CIMC Firmware Version 4.1(2f) M4 Common Update Process for Stealthwatch v7.1.3 and v7.2.1

This document provides instructions for updating CIMC firmware to version 4.1(2f) for UCS C-Series M4 hardware for all appliances for Stealthwatch versions 7.1.3 and 7.2.1.

The ISO and SWU files are available for download through Cisco Software Central. For specific instructions for downloading the required files, go to **1. Download the ISO and SWU File(s)**.

If your current firmware version is:

- 2.x, make sure to download the SWU file and install it before installing the required ISO file(s)
- 3.x or later, only download the required ISO file(s) since an ISO file is not needed

> **Required ISO file(s):** The Flow Collector 5020 and 5200 Database appliances require a different ISO file than all other appliances.

This update process applies to UCS C-Series M4 hardware for the Stealthwatch appliances shown in the following table.

M4 Hardware	
Stealthwatch Management Console 2200	Flow Sensor 1200
Flow Collector 4200	Flow Sensor 2200
Flow Collector 5020 Engine	Flow Sensor 3200
Flow Collector 5020 Database*	Flow Sensor 4200
Flow Collector 5200 Engine	UDP Director 2200
Flow Collector 5200 Database*	___

**Requires the ucs-c240m4-huu-4.1.2f-sna.iso file*

> Make sure you update all physical appliances.

Before You Begin

Make sure to plan for the time and resources needed to complete the update process. Specifically, confirm that you can do the following:

- log in to the CIMC web interface
- mount remote ISO in the CIMC
- access and use the virtual console
- shut down, start, and restart your appliances through the CIMC
- check hardware and RAID status

Downtime: The update process can require 90 minutes or longer to complete.

1. Download the ISO and SWU File(s)

An ISO file for the applicable appliance model is required to complete the update process.

> Make sure to download the SWU file if your firmware version is 2.x. If your firmware version is 3.x or later, you don't need to download the SWU file.

Use the following instructions to download the required ISO file(s) and SWU file (if you're current firmware version is 2.x):

1. Go to Cisco Software Central, https://software.cisco.com.
2. In the Download and Upgrade section, select **Access downloads**.
3. Type **Secure Network Analytics** in the **Select a Product** field. Press **Enter**.
4. Choose the appliance model from the drop-down list, then press **Enter**.
5. Under Select a Software Type, choose **Secure Network Analytics Patches**, then choose **Firmware > Firmware** in the All Release area to locate the files.
6. If your CIMC firmware version is currently 2.x, download and save the SWU file, patch-common-SW7VM4-FIRMWARE-01.swu.
7. Locate, download, and save the ISO file, based on appliance model:

    - **ucs-c220m4-huu-4.1.2f-sna.iso** –
      ISO file for ALL appliances except for the Flow Collector 5020 and 5200 Database appliances
    - **ucs-c240m4-huu-4.1.2f-sna.iso** –
      ISO file specifically for the Flow Collector 5020 and 5200 Database appliances

2. Install the SWU File (If Needed)

> If your firmware version is 3.x or later, you don't need to install the SWU. Skip this step and go to **3. Update the CIMC Firmware Version Using the Required ISO File**.

To install the SWU file, complete the following steps:

1. Log in to the SMC.
2. Click the **Global Settings** icon, then click **Central Management**.
3. Click **Update Manager**.
4. On the Update Manager page, click **Upload**, and then open the saved patch update file: update-common-SW7VM4-FIRMWARE-02.swu.
5. Click the **Actions** menu for the appliance, then click **Install Update**.

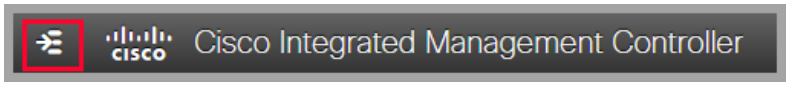
> The installation process can take up to 90 minutes; the appliance restarts automatically.

3. Update the CIMC Firmware Version Using the Required ISO File

> Make sure your firmware version is 3.x or later. If your firmware version is v2.x, install the update-common-SW7VM4-FIRMWARE-02.swu before installing the ISO file.

Follow these instructions to update the CIMC Firmware for your UCS M4 hardware.

1. Log in to the CIMC.
2. Click the **Toggle Navigation** icon to display the side menu.

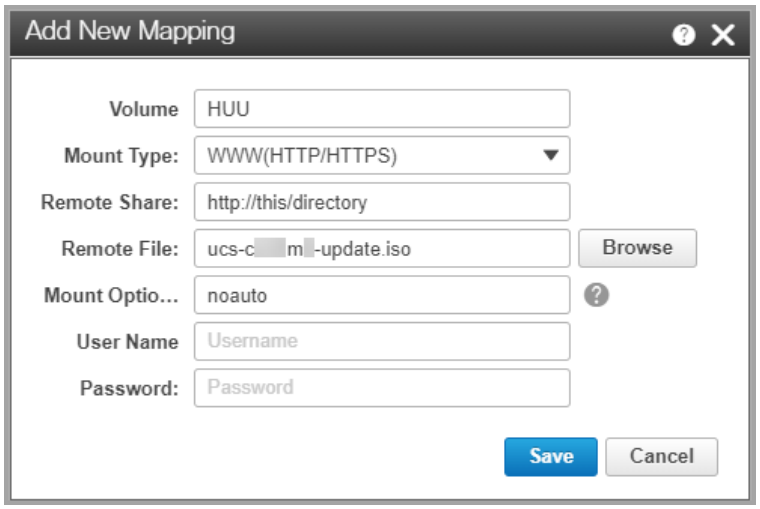


3. Select the **Compute** tab from the side menu.
4. Select the **Remote Management** tab, and then select the **Virtual Media** tab.

> If there is another file already mapped, click **Unmap** and **Delete** to remove it so the new ISO file can be loaded.

5. Click **Add New Mapping** menu.

   The Add New Mapping dialog box displays.



6. Complete the following fields:
    - Enter **HUU** in the **Volume** field.
    - Choose **WWW(HTTP/HTTPS)** for the **Mount Type** field.

    > If you choose to select another mount type, make sure the corresponding communication port is enabled.

    - Enter the path of the file share of the ISO file in the **Remote Share** field. For example: **http://this/directory**
    - Select the **Remote** file.
    - Select **noauto** in the **Mount Options** field.
    - Enter **User Name** and **Password**, if required.
7. Click **Save**.
8. Locate the Current Mappings section to confirm the **Status** column shows **OK**.
9. Click **Save Changes**.
10. Select **Launch KVM** on the toolbar, and select **HTML based KVM**.

    The Virtual Console dialog box displays.

11. Select **Macros** > **Static Macros** > **Ctrl-Alt-Del**.

    The reboot process begins.

12. Press the **F6** key on your keyboard when the Cisco logo and boot options display within the KVM virtual console screen.

13. Select **Cisco CIMC-Mapped vDVD1.22** when the Please Select Boot Device dialog box displays.

    The Cisco Software License Agreement dialog box displays.

14. Click **I Agree**.

    The Cisco Software License Agreement dialog box closes, and the Cisco Host Upgrade Utility window displays.

15. Select **Update HDD Firmware**.

    The HDD Firmware Update dialog box displays.

16. Select **Update All**, then click **Close**.

    The HDD Firmware Update dialog box closes.

17. Select **Update All** on the Cisco Host Upgrade Utility window, and follow the on-screen prompts to continue with the update.

    The **Status** displays as **In Progress** until **Completed**.

18. Note that the process can take up to 90 minutes or more; one of following notifications displays:

    - **Success** – firmware update has installed successfully
    - **Skipped** – firmware does not need to be updated

19. Make sure to select **Activate**, if prompted.

20. Click **Exit** on the Cisco Host Upgrade Utility window.

    The CIMC updates and restarts.

> The update process can take 90 minutes or longer.

Contacting Support

If you need technical support, please do one of the following:

- Contact your local Cisco Partner
- Contact Cisco Support
    - To open a case by web: http://www.cisco.com/c/en/us/support/index.html
    - To open a case by email: tac@cisco.com
    - For phone support: 1-800-553-2447 (U.S.)
    - For worldwide support numbers: www.cisco.com/en/US/partner/support/tsd_cisco_worldwide_contacts.html

Copyright Information