Firmware Management

This chapter includes the following sections:

Overview of Firmware

Cisco UCS uses firmware obtained from and certified by Cisco to upgrade firmware on the following endpoints:

- Endpoints physically located on servers, such as the BIOS, storage controller (RAID controller), and baseboard management controller (BMC)
- Endpoints physically located on adapters, including NIC and HBA firmware, and Option ROM (where applicable)
- I/O modules
- Fabric interconnects
- Cisco UCS Manager

Cisco maintains a set of best practices for managing firmware images and updates in this document and in the following technical note: Unified Computing System Firmware Management Best Practices.

This document uses the following definitions for managing firmware:

Upgrade	Changes the firmware running on an endpoint to another image, such as a release or patch. Upgrade includes both update and activation.
Update	Copies the firmware image to the backup partition on an endpoint.
Activate	Sets the firmware in the backup partition as the active firmware version on the endpoint. Activation can require or cause the reboot of an endpoint.

Image Management

Cisco delivers all firmware updates or packages to Cisco UCS components in images. These images can be the following:

- Component image, which contains the firmware for one component
- Package, which is a collection of component images

Cisco also provides release notes with each image, which you can obtain from the same website from which you obtained the image.

Cisco UCS Manager provides mechanisms to download both component images and packages to the fabric interconnect.

Image Headers

Every 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

Image Catalog

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 packages 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 (were) in each downloaded package.
Images	The images view lists the component images available on the system. You cannot use this view to see packages. 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. Cisco UCS Manager deletes a package after all images in the package have been deleted.

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. If Cisco UCS Manager reports that the bootflash is out of space, delete obsolete images to free up space.

Firmware Upgrades

Cisco UCS firmware is upgraded through a combination of the following methods:

- Direct upgrade at the endpoints. For a cluster configuration with two fabric interconnects, a direct upgrade can be minimally disruptive to data traffic. However, it requires that the Cisco UCS instance does not include firmware policies for those endpoints that you upgrade directly. You cannot avoid disruption to traffic in a Cisco UCS instance with only one fabric interconnection.
- Upgrades to server endpoints through service profiles that include a host firmware package, a management firmware package, or both. This method is disruptive to data traffic and should be performed during a maintenance window.

Note Direct upgrade is not available for all endpoints, including the server BIOS, storage controller, HBA firmware, and HBA option ROM. You must upgrade those endpoints through the host firmware package included in the service profile associated with the server.

Guidelines and Cautions for Firmware Upgrades

Before you upgrade the firmware for any endpoint in a Cisco UCS instance, consider the following guidelines and cautions:

Determine Appropriate Type of Firmware Upgrade for Each Endpoint

Some endpoints, such as adapters and the server BMC, can be upgraded through either a direct firmware upgrade or a firmware package included in a service profile. The configuration of a Cisco UCS instance determines how you upgrade these endpoints. If the service profiles associated with the servers include a host firmware package, upgrade the adapters for those servers through the firmware package. In the same way, if the service profiles associated with the servers include a management firmware package, upgrade the BMC for those servers through the firmware package.

Upgrades of a BMC through a management firmware package or an adapter through a firmware package in the service profile associated with the server take precedence over direct firmware upgrades. You cannot directly upgrade an endpoint if the service profile associated with the server includes a firmware package. To perform a direct upgrade, you must remove the firmware package from the service profile.

No Server or Chassis Maintenance

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

Number of Fabric Interconnects

For a cluster configuration with two fabric interconnects, you can take advantage of the failover between the fabric interconnects and perform a direct firmware upgrade of the endpoints without disrupting data traffic. However, you cannot avoid disrupting data traffic for those endpoints which must be upgraded through a host or management firmware package.

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.

Impact of Activation

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

If a server is not associated with a service profile, the activated firmware moves into 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 an unassociated server to activate the firmware.

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 it and the I/O module, Cisco UCS Manager automatically 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.

For more information about the impact of activation, see Outage Impacts of Direct Firmware Upgrades, page 7.

Cannot Upgrade Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter

The firmware on the Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter (N20-AI0002) is burned into the hardware at manufacture. You cannot upgrade the firmware on this adapter.

Firmware Versions

The firmware versions on an endpoint depend upon the type of endpoint. The endpoints physically located on a fabric interconnect have different versions than those physically located on a server or I/O module.

Firmware Versions in BMC, I/O Modules, and Adapters

Each BMC, I/O module, and adapter has two slots for firmware in flash. Each slot holds a version of firmware. One slot is active and the other is the backup slot. A component boots from whichever slot is designated as active.

The following firmware version terminology is used in Cisco UCS Manager:

Running Version	The running version is the firmware that is active and in use by the endpoint.
Startup Version	The startup version is the firmware that will be used when the endpoint next boots up. Cisco UCS Manager uses the activate operation to change the startup version.
Backup Version	The backup version is the firmware in the other slot and is not in use by the endpoint. This version can be firmware that you have updated to the endpoint but have not yet activated, or it can be an older firmware version that was replaced by a recent activate. Cisco UCS Manager uses the update operation to replace the image in the backup slot.

If the endpoint cannot boot from the startup version, it boots from the backup version.

Firmware Versions in the Fabric Interconnect and Cisco UCS Manager

You can only activate the fabric interconnect firmware and Cisco UCS Manager on the fabric interconnect. The fabric interconnect and Cisco UCS Manager firmware do not have backup versions, because all the images are stored on the fabric interconnect. As a result, the number of bootable fabric interconnect images is not limited to two, like the server BMC and adapters. Instead, the number of bootable fabric interconnect images is limited by the available space in the memory of the fabric interconnect and the number of images stored there.

The fabric interconnect and Cisco UCS Manager firmware have running and startup versions of the kernel and system firmware. The kernel and system firmware must run the same versions of firmware.

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 instance.

You can directly upgrade the firmware on the following endpoints:

- Adapters
- BMC
- I/O modules
- Cisco UCS Manager
- Fabric interconnects

Note Upgrades of a BMC through a management firmware package or an adapter through a firmware package in the service profile associated with the server take precedence over direct firmware upgrades. You cannot directly upgrade an endpoint if the service profile associated with the server includes a firmware package. To perform a direct upgrade, you must remove the firmware package from the service profile.

Stages of a Direct Firmware Upgrade

Cisco UCS Manager separates the direct upgrade process into two stages to ensure 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:

- Adapters
- BMCs
- I/O modules

You can set the update as Startup Version Only to avoid rebooting the endpoint immediately. This allows you to perform the update at any time and then activate and reboot during a maintenance period.

Caution Do not remove the hardware that contains the endpoint or perform any maintenance on it until the update process has completed. If the hardware is removed or otherwise unavailable due to maintenance, the firmware update fails. This failure may 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.

For Cisco UCS Manager and the fabric interconnects, only the activate stage occurs because the specified firmware image already exists on the fabric interconnect. During activation, 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 it and the I/O module, Cisco UCS Manager automatically 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.

Recommended Order of Components for Firmware Activation

If you upgrade firmware by individual components in a Cisco UCS instance, we recommend that you activate the updates in the required order for quicker activation and to avoid potential issues with conflicting firmware versions.

Recommended Order when Updating from Cisco UCS, Release 1.0(2)

1. Adapter (interface card)
2. BMC
3. I/O module
4. Cisco UCS Manager
5. Fabric interconnect

Recommended Order when Updating from Cisco UCS, Release 1.0(1)

1. Adapter (interface card)
2. BMC
3. I/O module
4. Fabric interconnect
5. Cisco UCS Manager

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 instance.

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. Console sessions are not 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 ten minutes to become available after a firmware upgrade.

Outage Impact of a BMC Firmware Upgrade

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

- 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.

Firmware Upgrades through Service Profiles

You can use service profiles to upgrade the server and adapter firmware, including the BIOS on the server, by defining the following policies and including them in the service profile associated with a server:

- Host Firmware Package policy
- Management Firmware Package policy

Note 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 includes the following firmware for server and adapter endpoints:

- Adapter firmware images
- Storage controller firmware images
- Fibre Channel adapter firmware images
- BIOS firmware images
- HBA Option ROM firmware images

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.

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 which 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, which 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.

Prerequisites

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.

Management Firmware Package

This policy enables you to specify a set of firmware versions that make up the management firmware package (also known as a management firmware pack). The management firmware package only includes the baseboard management controller (BMC) on the server. You do not need to use this package if you upgrade the BMC directly.

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

This policy ensures that the BMC firmware is identical on all servers associated with service profiles which use the same policy. Therefore, if you move the service profile from one server to another, the firmware versions are maintained.

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

Prerequisites

This policy is not dependent upon any other policies. However, you must ensure that the appropriate firmware has been downloaded to the fabric interconnect.

Stages of a Firmware Upgrade through Service Profiles

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

Caution 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 and/or management firmware packages and include them in the appropriate firmware policies.
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. For a host firmware package, the server is rebooted to ensure that the endpoints are running the versions specified in the firmware package.

Existing Service Profile

If the service profile is already associated with a server, Cisco UCS Manager upgrades the firmware as soon as you save the changes to the host firmware packages. For a host firmware package, Cisco UCS Manager reboots the server as soon as the change is saved.

Firmware Downgrades

You downgrade firmware in a Cisco UCS instance in the same way that you upgrade firmware. The package or version that you select when you update the firmware determines whether you are performing an upgrade or a downgrade.

Completing the Prerequisites for Upgrading the Firmware

Prerequisites for Upgrading and Downgrading Firmware

All endpoints in a Cisco UCS instance must be fully functional and all processes must be complete before you begin a firmware upgrade or downgrade on those endpoints. You cannot upgrade or downgrade an endpoint that is not in a functional state. For example, the firmware on a server that has not been discovered cannot be upgraded or downgraded. An incomplete process, such as an FSM that has failed after the maximum number of retries, can cause the upgrade or downgrade on an endpoint to fail. If an FSM is in progress, Cisco UCS Manager queues up the update and activation and runs them when the FSM has completed successfully.

Before you upgrade or downgrade firmware in a Cisco UCS instance, complete the following prerequisites:

- Back up the configuration into an All Configuration backup file.
- For a cluster configuration, verify that the high availability status of the fabric interconnects shows that both are up and running.
- For a standalone configuration, verify that the Overall Status of the fabric interconnect is Operable.
- Verify that all servers, I/O modules, and adapters are fully functional. An inoperable server cannot be upgraded.
- Verify that all servers have been discovered. They do not need to be powered on or associated with a service profile.

Creating an All Configuration Backup File

Before You Begin

Obtain the backup server IP address and authentication credentials.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope system**	Enters system mode.
Step 2	UCS-A /system # **create backup** *URL* **all-configuration enabled**}	Creates an enabled All Configuration backup operation that runs as soon as you enter the **commit-buffer** command. The all-configuration option backs up the server, fabric, and system related configuration. Specify the *URL* for the backup file using one of the following syntax: • **ftp:**//*hostname*/*path* • **scp:**//*username@hostname*/*path* • **sftp:**//*username@hostname*/*path* • **tftp:**//*hostname*:*port-num*/*path*

	Command or Action	Purpose
Step 3	UCS-A /system # **commit-buffer**	Commits the transaction.

The following example uses SCP to create an All Configuration backup file on the host named host35 and commits the transaction:

```
UCS-A# scope system
UCS-A /system* # create backup scp://user@host35/backups/all-config.bak all-configuration
enabled
Password:
UCS-A /system* # commit-buffer
UCS-A /system #
```

Verifying the Operability of a Fabric Interconnect

If your Cisco UCS instance is running in a high availability cluster configuration, you must verify the operability of both fabric interconnects.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope fabric-interconnect a** {**a** | **b**}	Enters fabric interconnect mode for the specified fabric interconnect.
Step 2	UCS-A /fabric-interconnect # **show**	Displays information about the fabric interconnect. Verify that the operability of the fabric interconnects is in the Operable state. If the operability is not in the Operable state, run a **show tech-support** command and contact Cisco Technical Support. Do not proceed with the firmware upgrade. For more information about the **show tech-support** command, see the *Cisco UCS Troubleshooting Guide*.

The following example displays that the operability for both fabric interconnects is in the Operable state:

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric-interconnect # show
Fabric Interconnect:
    ID OOB IP Addr     OOB Gateway     OOB Netmask     Operability
    -- --------------- --------------- --------------- -----------
    A  192.168.100.10  192.168.100.20  255.255.255.0   Operable

UCS-A /fabric-interconnect # exit
UCS-A# scope fabric-interconnect b
UCS-A /fabric-interconnect # show
Fabric Interconnect:
    ID OOB IP Addr     OOB Gateway     OOB Netmask     Operability
    -- --------------- --------------- --------------- -----------
    B  192.168.100.11  192.168.100.20  255.255.255.0   Operable
```

Verifying the High Availability Status and Roles of a Cluster Configuration

The high availability status is the same for both fabric interconnects in a cluster configuration.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **show cluster state**	Displays the operational state and leadership role for both fabric interconnects in a high availability cluster. Verify that both fabric interconnects (A and B) are in the Up state and HA is in the Ready state. If the fabric interconnects are not in the Up state or HA is not in the Ready state, run a **show tech-support** command and contact Cisco Technical Support. Do not proceed with the firmware upgrade. For more information about the **show tech-support** command, see the *Cisco UCS Troubleshooting Guide*. Also note which fabric interconnect has the primary role and which has the subordinate role; you will need to know this information to upgrade the firmware on the fabric interconnects.

The following example displays that both fabric interconnects are in the Up state, HA is in the Ready state, fabric interconnect A has the primary role, and fabric interconnect B has the subordinate role:

```
UCS-A# show cluster state
Cluster Id: 0x4432f72a371511de-0xb97c000de1b1ada4

A: UP, PRIMARY
B: UP, SUBORDINATE

HA READY
```

Verifying the Overall Status of an I/O Module

If your Cisco Cisco UCS is running in a high availability cluster configuration, you must verify the status for both I/O modules in all chassis.

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# **show**	Shows the status of the specified I/O module on the specified chassis. Verify that the overall status of the I/O module is in the Operable state. If the overall status is not in the Operable state, run a **show tech-support** command and contact Cisco Technical Support. Do not proceed with the firmware upgrade. For more information about the **show tech-support** command, see the *Cisco UCS Troubleshooting Guide*.

The following example displays that the overall status for both I/O modules on chassis 1 is in the Operable state:

```
UCS-A# scope chassis 1
UCS-A /chassis # scope iom 1
UCS-A /chassis/iom # show
IOM:
    ID         Side  Fabric ID Overall Status
    ---------- ----- --------- --------------
             1 Left  A         Operable

UCS-A /chassis/iom # exit
UCS-A /chassis # scope iom 2
UCS-A /chassis/iom # show
IOM:
    ID         Side  Fabric ID Overall Status
    ---------- ----- --------- --------------
             2 Right B         Operable
```

Verifying the Overall Status of a Server

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope server** *chassis-id/server-id*	Enters chassis server mode for the specified server in the specified chassis.
Step 2	UCS-A /chassis/server # **show status detail**	Shows the status detail of the server. Verify that the overall status of the server is Ok, Unavailable, or any value that does not indicate a failure. If the overall status is in a state that indicates a failure, such as Discovery Failed, the endpoints on that server cannot be upgraded.

The following example displays that the overall status for server 7 on chassis 1 is in the Ok state:

```
UCS-A# scope server 1/7
UCS-A /chassis/server # show status detail
Server 1/7:
    Slot Status: Equipped
    Conn Path: A,B
    Conn Status: A,B
    Managing Instance: B
    Availability: Unavailable
    Admin State: In Service
    Overall Status: Ok
    Oper Qualifier: N/A
    Discovery: Complete
    Current Task:
```

Verifying the Overall Status of an Adapter

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope server** *chassis-id/server-id*	Enters chassis server mode for the specified server in the specified chassis
Step 2	UCS-A /chassis/server # **show adapter status**	Displays the status of the adapter. Verify that the overall status of the adapter is in the Operable state. If the overall status of the adapter is in any state other than Operable, you cannot upgrade it. However, you can proceed with the upgrade for the other adapters in the Cisco UCS instance.

The following example displays that the overall status for the adapter in server 7 on chassis 1 is in the Operable state:

```
UCS-A# scope server 1/7
UCS-A /chassis/server # show adapter status
Server 1/1:
    Overall Status
    --------------
    Operable
```

Obtaining Images from Cisco

Procedure

Step 1 In a web browser, navigate to http://www.cisco.com.

Step 2 Under **Support**, click **Download Software**.

Step 3 Click **Unified Computing**.

Step 4 Enter your Cisco.com username and password to log in.

Step 5 Click **Cisco Unified Computing System**.

Step 6 Click **Unified Computing System (UCS) Complete Software Bundle**.

Step 7 Under the **Latest Releases** folder, click the link for the latest release of Cisco UCS.
Images for earlier releases are archived under the **All Releases** link.

Step 8 Click the Release Notes link to download the latest version of the Release Notes.

Step 9 Click one of the following buttons and follow the instructions provided:

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

Step 10 Follow the prompts to complete your download of the image.

Step 11 Read the Release Notes before upgrading Cisco UCS.

What to Do Next

Download the firmware image to the fabric interconnect.

Downloading a Firmware Package to the Fabric Interconnect

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 package for Cisco UCS. Using the download path provided by Cisco, specify the URL using 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*
Step 3	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.

The following example uses SCP to download the ucs-k9-bundle.1.0.0.988.gbin firmware package.

```
UCS-A# scope firmware
UCS-A /firmware # download image scp://user1@192.168.10.10/images/ucs-k9-bundle.1.0.1.100.gbin
```

What to Do Next

Display the download status to confirm that the firmware package has completely downloaded, and then directly update the firmware at 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.

The following example displays the download status for the ucs-k9-bundle.1.0.0.988.gbin firmware package. The **show download-task** command is entered multiple times until the download state indicates that the firmware package has been downloaded:

```
UCS-A# scope firmware
UCS-A /firmware # show download-task

Download task:
File Name Protocol Server          Userid          State
--------- -------- --------------- --------------- -----
ucs-k9-bundle.1.0.0.988.gbin
          Scp      10.193.32.11    user1           Downloading

UCS-A /firmware # show download-task

Download task:
File Name Protocol Server          Userid          State
--------- -------- --------------- --------------- -----
ucs-k9-bundle.1.0.0.988.gbin
          Scp      10.193.32.11    user1           Downloading

UCS-A /firmware # show download-task

Download task:
File Name Protocol Server          Userid          State
--------- -------- --------------- --------------- -----
ucs-k9-bundle.1.0.0.988.gbin
          Scp      10.193.32.11    user1           Downloaded
```

Directly Upgrading Firmware at Endpoints

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

	Command or Action	Purpose
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.

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

```
UCS-A# scope firmware
UCS-A /firmware # show image
Name                                                 Type                 Version
---------------------------------------------------- -------------------- -------
ucs-2100.1.0.0.988.gbin                              Iom                  1.0(0.988)
ucs-6100-k9-kickstart.4.0.1a.N2.1.0.988.gbin         Switch Kernel
4.0(1a)N2(1.0.988)
ucs-6100-k9-system.4.0.1a.N2.1.0.988.gbin            Switch Software
4.0(1a)N2(1.0.988)
ucs-b200-m1-bios.S5500.86B.01.00.0030-978a.021920.gbin  Server Bios
S5500.86B.01.00.0030-978a.021920
ucs-b200-m1-k9-bmc.1.0.0.988.gbin                    Bmc                  1.0(0.988)
ucs-b200-m1-sasctlr.2009.02.09.gbin                  Storage Controller   2009.02.09
ucs-m71kr-e-cna.1.0.0.988.gbin                       Adapter              1.0(0.988)
ucs-m71kr-e-hba.zf280a4.gbin                         Host Hba             zf280a4
ucs-m71kr-e-optionrom.ZN502N5.gbin                   Host Hba Optionrom   ZN502N5
ucs-m71kr-q-cna.1.0.0.988.gbin                       Adapter              1.0(0.988)
ucs-m71kr-q-optionrom.1.69.gbin                      Host Hba Optionrom   1.69
ucs-m81kr-vic.1.0.0.988.gbin                         Adapter              1.0(0.988)
ucs-manager-k9.1.0.0.988.gbin                        System               1.0(0.988)
```

Updating and Activating the Firmware on an Adapter

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	UCS-A /chassis/server/adapter # **commit-buffer**	(Optional) 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,

	Command or Action	Purpose
		if the firmware update does not complete successfully, the firmware activation will 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	UCS-A /chassis/server/adapter # **show firmware**	(Optional) 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* [**ignorecompcheck** [**set-startup-only**] | **set-startup-only**]	Activates the selected firmware version on the adapter. 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. Use the **ignorecompcheck** keyword if you want to ignore the compatibility check and activate the firmware regardless of any possible incompatibilities or currently executing tasks.
Step 7	UCS-A /chassis/server/adapter # **commit-buffer**	Commits the transaction.
Step 8	UCS-A /chassis/server/adapter # **show firmware**	(Optional) 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.

The following example updates and activates the adapter firmware to version 1.2(1) 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       State
-------------------------------------------------- -------------------- ------------- -----
ucs-m81kr-vic.1.2.1.gbin                          Adapter              1.2(1)        Active

UCS-A# /chassis/server/adapter # update firmware 1.2(1)
UCS-A# /chassis/server/adapter* # activate firmware 1.2(1) ignorecompcheck set-startup-only
UCS-A# /chassis/server/adapter* # commit-buffer
UCS-A# /chassis/server/adapter #
```

The following example updates the adapter firmware to version 1.2(1), verifies that the firmware update completed successfully before starting the firmware activation, activates the adapter firmware, and verifies that the firmware activation completed successfully:

```
UCS-A# scope adapter 1/1/1
UCS-A# /chassis/server/adapter # show image
Name                                               Type                Version       State
-------------------------------------------------- ------------------- ------------- -----
ucs-m81kr-vic.1.2.1.gbin                           Adapter             1.2(1)        Active

UCS-A# /chassis/server/adapter # update firmware 1.2(1)
UCS-A# /chassis/server/adapter* # commit-buffer
UCS-A# /chassis/server/adapter # show firmware
Adapter 1:
    Running-Vers: 1.1(1)
    Update-Status: Updating
    Activate-Status: Ready

UCS-A# /chassis/server/adapter # show firmware
Adapter 1:
    Running-Vers: 1.1(1)
    Update-Status: Ready
    Activate-Status: Ready

UCS-A# /chassis/server/adapter # activate firmware 1.2(1) ignorecompcheck
UCS-A# /chassis/server/adapter* # commit-buffer
UCS-A# /chassis/server/adapter # show firmware
Adapter 1:
    Running-Vers: 1.1(1)
    Update-Status: Ready
    Activate-Status: Activating

UCS-A# /chassis/server/adapter # show firmware
Adapter 1:
    Running-Vers: 1.2(1)
    Update-Status: Ready
    Activate-Status: Ready
```

Updating and Activating the firmware on a BMC

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 bmc**	Enters chassis server BMC mode.
Step 3	UCS-A /chassis/server/bmc # **show image**	Displays the available software images for the adapter.
Step 4	UCS-A /chassis/server/bmc # **update firmware** *version-num*	Updates the selected firmware version on the BMC in the server.
Step 5	UCS-A /chassis/bmc # **commit-buffer**	(Optional) 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

	Command or Action	Purpose
		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 will 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 6	UCS-A /chassis/bmc # **show firmware**	(Optional) 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/bmc # **activate firmware** *version-num* [**ignorecompcheck**]	Activates the selected firmware version on the BMC in the server. Use the **ignorecompcheck** keyword if you want to ignore the compatibility check and activate the firmware regardless of any possible incompatibilities or currently executing tasks.
Step 8	UCS-A /chassis/server/bmc # **commit-buffer**	Commits the transaction.
Step 9	UCS-A /chassis/bmc # **show firmware**	(Optional) 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.

The following example updates and activates the BMC firmware to version 1.2(1) in the same transaction, without verifying that the firmware update and firmware activation completed successfully:

```
UCS-A# scope server 1/1
UCS-A# /chassis/server # scope bmc
UCS-A# /chassis/server/bmc # show image
Name                                               Type                 Version       State
-------------------------------------------------- -------------------- ------------- -----
ucs-b200-m1-k9-bmc.1.2.1.gbin                      Bmc                  1.2(1)        Active

UCS-A# /chassis/server/bmc # update firmware 1.2(1)
UCS-A# /chassis/server/bmc* # activate firmware 1.2(1) ignorecompcheck set-startup-only
UCS-A# /chassis/server/bmc* # commit-buffer
UCS-A# /chassis/server/bmc #
```

The following example updates the BMC firmware to version 1.2(1), verifies that the firmware update completed successfully before starting the firmware activation, activates the BMC firmware, and verifies that the firmware activation completed successfully:

```
UCS-A# scope server 1/1
UCS-A# /chassis/server # scope bmc
UCS-A# /chassis/server/bmc # show image
Name                                               Type                Version       State
-------------------------------------------------- ------------------- ------------- -----
ucs-b200-m1-k9-bmc.1.2.1.gbin                      Bmc                 1.2(1)        Active


UCS-A# /chassis/server/bmc # update firmware 1.2(1)
UCS-A# /chassis/server/bmc* # commit-buffer
UCS-A# /chassis/server/bmc # show firmware
Running-Vers    Update-Status   Activate-Status
--------------- --------------- ---------------
1.1(1)          Updating        Ready

UCS-A# /chassis/server/bmc # show firmware
Running-Vers    Update-Status   Activate-Status
--------------- --------------- ---------------
1.1(1)          Ready           Ready

UCS-A# /chassis/server/bmc # activate firmware 1.2(1) ignorecompcheck
UCS-A# /chassis/server/bmc* # commit-buffer
UCS-A# /chassis/server/bmc # show firmware
Running-Vers    Update-Status   Activate-Status
--------------- --------------- ---------------
1.1(1)          Ready           Activating

UCS-A# /chassis/server/bmc # show firmware
Running-Vers    Update-Status   Activate-Status
--------------- --------------- ---------------
1.2(1)          Ready        Ready
```

Updating an Activating the Firmware on an I/O Module

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

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	UCS-A /chassis/iom # **commit-buffer**	(Optional) Commits the transaction.

	Command or Action	Purpose
		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 will 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 6	UCS-A /chassis/iom # **show firmware**	(Optional) 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* [**ignorecompcheck** [**set-startup-only**] | **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. Use the **ignorecompcheck** keyword if you want to ignore the compatability check and activate the firmware regardless of any possible incompatibilities or currently executing tasks.
Step 8	UCS-A /chassis/iom # **commit-buffer**	Commits the transaction.
Step 9	UCS-A /chassis/iom # **show firmware**	(Optional) 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.

The following example updates and activates the I/O module firmware to version 1.2(1) in the same transaction, without verifying that the firmware update and firmware activation completed successfully:

```
UCS-A# scope chassis 1
UCS-A# /chassis # scope iom 1
UCS-A# /chassis/iom # show image
Name                                     Type                 Version       State
```

```
---------------------------------------------- -------------------- ------------ -----
ucs-2100.1.2.1.gbin                            Iom                  1.2(1)       Active

UCS-A# /chassis/iom # update firmware 1.2(1)
UCS-A# /chassis/iom* # activate firmware 1.2(1) ignorecompcheck set-startup-only
UCS-A# /chassis/iom* # commit-buffer
UCS-A# /chassis/iom #
```

The following example updates the I/O module firmware to version 1.2(1), 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:

```
UCS-A# scope chassis 1
UCS-A# /chassis # scope iom 1
UCS-A# /chassis/iom # show image
Name                                           Type                 Version       State
---------------------------------------------- -------------------- ------------ -----
ucs-2100.1.2.1.gbin                            Iom                  1.2(1)       Active

UCS-A# /chassis/iom # update firmware 1.2(1)
UCS-A# /chassis/iom* # commit-buffer
UCS-A# /chassis/iom # show firmware
IOM      Fabric ID Running-Vers    Update-Status   Activate-Status
-------- --------- --------------- --------------- ---------------
       1 A         1.1(1)          Updating        Ready

UCS-A# /chassis/iom # show firmware
IOM      Fabric ID Running-Vers    Update-Status   Activate-Status
-------- --------- --------------- --------------- ---------------
       1 A         1.1(1)          Ready           Ready

UCS-A# /chassis/iom # activate firmware 1.2(1) ignorecompcheck
UCS-A# /chassis/iom* # commit-buffer
UCS-A# /chassis/iom # show firmware
IOM      Fabric ID Running-Vers    Update-Status   Activate-Status
-------- --------- --------------- --------------- ---------------
       1 A         1.1(1)          Ready           Activating

UCS-A# /chassis/iom # show firmware
IOM      Fabric ID Running-Vers    Update-Status   Activate-Status
-------- --------- --------------- --------------- ---------------
       1 A         1.2(1)          Ready           Ready
```

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 the UCS Manager (system).
Step 3	UCS-A /system # **activate firmware** *version-num* [**ignorecompcheck**]	Activates the selected firmware version on the system. Use the **ignorecompcheck** keyword if you want to ignore the compatibility check and activate the firmware regardless of any possible incompatibilities or currently executing tasks.

	Command or Action	Purpose
		Note Activating the 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 disconnects all active sessions, logs out all users, and then activates the software. When the upgrade is complete, you are prompted to log back in.

The following example upgrades the UCS Manager to version 1.2(1) and commits the transaction:

```
UCS-A# scope system
UCS-A# /system # show image
Name                                               Type             Version     State
-------------------------------------------------- ---------------- ----------- -----
ucs-manager-k9.1.2.1.gbin                          System           1.2(1)      Active

UCS-A# /system # activate firmware 1.2(1)
UCS-A# /system* # commit-buffer
UCS-A# /system #
```

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, page 12.

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 instance, you must know the running kernel version and the running system version. If you do not plan to create additional accounts, we recommend 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.

	Command or Action	Purpose
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.

The following example upgrades the fabric interconnect to version 4.0(1a)N2(1.2.1) and commits the transaction:

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric-interconnect # show image
Name                                        Type                 Version           State
------------------------------------------- -------------------- ----------------- -----
ucs-6100-k9-kickstart.4.0.1a.N2.1.2.1.gbin   Fabric Interconnect  4.0(1a)N2(1.2.1)  Active
ucs-6100-k9-system.4.0.1a.N2.1.2.1.gbin      Fabric Interconnect  4.0(1a)N2(1.2.1)  Active

UCS-A /fabric-interconnect # activate firmware kernel-version 4.0(1a)N2(1.2.1) system-version
 4.0(1a)N2(1.2.1)
UCS-A /fabric-interconnect* # commit-buffer
UCS-A /fabric-interconnect #
```

Updating Firmware through Service Profiles

Configuring a Host Firmware Package

Caution If the policy is included in one or more service profiles that is associated with a server, as soon as you save the host firmware package policy, Cisco UCS Manager updates and activates the firmware in the server and adapter with the new versions and reboots the server.

Before You Begin

Ensure that the appropriate firmware has been 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	UCS-A /org/fw-host-pack # **set descr** *description*	(Optional) Provides a description for the host firmware package.

	Command or Action	Purpose
		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** | **host-hba** | **host-hba-combined** | **host-hba-optionrom** | **host-nic** | **server-bios** | **storage-controller** | **unspecified**} *version-num*	Creates a package image for the host firmware package and enters organization firmware host package image mode. 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 firmware version must match the model numbers (PID) on the servers that are associated with this firmware pack. If you select a firmware version with the wrong model number, Cisco UCS Manager cannot install the firmware update.
Step 5	UCS-A org/fw-host-pack/pack-image # **set version** *version-num*	(Optional) Specifies the package image version number. Changing this number triggers firmware updates on all components using the firmware through a service profile. Use this step is only when updating a host firmware package, not when creating a package. **Note** The host firmware package can contain multiple package images. Repeat steps 5 and 6 create additional package images for other components.
Step 6	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.

The following example creates the app1 host firmware package, creates a storage controller package image with version 2009.02.09 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 UCS storage-controller 2009.02.09
UCS-A /org/fw-host-pack/pack-image* # commit-buffer
UCS-A /org/fw-host-pack/pack-image #
```

What to Do Next

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

Configuring a Management Firmware Package

Caution If the policy is included in a one or more service profiles that is associated with a server, as soon as you save the management firmware package policy, Cisco UCS Manager updates and activates the BMC firmware in the server with the new version.

Before You Begin

Ensure that the appropriate firmware has been 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-mgmt-pack** *pack-name*	Creates a management firmware package with the specified package name and enters organization firmware management package mode.
Step 3	UCS-A /org/fw-mgmt-pack # **set descr** *description*	(Optional) Provides a description for the management 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-mgmt-pack # **create pack-image** *hw-vendor-name hw-model* **bmc** *version-num*	Creates a package image for the management firmware package and enters organization firmware management package image mode. 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 firmware version must match the model numbers (PID) on the servers that are associated with this firmware pack. If you select a firmware version with the wrong model number, Cisco UCS Manager cannot install the firmware update.
Step 5	UCS-A org/fw-mgmt-pack/pack-image # **set version** *version-num*	(Optional) Specifies the package image version number. Changing this number triggers firmware updates on all components using the firmware through a service profile. Use this step is only when updating a host firmware package, not when creating a package.
Step 6	UCS-A org/fw-mgmt-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.

The following example creates the bmc1 host firmware package, creates a BMC package image with version 1.0(0.988) firmware, and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # create fw-mgmt-pack bmc1
UCS-A /org/fw-mgmt-pack* # set descr "This is a management firmware package example."
UCS-A /org/fw-mgmt-pack* # create pack-image Cisco UCS bmc 1.0(0.988)
UCS-A /org/fw-mgmt-pack/pack-image* # commit-buffer
UCS-A /org/fw-mgmt-pack/pack-image #
```

What to Do Next

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