

Removing a Service Pack from the Cisco UCS Manager Software

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope system**	Enters system mode.
Step 2	UCS-A /system # **remove service-pack**	Removes the activated service pack from the system. All CLI sessions are terminated while removing the service pack from the system.
Step 3	UCS-A /system # **commit-buffer**	Commits the transaction.

Example

The following example removes the service pack from Cisco UCS Manager and commits the transaction:

```
UCS-A# scope system
UCS-A# /system # remove service-pack
As part of activation, all cli sessions will be terminated.
Continue with activation? (yes/no)yes
UCS-A# /system* # commit-buffer
```

IOM Firmware

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.

Updating and Activating the Firmware on an IOM

If your system is running in a high availability cluster configuration, you must update and activate both I/O modules.

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

	Command or Action	Purpose
Step 1	UCS-A# **scope chassis** *chassis-id*	Enters chassis mode for the specified chassis.
Step 2	UCS-A /chassis # **scope iom** *iom-id*	Enters chassis I/O module mode for the selected I/O module.
Step 3	UCS-A /chassis/iom # **show image**	Displays the available software images for the I/O module.
Step 4	UCS-A /chassis/iom # **update firmware** *version-num*	Updates the selected firmware version on the I/O module.
Step 5	(Optional) UCS-A /chassis/iom # **commit-buffer**	Commits the transaction. Use this step only if you intend to use the **show firmware** command in Step 6 to verify that the firmware update completed successfully before activating the firmware in Step 7. You can skip this step and commit the **update-firmware** and **activate-firmware** commands in the same transaction; however, if the firmware update does not complete successfully, the firmware activation does not start.

	Command or Action	Purpose
		Cisco UCS Manager copies the selected firmware image to the backup memory partition and verifies that image is not corrupt. The image remains as the backup version until you explicitly activate it.
Step 6	(Optional) UCS-A /chassis/iom # **show firmware**	Displays the status of the firmware update. Use this step only if you want to verify that the firmware update completed successfully. The firmware update is complete when the update status is Ready. The CLI does not automatically refresh, so you may have to enter the **show firmware** command multiple times until the task state changes from Updating to Ready. Continue to Step 7 when the update status is Ready.
Step 7	UCS-A /chassis/iom # **activate firmware** *version-num* [**set-startup-only**]	Activates the selected firmware version on the I/O module. Use the **set-startup-only** keyword if you want to reboot the I/O module only when the fabric interconnect in its data path reboots. If you do not use the **set-startup-only** keyword, the I/O module reboots and disrupts traffic. In addition, if Cisco UCS Manager detects a protocol and firmware version mismatch between it and the I/O module, it updates the I/O module with the firmware version that matches its own and then activates the firmware and reboots the I/O module again.
Step 8	UCS-A /chassis/iom # **commit-buffer**	Commits the transaction.
Step 9	(Optional) UCS-A /chassis/iom # **show firmware**	Displays the status of the firmware activation. Use this step only if you want to verify that the firmware activation completed successfully. The CLI does not automatically refresh, so you may have to enter the **show firmware** command multiple times until the task state changes from Activating to Ready.

Example

The following example updates and activates the I/O module firmware in the same transaction, without verifying that the firmware update and firmware activation completed successfully:

The following example updates the I/O module firmware, verifies that the firmware update completed successfully before starting the firmware activation, activates the I/O module firmware, and verifies that the firmware activation completed successfully:

Fabric Interconnect Firmware

Activating the Firmware on a Fabric Interconnect

When updating the firmware on two fabric interconnects in a high availability cluster configuration, you must activate the subordinate fabric interconnect before activating the primary fabric interconnect. For more information about determining the role for each fabric interconnect, see Verifying the High Availability Status and Roles of a Cluster Configuration.

For a standalone 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

	Command or Action	Purpose
Step 1	UCS-A# **scope fabric-interconnect** {**a** | **b**}	Enters fabric interconnect mode for the specified fabric interconnect.
Step 2	UCS-A /fabric-interconnect # **show image**	Displays the available software images for the fabric interconnect.
Step 3	UCS-A /fabric-interconnect # **activate firmware** {**kernel-version** *kernel-ver-num* | **system-version** *system-ver-num*}	Activates the selected firmware version on the fabric interconnect.
Step 4	UCS-A /fabric-interconnect # **commit-buffer**	Commits the transaction. Cisco UCS Manager updates and activates the firmware, and then 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.

Example

The following example upgrades the fabric interconnect to version 5.0(3)N2(3.10.123) and commits the transaction:

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric-interconnect # show image
Name                                        Type                 Version
------------------------------------------- -------------------- -------
ucs-6300-k9-kickstart.5.0.3.N2.3.10.123.bin   Fabric Interconnect Kernel
                                                                   5.0(3)N2(3.10.123)
ucs-6300-k9-system.5.0.3.N2.3.10.123.bin      Fabric Interconnect System
                                                                   5.0(3)N2(3.10.123)

UCS-A /fabric-interconnect # activate firmware kernel-version 5.0(3)N2(3.10.123)
system-version 5.0(3)N2(3.10.123)
UCS-A /fabric-interconnect* # commit-buffer
UCS-A /fabric-interconnect #
```

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: **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

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope firmware**	
Step 2	UCS-A /firmware # **show image type** fabric-interconnect-service-pack	Displays the available service packs for the fabric interconnects.
Step 3	UCS-A /firmware # **exit**	
Step 4	UCS-A# **scope fabric-interconnect** {**a** | **b**}	Enters fabric-interconnect mode.
Step 5	UCS-A /fabric-interconnect # **activate service-pack** *version-num* [**security**]	Activates the selected service -pack version on the system. **Note** 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.
Step 6	UCS-A /fabric-interconnect # **commit-buffer**	Commits the transaction.
Step 7	(Optional) UCS-A /fabric-interconnect # **show version**	Shows a summary of the firmware versions, including the service pack version, on the fabric interconnect.

Example

The following example upgrades fabric interconnect a and commits the transaction:

Removing 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

	Command or Action	Purpose
Step 1	UCS-A# **scope fabric-interconnect** {**a** | **b**}	Enters fabric-interconnect mode.
Step 2	UCS-A /fabric-interconnect # **remove service-pack security**	Removes the activated service pack from the fabric interconnect.
Step 3	UCS-A /fabric-interconnect # **commit-buffer**	Commits the transaction.

Example

The following example removes the service pack from fabric interconnect a and commits the transaction:

```
UCS-A# scope fabric-interconnect a
UCS-A# /fabric-interconnect # remove service-pack security
UCS-A# /fabric-interconnect* # commit-buffer
```

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 and Activating 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

	Command or Action	Purpose
Step 1	UCS-A# **scope adapter** *chassis-id* / *blade-id* / *adapter-id*	Enters chassis server adapter mode for the specified adapter.
Step 2	UCS-A /chassis/server/adapter # **show image**	Displays the available software images for the adapter.
Step 3	UCS-A /chassis/server/adapter # **update firmware** *version-num*	Updates the selected firmware version on the adapter.
Step 4	(Optional) UCS-A /chassis/server/adapter # **commit-buffer**	Commits the transaction. Use this step only if you intend to use the **show firmware** command in Step 5 to verify that the firmware update completed successfully before activating the firmware in Step 6. You can skip this step and commit the **update-firmware** and **activate-firmware** commands in the same transaction; however, if the firmware update does not complete successfully, the firmware activation does not start. Cisco UCS Manager copies the selected firmware image to the backup memory partition and verifies that image is not corrupt. The image remains as the backup version until you explicitly activate it.
Step 5	(Optional) UCS-A /chassis/server/adapter # **show firmware**	Displays the status of the firmware update. Use this step only if you want to verify that the firmware update completed successfully. The firmware update is complete when the update status is Ready. The CLI does not automatically refresh, so you may have to enter the **show firmware** command multiple times until the task state changes from Updating to Ready. Continue to Step 6 when the update status is Ready.
Step 6	UCS-A /chassis/server/adapter # **activate firmware** *version-num* [**set-startup-only**]	Activates the selected firmware version on the adapter.

	Command or Action	Purpose
		Use the **set-startup-only** keyword if you want to move the activated firmware into the pending-next-boot state and not immediately reboot the server. The activated firmware does not become the running version of firmware on the adapter until the server is rebooted. You cannot use the **set-startup-only** keyword for an adapter in the host firmware package.
Step 7	UCS-A /chassis/server/adapter # **commit-buffer**	Commits the transaction. 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.
Step 8	(Optional) UCS-A /chassis/server/adapter # **show firmware**	Displays the status of the firmware activation. Use this step only if you want to verify that the firmware activation completed successfully. The CLI does not automatically refresh, so you may have to enter the **show firmware** command multiple times until the task state changes from Activating to Ready.

Example

The following example updates and activates the adapter firmware to version 4.1(0.123) in the same transaction, without verifying that the firmware update and firmware activation completed successfully:

```
UCS-A# scope adapter 1/1/1
UCS-A# /chassis/server/adapter # show image
Name                                       Type                Version
------------------------------------------ ------------------- -------
ucs-m82-8p-vic.4.1.0.123.bin               Adapter             4.1(0.123)

UCS-A# /chassis/server/adapter # update firmware 4.1(0.123)
UCS-A# /chassis/server/adapter* # activate firmware 4.1(0.123) set-startup-only
UCS-A# /chassis/server/adapter* # commit-buffer
UCS-A# /chassis/server/adapter #
```

The following example updates the adapter firmware to version 4.1(0.123), verifies that the firmware update completed successfully before starting the firmware activation, activates the adapter firmware, and verifies that the firmware activation completed successfully:

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 and Activating the BIOS Firmware on a Server

Important You can update and activate BIOS firmware on a server using the Cisco UCS Manager CLI on all M3 generation servers. The earlier servers do not support BIOS firmware update using the Cisco UCS Manager CLI.

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

	Command or Action	Purpose
Step 1	UCS-A# **scope server** *chassis-id* / *blade-id*	Enters chassis server mode for the specified server.
Step 2	UCS-A /chassis/server # scope bios	Enters chassis server BIOS mode.
Step 3	UCS-A /chassis/server/bios # **show image**	Displays the available BIOS firmware images.
Step 4	UCS-A /chassis/server/bios # **update firmware** *version-num*	Updates the selected BIOS firmware for the server.
Step 5	(Optional) UCS-A /chassis/server/bios # **commit-buffer**	Commits the transaction. Use this step only if you intend to use the **show firmware** command in Step 6 to verify that the firmware update completed successfully before activating the firmware in Step 7. You can skip this step and commit the **update-firmware** and **activate-firmware** commands in the same transaction; however, if the firmware update does not complete successfully, the firmware activation does not start. Cisco UCS Manager copies the selected firmware image to the backup memory partition and verifies that image is not corrupt. The image remains as the backup version until you explicitly activate it.

	Command or Action	Purpose
Step 6	(Optional) UCS-A /chassis/server/bios # **show firmware**	Displays the status of the firmware update. Use this step only if you want to verify that the firmware update completed successfully. The firmware update is complete when the update status is Ready. The CLI does not automatically refresh, so you may have to enter the **show firmware** command multiple times until the task state changes from Updating to Ready. Continue to Step 7 when the update status is Ready.
Step 7	UCS-A /chassis/server/bios # **activate firmware** *version-num*	Activates the selected server BIOS firmware version.
Step 8	UCS-A /chassis/server/bios # **commit-buffer**	Commits the transaction.
Step 9	(Optional) UCS-A /chassis/bios # **show firmware**	Displays the status of the firmware activation. Use this step only if you want to verify that the firmware activation completed successfully. The CLI does not automatically refresh, so you may have to enter the **show firmware** command multiple times until the task state changes from Activating to Ready.

Example

The following example updates and activates the BIOS firmware in the same transaction, without verifying that the firmware update and activation completed successfully:

```
UCS-A# scope server 1/1
UCS-A# /chassis/server # scope bios
UCS-A# /chassis/server/bios # show image
Name                                        Type                Version
------------------------------------------- ------------------- -------
ucs-b200-m2-bios.S5500.2.1.3c.0.081120151437.bin
                                           Server BIOS         S5500.2.1.3c.0.081120151437
ucs-b200-m3-bios.B200M3.2.2.6c.0.110420151250.bin
                                             Server BIOS
B200M3.2.2.6c.0.110420151250
ucs-b200-m4-bios.B200M4.3.1.0.4.113020151739.bin
                                           Server BIOS         B200M4.3.1.0.4.113020151739

UCS-A# /chassis/server/bios # update firmware B200M4.3.1.0.4.113020151739
UCS-A# /chassis/server/bios* # activate firmware B200M4.3.1.0.4.113020151739
UCS-A# /chassis/server/bios* # commit-buffer
UCS-A# /chassis/server/bios #
```

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 and 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

	Command or Action	Purpose
Step 1	UCS-A# **scope server** *chassis-id* / *blade-id*	Enters chassis server mode for the specified server.
Step 2	UCS-A /chassis/server # **scope cimc**	Enters chassis server CIMC mode.
Step 3	UCS-A /chassis/server/cimc # **show image**	Displays the available software images for the adapter.
Step 4	UCS-A /chassis/server/cimc # **update firmware** *version-num*	Updates the selected firmware version on the CIMC in the server.
Step 5	(Optional) UCS-A /chassis/server/cimc # **commit-buffer**	Commits the transaction. Use this step only if you intend to use the **show firmware** command in Step 6 to verify that the firmware update completed successfully before activating the firmware in Step 7. You can skip this step and commit the **update-firmware** and **activate-firmware** commands in the same transaction; however, if the firmware update does not complete successfully, the firmware activation does not start. Cisco UCS Manager copies the selected firmware image to the backup memory partition and verifies that image is not corrupt. The image remains as the backup version until you explicitly activate it.

	Command or Action	Purpose
Step 6	(Optional) UCS-A /chassis/server/cimc # **show firmware**	Displays the status of the firmware update. Use this step only if you want to verify that the firmware update completed successfully. The firmware update is complete when the update status is Ready. The CLI does not automatically refresh, so you may have to enter the **show firmware** command multiple times until the task state changes from Updating to Ready. Continue to Step 7 when the update status is Ready.
Step 7	UCS-A /chassis/server/cimc # **activate firmware** *version-num*	Activates the selected firmware version on the CIMC in the server.
Step 8	UCS-A /chassis/server/cimc # **commit-buffer**	Commits the transaction.
Step 9	(Optional) UCS-A /chassis/server/cimc # **show firmware**	Displays the status of the firmware activation. Use this step only if you want to verify that the firmware activation completed successfully. The CLI does not automatically refresh, so you may have to enter the **show firmware** command multiple times until the task state changes from Activating to Ready.

Example

The following example updates and activates the CIMC firmware in the same transaction, without verifying that the firmware update and firmware activation completed successfully:

The following example updates the CIMC firmware, verifies that the firmware update completed successfully before starting the firmware activation, activates the CIMC firmware, and verifies that the firmware activation completed successfully:

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

	Command or Action	Purpose
Step 1	UCS-A# **scope chassis** *chassis-id*	Enters chassis mode for the specified chassis.
Step 2	UCS-A /chassis # **scope psu** *psu-id*	Enters PSU mode for the specified PSU.
Step 3	UCS-A /chassis/psu # **show detail**	Displays the available software images for the PSU.
Step 4	UCS-A /chassis/psu # **update firmware** *version-num* [**force**]	Updates the selected firmware version on the PSU. You can use the optional **force** keyword to activate the firmware regardless of any possible incompatibilities or currently executing tasks. **Caution** Review the checklist that displays and ensure you have met all the requirements before you continue with the upgrade.
Step 5	(Optional) UCS-A /chassis/psu # **commit-buffer**	Commits the transaction. Cisco UCS Manager copies the selected firmware image to the backup memory partition and verifies that image is not corrupt. The image remains as the backup version until you explicitly activate it.

Example

The following example shows how to update the PSU firmware and commit the transaction:

```
UCS-A# scope chassis 1
UCS-A# /chassis # scope psu 2
UCS-A# /chassis/psu # show detail
PSU:
    PSU: 2
    Overall Status: Operable
    Operability: Operable
    Threshold Status: OK
    Power State: On
    Presence: Equipped
    Thermal Status: OK
    Voltage Status: OK
    Product Name: Platinum II AC Power Supply for UCS 5108 Chassis
    PID: UCSB-PSU-2500ACDV
    VID: V01
    Part Number: 341-0571-01
    Vendor: Cisco Systems Inc
    Serial (SN): DTM190304FD
    HW Revision: 0
    Firmware Version: 05.10
    Type: DV
    Wattage (W): 2500
```

```
    Input Source: 210AC 50 380DC
    Current Task:
UCS-A# /chassis/psu # update firmware 05.10
UCS-A# /chassis/psu* # commit-buffer
UCS-A# /chassis/psu #
```

Activating 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

	Command or Action	Purpose
Step 1	UCS-A# **scope chassis** *chassis-id*	Enters chassis mode for the specified chassis.
Step 2	UCS-A /chassis # **scope psu** *psu-id*	Enters PSU mode for the specified PSU.
Step 3	UCS-A /chassis/psu # **activate firmware** *version-num*	Activates the selected firmware version on the PSU.
Step 4	Required: UCS-A /chassis/psu # **commit-buffer**	Commits the transaction. **Note** Committing the transaction resets the end points.

Example

The following example activates the PSU firmware and commits the transaction:

```
UCS-A# scope chassis 1
UCS-A# /chassis # scope psu 2
UCS-A# /chassis/psu # activate firmware 03.10
Warning: When committed this command will reset the end-point
UCS-A# /chassis/psu* # commit-buffer
UCS-A# /chassis/psu #
```

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 M3 and M4 Blade Server Board Controller Firmware

The following guidelines apply to Cisco UCS B-Series M3 and M4 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.

Some Cisco UCS B200 M4 blade servers running on releases prior to Release 2.2(4b) may generate a false Cisco UCS Manager alert, documented in CSCuu15465. This false board controller mismatch alert was resolved in Cisco UCS Manager Capability Catalogs 2.2(4c)T and 2.2(5b)T. You will not see this alert if you use either the 2.2(4c)T or the 2.2(5b)T capability catalog.

Note For more information, refer to https://tools.cisco.com/bugsearch/bug/CSCuu15465

You can apply the capability catalog update as follows:

1. Download 2.2(4c) Infra/Catalog or 2.2(5b) Infra/Catalog software bundle. Obtaining Software Bundles from Cisco, on page 3, provides detailed information about downloading software bundles.
2. Load catalog version 2.2(4c)T or 2.2(5b)T (or the catalog version included) and activate the catalog. Activating a Capability Catalog Update provides detailed information about activating a capability catalog through Cisco UCS Manager.
3. Decommission the newly inserted blade server.
4. Associate the service profile with the host firmware pack policy that has the earlier board controller version.

   When the service profile is associated with the updated host firmware pack policy, any false mismatch alert (such as the one caused by the CSCuu15465 bug) will no longer be raised.
5. Click **Save**.
6. Re-discover the blade server.

Guidelines for Activating Cisco UCS C-Series M3 and M4 Rack Server Board Controller Firmware

The following guidelines apply to Cisco UCS C-Series M3 and M4 rack-server board controller firmware:

- The board controller firmware and the CIMC firmware must be of the same package version.
- When you upgrade the C-Series server firmware for Cisco UCS C220 M4 or C240 M4 servers to Cisco UCS Manager 2.2(6c), you will see the following critical alarm:

```
Board controller upgraded, manual a/c power cycle required on server x
```

This alarm, documented in CSCuv45173, is incorrectly categorized as a critical alarm. It does not impact the functionality of the server, and can be ignored.

To avoid seeing this alarm, you can do one of the following:

- Create a custom host firmware package in Cisco UCS Manager to exclude the board controller firmware from the Cisco UCS Manager 2.2(6c) update and keep the older version.
- Upgrade Cisco UCS Manager infrastructure (A Bundle) to Release 2.2(6c) and continue to run the host firmware (C Bundle) on any Cisco UCS C220 M4 or C240 M4 server at a lower version, according to the mixed firmware support matrix in Table 2 of the *Release Notes for Cisco UCS Manager, Release 2.2*.

Note For more information, refer to https://tools.cisco.com/bugsearch/bug/CSCuv45173.

- 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**.

Activating the Board Controller Firmware on Cisco UCS B-Series M3 and Higher Blade Servers

The board controller firmware controls many of the server functions, including eUSBs, LEDs, and I/O connectors.

Note This activation procedure causes the server to reboot. Depending upon whether the service profile associated with the server includes a maintenance policy, the reboot can occur immediately. Cisco recommends that you upgrade the board controller firmware through the host firmware package in the service profile as the last step of upgrading a Cisco UCS domain, along with upgrading the server BIOS. This reduces the number of times a server needs to reboot during the upgrade process.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope server** *chassis-id / server-id*	Enters chassis server mode for the specified server.
Step 2	UCS-A /chassis/server # **scope boardcontroller**	Enters board controller mode for the server.
Step 3	(Optional) UCS-A /chassis/server/boardcontroller # **show image**	Displays the available software images for the board controller.
Step 4	(Optional) UCS-A /chassis/server/boardcontroller # **show firmware**	Displays the current running software image for the board controller.
Step 5	UCS-A /chassis/server/boardcontroller # **activate firmware** *version-num*	Activates the selected firmware version on the board controller in the server.

	Command or Action	Purpose
Step 6	UCS-A /chassis/server/boardcontroller # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example activates the M3 board controller firmware:

Activating the Board Controller Firmware on a Cisco UCS C-Series M3 and Higher Rack Servers

The board controller firmware controls many of the server functions, including eUSBs, LEDs, and I/O connectors.

Note This activation procedure causes the server to reboot. Depending upon whether the service profile associated with the server includes a maintenance policy, the reboot can occur immediately. Cisco recommends that you upgrade the board controller firmware through the host firmware package in the service profile as the last step of upgrading a Cisco UCS domain, along with upgrading the server BIOS. This reduces the number of times a server needs to reboot during the upgrade process.

The following limitations apply to M3 and higher board controller firmware:

- You must be using Cisco UCS Manager, Release 2.2(1a) or greater.
- 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**.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope server** *server-id*	Enters chassis server mode for the specified server.
Step 2	UCS-A /server # **scope boardcontroller**	Enters board controller mode for the server.
Step 3	(Optional) UCS-A /server/boardcontroller # **show image**	Displays the available software images for the board controller.
Step 4	(Optional) UCS-A /server/boardcontroller # **show firmware**	Displays the current running software image for the board controller.
Step 5	UCS-A /server/boardcontroller # **activate firmware** *version-num*	Activates the selected firmware version on the board controller in the server.
Step 6	UCS-A /server/boardcontroller # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example activates the M3 board controller firmware:

```
UCS-A# scope server 7
UCS-A# /server # scope boardcontroller
UCS-A# /server/boardcontroller # show image
Name                                  Type              Version     State
------------------------------------- ----------------- ---------   -----
ucs-c220-m3-brdprog.3.0.bin           Board Controller    3.0      Active
ucs-c220-m3-brdprog.3.0.bin           Board Controller    3.0       Active

UCS-A# /server/boardcontroller # show firmware
BoardController:
    Running-Vers: N/A
    Package-Vers:
    Activate-Status: Ready

UCS-A# /server/boardcontroller # activate firmware 3.0 force
Warning: When committed this command will reset the end-point.

UCS-A# /server/boardcontroller* # commit-buffer
```