Upgrade CIMC Firmware on Cisco Secure Workload Hardware

First Published: 2021-10-29

About This Firmware Upgrade

This Cisco Integrated Management Controller (CIMC) upgrade procedure is supported on M4 and M5 hardware, when running Cisco Secure Workload version 3.6 or later or Cisco Tetration version 3.4 or later.

The Cisco Secure Workload/Tetration physical appliance bundles a Unified Computing System (UCS) CIMC Host Upgrade Utility (HUU) ISO image. The firmware upgrade option on the Secure Workload/Tetration **Cluster Status** page can be used to update a physical bare-metal installation to the version of UCS firmware included in the HUU ISO image bundled in the Secure Workload/Tetration RPM files.

For information about new and changed features in each CIMC version, see the applicable release notes available from https://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-c-series-integrated-management-controller/products-release-notes-list.html.

Important

- Upgrading CIMC firmware is optional.
- The procedure below should be performed only when recommended by TAC team.
- The upgrade process may take up to 4 hours per bare metal host.

Firmware Upgrade Procedure

Note In this process and document, "upgrade" and "update" are used interchangeably.

Before you begin

- Upgrade Cisco Secure Workload before upgrading CIMC.
- Only one bare-metal host can have its UCS firmware updated at a time.
- Before starting the firmware update, verify that all services are healthy:

  In Secure Workload 3.6.x: Choose **Troubleshoot** > **Service Status**.

  In Tetration 3.4.x or 3.5.x: Choose **Maintenance** > **Service Status**.
- A firmware update on a bare-metal host can be initiated when the status is `Active` or `Inactive`, but not when the bare-metal host state is `Initialized` or `SKU Mismatch`.

- In order to start the firmware update, the **Orchestrator State** on the **Cluster Status** page must be `Idle`.

Procedure

Step 1 In the Secure Workload/Tetration web interface, navigate to the **Cluster Status** page:

In Secure Workload 3.6.x: Choose **Troubleshoot > Cluster Status**

In Tetration 3.4.x or 3.5.x: Choose **Maintenance > Cluster Status**

Step 2 Choose **Firmware upgrade** from the **Select action** drop-down menu.

Step 3 Select the bare-metal host to be updated and click **Apply**.

When you initiate a firmware update, the installer will verify that the update can continue, gracefully shut down the bare-metal host if needed, and then start the upgrade.

The overall update process can take two or more hours for M4 hardware, or one or more hours for M5 hardware.

The following behaviors are temporary and expected:

- When the firmware upgrade is initiated, the **Cluster Status** page may display errors for up to 10 minutes while backend services fail over.
- During the firmware upgrade, the firmware details normally shown on the **Cluster Status** page will not be displayed for the bare-metal host being updated, and after the update is complete it may take up to 15 minutes for the firmware details to display again.
- During the firmware upgrade, the node will be shown as inactive on the **Cluster Status** page.
- Once the firmware update process is initiated, the **Service Status** page may indicate some services are unhealthy since a bare-metal host, and all the virtual machines running on that bare-metal host, are no longer active in the cluster.

After the firmware update is completed, it may take an additional 30 minutes for the bare-metal host to become active in the cluster again, and additional time may be needed for all services to become healthy again. If services do not recover within two hours following a firmware update, please contact Cisco TAC for assistance.

Step 4 To view details about a bare-metal host, click a bare-metal host in the list on the **Cluster Status** page.

Once a firmware update is initiated, you can click the **View Firmware Upgrade Logs** button to view the status of the firmware update. This log will display the overall status of the firmware update at the very top of the listing; this status entry will be one of the following:

- **Firmware update has been triggered** – The firmware update was requested but has not yet started. Pre-checks are being conducted.
- **Firmware update is running** – The firmware update has started. When a firmware update reaches this state, CIMC and HUU are in control of the update, and the Secure Workload cluster will report the status information it receives from CIMC about the update.
- **Firmware update has timed out** – This indicates that some process in the firmware update has exceeded the time alloted to complete it. The overall firmware update process has a 240-minute time limit once it enters the **Firmware update is running** phase. During the firmware update, CIMC may become unreachable when it reboots into the new version; this unreachable state has a timeout of 40 minutes before the firmware update is declared as “timed out.” Once the firmware update has started, the monitoring of that update will time out after 120 minutes.

- **Firmware update has failed with an error** – This indicates that an error occurred and the firmware update has failed. CIMC usually does not give an indication of success or failure, so this state usually indicates an error occurred prior to the firmware update actually running.
- **Firmware update has finished** – The firmware update finished successfully. Since CIMC usually does not give an indication of success or failure, it is best to verify that the UCS firmware versions are updated once those details become available in the **Cluster Status** page. Note that it can take up to 15 minutes for those details to become available. For expected versions, see CIMC Versions, on page 3, below.
- If an undetected failure occurs, the upgrade may appear to be running, but will time out after 240 minutes (4 hours). If this occurs, try the upgrade again; if it fails again, contact TAC.

To refresh the status view, close the upgrade status window and then click the **View Firmware Upgrade Logs** button again.

Below the overall status in the **View Firmware Upgrade Logs** pop-up window, an Update progress section provides time-stamped log messages indicating the progress of the firmware update. Once the **Rebooting Host In Progress** status is displayed in these log messages, CIMC is in control of the update and the cluster is monitoring that update—most subsequent log messages come directly from CIMC and are only added to the list of log messages if the status of the update changes.

Below the Update progress section of the **View Firmware Upgrade Logs** pop-up window, a Component update status section will be shown once CIMC starts providing individual component updates. This section can give a quick overview of the status of the update of the various UCS components on the bare-metal host.

CIMC Versions

Instructions in this document apply to the following versions.

The CIMC HUU ISO versions in the table below are bundled with the applicable Secure Workload/Tetration version.

Secure Workload/ Tetration Version	UCS-C220-M4	UCS-C220-M5	UCS-C220-M6
3.9	4.1(2k)	4.2(3b)	4.2.3b
3.8	4.1(2k)	4.2(3b)	4.2.3b
3.7	4.1(2b)	4.1(3f)	NA
3.6	4.1(2b)	4.1(3b)	NA
3.4 and 3.5	4.1(1g)	4.1(1g)	NA

Secure Workload/ Tetration Version	UCS-C220-M4	UCS-C220-M5
3.6	4.1(2b)	4.1(3b)
3.4 and 3.5	4.1(1g)	4.1(1g)

Older Versions

Instructions in this document do *not* apply to the following versions. To upgrade CIMC for these versions, contact Cisco TAC.

These versions ship with the hardware for both new and replacement (RMA) hardware.

Secure Workload/ Tetration Version	UCS-C220-M4	UCS-C220-M5
3.2 and 3.3 (Instructions in this document do *not* apply.)	2.0(10e)	4.0(1a)
2.2 to 3.1 (Instructions in this document do *not* apply.)	2.0(10e)	N/A