CIMC Firmware Version 4.3(2.250016) M5 Update Patch for Secure Network Analytics v7.5.0

This document provides a description of the CIMC 4.3(2.250016) Firmware M5 Common Update Patch for Secure Network Analytics along with instructions for installing the patch.

This firmware update can be performed using either the SWU file/procedure or the ISO file/procedure outlined below:

- The SWU file, patch-common-SNA-FIRMWARE-20250403-v2-01.swu, updates the CIMC firmware to version 4.3(2.250016) for UCS C-Series M6 hardware running Secure Network Analytics v7.5.0.
- Alternatively, you can also use the ISO file, patch-common-SNA-FIRMWARE-20250403-M5-REL.iso, to update the CIMC firmware to version 4.3(2.250016) for UCS C-Series M6 hardware with Secure Network Analytics v7.5.0.

> As part of the update process, make sure to install the required rollup patches on your appliances.

M5 Hardware

This patch applies to UCS C-Series M5 hardware for the Secure Network Analytics appliances shown in the following table.

M5 Hardware	
Manager 2210	Flow Sensor 1210
Data Node 6200	Flow Sensor 3210
Flow Collector 4210	Flow Sensor 4210
Flow Collector 5210 Engine	Flow Sensor 4240
Flow Collector 5210 Database	UDP Director 2210

> Make sure you update all physical appliances.

Additional Information

For more details about CIMC version 4.3(2.250016), refer to Release Notes for Cisco UCS Rack Server Software.

Download and Installation

You can download and install the CIMC 4.3(2.250016) Firmware M5 Common Update Patch via either of the following ways:

- **Downloading and Installing via SWU**
- **Downloading and Installing via ISO**

Downloading and Installing via SWU

Download

To download the common update patch file, complete the following steps:

1. Log in to Cisco Software Central, https://software.cisco.com.
2. In the Download and Upgrade area, choose **Access downloads**.
3. Type **Secure Network Analytics** in the **Select a Product** search box.
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 patch.
6. Download and save the file, patch-common-SNA-FIRMWARE-20250403-v2-01.swu.

Installation

To install the common update patch update file, complete the following steps:

1. Log in to the Manager.
2. On the Network Analytics page, choose **Configure** > **Global** > **Central Management**.
3. Click **Update Manager**.
4. On the Update Manager page, click **Upload**, and then open the saved file, patch-common-SNA-FIRMWARE-20250403-v2-01.swu.
5. Click the **Actions** menu for the appliance, then click **Install Update**.

   The patch stops the Vertica Database, then restarts the appliance.
6. Make sure you restart Vertica on any Data Node after the update patch file successfully installs on **all** Data Nodes.

a. Log in to the Manager.
b. Go to **Central Management** > **Data Store** > **Database Control**.
c. Under the Database Control tab, click the ⋯ (**Ellipsis**) icon in the Actions column for the database.
d. Choose **Start**.
e. Confirm the database status is shown as Connected. The installation process can take up to 90 minutes; the appliance restarts automatically.

Downloading and Installing via ISO

Download

To download the update patch file, complete the following steps:

1. Log in to Cisco Software Central, https://software.cisco.com.
2. In the Download and Upgrade area, choose **Access downloads**.
3. Type Secure Network Analytics in the **Select a Product** search box.
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 patch.
6. Download and save the file, patch-common-SNA-FIRMWARE-20250403-M5-REL.iso.
7. There are two ways of installing ISO:
   - **Installation Using vKVM-Mapped vDVD**
   - **Installation Using CIMC-Mapped vDVD**

Before Installation

> If you have firewall rules enabled for Cisco Integrated Management Controller (CIMC), specify 169.254.254.2 in the list of allowed hosts to ensure the update is successful. Otherwise you can skip this step and go to **Installation Using vKVM-Mapped vDVD** or **Installation Using CIMC-Mapped vDVD**, depending on your preferred installation method.

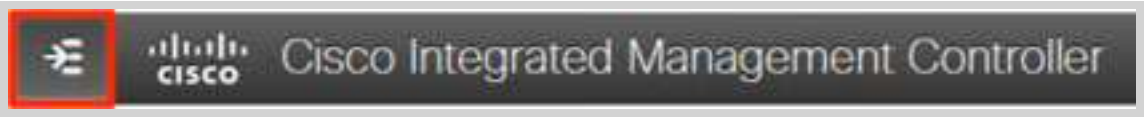
1. Log in to the unit's Cisco Integrated Management Controller (CIMC) interface using a web browser.
2. Choose **Networking > Network Security**.
3. In the **IP Filtering (Allow Listing)** menu, enter **169.254.254.2** IP value in the **IP filter** field.
4. Click **Save Changes**.

Installation Using vKVM-Mapped vDVD

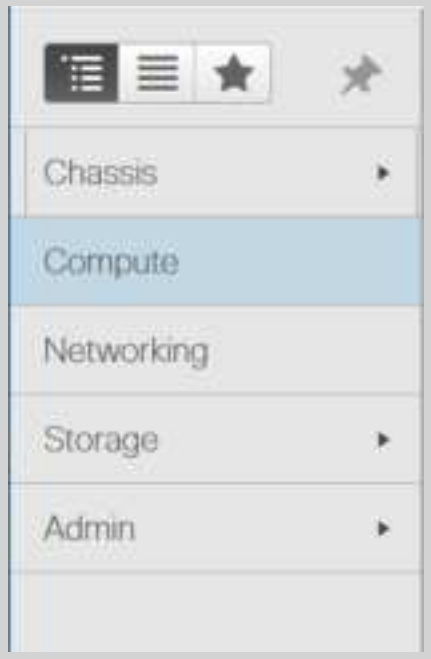
This installation method updates the firmware by accessing the firmware update ISO file stored on the machine used to connect to the CIMC UI.

> To install the firmware patch from an ISO image, use the vKVM console of an M5 machine.

1. Log in to the unit's Cisco Integrated Management Controller (CIMC) interface using a web browser.
2. Click **Toggle Navigation** icon to display the side menu.

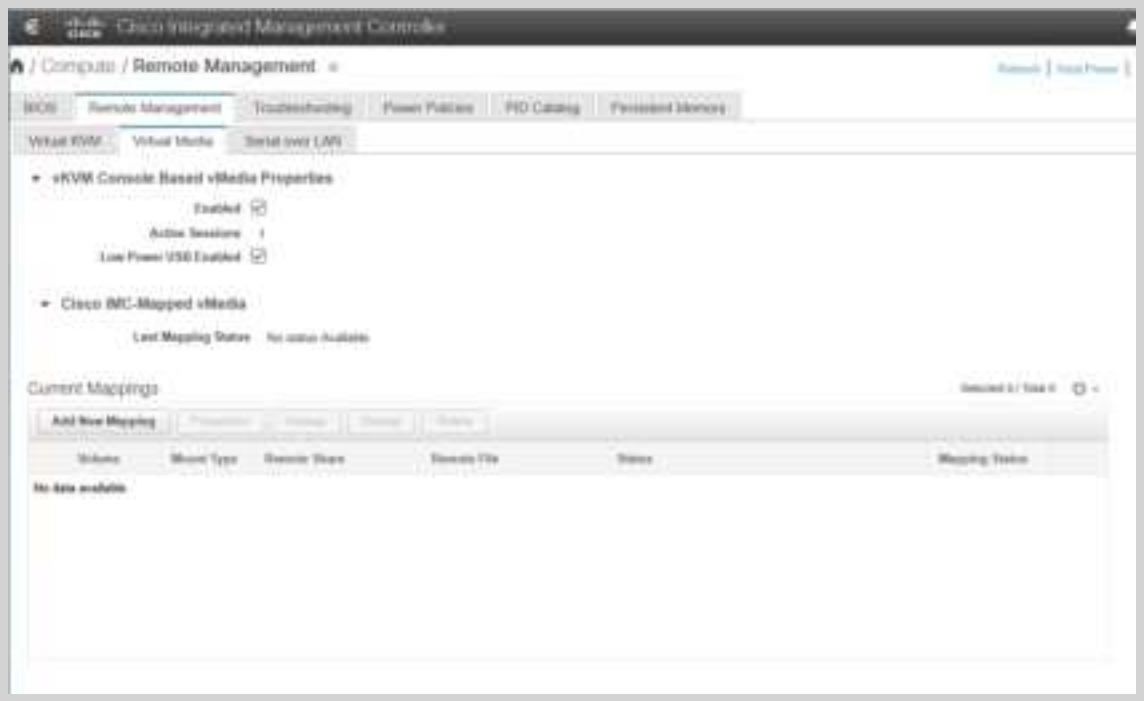


3. Select **Compute** from the side menu.



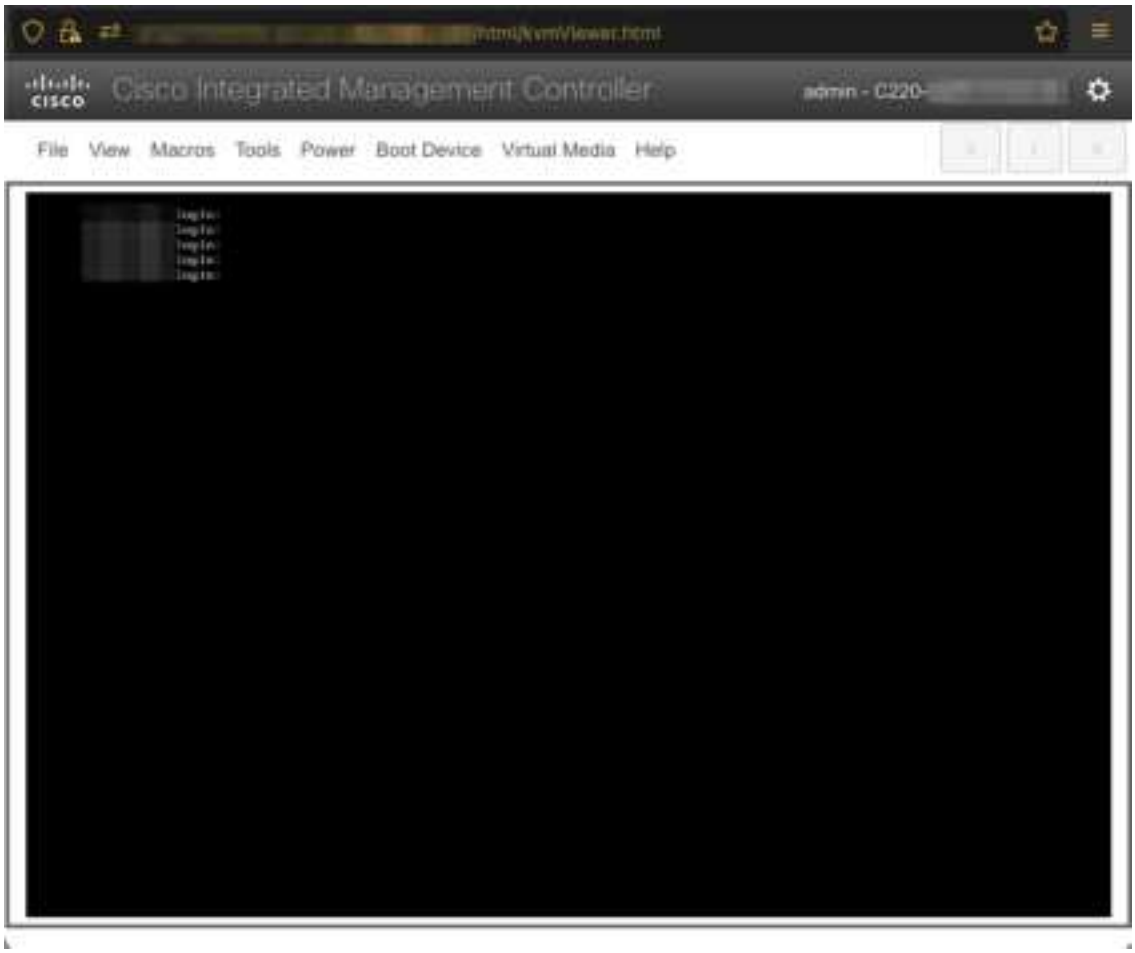
4. Select **Remote Management** , and then select the **Virtual Media** tab.

   If there is another file listed in **Current Mappings**, select it, click **Unmap** and don’t save the volume. Then, select it again and click **Delete** to remove it.

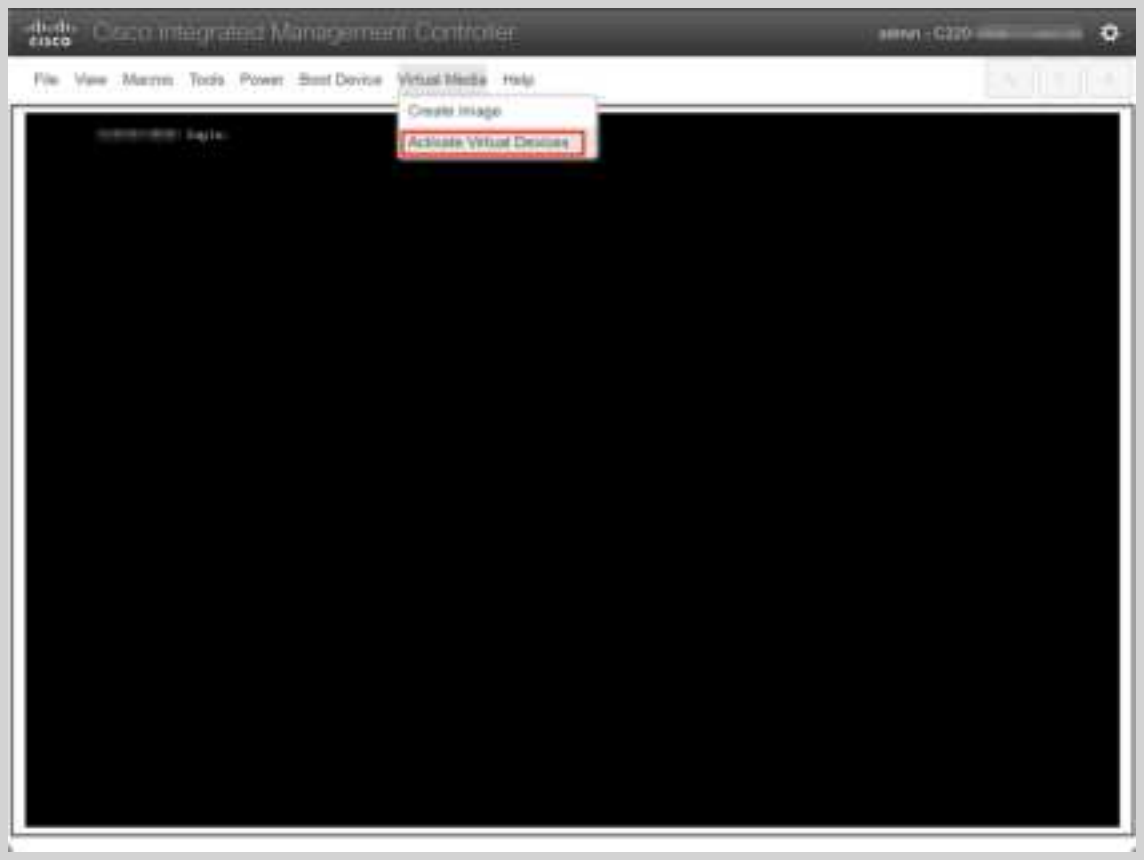


5. Select **Launch KVM** on the toolbar, if prompted, select **HTML** based KVM.

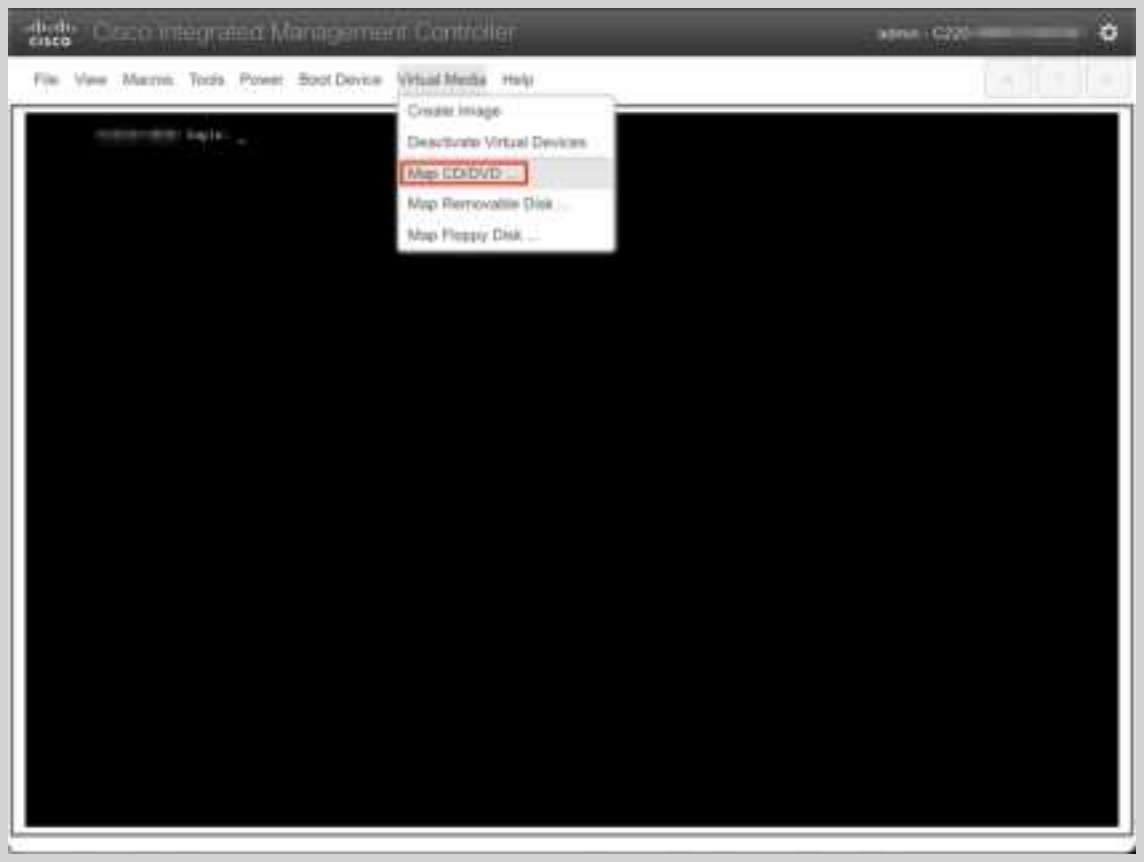
6. The **Virtual Console** opens in a new browser tab.



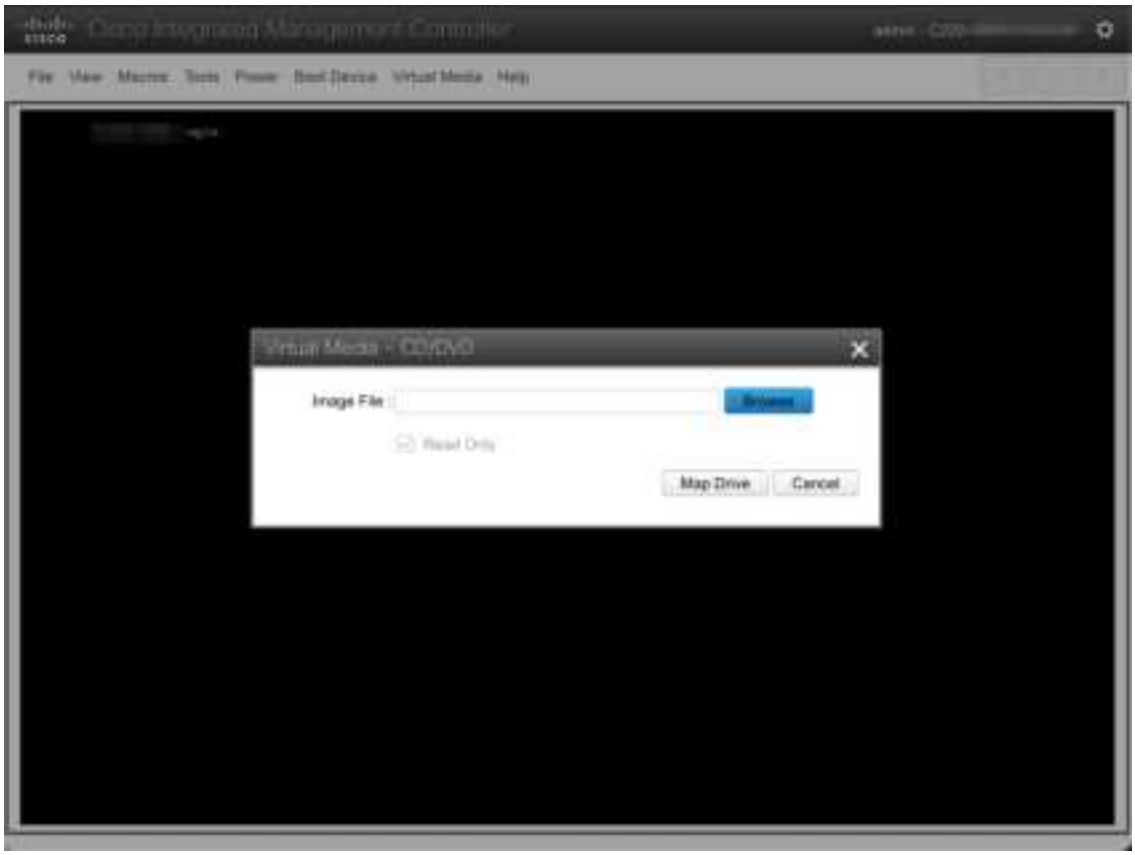
7. Select **Virtual Media > Activate Virtual Devices** to activate a virtual drive



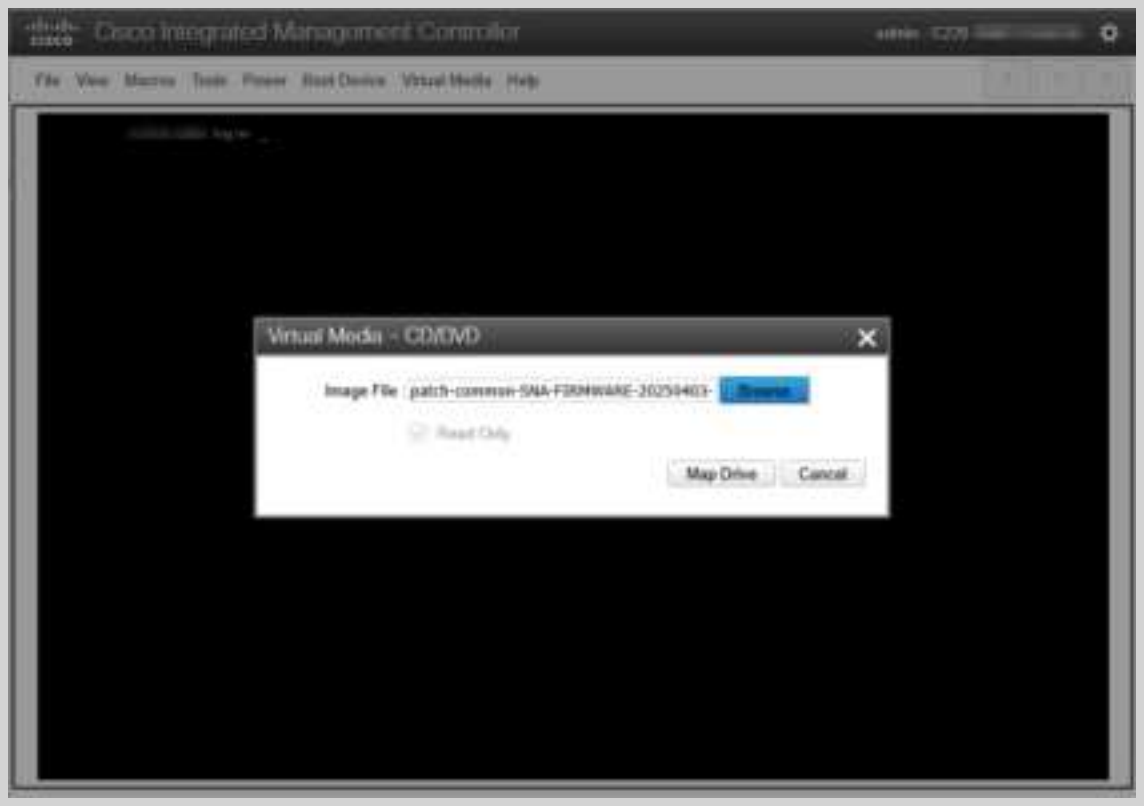
8. If the activation is unsuccessful, repeat the Activate Virtual Devices step.
9. Once the activation is successful, you can see additional options under the **Virtual Media** pull-down menu.
10. Click **Map CD/DVD** option.



A new window appears, allowing you to browse to the locally stored ISO file. Browse to the ISO file and select it.

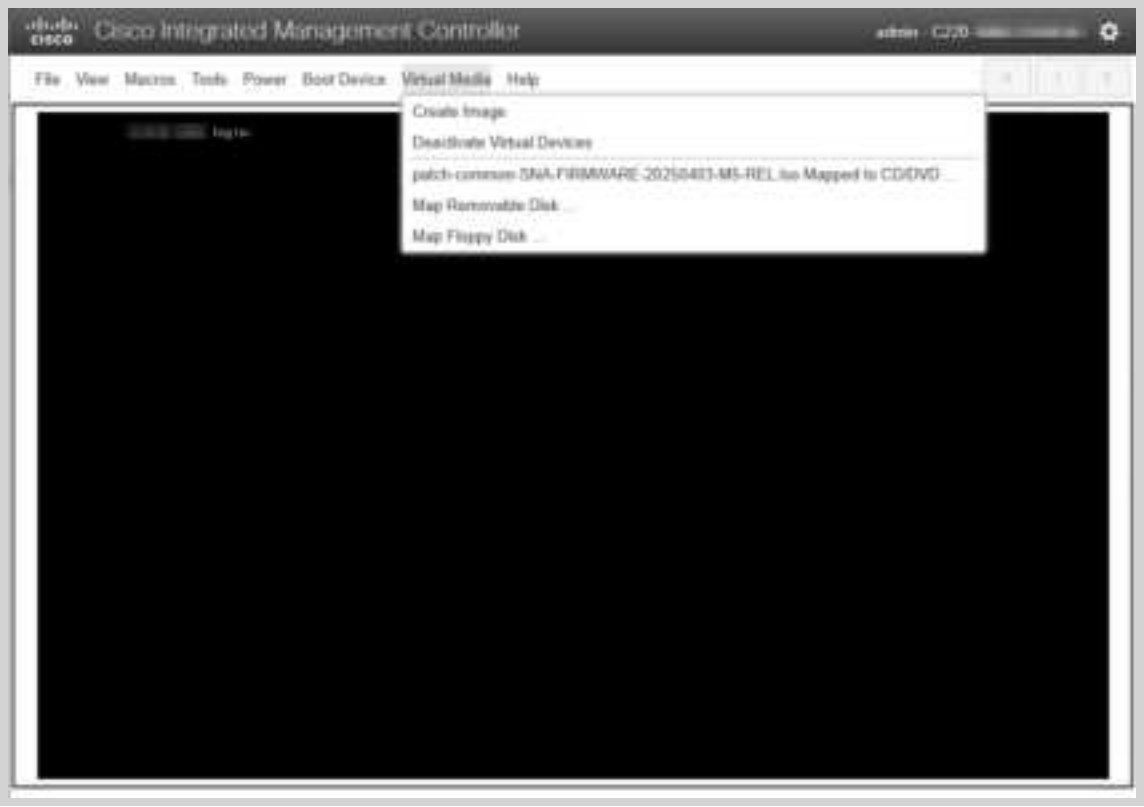


11. Click **Map Drive** to map the virtual drive to the selected ISO file.

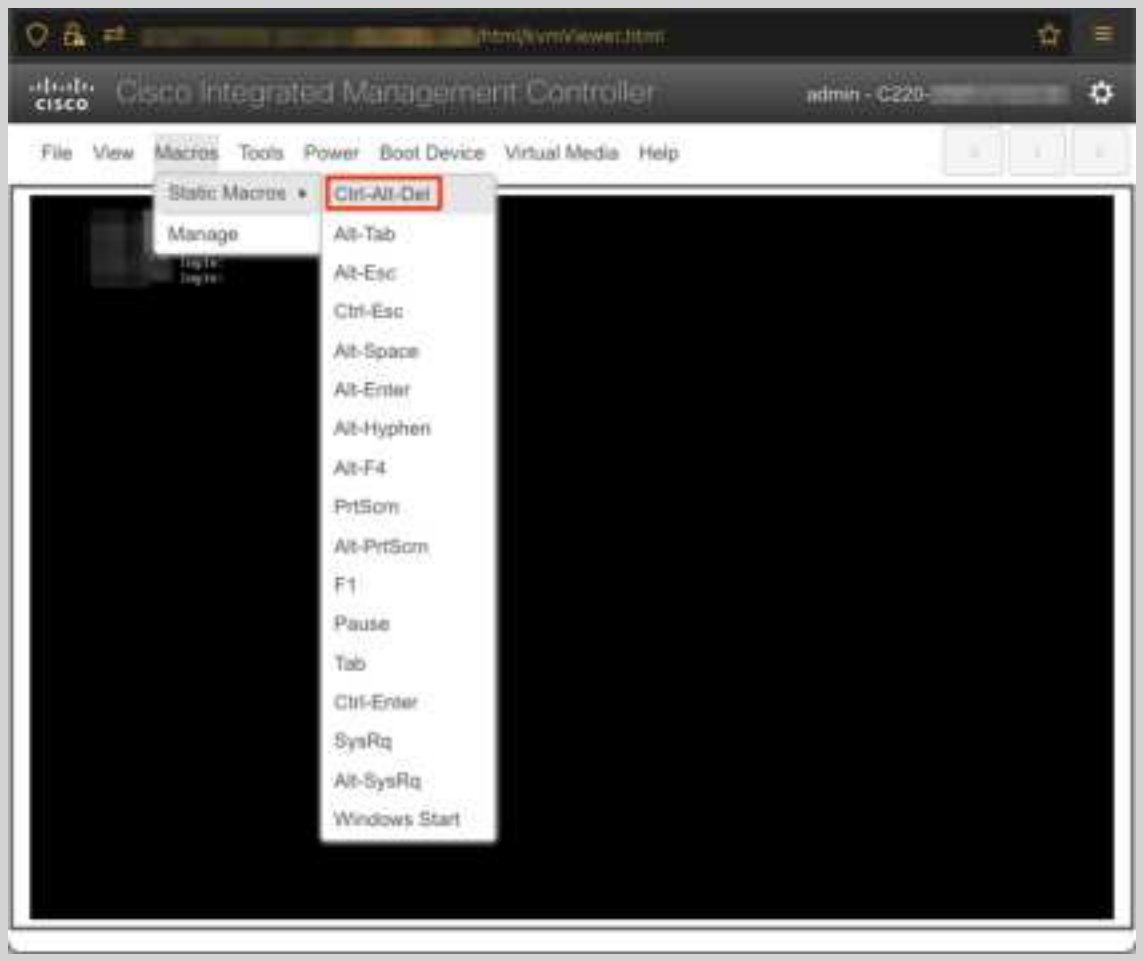


12. Click **Virtual Media** drop-down menu to verify that the firmware ISO file is mapped.

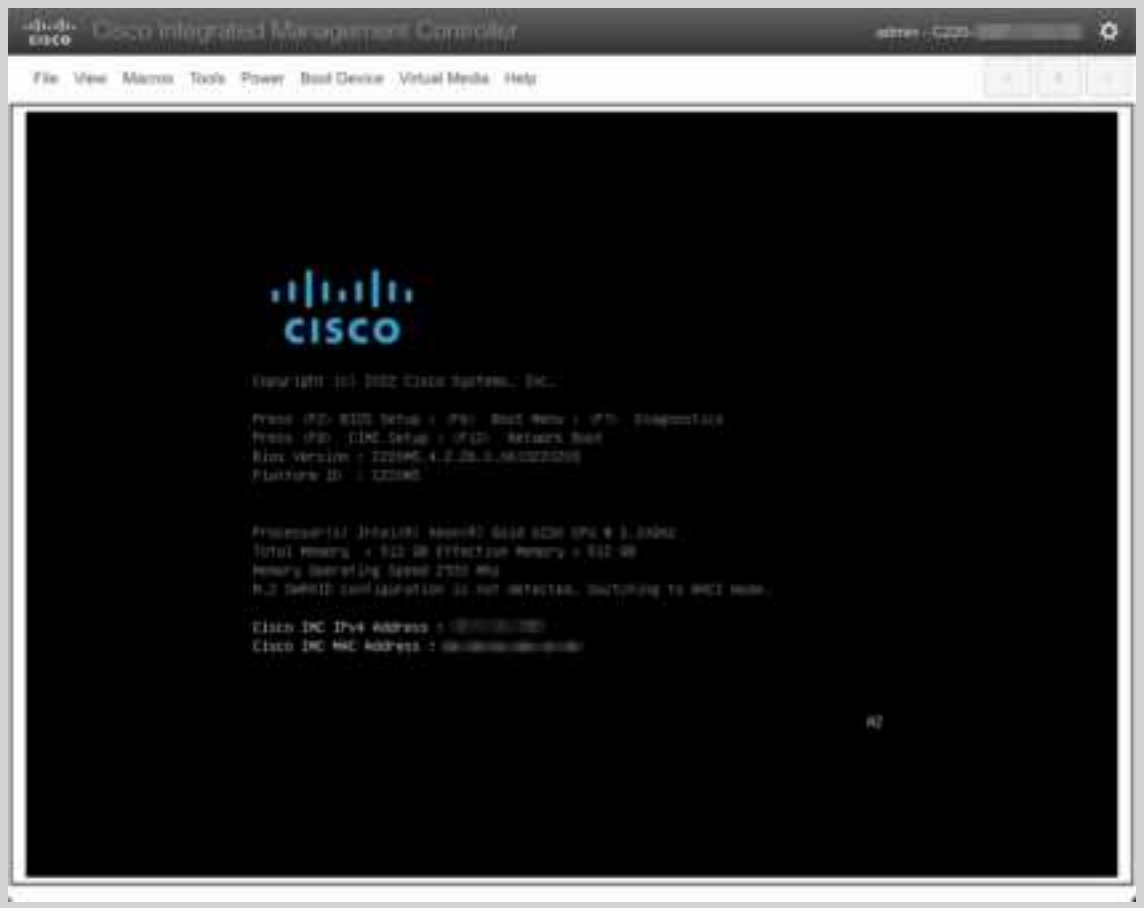
> Do not click the mapped file, as this will unmap the file.



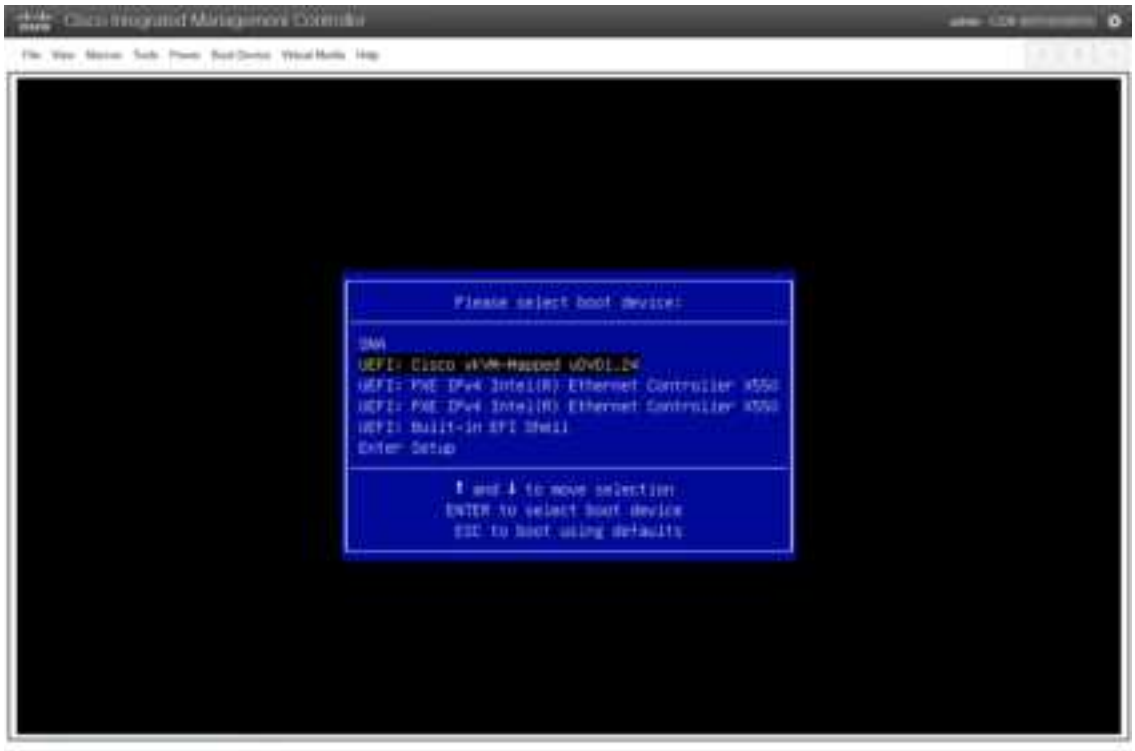
13. Select **Macros > Static Macros > Ctrl-Alt-Del** to begin the reboot process.



14. Press the **F6** key on your keyboard when the Cisco logo and boot messages appear in the KVM virtual console screen.

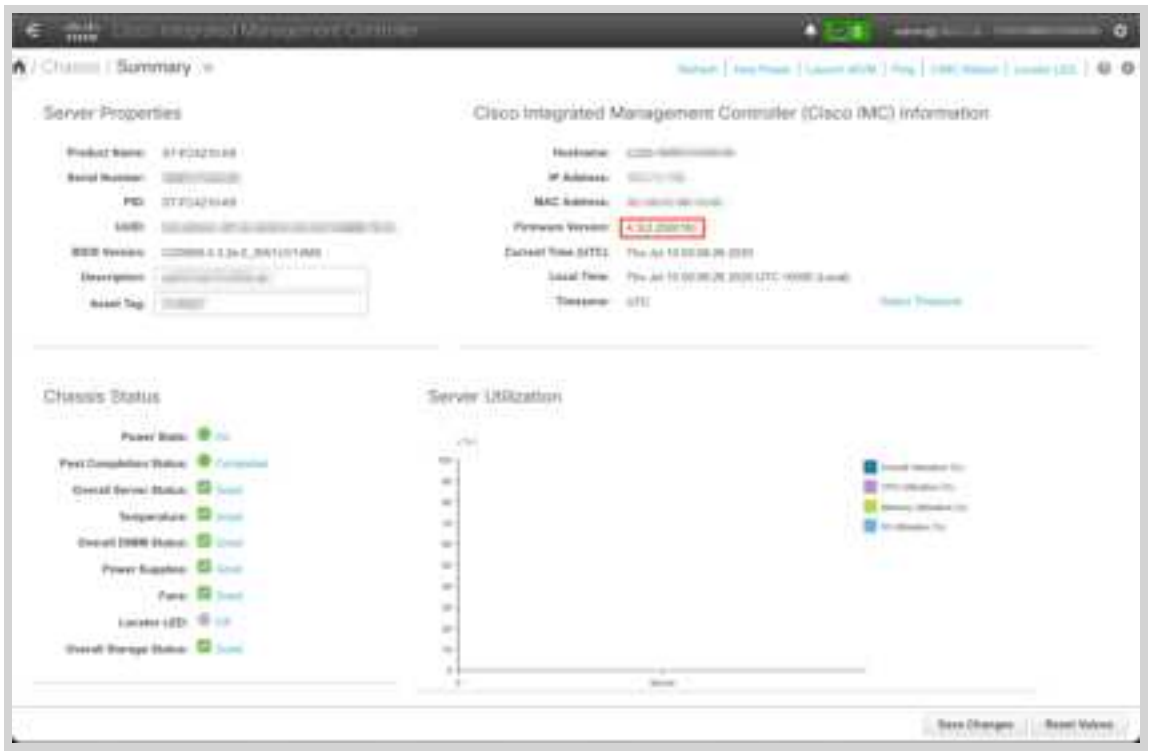


15. When the **Please Select Boot Device** dialog box appears, select **Cisco vKVM-Mapped vDVD1.24**.



The firmware update initiates. The CIMC may reboot during the update process, causing a temporary loss of connection. If this occurs, log in to the CIMC again and re-launch the vKVM Console to continue monitoring the update. Once the firmware update is complete, the ISO will be ejected or unmounted, and the SNA appliance will reboot.

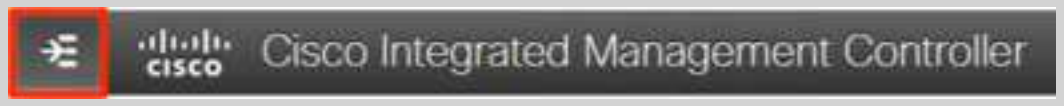
16. Verify on the **CIMC Chassis Summary** page that the firmware has been updated.



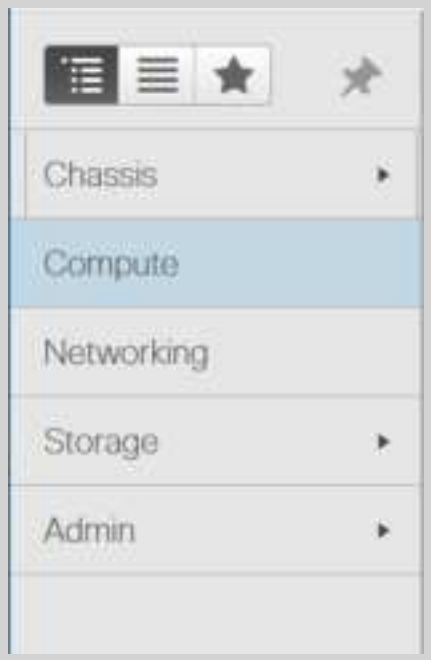
Installation Using CIMC-Mapped vDVD

This installation method updates the firmware by accessing the ISO file stored on an HTTP/S server.

1. Log in to the unit's Cisco Integrated Management Controller (CIMC) interface using a web browser.
2. Click **Toggle Navigation** to display the side menu.

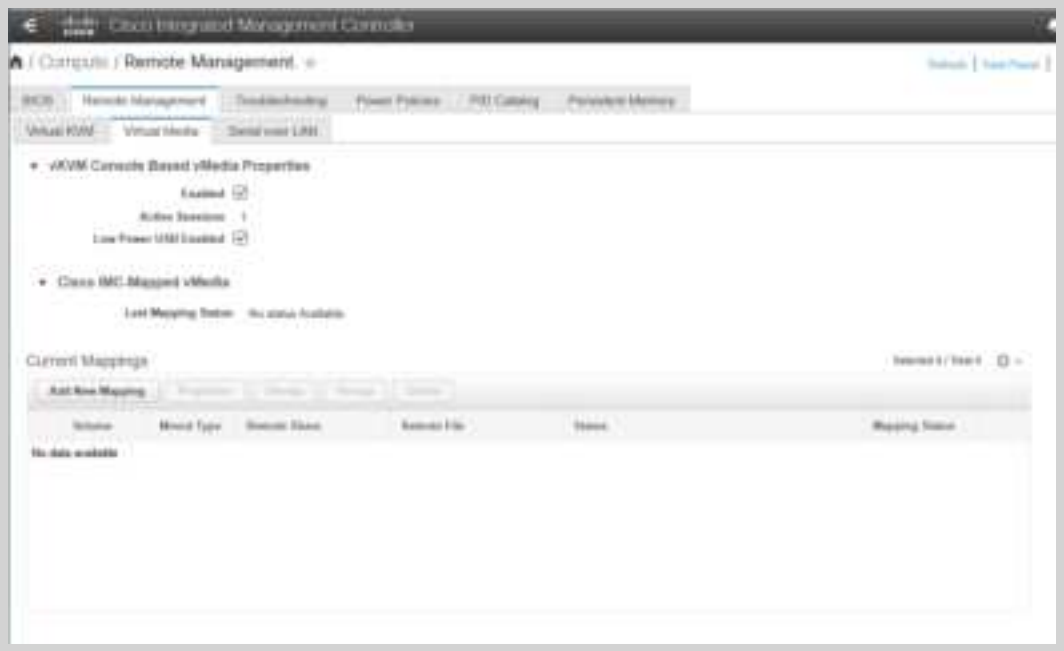


3. Select **Compute** from the side menu.

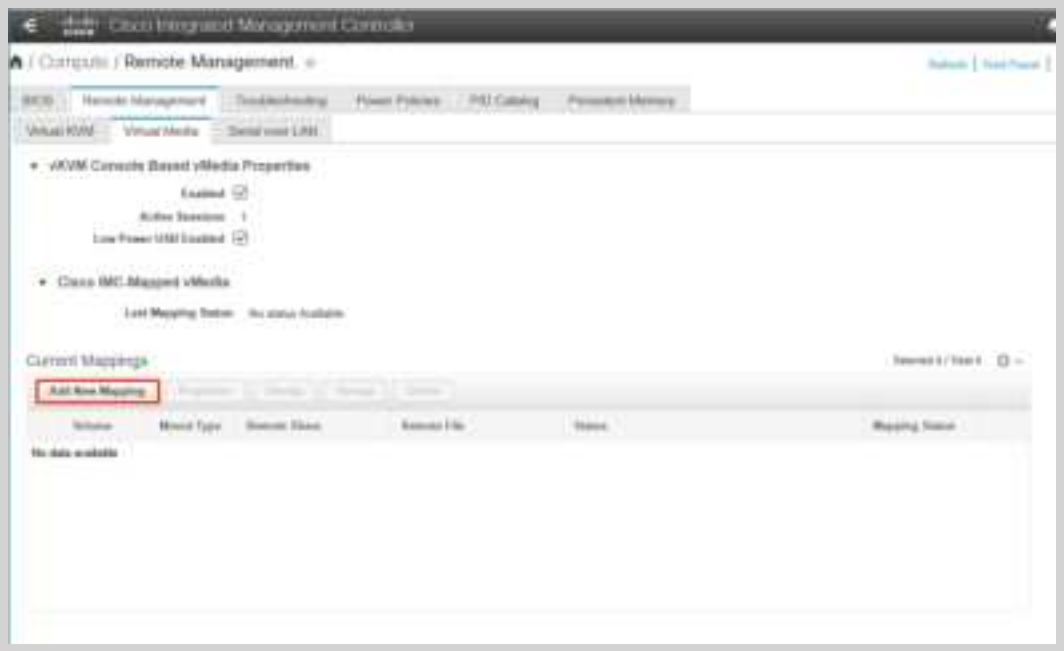


4. Select **Remote Management**, and then select **Virtual Media**.

> If another file is already mapped, select it and click **Unmap** without saving the volume. Then, select the file again and click **Delete** to remove it. This will allow you to load the new ISO file.



5. Click **Add New Mapping** button to open **Add New Mapping** dialog.



6. Complete the following fields in the **Add New** dialog box:
    - Enter "HUU" or another meaningful name in the **Volume** field. This name appears in the Current Mappings window and can help indicate the mapping's purpose. Example: FW_Patch_2025

- Choose WWW(HTTP/HTTPS) for the **Mount Type** field.

  > If you select another mount type, ensure the corresponding communication port is enabled.

- Enter the file share path of the ISO file in the Remote Share field.

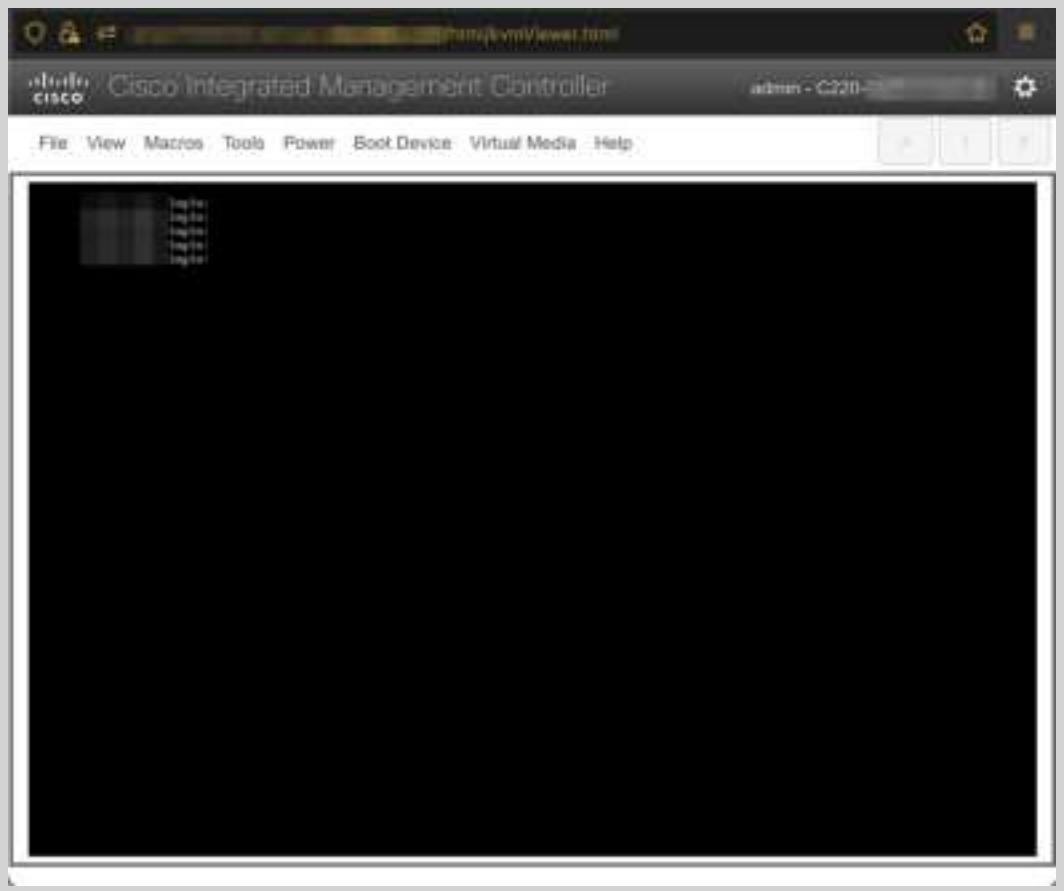
  Example: http[s]://serverip/directory/

- Enter the ISO filename in the **Remote File** field.
- Select **noauto** for the **Mount Options** field.
- Enter **User Name** and **Password**, if required.

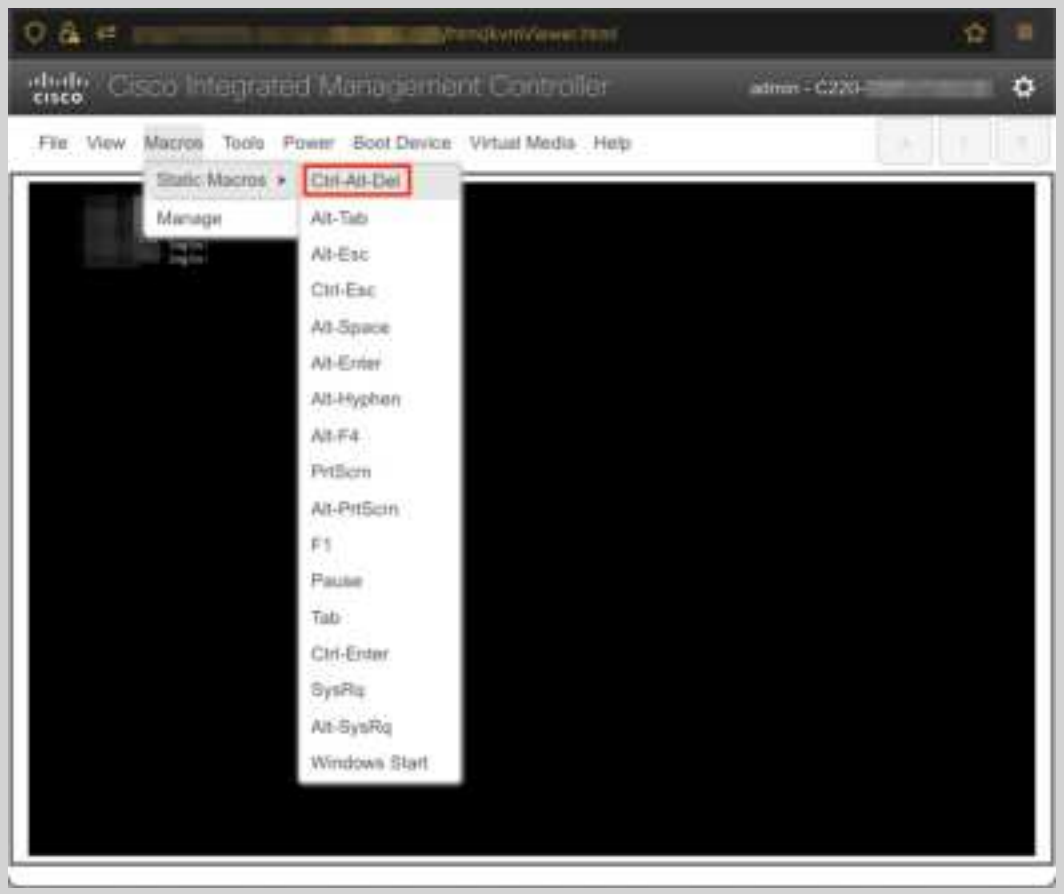
7. Click **Save**.
8. In the **Current Mappings** section, verify that the **Status** column displays OK and the **Mapping Status** column displays Mapped.

9. Click **Save Changes**.
10. Select **Launch KVM** on the toolbar, if prompted, select **HTML based KVM**.

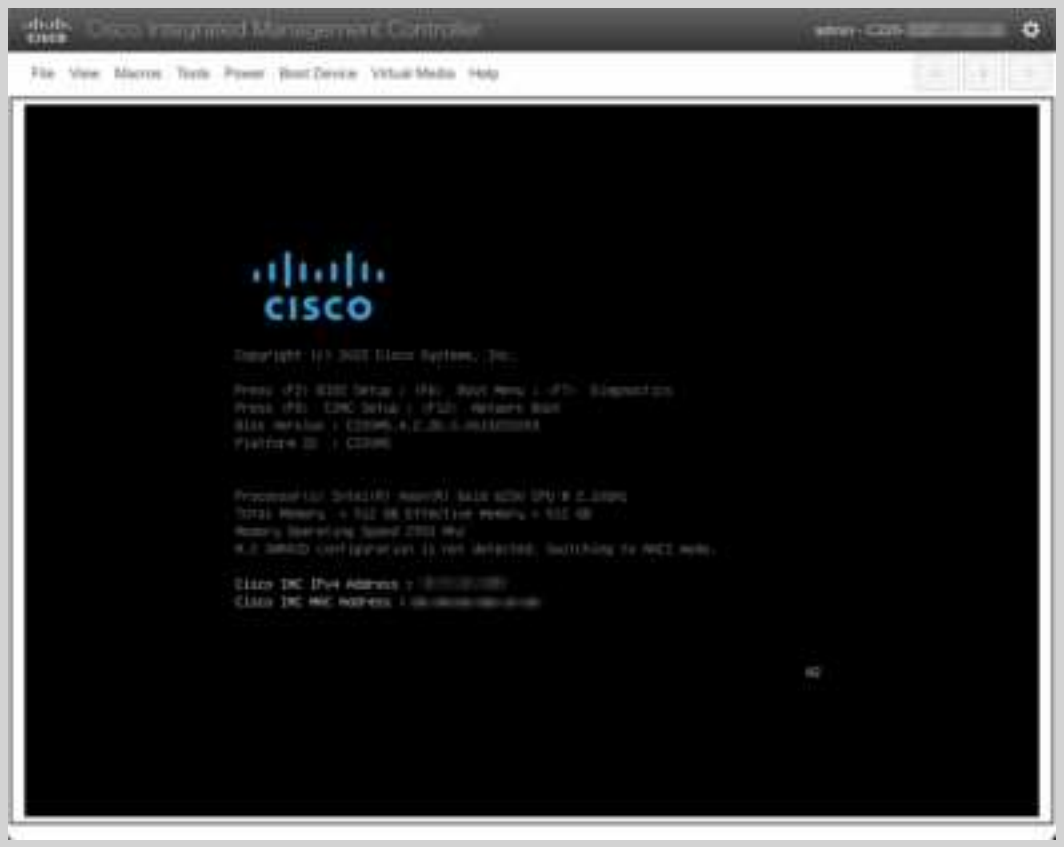
11. The **Virtual Console** opens in a new browser tab.



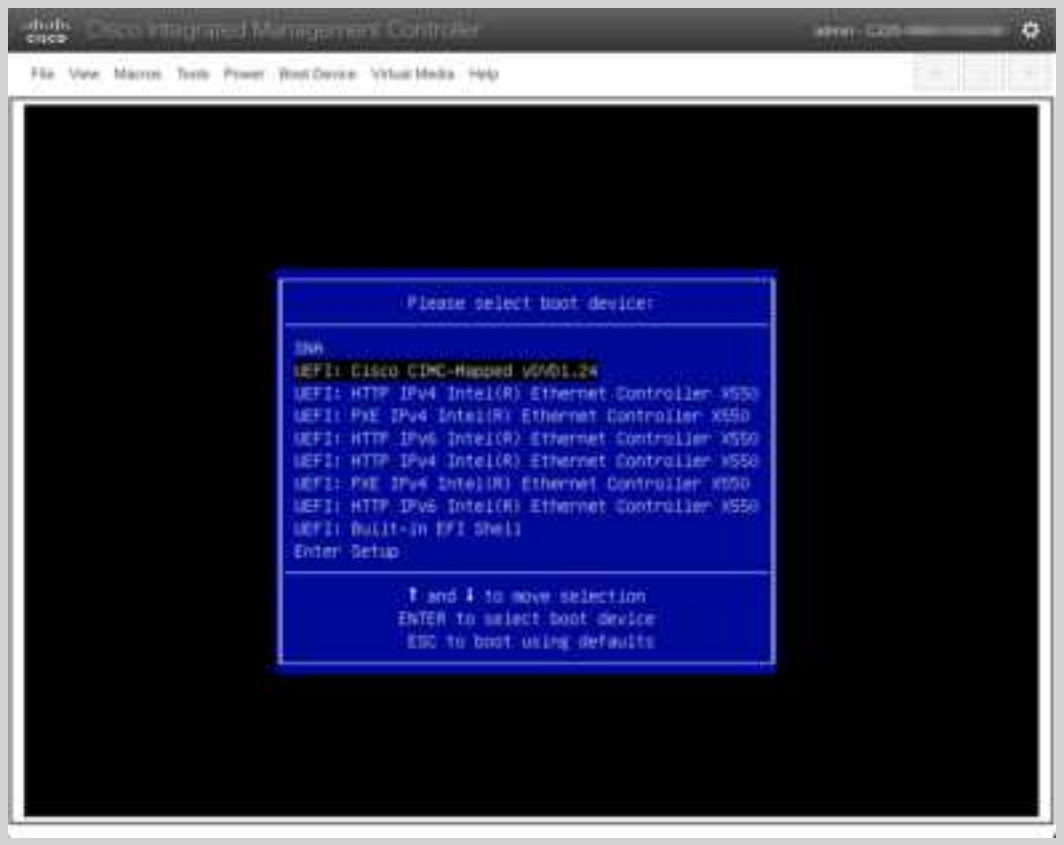
12. Select **Macros > Static Macros > Ctrl-Alt-Del** to begin the reboot process.



13. Press the F6 key on your keyboard when the Cisco logo and boot messages appear in the KVM virtual console screen.

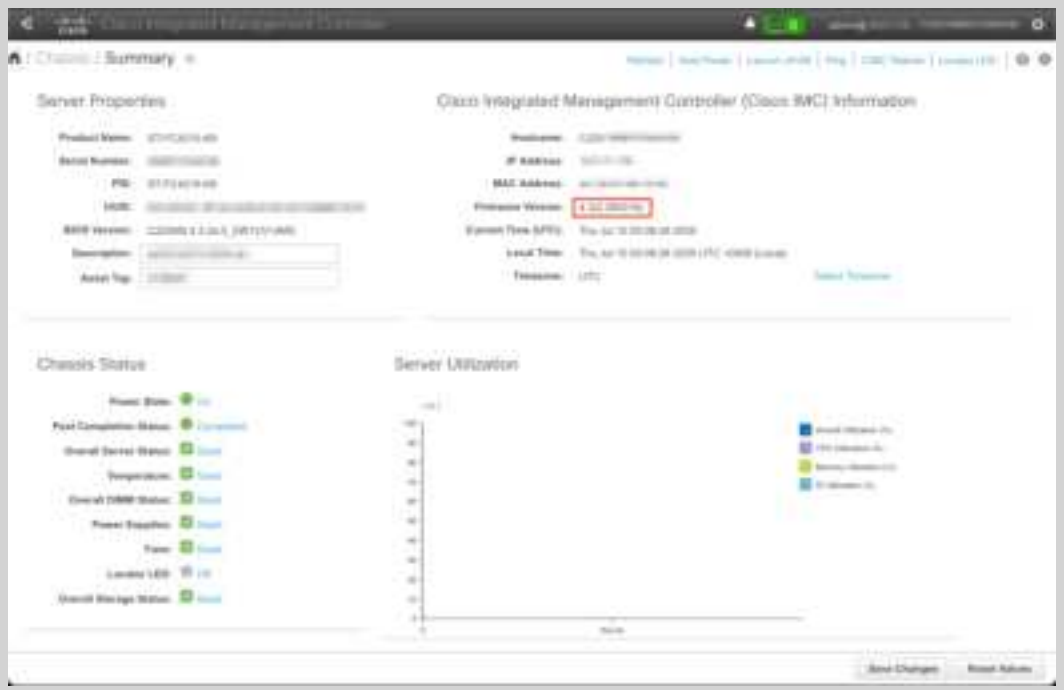


14. When the **Please Select Boot Device** dialog box appears, select **Cisco CIMC-Mapped vDVD1.24**.



The firmware update initiates. The CIMC may reboot during the update process, causing a temporary loss of connection. If this occurs, log in to the CIMC again and re-launch the vKVM Console to continue monitoring the update. Once the firmware update is complete, the ISO will be ejected or unmounted, and the SNA appliance will reboot.

15. Verify on the CIMC Chassis Summary page that the firmware has been updated.



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
    - 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