UpgradingFirmwarethroughFirmwarePackages in Service Profiles

This chapter includes the following sections:

Firmware Upgrades through Firmware Packages in Service Profiles

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

If the default host firmware pack is updated, and the server is not associated with a service profile, the server reboots and new firmware is applied. This behavior is not managed by the Firmware Auto Sync Server policy because it is only for recently discovered servers.

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.

Note Cisco UCS no longer supports the creation of new management firmware packages. You can modify and update existing management firmware packages, if desired. However, we recommend that you remove the management firmware packages from all service profiles and use host firmware packages to update the Cisco Integrated Management Controller (CIMC) on the servers.

Host Firmware Package

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

- **Adapter**
- **Server BIOS**
- **CIMC**
- **Board Controller**
- **Flex Flash Controller**
- **Graphics Card**
- **Host HBA**
- **Host HBA Option ROM**
- **Host NIC**
- **Host NIC Option ROM**
- **Local Disk**

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

To update local disk firmware, always include the **Blade Package** in the host firmware package. The blade package contains the local disk firmware for blade and rack servers.

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

Remember To update local disk firmware for blade or rack servers, always include the blade package in the host firmware package. The blade package contains the local disk firmware for both blade and rack servers.

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

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

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

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

This policy ensures that the host firmware is identical on all servers associated with service profiles 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.

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

Note Cisco UCS no longer supports the creation of new management firmware packages. You can modify and update existing management firmware packages, if desired. However, we recommend that you remove the management firmware packages from all service profiles and use host firmware packages to update the Cisco Integrated Management Controller (CIMC) on the servers.

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 includes the Cisco Integrated Management Controller (CIMC) on the server. You do not need to use this package if you upgrade the CIMC directly.

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

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 Firmware Packages in Service Profiles

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

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

New Service Profile

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

Firmware Package Policy Creation

During this stage, you create the host firmware packages.

Service Profile Association

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

Existing Service Profile

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

Effect of Updates to Firmware Packages in Service Profiles

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

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

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

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

Creating or Updating a Host Firmware Package

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

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

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

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

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 2	UCS-A org/ # **create fw-host-pack** *pack-name*	Creates a host firmware package with the specified package name and enters organization firmware host package mode.
Step 3	UCS-A /org/fw-host-pack # **set descr** *description*	(Optional) Provides a description for the host firmware package. **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any **show** command output.
Step 4	UCS-A org/fw-host-pack # **create pack-image** "*hw-vendor-name*" "*hw-model*" {**adapter** | **board-controller** | **cimc** | **graphics-card** | **host-hba** |	Creates a package image for the host firmware package and enters organization firmware host package image mode. The *hw-vendor-name* must match the full name of the vendor, and must begin and end with quotation

	Command or Action	Purpose
	host-hba-optionrom | **host-nic** | **local-disk** | **raid-controller** | **server-bios**} "*version-num*"	marks. The *hw-vendor-name* and *hw-model* values are labels that help you easily identify the package image when you enter the **show image detail** command. The *version-num* value specifies the version number of the firmware being used for the package image. The model and model number (PID) must match the servers that are associated with this firmware package. If you select the wrong model or model number, Cisco UCS Manager cannot install the firmware update.
Step 5	UCS-A org/fw-host-pack # **create exclude-server-component** {**adapter** | **board-controller** | **cimc** | **flexflash-controller** | **graphics-card** | **host-hba** | **host-hba-optionrom** | **host-nic** | **host-nic-optionrom** | **local-disk** | **psu** | **raid-controller** | **sas-expander** | **server-bios** | **storage-controller-onboard-device** | **storage-controller-onboard-device-cpld** | **storage-device-bridge** | **unspecified**	Excludes the specified component from the host firmware package. **Note** **local-disk** is excluded from the host firmware package by default.
Step 6	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 only when updating a host firmware package, not when creating a package. **Note** The host firmware package can contain multiple package images. Repeat Step 4, and Step 5, to create additional package images for other components.
Step 7	UCS-A org/fw-host-pack/pack-image # **commit-buffer**	Commits the transaction. Cisco UCS Manager verifies the model numbers and vendor against all servers associated with service profiles that include this policy. If the model numbers and vendor match a firmware version in the policy, Cisco UCS Manager updates the firmware according to the settings in the maintenance policies included in the service profiles.

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

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

```
UCS-A /org/fw-host-pack/pack-image* # commit-buffer
UCS-A /org/fw-host-pack/pack-image #
```

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

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

What to Do Next

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

Updating a Management Firmware Package

Note Cisco UCS no longer supports the creation of new management firmware packages. You can modify and update existing management firmware packages, if desired. However, we recommend that you remove the management firmware packages from all service profiles and use host firmware packages to update the Cisco Integrated Management Controller (CIMC) on the servers.

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

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 2	UCS-A org/ # **scope fw-mgmt-pack** *pack-name*	Scope to 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.

	Command or Action	Purpose
Step 4	UCS-A org/fw-mgmt-pack # **create pack-image** "*hw-vendor-name*" "*hw-model*" **cimc** "*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 model and model number (PID) must match the servers that are associated with this firmware package. If you select the wrong model or model number, Cisco UCS Manager cannot install the firmware update.
Step 5	UCS-A org/fw-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 only when updating a 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 according to the settings in the maintenance policies included in the service profiles.

The following example updates the cimc1 host firmware package, creates a CIMC package image with version 1.0(0.988) firmware, and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # scope fw-mgmt-pack cimc1
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 Systems Inc" "SB-1600-CTRL" cimc
"2.3(200.166)"
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.