

# Atualização do firmware da nuvem privada do Cisco Secure Endpoint

## Contents

---

[Introdução](#)

[Pré-requisitos](#)

[Tempo de inatividade necessário](#)

[Etapas de atualização do firmware](#)

[Modo Proxy ou Conectado](#)

[Modo Airgap](#)

[Verificação adicional](#)

[Instruções antigas \(para correção do CVE-2024-20356\)](#)

[Etapas de atualização do firmware](#)

[Modo Proxy ou Conectado](#)

[Modo Airgap](#)

[Etapas de verificação](#)

---

## Introdução

Este artigo descreve o processo de atualização do firmware para um dispositivo Cisco Secure Endpoint Private Cloud UCS. A documentação anterior referente à remediação do CVE-2024-20356 foi movida para uma seção de instruções legadas.

## Pré-requisitos

- Secure Endpoint Private Cloud UCS Appliance com Private Cloud versão 4.2.5 ou superior.
  - As instruções herdadas são aplicáveis a um dispositivo de nuvem privada com versões 3.9.x a 4.2.4.
- Acesso à interface de usuário da Web do CIMC do dispositivo UCS de nuvem privada.

## Tempo de inatividade necessário

A atualização do RPM através do Opadmin leva aproximadamente 10 minutos. A própria atualização do firmware leva aproximadamente 40 minutos para ser concluída. Durante esse período, a funcionalidade do Cisco Secure Endpoint não estará disponível.

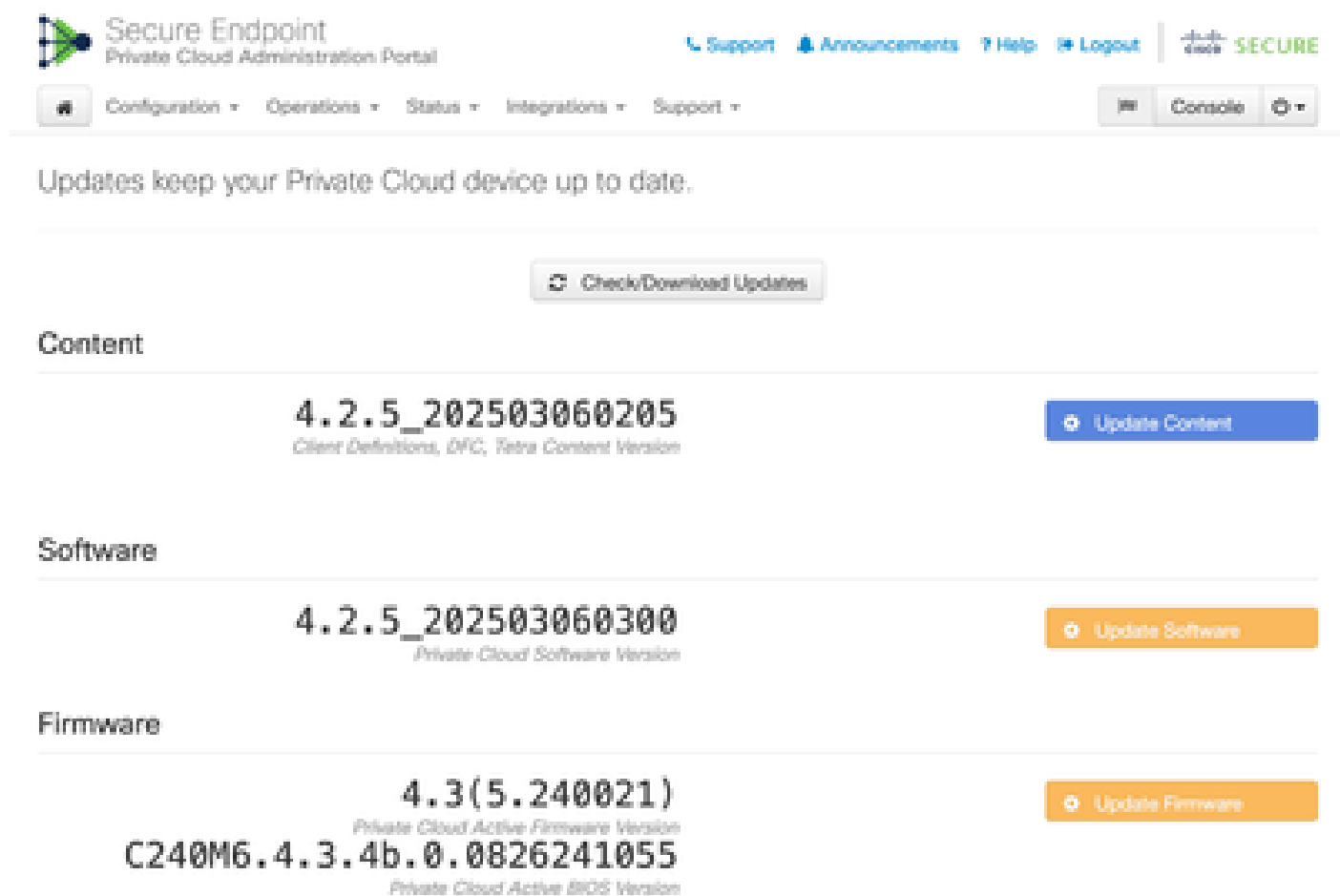
Após a conclusão da atualização do firmware, o dispositivo UCS será reinicializado. Isso pode levar mais 10 minutos.

O tempo de inatividade total é de aproximadamente 60 minutos.

## Etapas de atualização do firmware

## Modo Proxy ou Conectado

1. Navegue até Operações > Atualizações, conforme mostrado na imagem.

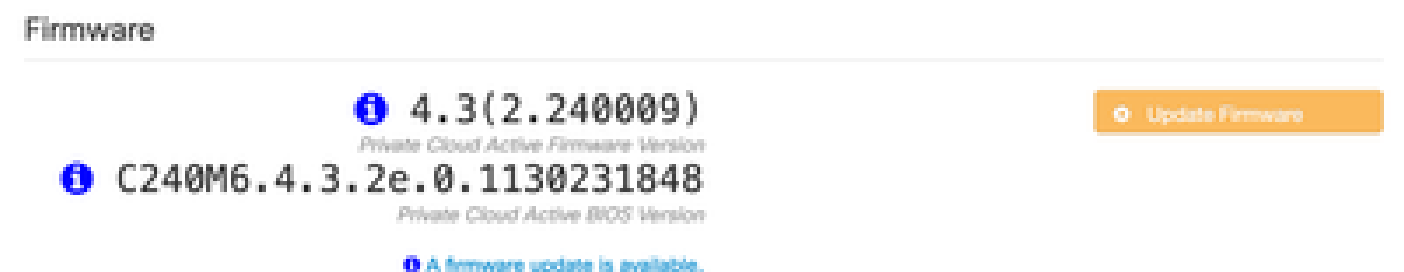


The screenshot shows the 'Secure Endpoint Private Cloud Administration Portal'. The top navigation bar includes links for Support, Announcements, Help, and Logout, along with a 'SECURE' status indicator. Below the navigation bar, there's a section titled 'Updates keep your Private Cloud device up to date.' with a 'Check/Download Updates' button. The main content area is divided into three sections: 'Content', 'Software', and 'Firmware'. Each section displays a version number and a corresponding 'Update' button.

| Section  | Version                                                                                                                                 | Update Button   |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| Content  | 4.2.5_202503060205<br><i>Client Definitions, DFC, Telemetry Content Version</i>                                                         | Update Content  |
| Software | 4.2.5_202503060300<br><i>Private Cloud Software Version</i>                                                                             | Update Software |
| Firmware | 4.3(5.240021)<br><i>Private Cloud Active Firmware Version</i><br>C240M6.4.3.4b.0.0826241055<br><i>Private Cloud Active BIOS Version</i> | Update Firmware |

2. O equipamento deverá verificar diariamente se há atualizações de firmware novas. Se ele ainda não tiver sido marcado e marcado como disponível, clique no botão Check/Download Updates.

3. Clique no botão Update Firmware, como mostrado na imagem.



This screenshot shows the 'Firmware' section of the portal. It displays the current firmware version '4.3(2.240009)' and the BIOS version 'C240M6.4.3.2e.0.1130231848'. An information icon (i) is present next to the version numbers. A blue banner at the bottom states 'A firmware update is available.' The 'Update Firmware' button is highlighted in orange.

| Section  | Version                                                                                                                                                                           | Update Button   |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| Firmware | 4.3(2.240009)<br><i>Private Cloud Active Firmware Version</i><br>C240M6.4.3.2e.0.1130231848<br><i>Private Cloud Active BIOS Version</i><br><i>A firmware update is available.</i> | Update Firmware |

4. A atualização do firmware será iniciada, conforme mostrado na imagem.

## 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    1:1.0.0-1    dev-firmware    1.8 G

Transaction Summary
-----
Upgrade 1 Package

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

5. Aguarde até que a atualização seja concluída. Depois de fazer isso, ainda precisamos reinicializar o dispositivo e concluir a atualização do firmware. Consulte as etapas abaixo:
6. No navegador da Web, faça login na interface do usuário da Web do CIMC do equipamento e abra o console KVM.
7. Reinicialize o dispositivo com (a partir do SSH ou do console KVM do CIMC): reinicialização de `amp-ctl`
8. No console KVM do CIMC, aguarde a reinicialização do equipamento. No menu do carregador de inicialização, use a seta para baixo para selecionar 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. O carregador de inicialização aguardará alguns segundos antes de inicializar o equipamento normal. Use a seta para baixo para selecionar UCS Appliance Firmware Update e pressione 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. O equipamento será inicializado no atualizador de firmware, atualizará o firmware e reinicializará o equipamento.

11. O CIMC pode desconectá-lo durante esse processo.

## Modo Airgap

1. Baixe uma nova versão do amp-sync. Na versão 4.2.5, uma nova versão do amp-sync está disponível, que busca as atualizações de firmware juntamente com as atualizações de conteúdo e software.
2. Crie um novo ISO de atualização usando amp-sync.
3. Monte o ISO de atualização como para uma atualização normal do equipamento.
4. Navegue até Operações > Atualizações.
5. Clique no botão Check Update ISO.
6. Quando as atualizações estiverem disponíveis, clique no botão Update Firmware.
7. Aguarde até que a atualização seja concluída. Depois de fazer isso, ainda precisamos reinicializar o dispositivo e concluir a atualização do firmware. Consulte as etapas abaixo:
8. No navegador da Web, faça login na interface do usuário da Web do CIMC do equipamento e abra o console KVM.
9. Reinicialize o dispositivo com (a partir do SSH ou do console KVM do CIMC): reinicialização de amp-ctl
10. No console KVM do CIMC, aguarde a reinicialização do equipamento. No menu do

carregador de inicialização, use a seta para baixo para selecionar Cisco AMP Private Cloud.

11. O carregador de inicialização aguardará alguns segundos antes de inicializar o equipamento normal. Use a seta para baixo para selecionar UCS Appliance Firmware Update e pressione Enter.
12. O equipamento será inicializado no atualizador de firmware, atualizará o firmware e reinicializará o equipamento.
13. O CIMC pode desconectá-lo durante esse processo.

## Verificação adicional

1. Navegue até Operações > Atualizações.
2. Confirme se as versões ativa do firmware e do BIOS foram atualizadas.
3. Como alternativa, na IU da Web do CIMC, vá para o menu: Admin -> Firmware Management

(Gerenciamento de firmware), conforme mostrado na imagem.



| Component | Available Version | Installed Version | Available Version | Status                 | Progress % |
|-----------|-------------------|-------------------|-------------------|------------------------|------------|
| BIOS      | 4.22 (202401)     | 4.22 (202401)     | 4.22 (202401)     | Completed Successfully | 100        |
| UEFI      | 4.22 (202401)     | 4.22 (202401)     | 4.22 (202401)     | Completed Successfully | 100        |
| UEFI BIOS | 4.22 (202401)     | 4.22 (202401)     | 4.22 (202401)     | Completed Successfully | 100        |
| UEFI BIOS | 4.22 (202401)     | 4.22 (202401)     | 4.22 (202401)     | Completed Successfully | 100        |

## Instruções antigas (para correção do CVE-2024-20356)

Essas instruções podem ser usadas para dispositivos de nuvem privada com versões 3.9.x até 4.2.4.

## Etapas de atualização do firmware

### Modo Proxy ou Conectado

1. Execute os seguintes comandos na linha de comando do equipamento (através do SSH ou do CIMC KVM): `yum install -y ucs-firmware`
2. No navegador da Web, faça login na interface do usuário da Web do CIMC do equipamento e abra o console KVM.
3. Reinicialize o dispositivo com (a partir do SSH ou do console KVM do CIMC): reinicialização de `amp-ctl`
4. No console KVM do CIMC, aguarde a reinicialização do equipamento. No menu do carregador de inicialização, um novo item do menu "Atualização do firmware do dispositivo UCS" estará disponível (veja a captura de tela abaixo).
5. O carregador de inicialização aguardará alguns segundos antes de inicializar o equipamento normal. Use a seta para baixo para selecionar "Atualização do firmware do dispositivo UCS" e pressione Enter.
6. O equipamento será inicializado no atualizador de firmware, atualizará o firmware e reinicializará o equipamento.
7. O CIMC pode desconectá-lo durante esse processo.

```
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.
```

## Modo Airgap

1. Crie um novo ISO de atualização usando amp-sync.
2. Monte o ISO de atualização como para uma atualização normal do equipamento.
3. Execute os seguintes comandos na linha de comando do equipamento (através do SSH ou do CIMC KVM): `yum install -y ucs-firmware`
4. No navegador da Web, faça login na interface do usuário da Web do CIMC do equipamento e abra o console KVM.
5. Reinicialize o dispositivo com (a partir do SSH ou do console KVM do CIMC): reinicialização de `amp-ctl`
6. No console KVM do CIMC, aguarde a reinicialização do equipamento. No menu do carregador de inicialização, um novo item do menu "Atualização do firmware do dispositivo UCS" estará disponível (veja a captura de tela acima).
7. O carregador de inicialização aguardará alguns segundos antes de inicializar o equipamento normal. Use a seta para baixo para selecionar "Atualização do firmware do dispositivo UCS" e pressione Enter.
8. O equipamento será inicializado no atualizador de firmware, atualizará o firmware e reinicializará o equipamento.
9. O CIMC pode desconectá-lo durante esse processo.

## Etapas de verificação

1. Na IU da Web do CIMC, vá para o menu: Admin -> Firmware Management (veja a captura

de tela abaixo).

2. A versão do BMC deve ser 4.3(2.240009).

#### Firmware Management

| <div>Update 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                   |               |

### Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.