



Overview of Upgrading to Release 2.0

This chapter includes the following sections:

- [Overview of Firmware, page 1](#)
- [Firmware Image Management, page 2](#)
- [Firmware Versions, page 3](#)
- [Firmware Upgrade to Cisco UCS, Release 2.0, page 4](#)

Overview of Firmware

Cisco UCS uses firmware obtained from and certified by Cisco to support the endpoints in a Cisco UCS domain. Each endpoint is a component in the Cisco UCS domain that requires firmware to function. The upgrade order for the endpoints in a Cisco UCS domain 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 domain.



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.

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 to fabric interconnects in a Cisco UCS domain 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 domain. 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 UCS-Managed 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 version terminology used depends upon the type of endpoint, as follows:

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 2.0

The firmware upgrade to Cisco UCS, Release 2.0 needs to be planned with scheduled maintenance windows for standalone fabric interconnects. With this firmware upgrade, you should expect the following data traffic interruptions:

- With a cluster configuration, no data traffic disruption if the correct sequence of steps is followed. 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 domain does not include firmware policies for those endpoints that you upgrade directly. You cannot avoid disruption to traffic in a Cisco UCS domain with only one fabric interconnect.



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.

- Upgrades to server endpoints through service profiles that include a host firmware package, a management firmware package, or both. This method can be disruptive to data traffic and should be performed during a maintenance window.

Cautions, Guidelines, and Limitations for Firmware Upgrades

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

**Note**

The Cisco UCS Manager GUI does not allow you to choose options that a release does not support. If a Cisco UCS domain includes hardware that is not supported in the release to which you are upgrading, Cisco UCS Manager GUI does not display the firmware as an option for that hardware or allow you to upgrade to it.

Configuration Changes and Settings that Can Impact Upgrades

Depending upon the configuration of your Cisco UCS domain, 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.

Impact of Upgrade to Cisco UCS, Release 2.1(2) and Higher on Initiator IQNs Defined at the Service Profile Level

If there are two iSCSI vNICs and both use the same initiator IQN (which is supported in Cisco UCS Release 2.0(1)), upgrading creates a single service profile level initiator IQN and resets the initiator IQNs on the iSCSI vNICs to have no value.

If the same initiator IQNs are used in iSCSI vNICs across service profiles in Cisco UCS Release 2.0(1), the upgrade creates duplicate initiator IQNs at the service profile level. This configuration generates faults for each iSCSI vNIC that has a duplicate initiator IQN defined at the service profile level. Changing the duplicate initiator IQNs at the service profile level clears these faults. You must clear these faults before you perform any service profile related operations, such as updating a host firmware package.

Default Maintenance Policy Should be Configured for User Acknowledgment

The default maintenance policy is configured to immediately reboot the server when disruptive changes are made to the service profile, such as server firmware upgrades through a host maintenance policy. We recommend that you change the reboot policy setting in the default maintenance policy to user acknowledgment to avoid unexpected disruption of server traffic.

When you configure the reboot policy in the default maintenance policy to User Ack, the list of disruptive changes are listed with the pending activities. You can then control when the servers are rebooted.

Overlapping FCoE VLAN IDs and Ethernet VLAN IDs Are No Longer Allowed with Cisco UCS Release 2.0 and Higher



Caution

In Cisco UCS 1.4 and earlier releases, Ethernet VLANs and FCoE VLANs could have overlapping VLAN IDs. However, starting with Cisco UCS release 2.0, overlapping VLAN IDs are not allowed. If Cisco UCS Manager detects overlapping VLAN IDs during an upgrade, it raises a critical fault. If you do not reconfigure your VLAN IDs, Cisco UCS Manager raises a critical fault and drops Ethernet traffic on the overlapped VLANs. Therefore, we recommend that you ensure there are no overlapping Ethernet and FCoE VLAN IDs before you upgrade to Cisco UCS Release 2.2.

Be aware that when an uplink trunk is configured with VLAN ID 1 defined and set as the native VLAN, changing the Ethernet VLAN 1 ID to another value can cause network disruption and flapping on the fabric interconnects, resulting in an HA event that introduces a large amount of traffic and makes services temporarily unavailable.

If you did not explicitly configure the FCoE VLAN ID for a VSAN in Cisco UCS 1.4 and earlier releases, Cisco UCS Manager assigned VLAN 1 as the default FCoE VLAN for the default VSAN (with default VSAN ID 1). In those releases, VLAN 1 was also used as the default VLAN for Ethernet traffic. Therefore, if you accepted the default VLAN ID for the FCoE VLAN and one or more Ethernet VLANs, you must reconfigure the VLAN IDs for either the FCoE VLAN(s) on the VSAN(s) or the Ethernet VLAN(s).

For a new installation of Cisco UCS Release 2.2, the default VLAN IDs are as follows:

- The default Ethernet VLAN ID is 1.
- The default FCoE VLAN ID is 4048.

After an upgrade from Cisco UCS Release 1.4, where VLAN ID 4048 was used for FCoE storage port native VLAN, to release 2.0, the default VLAN IDs are as follows:

- The default Ethernet VLAN ID is 1.
- The current default FCoE VLAN ID is preserved. Cisco UCS Manager raises a critical fault on the conflicting Ethernet VLAN, if any. You must change one of the VLAN IDs to a VLAN ID that is not used or reserved.



Note

If a Cisco UCS domain uses one of the default VLAN IDs, which results in overlapping VLANs, you can change one or more of the default VLAN IDs to any VLAN ID that is not used or reserved. From release 2.0 and higher, VLANs with IDs from 3968 to 4047 are reserved.

VSANs with IDs in the Reserved Range are not Operational

A VSAN with an ID in the reserved range is not operational after an upgrade. Make sure that none of the VSANs configured in Cisco UCS Manager are in these reserved ranges:

- If you plan to use FC switch mode in a Cisco UCS domain, do not configure VSANs with an ID in the range from 3040 to 4078.
- If you plan to use FC end-host mode in a Cisco UCS domain, do not configure VSANs with an ID in the range from 3840 to 4079.

If a VSAN has an ID in the reserved range, change that VSAN ID to any VSAN ID that is not used or reserved.

IQN Names Must Be Unique for Each iSCSI vNIC

If a Cisco UCS domain is configured for iSCSI boot, before you upgrade from Cisco UCS, Release 2.0(1) to Release 2.0(2) or higher, you must ensure that all iSCSI vNICs used across multiple service profiles have unique initiator names. Changing initiator names also involves storage side configuration, which is beyond the scope of this document.

Cisco provides a script for Cisco UCS PowerTool that identifies duplicate IQN names within a Cisco UCS domain. For more information, see [Obtaining Cisco UCS Power Tool and Running the Duplicate IQN Script](#).

If you do not ensure that all iSCSI vNICs have unique names across all service profiles before you upgrade, Cisco UCS Manager raises a fault on the iSCSI vNICs to warn you that duplicate IQNs are present. Also, if you do not ensure that there are no duplicate IQN names within a service profile (for example, the same name used for both iSCSI vNICs), Cisco UCS reconfigures the service profile to have a single IQN. For information on how to clear this fault and reconfigure the duplicate IQNs, see the [Cisco UCS B-Series Troubleshooting Guide](#).

Impact of Upgrade from a Release Prior to Release 1.3(1i)

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 domain, 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 Limitations for Firmware Upgrades

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

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 During or Prior to Upgrade

During or prior to Cisco UCS infrastructure and server firmware upgrades:

- Do not remove, insert or replace any local storage hard disks or SSDs in the servers.
- Ensure that no storage operations are running, including Rebuild, Association, Copyback, BGI, and so on.

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 Guidelines and Limitations for Upgrades

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

Determine the 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 domain 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.

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

When you upgrade a Cisco UCS domain, 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 domain.

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.

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.

Summary of Steps for Upgrading from Release 2.0



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 2.0, upgrade the components in the following order.

- 1 Complete all prerequisite steps, as described in [Prerequisites for Upgrading and Downgrading Firmware](#).

- 2 Obtain the following firmware images from Cisco.com and download them to the fabric interconnect. For more information, see [Downloading the Cisco UCS, Release 2.1 Firmware](#).
 - Cisco UCS Infrastructure Software Bundle—Required for all Cisco UCS domains.
 - Cisco UCS B-Series Blade Server Software Bundle—Required for all Cisco UCS domains that include blade servers.
 - Cisco UCS C-Series Rack-Mount UCS-Managed Server Software Bundle—Only required for Cisco UCS domains 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.
- 3 (Optional) Disable Call Home—If the Cisco UCS domain includes Call Home or Smart Call Home, disable Call Home to ensure you do not receive unnecessary alerts when Cisco UCS Manager restarts components.
- 4 Update adapters, CIMC, and IOMs—If you prefer, you can upgrade the CIMC and the adapters in a host firmware package as part of the last upgrade step. Certain adapters must be upgraded in a host firmware package.
- 5 Activate adapters—Choose **Ignore Compatibility Check** and **Set Startup Version Only** when performing this step.
- 6 Activate CIMC—Choose **Ignore Compatibility Check** when performing this step.
- 7 Activate Cisco UCS Manager—Choose **Ignore Compatibility Check** when performing this step.
- 8 Activate the I/O modules—Choose **Ignore Compatibility Check** and **Set Startup Version Only** when performing this step.
- 9 Activate the subordinate fabric interconnect—Choose **Ignore Compatibility Check** when performing this step.
- 10 To avoid control plane disruption, manually failover the primary fabric interconnect to the fabric interconnect that has already been upgraded.
- 11 Verify that the data path has been restored.
- 12 Activate the primary fabric interconnect—Choose **Ignore Compatibility Check** when performing this step.
- 13 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.
- 14 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. While some of these components can be upgraded directly at the endpoint, such as the BIOS on M3 servers, we recommend that you upgrade the following firmware in a host firmware package:
 - BIOS
 - Storage controller
 - Certain adapters

For information on how to upgrade these endpoints directly, see the [Cisco UCS Manager Configuration Guides](#).

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