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 components:

- Servers, including the BIOS, storage controller, and server controller (BMC)
- 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 the following technical note: Unified Computing System Firmware Management Best Practices.

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 Updates

You can use any of the Cisco UCS Manager interfaces to update firmware in the system, including Cisco UCS Manager GUI and the Cisco UCS Manager CLI.

You can use either of the following methods to update the firmware:

- Direct update at the endpoints.
- Updates to server components through service profiles that include a host firmware package policy and a management firmware package policy.

Note Direct update is not available for some server components, such as BIOS and storage controller.

Firmware Versions

The firmware versions on a component depend upon the type of component.

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 the GUI and CLI:

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

If the component cannot boot from the startup version, the component boots from the backup version.

Firmware Versions in the Fabric Interconnect and Cisco UCS Manager

You can update 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 flash memory.

Note There are running and startup versions of the fabric interconnect and Cisco UCS Manager firmware, but there are no backup versions.

Direct Firmware Update at Endpoints

You can perform direct firmware updates on the following endpoints:

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

Note You cannot update the BIOS firmware directly. You must perform the BIOS firmware update through a host firmware package in a service profile. If the BIOS fails, you can use Cisco UCS Manager to recover the BIOS.

Stages of a Direct Firmware Update

Cisco UCS Manager separates the direct update process into stages to ensure that you can push the firmware to a component while the system is running without affecting uptime on the server or other components. Because you do not need to reboot the server until after you activate, you can perform that task overnight or during other maintenance periods.

When you manually update firmware, the following stages occur:

Update

During this stage, the system pushes the selected firmware version to the component. The update process always overwrites the firmware in the backup slot on the component. The update stage applies only to I/O modules, BMCs, and adapters.

Activate

During this stage, the system sets the specified image version (normally the backup version) as active and reboots the endpoint. When the endpoint is rebooted, the backup slot becomes the active slot, and the active slot becomes the backup slot. The firmware in the new active slot becomes the startup version and the running version.

If the component cannot boot from the startup firmware, it defaults to the backup version and raises an alarm.

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 following order for quicker activation:

1. Adapter
2. BMC
3. I/O module
4. Fabric interconnect or Cisco UCS Manager

Note Consider the following when activating the firmware:

- You can update all components in parallel.
- While activating adapters and I/O modules, you can use the set-startup-only option to set the startup version and skip the reset.
- Activating a fabric interconnect resets the fabric interconnect and all I/O modules connected to it.

Outage Impacts of Direct Firmware Updates

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

Outage Impact of a Fabric Interconnect Firmware Update

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

- The fabric interconnect restarts.
- The corresponding I/O modules restart.

Outage Impact of a Cisco UCS Manager Firmware Update

A firmware update to Cisco UCS Manager disrupts Cisco UCS Manager GUI, but not Cisco UCS Manager CLI. The following disruptions occur in Cisco UCS Manager GUI during a firmware update:

- All users logged into Cisco UCS Manager GUI are logged out and their sessions ended.
- Any unsaved work in progress is lost.

Outage Impact of an I/O Module Firmware Update

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

- I/O modules restart when the corresponding fabric interconnect is updated.
- An I/O module can take a few minutes to become available after a firmware update.

Outage Impact of a BMC Firmware Update

When you update the firmware for a BMC in a server, you impact only the BMC and internal processes. You do not interrupt server traffic. This firmware update 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 Update

When you activate the firmware for an adapter, you cause the following outage impacts and disruptions:

- The server resets.
- Server traffic is disrupted.

Firmware Updates through Service Profiles

You can use service profiles to update 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 update the firmware on an I/O module, fabric interconnect, or Cisco UCS Manager through service profiles. You must update the firmware on those components directly.

Host Firmware Pack

This policy enables you to specify a common set of firmware versions that make up the host firmware pack. The host firmware includes the following server and adapter components:

- BIOS
- SAS controller
- Emulex Option ROM (applicable only to Emulex-based Converged Network Adapters [CNAs])
- Emulex firmware (applicable only to Emulex-based CNAs)
- QLogic option ROM (applicable only to QLogic-based CNAs)
- Adapter firmware

The firmware pack 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 of the component in the firmware pack, 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 update and completes the association.

Management Firmware Pack

This policy enables you to specify a common set of firmware versions that make up the management firmware pack. The management firmware includes the server controller (BMC) on the server.

The firmware pack 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 Update through Service Profiles

If you use policies in service profiles to update server and adapter firmware, you must complete 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.

Associate

During this stage, you include a firmware policy in a service profile, and then associate the service profile with a server. The system pushes the selected firmware versions to the endpoints and reboots to ensure that the endpoints are running the versions specified in the firmware pack.

When the firmware versions in the policies change, the system performs firmware updates (wherever necessary), activates, and reboots the endpoints.

Caution As this type of update requires a reboot of the endpoints, it can be disruptive.

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.

Obtaining Images from Cisco

Procedure

Step 1 In a web browser, navigate to the web link provided by Cisco to obtain firmware images for Cisco UCS.

Step 2 Choose one or more firmware images and copy them to a network server.

Step 3 Read the release notes provided with the image or images.

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.

Display 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** 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 Updating Firmware at Endpoints

Display 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.

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 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.

	Command or Action	Purpose
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 # **activate firmware** *version-num*	Activates the selected firmware version on the adapter.
Step 5	UCS-A /chassis/server/adapter # **commit-buffer**	Commits the transaction.

The following example updates and activates the adapter firmware to version 1.0(0.988):

```
UCS-A# scope adapter 1/3/1
UCS-A# /chassis/server/adapter # show image
Name                                               Type                 Version      State
-------------------------------------------------- -------------------- ------------ -----
ucs-m71kr-e-cna.1.0.0.988.gbin                     Adapter              1.0(0.988)   Active
ucs-m71kr-q-cna.1.0.0.988.gbin                     Adapter              1.0(0.988)   Active
ucs-m81kr-vic.1.0.0.988.gbin                           Adapter          1.0(0.988)   Active
UCS-A# /chassis/server/adapter # update firmware 1.0(0.988)
UCS-A# /chassis/server/adapter* # activate firmware 1.0(0.988)
UCS-A# /chassis/server/adapter* # commit-buffer
UCS-A# /chassis/server/adapter #
```

Updating 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 # **update firmware** *version-num*	Updates the selected firmware version on the BMC in the server.
Step 4	UCS-A /chassis/server/bmc # **activate firmware** *version-num*	Activates the selected firmware version on the BMC in the server.
Step 5	UCS-A /chassis/server/bmc # **commit-buffer**	Commits the transaction.

The following example updates and activates the BMC firmware to version 1.0(0.988):

```
UCS-A# scope server 1/3
UCS-A# /chassis/server # scope bmc
UCS-A# /chassis/server/bmc* # update firmware 1.0(0.988)
UCS-A# /chassis/server/bmc* # activate firmware 1.0(0.988)
UCS-A# /chassis/server/bmc* # commit-buffer
UCS-A# /chassis/server/bmc #
```

Updating an I/O Module

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 # **activate firmware** *version-num*	Activates the selected firmware version on the I/O module.
Step 6	UCS-A /chassis/iom # **commit-buffer**	Commits the transaction.

The following example upgrades the I/O module to version 1.0(0.988):

```
UCS-A# scope chassis 1
UCS-A# /chassis # scope iom 1
UCS-A# /chassis/iom # show image
Name                                               Type                Version       State
-------------------------------------------------- ------------------- ------------- -----
ucs-2100.1.0.0.988.gbin                            Iom                 1.0(0.988)    Active
UCS-A# /chassis/iom # update firmware 1.0(0.988)
UCS-A# /chassis/iom* # activate firmware 1.0(0.988)
UCS-A# /chassis/iom* # commit-buffer
UCS-A# /chassis/iom #
```

Updating a Fabric Interconnect

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.

The following example upgrades the fabric interconnect to version 4.0(1a)N2(1.0.988):

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric-interconnect # show image
Name                                               Type                Version     State
-------------------------------------------------- ------------------- ----------- -----
ucs-6100-k9-kickstart.4.0.1a.N2.1.0.988.gbin       Switch Kernel       4.0(1a)N2(1.0.988)
                                                                                   Active
ucs-6100-k9-system.4.0.1a.N2.1.0.988.gbin          Switch Software     4.0(1a)N2(1.0.988)
                                                                                   Active
UCS-A /fabric-interconnect # activate firmware kernel-version 4.0(1a)N2(1.0.988)
system-version 4.0(1a)N2(1.0.988)
UCS-A /fabric-interconnect* # commit-buffer
```

Updating the UCS Manager

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 optional **ignorecompcheck** keyword to have the system ignore the compatibility check. **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.

The following example upgrades the UCS Manager to version 1.0(0.988):

```
UCS-A# scope system
UCS-A# /system # show image
Name                                               Type             Version     State
-------------------------------------------------- ---------------- ----------- -----
ucs-manager-k9.1.0.0.988.gbin                      System           1.0(0.988)  Active
UCS-A# /system # activate firmware 1.0(0.988)
UCS-A# /system* # commit-buffer
UCS-A# /system #
```

Updating Firmware through Service Profiles

Configuring a Host Firmware Pack

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 pack with the specified package name and enters organization firmware host pack mode.
Step 3	UCS-A /org/fw-host-pack # **set descr** *description*	(Optional) Provides a description for the host firmware pack. **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 pack and enters organization firmware host pack 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.
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 pack, not when creating a pack. **Note** The host firmware pack 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.

The following example creates the app1 host firmware pack, 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 pack 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 Pack

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 pack with the specified package name and enters organization firmware management pack mode.
Step 3	UCS-A /org/fw-mgmt-pack # **set descr** *description*	(Optional) Provides a description for the management firmware pack. **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 pack and enters organization firmware management pack 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.
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 pack, not when creating a pack.

	Command or Action	Purpose
Step 6	UCS-A org/fw-mgmt-pack/pack-image # **commit-buffer**	Commits the transaction.

The following example creates the bmc1 host firmware pack, 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 pack 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.