



Cautions, Guidelines, and Limitations

This chapter includes the following sections:

- [Cautions, Guidelines, and Limitations for Firmware Upgrades, page 1](#)
- [Cautions, Guidelines, and Limitations for Managing Firmware in Cisco UCS Central, page 8](#)

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.

Clear any faults before you upgrade the firmware.

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 4030 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.

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 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.

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.



Note

If the internal power sequencer firmware for NX-OS is updated as part of the Cisco UCS upgrade process, then the fabric interconnect will boot to the loader prompt. Power-cycle the fabric interconnect in order to continue.

Unsupported Hardware Leads to Discovery Failure

When you add new servers or adapters to an existing Cisco UCS system with a Cisco UCS Manager release that does not support these servers and adapters, discovery of the system fails. The FSM displays an error message that the server or adapter is not supported on the current UCS firmware version. To resolve this issue, do one of the following:

- Update the Capability Catalog to the latest compatible release
- Upgrade the Cisco UCS Manager infrastructure firmware to the version required by the new hardware. The hardware support matrix in the Release Notes provides compatibility details.

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.

Cautions, Guidelines, and Limitations for Upgrading with Auto Install

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



Note

These guidelines are specific to Auto Install and are in addition to those listed in [Cautions, Guidelines, and Limitations for Firmware Upgrades](#), on page 1.

State of the Endpoints

Before you begin an upgrade, all affected endpoints must be in the following state:

- For a cluster configuration, verify that the high availability status of the fabric interconnects shows that both are up and running.
- For a standalone configuration, verify that the Overall Status of the fabric interconnect is Operable.
- For all endpoints to be upgraded, verify that they are in an Operable state.
- For all servers to be upgraded, verify that all the servers have been discovered and that discovery did not fail. Install Server Firmware will fail if any server endpoints cannot be upgraded.

Recommendations for the Default Host Firmware Policy

After you upgrade Cisco UCS Manager, a new host firmware policy named "default" is created, and assigned to all service profiles that did not already include a host firmware policy. The default host firmware policy is blank. It does not contain any firmware entries for any components. This default policy is also configured for an immediate reboot rather than waiting for user acknowledgment before rebooting the servers.

During the upgrade of server firmware, you can add firmware for the blade and rack mount servers in the Cisco UCS domain to the default host firmware policy. To complete the upgrade, all servers must be rebooted.

Every service profile that is assigned the default host firmware policy reboots the associated server according to the maintenance policy included in the service profile. If the maintenance policy is set to immediate reboot, you cannot cancel the upgrade or prevent the servers from rebooting after you complete the configuration in the **Install Server Firmware** wizard. We recommend that you verify the maintenance policy associated with these service profiles to ensure that they are set for a timed reboot or for user acknowledgment.



Note

If you are upgrading from a release prior to 2.1(2a), you may be impacted by CSCup57496. After manually upgrading the CIMC and associating a service profile, remove the Management Firmware pack to activate the firmware of CIMC. For more information, please refer to <https://tools.cisco.com/bugsearch/bug/CSCup57496>.

Time, Date, and Time Zone on Fabric Interconnects Must Be Identical

To ensure that the fabric interconnects in a cluster configuration are in sync, you must ensure that they are configured for the same date, time, and time zone. We recommend that you configure an NTP server and the correct time zone in both fabric interconnects. If the date, time or time zone in the fabric interconnects are out of sync, the Auto Install might fail.

Cannot Upgrade Infrastructure and Server Firmware Simultaneously

You cannot upgrade the infrastructure firmware at the same time as you upgrade server firmware. We recommend that you upgrade the infrastructure firmware first and then upgrade the server firmware. Do not begin the server firmware upgrade until the infrastructure firmware upgrade is completed.

Required Privileges

Users must have the following privileges to upgrade endpoints with Auto Install:

Privileges	Upgrade Tasks User Can Perform
admin	<ul style="list-style-type: none"> • Run Install Infrastructure Firmware • Run Install Server Firmware • Add, delete, and modify host firmware packages
Service profile compute (ls-compute)	Run Install Server Firmware
Service profile server policy (ls-server-policy)	Add, delete, and modify host firmware packages
Service profile config policy (ls-config-policy)	Add, delete, and modify host firmware packages

Impact of Host Firmware Packages and Management Firmware Packages on Install Server Firmware

Because Install Server Firmware uses host firmware packages to upgrade the servers, you do not have to upgrade all servers in a Cisco UCS domain to the same firmware versions. However, all servers which have associated service profiles that include the host firmware packages you selected when you configured Install Server Firmware are upgraded to the firmware versions in the specified software bundles.

If the service profiles associated with servers include a management firmware package as well as a host firmware package, Install Server Firmware uses the firmware version in the management firmware package to upgrade the CIMC on the servers. The CIMC is not upgraded to the firmware version in the host firmware package, even if it is a more recent version of the CIMC than the one in the management firmware package. If you want to use the host firmware packages to upgrade the CIMC in the servers, you must remove the management firmware packages from the associated service profiles.

Effect of Using Install Server Firmware on Servers Whose Service Profiles Do Not Include a Host Firmware Package

If you use Install Server Firmware to upgrade server endpoints on servers that have associated service profiles without host firmware packages, Install Server Firmware uses the default host firmware package to upgrade the servers. You can only update the default host firmware package through Install Server Firmware.

If you want to upgrade the CIMC or adapters in a server with an associated service profile that has previously been updated through the default host firmware package in Install Server Firmware, you must use one of the following methods:

- Use Install Server Firmware to modify the default host firmware package and then upgrade the server through Install Server Firmware.
- Create a new host firmware package policy, assign it to the service profile associated with the server, and then upgrade the server through that host firmware package policy.
- Disassociate the service profile from the server and then directly upgrade the server endpoints.

Upgrading Server Firmware on Newly Added Servers

If you add a server to a Cisco UCS domain after you run Install Server Firmware, the firmware on the new server is not automatically upgraded by Install Server Firmware. If you want to upgrade the firmware on a newly added server to the firmware version used when you last ran Install Server Firmware, you must manually upgrade the endpoints to upgrade the firmware on that server. Install Server Firmware requires a change in firmware version each time. You cannot rerun Install Server Firmware to upgrade servers to the same firmware version.

**Note**

After you finish the upgrade to Release 2.2, you can use the **Firmware Auto Sync Server** policy in Cisco UCS Manager to automatically update newly discovered servers. See the appropriate *Cisco UCS B-Series Firmware Management Guide* for details.

Cautions, Guidelines, and Limitations for Managing Firmware in Cisco UCS Central

Before you start managing Cisco UCS Manager firmware from Cisco UCS Central, consider the following cautions, guidelines and limitations:

- The firmware policies you define for a domain group will be applied to any new Cisco UCS Domain added to this domain group. If a firmware policy is not defined in the domain group, Cisco UCS Domain will inherit the policy from the parent domain group.
- The global policies will remain global in Cisco UCS Manager even when Cisco UCS Manager loses connection with Cisco UCS Central. If you want to apply any changes to any of the policies that are global in Cisco UCS Manager, you must change the ownership to local from global.
- When you create a host firmware package from Cisco UCS Central, it must be associated to a service profile to deploy updates in Cisco UCS domains.
- When you modify a host firmware package in Cisco UCS Central, the changes are applied to Cisco UCS domains during the next maintenance schedule associate with the host firmware update.
- The host firmware maintenance policies you define in Cisco UCS Central apply to the org-root in Cisco UCS domains. You cannot define separate host maintenance policies for sub organizations in a Cisco UCS Domain from Cisco UCS Central.
- Any server with no service profile association will get upgraded to the default version of the host firmware pack. Since these servers do not have a maintenance policy, they will reboot immediately.
- If you specify a maintenance policy in Cisco UCS Central and enable user acknowledgment and do not specify a schedule, you can acknowledge the pending task only from Cisco UCS Manager. To acknowledge pending activities from Cisco UCS Central, you must schedule maintenance using global schedulers and enable user acknowledgment.
- When you schedule a maintenance policy in Cisco UCS Central and enable user acknowledgment, that task will be displayed on the pending activities tab at the time specified in the schedule.
- You can view the pending activity for a maintenance policy only from the domain group section.
- Make sure to enable user acknowledgment for any firmware schedule to avoid any unexpected reboot in the Cisco UCS domains.