

Cisco Secure Endpoint Private Cloud Firmware Upgrade

Contents

[Introduction](#)

[Prerequisites](#)

[Required Downtime](#)

[Firmware Upgrade Steps](#)

[Proxy or Connected Mode](#)

[Airgap Mode](#)

[Additional verification](#)

[Legacy Instructions \(For remediation of CVE-2024-20356\)](#)

[Firmware Upgrade Steps](#)

[Proxy or Connected Mode](#)

[Airgap Mode](#)

[Verification Steps](#)

Introduction

This article describes the process of upgrading the firmware for a Cisco Secure Endpoint Private Cloud UCS appliance. Previous documentation regarding remediation of CVE-2024-20356 has been moved to a Legacy Instructions section.

Prerequisites

- Secure Endpoint Private Cloud UCS Appliance with Private Cloud version 4.2.5 or above.
 - Legacy instructions are applicable to a Private Cloud appliance with versions 3.9.x to 4.2.4.
- Access to the Private Cloud UCS Appliance CIMC web UI.

Required Downtime

The RPM upgrade through Opadmin takes approximately 10 minutes. The firmware upgrade itself takes approximately 40 minutes to complete. During this time the Cisco Secure Endpoint functionality will not be available.

After the firmware upgrade is complete, the UCS appliance will be rebooted. This can take another 10 minutes.

Total downtime is approximately 60 minutes.

Firmware Upgrade Steps

Proxy or Connected Mode

1. Navigate to **Operations > Updates**, as shown in the image.



Updates keep your Private Cloud device up to date.

[Check/Download Updates](#)

Content

4.2.5_202503060205

Client Definitions, DFC, Tetra Content Version

[Update Content](#)

Software

4.2.5_202503060300

Private Cloud Software Version

[Update Software](#)

Firmware

4.3(5.240021)

Private Cloud Active Firmware Version

C240M6.4.3.4b.0.0826241055

Private Cloud Active BIOS Version

[Update Firmware](#)

2. The appliance should check for any new firmware updates daily. If it has not been checked and marked as available yet, click the **Check/Download Updates** button.

3. Click the **Update Firmware** button, as shown in the image.

Firmware

4.3(2.240009)

Private Cloud Active Firmware Version

C240M6.4.3.2e.0.1130231848

Private Cloud Active BIOS Version

[Update Firmware](#)

[A firmware update is available.](#)

4. The firmware update will begin, as shown in the image.

🔄 Updating

The device is currently performing an update. Please wait for this page to redirect you; refreshing manually might cause problems.

📊 State	📅 Started	📅 Finished	🕒 Duration
▶ Running	2025-02-21 01:14:03 +0000	⌚ Please wait...	less than a minute

📄 Output

```
-----
Dependencies: Resolved

-----
Package           Arch      Version      Repository      Size
-----
Updating:
 ucs-firmware      x86_64    1:1.8.0-1    dev-firmware    1.8 G

Transaction Summary
-----
Upgrade 1 Package

Total download size: 1.8 G
Downloading packages:
Delta RPMs disabled because /usr/bin/applydelta-rpm not installed.
```

5. Wait for the update to complete. Once it has done so we still need to reboot the appliance and complete the firmware update, see below steps:
6. In your web browser, log into the CIMC web UI of the appliance and open the KVM console.
7. Reboot the appliance with (either from SSH or the CIMC KVM console): *amp-ctl reboot*
8. In the CIMC KVM console, wait for the appliance to reboot. In the boot loader menu, use the down arrow to select **Cisco AMP Private Cloud**:

Please select boot device:

Cisco AMP Private Cloud

Recovery

UEFI: Built-in EFI Shell

UEFI: PXE IPv4 Intel(R) Ethernet Controller X550

UEFI: PXE IPv4 Intel(R) Ethernet Controller X550

Enter Setup

↑ and ↓ to move selection
ENTER to select boot device
ESC to boot using defaults

9. The boot loader will wait a couple of seconds before booting the normal appliance. Use the down arrow to select **UCS Appliance Firmware Update** and press enter:

CentOS Linux (3.10.0-1160.108.1.el7.x86_64) 7 (Core)

Cisco AMP Private Cloud Recovery

UCS Appliance Firmware Update

Use the ▲ and ▼ keys to change the selection.

Press 'e' to edit the selected item, or 'c' for a command prompt.

10. The appliance will boot into the firmware updater, update the firmware and reboot the appliance.
11. The CIMC may log you out during this process.

Airgap Mode

1. Download a new version of amp-sync. In 4.2.5, a new version of amp-sync is available which fetches the firmware updates alongside the content and software updates.
2. Create a new update ISO using amp-sync.
3. Mount the update ISO as for a normal appliance update.
4. Navigate to **Operations > Updates**.
5. Click the **Check Update ISO** button.
6. Once the updates are available, click the **Update Firmware** button.
7. Wait for the update to complete. Once it has done so we still need to reboot the appliance and complete the firmware update, see below steps:
8. In your web browser, log into the CIMC web UI of the appliance and open the KVM console.
9. Reboot the appliance with (either from SSH or the CIMC KVM console): *amp-ctl reboot*
10. In the CIMC KVM console, wait for the appliance to reboot. In the boot loader menu, use the down arrow to select **Cisco AMP Private Cloud**.
11. The boot loader will wait a couple of seconds before booting the normal appliance. Use the down arrow to select **UCS Appliance Firmware Update** and press enter.
12. The appliance will boot into the firmware updater, update the firmware and reboot the appliance.
13. The CIMC may log you out during this process.

Additional verification

1. Navigate to **Operations > Updates**.
2. Confirm that the active firmware and BIOS versions have been updated.
3. Alternatively, in the CIMC web UI, go to the menu: Admin -> Firmware Management as shown in the

Firmware Management

Update

Activate

	Component	Running Version	Backup Version	Bootloader Version	Status	Progress in %
<input type="checkbox"/>	BMC	4.3(2.240009)	4.2(3e)	4.3(2.240009)	Completed Successfully	
<input type="checkbox"/>	BIOS	C240M6.4.3.2e.0_EDR	C240M6.4.3.2e.0_EDR	N/A	Completed Successfully	
<input type="checkbox"/>	Cisco 12G SAS RAID Controller with 4GB FBWC (28 Drives)	52.20.0-4523	N/A	N/A	N/A	N/A
<input type="checkbox"/>	SASEXP1	65160900	65160700	65160700	None	

image.

Legacy Instructions (For remediation of CVE-2024-20356)

These instructions can be used for Private Cloud appliances with versions 3.9.x up to 4.2.4.

Firmware Upgrade Steps

Proxy or Connected Mode

1. Run the following commands on the appliance command line (either through SSH or CIMC KVM): *yum install -y ucs-firmware*
2. In your web browser, log into the CIMC web UI of the appliance and open the KVM console.

3. Reboot the appliance with (either from SSH or the CIMC KVM console): *amp-ctl reboot*
4. In the CIMC KVM console, wait for the appliance to reboot. In the boot loader menu, a new "UCS Appliance Firmware Update" menu item will be available (see screenshot below).
5. The boot loader will wait a couple of seconds before booting the normal appliance. Use the down arrow to select "UCS Appliance Firmware Update" and press enter.
6. The appliance will boot into the firmware updater, update the firmware and reboot the appliance.
7. The CIMC may log you out during this process.



```
CentOS Linux (3.10.0-1160.108.1.el7.x86_64) 7 (Core)
Cisco AMP Private Cloud Recovery
UCS Appliance Firmware Update
```

```
Use the ▲ and ▼ keys to change the selection.
Press 'e' to edit the selected item, or 'c' for a command prompt.
```

Airgap Mode

1. Create a new update ISO using *amp-sync*.
2. Mount the update ISO as for a normal appliance update.
3. Run the following commands on the appliance command line (either through SSH or CIMC KVM): *yum install -y ucs-firmware*
4. In your web browser, log into the CIMC web UI of the appliance and open the KVM console.
5. Reboot the appliance with (either from SSH or the CIMC KVM console): *amp-ctl reboot*
6. In the CIMC KVM console, wait for the appliance to reboot. In the boot loader menu, a new "UCS Appliance Firmware Update" menu item will be available (see screenshot above).
7. The boot loader will wait a couple of seconds before booting the normal appliance. Use the down arrow to select "UCS Appliance Firmware Update" and press enter.
8. The appliance will boot into the firmware updater, update the firmware and reboot the appliance.
9. The CIMC may log you out during this process.

Verification Steps

1. In the CIMC web UI, go to the menu: Admin -> Firmware Management (see example screenshot below).

2. The BMC version should be 4.3(2.240009).

Firmware Management

<div>Update</div> <div>Activate</div>						
	Component	Running Version	Backup Version	Bootloader Version	Status	Progress in %
<input type="checkbox"/>	BMC	4.3(2.240009)	4.2(3e)	4.3(2.240009)	Completed Successfully	
<input type="checkbox"/>	BIOS	C240M6.4.3.2e.0_EDR	C240M6.4.3.2e.0_EDR	N/A	Completed Successfully	
<input type="checkbox"/>	Cisco 12G SAS RAID Controller with 4GB FBWC (28 Drives)	52.20.0-4523	N/A	N/A	N/A	N/A
<input type="checkbox"/>	SASEXP1	65160900	65160700	65160700	None	