Overview of Upgrading from Cisco UCS, Release 1.0(2)

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.

Firmware Upgrade to Cisco UCS, Release 1.1(1)

The firmware upgrade to Cisco UCS, Release 1.1(1) must be planned with scheduled maintenance windows. With this firmware upgrade, you should expect the following:

- With a cluster configuration, data traffic disruption of up to one minute. Failover between the fabric interconnects prevents the longer disruption required for the fabric interconnects and I/O modules to reboot.
- With a standalone fabric interconnect, data traffic disruption of up to one minute for the servers to reboot and approximately ten minutes for the fabric interconnect and I/O module to reboot.

This firmware upgrade requires 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.

Required Order of Steps When Upgrading from Release 1.0(2) to Release 1.1(1)

When you upgrade from Cisco UCS, Release 1.0(2) to Release 1.1(1), upgrade the components in the following order. If you do not follow this order, the firmware upgrade may fail and the servers may experience communication issues with Cisco UCS Manager. In addition, the order of steps in this document and the recommended options minimize the disruption to data traffic.

1. Adapter (interface card)—If you plan to upgrade the adapters directly, perform this step first. However, if you prefer, you can omit this step and upgrade the adapters as part of the last step, in a host firmware package.
2. BMC—If you upgrade the adapters in the host firmware package, perform this step first.
3. I/O module.
4. Cisco UCS Manager.
5. Fabric interconnect.
6. Host firmware package—Must be the last step in the upgrade process. You must upgrade the BIOS and storage controller firmware during this step.

Guidelines and Cautions for Upgrading to Cisco UCS, Release 1.1(1)

Before you update 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 Partial Upgrades

We recommend that all endpoints in a Cisco UCS instance be updated to the same firmware release. New functionality and fixes within a firmware release for one endpoint may have dependencies upon the same functionality and fixes within another endpoint. Therefore, a mix of firmware releases can cause performance or other issues during ordinary usage, or may cause the update to fail.

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.

Do Not Activate All Endpoints Simultaneously

Do not select **ALL** from the **Filter** drop-down list in the **Activate Firmware** dialog box to activate all endpoints simultaneously. Many firmware releases and patches have dependencies that require the endpoints to be activated in a specific order for the firmware update to succeed. This order can change depending upon the contents of the release or patch. Activating all endpoints does not guarantee that the updates occur in the

required order and can disrupt communications between the endpoints and the fabric interconnects and Cisco UCS Manager. For information about the dependencies in a specific release or patch, see the release notes provided with that release or patch.

Impact of Activation

During a direct upgrade, you should configure **Set Startup Version Only** for an adapter or an I/O module. With this setting, the activated firmware moves into the pending-next-boot state, and the endpoint is not immediately rebooted. Cisco UCS Manager activates the firmware the next time the endpoint 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 6.

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.

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.