Overview

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 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.

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.

Cross-Version Firmware Support

Cisco UCS allows cross-version firmware support. For information about which Cisco UCS Manager A bundle software (Cisco UCS Manager, Cisco NX-OS, IOM firmware) can be mixed with the previous release's B or C bundles on the servers (host firmware (FW), BIOS, CIMC, adapter FW and drivers), see the Release Notes for Cisco UCS Software for your particular release.

In Cisco UCSM Release 2.2 and later releases, the adapter firmware version is different from the Cisco UCSM Release version.

Important If you implement cross-version firmware, you must ensure that the configurations for the Cisco UCS domain are supported by the firmware version on the server endpoints.

Firmware Auto Sync for FI Cluster

Addition of a secondary Fabric Interconnect to form a cluster – either as a replacement or a conversion from standby to HA requires the infrastructure bundle firmware versions to match. Administrators today manually upgrade/downgrade the replacement FI to the correct version before they connect it to the cluster. Firmware Auto Sync allows the users to automatically upgrade/downgrade the infrastructure bundle to the same version as the survivor FI when the replacement is added as standby to HA. The software package is the UCS software/firmware that resides on the FI.

Software and Hardware Requirements

The software package on the survivor FI should be greater than or equal to Cisco UCS Release 1.4. The model numbers of the Fabric Interconnects should be same. For example, firmware Auto Sync will not trigger for a combination of 61XX and 62XX FI models that are being setup for HA.

Implementation

With the earlier implementation, the user would compulsorily configure the replacement FI as standalone mode if there was a mismatch in the version of software packages. The replacement FI is manually upgraded/downgraded to the same version of software package on survivor FI through the usual upgrade/downgrade process. Then the replacement FI is added to the cluster since the upgrade/downgrade of the replacement FI is a manual process.

The user is now given an additional option of synchronization of the software packages of the replacement FI with the survivor FI along with the current option. If the user decides to Auto Sync the firmware, the software packages of the survivor FI are copied to the replacement FI. The software packages on the replacement FI are then activated and the FI is added to the cluster. The sync-up of the Cisco UCSM database and the configuration happens via the usual mechanisms once the HA cluster is formed successfully.

Firmware Auto Sync Benefits

In a UCS cluster where one Fabric Interconnect has failed, the Auto Sync feature ensures that the software package of the replacement FI is brought up to the same revision of the survivor. The whole process requires minimal end user interaction while providing clear and concise feedback during the procedure.

Options for Firmware Upgrades

You can upgrade Cisco UCS firmware through one or more of the following methods:

Note For a summary of steps and the required order in which to perform them in order to upgrade one or more Cisco UCS domains from one release to another, see the Cisco UCS upgrade guide for that upgrade path. If an upgrade guide is not provided for upgrading from a particular release, contact Cisco Technical Assistance Center as a direct upgrade from that release may not be supported.

Upgrading a Cisco UCS domain through Cisco UCS Manager

If you want to upgrade a Cisco UCS domain through the Cisco UCS Manager in that domain, you can choose one of the following upgrade options:

- Upgrade infrastructure and servers with Auto Install—This option upgrades all infrastructure components in the first stage. Then you can upgrade all server endpoints through host firmware packages in the second stage.
- Upgrade servers through firmware packages in service profiles—This option enables you to upgrade all server endpoints in a single step, reducing the amount of disruption caused by a server reboot. You can combine this option with the deferred deployment of service profile updates to ensure that server reboots occur during scheduled maintenance windows.
- Direct upgrades of infrastructure and server endpoints—This option enables you to upgrade many infrastructure and server endpoints directly, including the fabric interconnects, I/O modules, adapters, and board controllers. However, direct upgrade is not available for all endpoints, including the server BIOS, storage controller, HBA firmware, HBA option ROM and local disk. You must upgrade those endpoints through the host firmware package included in the service profile associated with the server.

Note The Cisco UCS Manager CLI does not allow you to upgrade hardware that is not supported in the release to which you are upgrading, Cisco UCS Manager CLI displays an error message if you attempt to upgrade hardware to an unsupported release.

Upgrading a Cisco UCS domain through Cisco UCS Central

If you have registered one or more Cisco UCS domains with Cisco UCS Central, you can manage and upgrade all firmware components in the domain through Cisco UCS Central. This option allows you to centralize the control of firmware upgrades and ensure that all Cisco UCS domains in your data center are the required levels.

You can use Cisco UCS Central to upgrade the capability catalog, infrastructure, and server endpoints in all registered Cisco UCS domains that are configured for global firmware management.

Firmware Upgrades through Auto Install

Auto Install enables you to upgrade a Cisco UCS domain to the firmware versions contained in a single package in the following two stages:

- Install Infrastructure Firmware—Uses the Cisco UCS Infrastructure Software Bundle to upgrade the infrastructure components, such as the fabric interconnects, the I/O modules, and Cisco UCS Manager.
- Install Server Firmware—Uses the Cisco UCS B-Series Blade Server Software Bundle to upgrade all blade servers in the Cisco UCS domain and/or the Cisco UCS C-Series Rack-Mount UCS-Managed Server Software Bundle to upgrade all rack servers.

These two stages are independent and can be run or scheduled to run at different times.

You can use Auto Install to upgrade the infrastructure components to one version of Cisco UCS and server components to a different version.

Note You cannot use Auto Install to upgrade either the infrastructure or the servers in a Cisco UCS domain if Cisco UCS Manager in that domain is at a release prior to Cisco UCS 2.1(1). However, after you upgrade Cisco UCS Manager to Release 2.1(1) or greater, you can use Auto Install to upgrade the remaining components in a Cisco UCS domain that is at the minimum required firmware level. For more information, see *Cautions, Guidelines, and Limitations for Upgrading with Auto Install* and the appropriate Cisco UCS upgrade guide.

Install Infrastructure Firmware

Install Infrastructure Firmware upgrades all infrastructure components in a Cisco UCS domain, including Cisco UCS Manager, and all fabric interconnects and I/O modules. All components are upgraded to the firmware version included in the selected Cisco UCS Infrastructure Software Bundle.

Install Infrastructure Firmware does not support a partial upgrade to only some infrastructure components in a Cisco UCS domain domain.

You can schedule an infrastructure upgrade for a specific time to accommodate a maintenance window. However, if an infrastructure upgrade is already in progress, you cannot schedule another infrastructure upgrade. You must wait until the current upgrade is complete before scheduling the next one.

Note You can cancel an infrastructure firmware upgrade if it is scheduled to occur at a future time. However, you cannot cancel an infrastructure firmware upgrade after the upgrade has begun.

Install Server Firmware

Install Server Firmware uses host firmware packages to upgrade all servers and their components in a Cisco UCS domain. All servers whose service profiles include the selected host firmware packages are upgraded to the firmware versions in the selected software bundles, as follows:

- Cisco UCS B-Series Blade Server Software Bundle for all blade servers in the chassis.
- Cisco UCS C-Series Rack-Mount UCS-Managed Server Software Bundle for all rack-mount servers that are integrated into the Cisco UCS domain.

Note You cannot cancel a server firmware upgrade process after you complete the configuration in the **Install Server Firmware** wizard. Cisco UCS Manager applies the changes immediately. However, the timing of the actual reboot of servers occurs depends upon the maintenance policy in the service profile associated with the server.

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.

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.	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.
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.

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 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.

Firmware Management in Cisco UCS Central

Cisco UCS Central enables you to manage all firmware components for all registered Cisco UCS domains.

Note To manage Cisco UCS domains firmware from Cisco UCS Central, you must enable the global firmware management option in Cisco UCS Manager. You can enable the global firmware management option when you register Cisco UCS Manager with Cisco UCS Central. You can also turn global management option on or off based on your management requirements.

The Cisco UCS domains are categorized into domain groups in Cisco UCS Central for management purposes. You can manage firmware for each domain group separately at the domain group level or for all domain groups from the domain group root. Cisco UCS Central provides you the option to manage the following Cisco UCS domain firmware packages:

- **Capability Catalog—** One capability catalog per domain group . All Cisco UCS domains registered to a particular domain group will use the capability catalog defined in the domain group.
- **Infrastructure Firmware—** One infrastructure firmware policy per domain group . All Cisco UCS domains registered to a particular domain group will use the same Infrastructure firmware version defined in the domain group.
- **Host Firmware—** You can have more than one host firmware policy for the different host firmware components in a domain group. The Cisco UCS domainsregistered in the domain group will be able to choose any defined host firmware policy in the group. Cisco UCS Central provides you the option to upgrade the host firmware globally to all Cisco UCS domains in a domain group at the same time.

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 domain.

You can directly upgrade the firmware on the following endpoints:

- Adapters
- CIMCs
- I/O modules
- Board controllers
- Cisco UCS Manager
- Fabric interconnects

The adapter and board controller firmware can also be upgraded through the host firmware package in the service profile. If you use a host firmware package to upgrade this firmware, you can reduce the number of times a server needs to be rebooted during the firmware upgrade process.

Note 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.

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
- CIMCs
- I/O modules

Caution Do not remove the hardware that contains the endpoint or perform any maintenance on it until the update process completes. If the hardware is removed or otherwise unavailable due to maintenance, the firmware update fails. This failure might 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.

The following endpoints only require activation because the specified firmware image already exists on the endpoint:

- Cisco UCS Manager
- Fabric interconnects
- Board controllers on those servers that support them

When the firmware is activated, 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 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.

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.

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 Manager Release 2.2

Scenarios for Firmware Upgrade to Cisco UCS Manager Release 2.2

Upgrading the Infrastructure software bundle (A bundle) directly to Cisco UCS Manager Release 2.2(x) is supported from Release 2.1(1) and later releases. While upgrading from releases earlier than Release 2.1(1), you must upgrade to Release 2.1(1) first for A, B, and C bundles, and then upgrade to Release 2.2(x).

The following table lists the upgrade paths for various Cisco UCS Manager releases.

Table 1: Upgrade Paths to Release 2.2

Upgrade From Release	Upgrade To Release	Recommended Upgrade Path
1.4(x)	2.2(x)	Upgrading directly to Release 2.2(x) is not supported from this release. To upgrade to Release 2.2(x), do the following in order: **1** Upgrade the Infrastructure A bundle to Release 2.0(1). **2** Upgrade the B and C bundles for all servers to Release 2.0(1). **3** Upgrade the Infrastructure A bundle to Release 2.1(1). **4** Upgrade the B and C bundles for all servers to Release 2.1(1). **5** Upgrade the Infrastructure A bundle to Release 2.2(x).
2.0(x)	2.2(x)	Upgrading directly to Release 2.2(x) is not supported from this release. To upgrade to Release 2.2(x), do the following in order: **1** Upgrade the Infrastructure A bundle to Release 2.1(1). **2** Upgrade the B and C bundles for all servers to Release 2.1(1). **3** Upgrade the Infrastructure A bundle to Release 2.2(x).
2.1(x)	2.2(x)	Upgrade directly to Release 2.2(x).

Firmware Downgrades

You downgrade firmware in a Cisco UCS domain 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.

Important

- You never need to downgrade the board controller firmware.
- The board controller firmware in Cisco UCS B-Series blade servers is not designed to be downgraded. When you are performing a full system firmware downgrade operation, if the system displays this error message “Error: Update failed: Server does not support board controller downgrade”, it is safe to ignore the error message and continue with downgrading system firmware. UCS Manager will automatically skip over the board controller firmware and continue with the downgrade of the other firmware components.
- The board controller firmware version of the blade server should be the same as or later than the installed software bundle version. Leaving the board controller firmware at a later version than the version that is currently running in your existing Cisco UCS environment does not violate the software matrix or TAC supportability.
- Board controller firmware updates are backward compatible with the firmware of other components.

Note The Cisco UCS Manager CLI does not allow you to downgrade hardware that is not supported in the release to which you are downgrading, Cisco UCS Manager CLI displays an error message if you attempt to downgrade hardware to an unsupported release.

Firmware Downgrade with Intel® Xeon® Processor E5-2600 v4 Product Family or TPM 2.0

In a Cisco UCS configuration with UCS B200 M4, C220 M4, or C240 M4 servers and either the Intel® Xeon® Processor E5-2600 v4 Product Family or TPM 2.0, the downgrade process will fail in the following scenarios:

- When you initiate downgrade for the CMC, BIOS, or the B and C bundles to a release before Cisco UCS Manager Release 2.2(7), Cisco UCS Manager will not initiate the downgrade process. An error message will be displayed, which will state that you cannot downgrade to the specified CIMC, BIOS or B or C bundles because it does not support the processor or TPM type installed on this server.
- When you initiate downgrade for Cisco UCS Manager first and then for the B and C bundles to a release before Cisco UCS Manager Release 2.2(7), BIOS and CIMC downgrade will be successful, but will fail in the FSM.

Firmware Downgrades and Auto Install

You cannot use Auto Install to downgrade a Cisco UCS domain to a Cisco UCS release that is earlier than Release 2.1.

Unsupported Features Must Be Removed Before Downgrade

If you plan to downgrade a Cisco UCS domain to an earlier release, you must first remove and unconfigure all features from the current release that are not supported in the earlier release and correct all failed configurations.

Note If you attempt to downgrade without removing or unconfiguring all features that are not supported in the earlier release, the downgrade will fail with the following message: "This operation is not supported for UCSM version below 2.1."

For example, if you plan to downgrade a Cisco UCS domain from Cisco UCS, Release 2.1 to Release 2.0, you must first remove or unconfigure unsupported features, such as VLAN port count optimization and correct service profile configuration that are failing due to iSCSI-related issues.

For example, if you plan to downgrade a Cisco UCS domain from Cisco UCS, Release 2.1 to Release 1.4, you must first remove or unconfigure unsupported features, such as the following:

- iSCSI configurations, including iSCSI vNICs and initiator IQNs from objects such as service profiles, service profiles templates, boot order policies, and LAN connectivity policies.
- FCoE uplink ports
- FCoE storage ports
- Unified uplink ports
- Appliance storage ports

If you downgrade a Cisco UCS domain with a Cisco UCS 2232PP FEX from Cisco UCS Release 2.1 and later releases to Release 1.4 without decommissioning and removing the 2232PP FEX, the DME process will crash and Cisco UCS Manager will become unresponsive.

SNMP Must be Disabled Before Downgrade

You must disable SNMP before downgrading from Cisco UCS Manager Release 2.2(8) to an earlier release. The downgrade process does not begin until SNMP is disabled.

Firmware Downgrades and Initiator IQN Settings

If an initiator IQN has been defined at the service profile level, downgrading from Cisco UCS, Release 2.1(2) to Cisco UCS, Release 2.0(1) copies the initiator IQN to all of the initiator IQNs defined at the iSCSI vNIC level.

If an initiator IQN has been defined at the service profile level and only one iSCSI vNIC is present in the service profile, downgrading from Cisco UCS, Release 2.1(2) to Cisco UCS Release 2.1(1) or below copies the service profile level initiator IQN to the initiator IQN defined at the iSCSI vNIC level.

If multiple iSCSI vNICs exist, downgrading to Cisco UCS, Release 2.0(2) through 2.1(1) generates an error message that the same initiator IQN cannot be copied to all of the initiator IQNs defined at the iSCSI vNIC level.

Unregister from Cisco UCS Central

If you downgrade Cisco UCS from Release 2.1(2) to any of the previous releases, and if you have this Cisco UCS domain registered in Cisco UCS Central, you must unregister the Cisco UCS domain from Cisco UCS Central before the downgrade.

Recommended Order of Steps for Firmware Downgrades

If you need to downgrade the firmware to an earlier release, we recommend that you do it in the following order:

1. Retrieve the configuration backup from the release to which you want to downgrade that you created when you upgraded to the current release.
2. Remove or unconfigure the features that are not supported in the release to which you want to downgrade.
3. Downgrade the Cisco UCS domain.
4. Perform an erase-config.
5. Import the configuration backup from the release to which you downgraded.