Managing Firmware

Firmware Upgrade in a Cisco UCS Domain through Intersight

You can upgrade the firmware for various components in a Cisco UCS Domain through Cisco Intersight by choosing one of the following upgrade options:

Fabric Firmware Upgrade

Through this process, you can upgrade all the fabric components in a Cisco UCS Domain, including the two Fabric Interconnects and I/O modules. These components are upgraded to the firmware version included in the selected fabric firmware bundle. Fabric firmware upgrade does not support a partial upgrade to only some components in a Cisco UCS Domain. The fabric firmware upgrade process is valid only for Cisco UCS 6400 Series Fabric Interconnects.

Fabric firmware bundles are available in the Cisco Intersight repository and have two component images:

- NXOS image
- CMC image

The following workflow illustrates the fabric firmware upgrade process:

1. **Fabric Selection**: You can initiate the fabric firmware upgrade process by selecting a Fabric Interconnect and performing an **Upgrade Firmware** action on it. Fabric Interconnects are always upgraded as a pair, in which Fabric Interconnect-B is upgraded before Fabric Interconnect-A.
2. **Bundle Selection**: After you select the Fabric Interconnect pair to be upgraded, you must select the fabric firmware bundle to which the Fabric Interconnects need to be upgraded. The firmware selection screen displays a list of available firmware bundles and information about their firmware version, size, release date, and description. The selected firmware bundle is downloaded from the Cisco Intersight repository.
3. **Impact Estimation**: The Summary screen shows a summary of the selected switches, the firmware version running on them, and the firmware version to which they will be upgraded. You can choose to upgrade by clicking **Upgrade**, or change the configuration by clicking **Back**.

4. **Upgrade Request Submission**: After you click **Upgrade**, confirm the upgrade request.

The following workflow illustrates the tasks that occur automatically after you submit an upgrade request:

1. The system validates whether there is enough storage space for the firmware bundle. If the space on the Fabric Interconnect is insufficient, the upgrade fails.
2. The system checks whether the selected firmware bundle is already in the Fabric Interconnect cache. If the firmware bundle is not present, it is downloaded to the Fabric Interconnect cache.
3. Both the IO modules are updated and activated on all the connected chassis. IO module upgrade is completed when the IO modules are rebooted.
4. Click **Continue** to acknowledge and begin firmware upgrade on Fabric Interconnect-B. After Fabric Interconnect-B upgrade is complete, the Fabric Interconnect reboots and comes up with the new image. IOM-B is rebooted along with the Fabric Interconnect-B, and comes up with the upgraded image.
5. Click **Continue** to acknowledge and begin firmware upgrade on Fabric Interconnect-A. After Fabric Interconnect-A upgrade is complete, the Fabric Interconnect reboots and comes up with the new image. IOM-A is rebooted along with the Fabric Interconnect-A, and comes up with the upgraded image.

Host Firmware Upgrade

Through this process, you can upgrade all the server components for Cisco UCS B-Series and C-Series FI-Attached servers that are in Intersight Managed Mode. These components are upgraded to the firmware version included in the selected host firmware bundle.

Server firmware bundles are available in the Cisco Intersight repository, and have the following component images:

- CIMC image
- BIOS image
- Network adapter image

Note Only UCS VIC 1400 Series adapters are supported.

- Storage controller image
- Board controller image
- Disk image
- GPU image
- Memory card image
- M-Switch and PLX images

The following workflow illustrates the host firmware upgrade process.

1. **Server Selection**: You can initiate the host firmware upgrade process by selecting a server and performing an **Upgrade Firmware** action on it.

2. **Bundle Selection**: After you confirm the server to be upgraded, you must select the host firmware bundle to which the server needs to be upgraded. The firmware selection screen displays a list of available firmware bundles and information about their firmware version, size, release date, and description. The selected firmware bundle will be downloaded from the Cisco Intersight repository.
3. **Impact Estimation**: The Summary screen shows a summary of the selected server, the firmware version running on it, and the firmware version to which it will be upgraded. You can choose to upgrade by clicking **Upgrade**, or change the firmware version by clicking **Back**.
4. **Upgrade Request Submission**: After you click **Upgrade**, select whether you want the firmware to be installed immediately or when the device reboots. Confirm the upgrade request.

   By default, firmware will be installed on next boot of the device.

The following workflow illustrates the tasks that occur automatically after you submit an upgrade request:

1. The system validates whether there is enough storage space for the firmware bundle. If the space on the Fabric Interconnect is insufficient, the upgrade fails.
2. The system checks whether the selected firmware bundle is already in the Fabric Interconnect cache. If the firmware bundle is not present, it is downloaded to the Fabric Interconnect cache.
3. Server firmware is upgraded as follows:
   - For B-Series servers:
     a. Adapter firmware is updated and activated. Adapter upgrade is completed when the server is rebooted.
     b. The Host Service Utility (HSU) is upgraded immediately or when the server reboots.
     c. All server components are upgraded.
   - For C-Series servers:
     a. The HSU is upgraded immediately or when the server reboots.
     b. All server components are upgraded.
4. Click **Continue** to acknowledge and begin firmware upgrade.

Upgrading Fabric Interconnect Firmware

You can upgrade Intersight managed Fabric Interconnect using Cisco Intersight.

Before you begin

Before you upgrade your Intersight managed Fabric Interconnect firmware, consider the following prerequisites:

- Only Cisco UCS 6400 Series Fabric Interconnects in a Cisco UCS Domain may be upgraded.
- You must have at least the following available storage in the Fabric Interconnect partitions for the firmware bundle to be downloaded:
  - 90 percent free space in /var/tmp

- 20 percent free space in /var/sysmgr
- 30 percent free space in /mnt/pss
- 18 percent free space in /bootflash

- Only Cisco UCS Domains that are claimed through Intersight may be upgraded.
- All servers in the Cisco UCS Domain must be at license tier Essentials or above.

Step 1 From the left navigation pane, click **Fabric Interconnects**, select a Fabric Interconnect, and perform an **Upgrade Firmware** action on it.

Step 2 On the **Upgrade Firmware** page, click **Start**.

Step 3 On the **General** page, confirm selection of the switch Domain and click **Next**.

Step 4 On the **Version** page, select the fabric firmware bundle to which the Fabric Interconnects need to be upgraded, and click **Next**.

This page displays a list of available firmware bundles and information about their firmware version, size, release date, and description. The selected firmware bundle will be downloaded from the Intersight repository.

During upgrade of Intersight Managed Fabric Interconnect, the Fabric Interconnect traffic evacuation is enabled by default. Fabric Interconnect traffic evacuation evacuates all traffic that flows through the Fabric Interconnect from all servers attached to it, while upgrading the system. The traffic will fail over to the peer Fabric Interconnect for fail over vNICs. Before the traffic evacuation on a Fabric Interconnect, the user must acknowledge that replay on peer Fabric Interconnect is completed and all vEths are up. Use the *show interface virtual status* command to check the vEth status for respective vEth from NXOS.

Before the traffic evacuation, you can check the traffic flowing through the Fabric Interconnect by viewing the Transmit (Tx) and Receive (Rx) stats of Host Interfaces (HIFs). After the traffic evacuation, you can check the traffic flowing through the Fabric Interconnect (FI) by viewing the Transmit (Tx) and Receive (Rx) stats of Network Interfaces (NIFs).

Note For Fabric Interconnect traffic evacuation to be functional, vNIC failover must be enabled in the LAN Connectivity Policy

Select **Advanced Mode** to disable the Fabric Interconnect traffic evacuation.

Step 5 On the **Summary** screen, verify the summary of the selected switches, the firmware version running on them, and the firmware version to which they will be upgraded, and click **Upgrade**.

You can choose to change the firmware version by clicking **Back**.

Step 6 Confirm the upgrade request.

The firmware upgrade workflow begins. You can check the status of the upgrade workflow in the **Execution Flow** pane. Acknowledge any messages in the **Execution Flow** pane and click **Continue** to proceed with the upgrade.

Upgrading Server Firmware

Before you begin

Before you upgrade your server, consider the following prerequisites:

- Only Cisco UCS B-Series M5, M6, C-Series M5, M6, M7 and X-Series M6 and M7 servers that are claimed through Intersight may be upgraded.
- Servers may be upgraded from a minimum of Cisco UCS HSU bundle release version 4.1(2a).
- All servers in the Cisco UCS Domain must be at license tier Essentials or higher.

Step 1 From the left navigation pane, click **Servers**, select a server, and perform an **Upgrade Firmware** action on it.

Note To upgrade more than one server, ensure that the selected servers are of the same model and management mode. Following are examples of valid selections:

- One or more B200 M5 servers
- One or more C220 M5 servers

Following are examples of invalid selections:

- C220 M5 and C240 M5 servers
- C220 M5 and B200 M5 servers

Step 2 On the **Upgrade Firmware** page, click **Start**.

Step 3 On the **General** page, confirm selection of the server and click **Next**.

Step 4 On the **Version** page, select the Cisco UCS HSU bundle to which the server must be upgraded, and click **Next**.

This page displays a list of available firmware bundles and information about their firmware version, size, release date, and description. The selected firmware bundle will be downloaded from the Cisco repository. By default, all the server components will be upgraded, including drives and storage controllers.

Select **Advanced Mode** to exclude drives and storage controllers from the upgrade.

Step 5 On the **Summary** screen, verify the summary of the selected servers, the firmware version running on them, and the firmware version to which they will be upgraded.

You can choose to change the configuration by clicking **Back**.

Step 6 Click **Upgrade**.

Step 7 In the **Upgrade Firmware** dialog box, choose one the following options:

a) **Reboot Immediately To Begin Upgrade**—By default, server firmware is upgraded on next boot. Enable this option if you choose to reboot immediately to begin firmware upgrade.

b) Click **Upgrade** to confirm the upgrade request.

The firmware upgrade workflow begins. You can check the status of the upgrade workflow in the **Execution Flow** pane. Acknowledge any messages in the **Execution Flow** pane and click **Continue** to proceed with the upgrade.

Upgrades and Replacement of RMA Servers and Fabric Interconnects

RMA is a Return Material Authorization process that enhances customer experience.

Upgrade of RMA Server

The RMA process triggers an automatic discovery workflow when you insert a new blade server, or when you replace an old blade server. The discovery workflow raises an alarm if the firmware of the blade server is outdated, and you will be asked to trigger an upgrade workflow.

Go to **Chassis > Inventory > Servers Below Minimum Version**, select the server that you want to upgrade and click **Upgrade**. Select the firmware version to which you want to upgrade the server. Relevant endpoints like Cisco IMC and Adaptor are upgraded to ensure that the server comes up in the Intersight Managed Mode, is available in the server list page, and is ready for use. You can upgrade the rest of the endpoints using the standard firmware upgrade method

Note The CMC version must be 4.1(3b), or later.

RMA support is not available for FI-attached C-Series servers in Intersight Managed Mode. You first need to convert the C-Series server in IMM to Standalone mode, verify the firmware, and then upgrade using HUU.

To convert the server from IMM to Standalone mode, See Converting a Server in Intersight Managed Mode to Standalone Mode.

To upgrade the firmware of C-Series Standalone server , See Upgrading UCS C-Series Standalone Servers Firmware.

Replacement of RMA Fabric Interconnect

When a single Fabric Interconnect, or a Fabric Interconnect cluster is faulty, and the Fabric Interconnects have been replaced, you can use the Replace option for migrating the configuration of the old Fabric Interconnects to the new ones. The workflows for replacing both a single Fabric Interconnect and a Fabric Interconnect cluster are detailed in the subsequent paragraphs.

Replacement of Single Fabric Interconnect

Remove the old Fabric Interconnect and connect the new Fabric Interconnect. Move all the cable connections, including servers, FEX fabrics, and blade chassis, from the old Fabric Interconnect to the new Fabric Interconnect.

Go to **Operate > Fabric Interconnects** to view the Fabric Interconnects that have been replaced and for which the Replace option is enabled. Select the Replace Fabric Interconnect option and click Replace in the confirmation page to trigger the replacement workflow.

As part of the workflow:

- The disconnected Fabric Interconnect is removed from inventory
- The domain profile is reassigned to the new Fabric Interconnect and deployed
- The servers, chassis, and FEX are inventoried and discovered under the new Fabric Interconnect
- The server and chassis profiles are redeployed with Fabric Interconnect related policies

Replacement of Fabric Interconnect Cluster

Remove the old Fabric Interconnect cluster and connect the new Fabric Interconnect cluster. Move all the cable connections, including servers, FEX fabrics, and blade chassis, from the old Fabric Interconnects to the new Fabric Interconnects. Claim the new Fabric Interconnects in Intersight. Select the **Replace UCS Domain** option that is displayed against the old cluster in Fabric Interconnects page and choose the new Fabric Interconnect cluster that will replace the old Fabric Interconnect cluster.

As part of the workflow

- The old device registration is merged with the new device registration
- The disconnected Fabric Interconnect cluster is removed from inventory
- The domain profile is reassigned to the new Fabric Interconnect cluster and deployed
- The servers, chassis, and FEX are inventoried and discovered under the new Fabric Interconnect cluster.
- The server and chassis profiles are redeployed with Fabric Interconnect related policies

Cisco Intersight Support for Auto Upgrade of IOM

You do not have to manually update the firmware of IOMs that have CMC lower than 4.1(3b). When the chassis is connected to the Fabric Interconnect, the firmware is automatically updated, the server port is configured in the Port Policy, the port policy is associated with the domain profile, and the domain profile is deployed.