Overview of Upgrading to Release 1.4(3)

This chapter includes the following sections:

Overview of Firmware

Cisco UCS uses firmware obtained from and certified by Cisco to support the endpoints in a Cisco UCS instance. Each endpoint is a component in the instance that requires firmware to function. The upgrade order for the endpoints in a Cisco UCS instance depends upon the upgrade path, but includes the following:

- Cisco UCS Manager
- I/O modules
- Fabric interconnects
- Endpoints physically located on adapters, including NIC and HBA firmware, and Option ROM (where applicable) that can be upgraded through firmware packages included in a service profile
- Endpoints physically located on servers, such as the BIOS, storage controller (RAID controller), and Cisco Integrated Management Controller (CIMC) that can be upgraded through firmware packages included in a service profile

See the required order of steps for your upgrade path to determine the appropriate order in which to upgrade the endpoints in your Cisco UCS instance.

Note Beginning with Cisco UCS, Release 1.4(1), Cisco is releasing firmware upgrades in multiple bundles, rather than one large firmware package. For more information see Firmware Image Management, on page 2.

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.

For Management Extensions and Capability Catalog upgrades, update and activate occur simultaneously. You only need to update or activate those upgrades. You do not need to perform both steps.

Note For more information about firmware management and upgrades of individual components, see the Cisco UCS Manager Configuration Guides.

Firmware Image Management

Cisco delivers all firmware updates to Cisco UCS components in bundles of images. Cisco UCS firmware updates are available to be downloaded in the following bundles:

Cisco UCS Infrastructure Software Bundle

This bundle includes the following firmware images that are required to update the following components:

- Cisco UCS Manager software
- Kernel and system firmware for the fabric interconnects
- I/O module firmware

Cisco UCS B-Series Blade Server Software Bundle

This bundle includes the following firmware images that are required to update the firmware for the blade servers in a Cisco UCS instance. In addition to the bundles created for a release, these bundles can also be released between infrastructure bundles to enable Cisco UCS Manager to support a blade server that is not included in the most recent infrastructure bundle.

- CIMC firmware
- BIOS firmware
- Adapter firmware
- Board controller firmware
- Third-party firmware images required by the new server

Cisco UCS C-Series Rack-Mount Server Software Bundle

This bundle includes the following firmware images that are required to update components on rack-mount servers that have been integrated with and are managed by Cisco UCS Manager:

- CIMC firmware
- BIOS firmware
- Adapter firmware
- Storage controller firmware

Note You cannot use this bundle for standalone C-series servers. The firmware management system in those servers cannot interpret the header required by Cisco UCS Manager. For information on how to upgrade standalone C-series servers, see the C-series configuration guides.

Cisco also provides release notes, which you can obtain on the same website from which you obtained the bundles.

Firmware 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 CIMC, I/O Modules, and Adapters

Each CIMC, 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 recently activated version. 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 CIMC 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.

Firmware Upgrade to Cisco UCS, Release 1.4

The firmware upgrade to Cisco UCS, Release 1.4(3) from Release 1.4(2) should be planned with scheduled maintenance windows if necessary to accommodate data disruption of up to one minute for the servers to reboot after endpoint activation and the updated host firmware package is applied.

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 1.4(1) or 1.4(2)

Note If you do not follow this order, the firmware upgrade may fail and the servers may experience communication issues with Cisco UCS Manager.

The order of steps in this document and the recommended options minimize the disruption to data traffic. Therefore, when you upgrade from any version of release 1.4 to a later version of release 1.4, upgrade the components in the following order.

1. Download the following firmware images:
   - Cisco UCS Infrastructure Software Bundle—Required for all Cisco UCS instances.
   - Cisco UCS B-Series Blade Server Software Bundle—Required for all Cisco UCS instances that include blade servers.
   - Cisco UCS C-Series Rack-Mount Server Software Bundle—Only required for Cisco UCS instances that include integrated rack-mount servers. This bundle contains firmware to enable Cisco UCS Manager to manage those servers and is not applicable to standalone C-Series rack-mount servers.
2. (Optional) Disable Call Home—If the Cisco UCS instance includes Call Home or Smart Call Home, disable Call Home to ensure you do not receive unnecessary alerts when Cisco UCS Manager restarts components.
3. Update adapters, CIMC, and IOMs—If you prefer, you can upgrade the adapters in a host firmware package as part of the last upgrade step.
4. Activate adapters—Choose **Ignore Compatibility Check** and **Set Startup Version Only** when performing this step.
5. Activate CIMC—Choose **Ignore Compatibility Check** when performing this step.
6. Activate Cisco UCS Manager—Choose **Ignore Compatibility Check** when performing this step.
7. Activate I/O modules—Choose **Ignore Compatibility Check** and **Set Startup Version Only** when performing this step.
8. Activate subordinate fabric interconnect—Choose **Ignore Compatibility Check** when performing this step.
9. Verify that the data path has been restored.
10. Activate primary fabric interconnect—Choose **Ignore Compatibility Check** when performing this step.
11. Update management firmware package(s) for servers—You do not need to perform this step if you updated and activated the CIMC on the servers directly.
12. Update host firmware package(s) for servers—Must be the last firmware upgraded. We recommend that you upgrade the board controller firmware during this step to avoid an additional reboot of servers with that firmware. You must upgrade the following firmware in a host firmware package:
    - BIOS
    - Storage controller
    - Certain adapters

13 (Optional) Enable Call Home—If you disabled Call Home before the upgrading the firmware, enable Call Home.

Required Order of Steps for Adding a Cisco UCS B230 Server

When you add the first B230 server, you must perform the steps in the following order to add support in Cisco UCS Manager for the server:

1 If you have not already done so, upgrade the Cisco UCS instance to Release 1.4(1) or later.

2 Insert the blade server into the chassis as described in the server installation guide.

3 Wait for Cisco UCS Manager to discover the new server. If server discovery does not begin within a few minutes, acknowledge the server.

Note You do not need to update the Management Extensions or Capability Catalog to add a B230 server. The required support is included in each Cisco UCS, Release 1.4 infrastructure bundle.

Required Order of Steps for Integrating a Cisco UCS Rack-Mount Server

After you complete the upgrade of the existing Cisco UCS components, you can integrate a Cisco UCS rack-mount server. When you integrate a rack-mount server, you must perform the steps in the following order:

1 If you have not already done so, configure the rack server discovery policy in Cisco UCS Manager.

2 Follow the instructions in the server installation guide for installing and integrating a rack-mount server in a system managed by Cisco UCS Manager.

3 Wait for Cisco UCS Manager to discover the new server. If server discovery does not begin within a few minutes, acknowledge the server.

Cautions, Guidelines, and Best Practices for Upgrading Cisco UCS

Before you update the firmware for any endpoint in a Cisco UCS instance, consider the following cautions, guidelines, and best practices.

Configuration Changes and Settings that Can Impact Upgrades

Depending upon the configuration of your Cisco UCS instance, the following changes may require you to make configuration changes after you upgrade. To avoid faults and other issues, we recommend that you make any required changes before you upgrade.

All Connectivity May Be Lost During Upgrades if vNIC Failover and NIC Teaming Are Both Enabled

All connectivity may be lost during firmware upgrades if you have configured both **Enable Failover** on one or more vNICs and you have also configured NIC teaming/bonding at the host operating system level. Please design for availability by using one or the other method, but never both.

To determine whether you have enabled failover for one or more vNICs in a Cisco UCS Cisco UCS instance, verify the configuration of the vNICs within each service profile associated with a server. For more information, see the Cisco UCS Manager configuration guide for the release that you are running.

VLAN 4048 is Reserved in Releases 1.4(1) and Higher

As of Release 1.4(1), VLAN 4048 is a reserved VLAN. If your Cisco UCS instance is configured to use VLAN 4048, you must reconfigure that VLAN to use a different ID before you upgrade.

Impact of Upgrade to Release 1.3(1i) or Higher

An upgrade from an earlier Cisco UCS firmware release to release 1.3(1i) or higher has the following impact on the Protect Configuration property of the local disk configuration policy the first time servers are associated with service profiles after the upgrade:

Unassociated Servers

After you upgrade the Cisco UCS instance, the initial server association proceeds without configuration errors whether or not the local disk configuration policy matches the server hardware. Even if you enable the Protect Configuration property, Cisco UCS does not protect the user data on the server if there are configuration mismatches between the local disk configuration policy on the previous service profile and the policy in the new service profile.

Note If you enable the Protect Configuration property and the local disk configuration policy encounters mismatches between the previous service profile and the new service profile, all subsequent service profile associations with the server are blocked.

Associated Servers

Any servers that are already associated with service profiles do not reboot after the upgrade. Cisco UCS Manager does not report any configuration errors if there is a mismatch between the local disk configuration policy and the server hardware.

When a service profile is disassociated from a server and a new service profile associated, the setting for the Protect Configuration property in the new service profile takes precedence and overwrites the setting in the previous service profile.

Hardware-Related Guidelines and Best Practices for Firmware Upgrades

The hardware in a Cisco UCS instance can impact how you upgrade. Before you upgrade any endpoint, consider the following guidelines and best practices:

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.

Avoid Replacing RAID-Configured Hard Disks Prior to Upgrade

Under the following circumstances, Cisco UCS Manager may scrub all data on a hard disk as part of the RAID synchronization process during an upgrade of the server firmware:

- The hard disks in the server are configured for RAID.
- One or more of the RAID-configured hard disks in the server are removed.
- The hard disk or disks are replaced with hard disks that are configured with a pre-existing RAID and the local disk configuration policy included in the service profile on the server is not used to configure those hard disks.
- The server firmware is upgraded, causing the server to reboot and Cisco UCS Manager to begin the RAID synchronization process.

If the original hard disks contained vital data that needs to preserved, avoid inserting new hard disks that are already configured for RAID.

Always Upgrade Cisco UCS Gen-2 Adapters through a Host Firmware Package

You cannot upgrade Cisco UCS Gen-2 adapters directly at the endpoints. You must upgrade the firmware on those adapters through a host firmware package.

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

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

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.

Firmware- and Software-Related Best Practices for Upgrades

Before you upgrade any endpoint, consider the following guidelines and best practices:

No Partial Upgrades

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

Determine Appropriate Type of Firmware Upgrade for Each Endpoint

Some endpoints, such as adapters and the server CIMC, 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 CIMC for those servers through the firmware package.

Upgrades of a CIMC 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.

Do Not Activate All Endpoints Simultaneously in Cisco UCS Manager GUI

If you use Cisco UCS Manager GUI to update the firmware, 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 for Adapters and I/O Modules

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 remains in the pending-next-boot state. Cisco UCS Manager does not reboot the endpoints or activate the firmware until the server is associated with a service profile. If necessary, you can manually reboot or reset an unassociated server to activate the firmware.

When you configure **Set Startup Version Only** for an I/O module, the I/O module is rebooted when the fabric interconnect in its data path is rebooted. If you do not configure **Set Startup Version Only** for an I/O module, the I/O module reboots and disrupts traffic. In addition, if Cisco UCS Manager detects a protocol and firmware version mismatch between the fabric interconnect and the I/O module, Cisco UCS Manager automatically updates the I/O module with the firmware version that matches the firmware in the fabric interconnect and then activates the firmware and reboots the I/O module again.

Select Ignore Compatibility Check When Upgrading

During a direct upgrade to a newer release, we recommend that you choose **Ignore Compatibility Check**. Newer releases may have incompatible code with older releases. This option ensures that the upgrade can proceed and avoids compatibility issues.

Disable Call Home before Upgrading to Avoid Unnecessary Alerts (Optional)

When you upgrade a Cisco UCS instance, Cisco UCS Manager restarts the components to complete the upgrade process. This restart causes events that are identical to service disruptions and component failures that trigger Call Home alerts to be sent. If you do not disable Call Home before you begin the upgrade, you can ignore the alerts generated by the upgrade-related component restarts.

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 CIMC Firmware Upgrade

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

- Any activities being performed on the server through the KVM console and vMedia are interrupted.

- Any monitoring or IPMI polling is interrupted.

Outage Impact of an Adapter Firmware Upgrade

If you activate the firmware for an adapter and do not configure the **Set Startup Version Only** option, you cause the following outage impacts and disruptions:

- The server reboots.
- Server traffic is disrupted.