

# Atualize a infraestrutura e o firmware do servidor no modo gerenciado Intersight para Intersight Private Virtual Appliance.

## Contents

---

### [Introdução](#)

#### [Pré-requisitos](#)

##### [Requisitos](#)

##### [Componentes Utilizados](#)

#### [Informações de Apoio](#)

#### [Configurar](#)

##### [Antes de Começar](#)

#### [Atualização de interconexão de estrutura](#)

#### [Atualização do servidor](#)

#### [Verificar](#)

#### [Informações Relacionadas](#)

---

## Introdução

Este documento descreve o processo de atualização para um domínio e servidor UCS em um Private Virtual Appliance (PVA).

### Pré-requisitos

#### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento geral e compreensão do Modo Gerenciado de Intervisão (IMM).
- Compreensão do PVA (Private Virtual Appliance) da Intersight.

#### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Interconexão em malha Cisco UCS 6454 de 54 portas, firmware 4.2.3(d)
- Servidor blade Cisco UCS B200 M5, firmware 4.2.1(a)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos usados neste documento começaram com uma configuração limpa (padrão). Se a rede estiver ativa, certifique-se de que você entenda o impacto

potencial de qualquer comando.

## Informações de Apoio

Um Private Virtual Appliance (PVA) é uma versão local da plataforma Cisco Intersight encapsulada em uma máquina virtual. Ele fornece os mesmos recursos e benefícios que o serviço Intersight baseado em nuvem, incluindo gerenciamento e automação de infraestrutura, mas dentro de uma rede privada. Isso atende às necessidades das empresas que exigem um alto nível de segurança de dados, como aquelas com requisitos rigorosos de conformidade e regulamentação.

Pacotes de pacotes de software para ambientes PVA são armazenados no Intersight e estão disponíveis para download através da conta do Dispositivo Intersight.

## Configurar

### Antes de Começar

Navegue até este link para configurar sua conta: [Criando uma conta do equipamento](#). Siga as etapas, aceite o contrato de licença e crie um nome de conta para ele.

## Atualização de interconexão de estrutura

Etapa 1. Depois que a conta do equipamento for criada, navegue para Downloads de software > Catálogo de software > Firmware.

Procure a versão do firmware a ser acessada. Clique em seu nome.

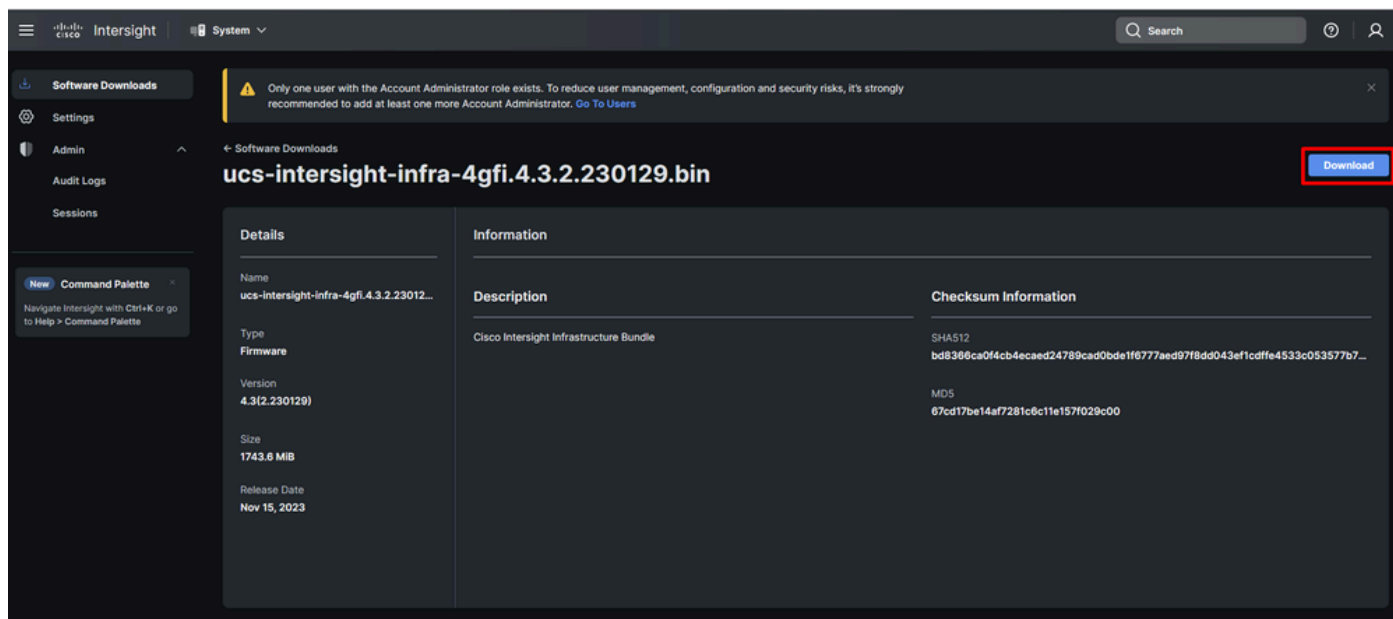


Dica: expanda a coluna de nome para ver o modelo do dispositivo e a versão.

Name	Type	Version	Size	Description	Release Date
intersight-ucs-server-410c-m7.5.2.0.230092.bin	Firmware	5.2(0.230092)	707.5 MB	Cisco Intersight Server Bundle	Nov 15, 2023
intersight-ucs-server-210c-m7.5.2.0.230092.bin	Firmware	5.2(0.230092)	710.4 MB	Cisco Intersight Server Bundle	Nov 15, 2023
intersight-ucs-infra-5gfl-4.3.2.230129.bin	Firmware	4.3(2.230129)	1784.3 MB	Cisco Intersight Infrastructur...	Nov 15, 2023
ucs-intersight-infra-4gfl-4.3.2.230129.bin	Firmware	4.3(2.230129)	1743.6 MB	Cisco Intersight Infrastructur...	Nov 15, 2023
intersight-ucs-server-210c-m6.5.2.0.230092.bin	Firmware	5.2(0.230092)	608.8 MB	Cisco Intersight Server Bundle	Nov 15, 2023
intersight-ucs-server-b200-m6.5.2.0.230100.bin	Firmware	5.2(0.230100)	566.6 MB	Cisco Intersight Server Bundle	Nov 15, 2023
intersight-ucs-server-b480-m5.5.2.0.230100.bin	Firmware	5.2(0.230100)	583.1 MB	Cisco Intersight Server Bundle	Nov 15, 2023
intersight-ucs-server-b200-m5.5.2.0.230100.bin	Firmware	5.2(0.230100)	583.1 MB	Cisco Intersight Server Bundle	Nov 15, 2023
intersight-ucs-server-c240-m7.4.3.2.230270.bin	Firmware	4.3(2.230270)	826.5 MB	Cisco Intersight Server Bundle	Nov 15, 2023
intersight-ucs-server-c220-m7.4.3.2.230270.bin	Firmware	4.3(2.230270)	805 MB	Cisco Intersight Server Bundle	Nov 15, 2023
intersight-ucs-server-c245-m6.4.3.2.230270.bin	Firmware	4.3(2.230270)	724.2 MB	Cisco Intersight Server Bundle	Nov 15, 2023
intersight-ucs-server-c225-m6.4.3.2.230270.bin	Firmware	4.3(2.230270)	712 MB	Cisco Intersight Server Bundle	Nov 15, 2023

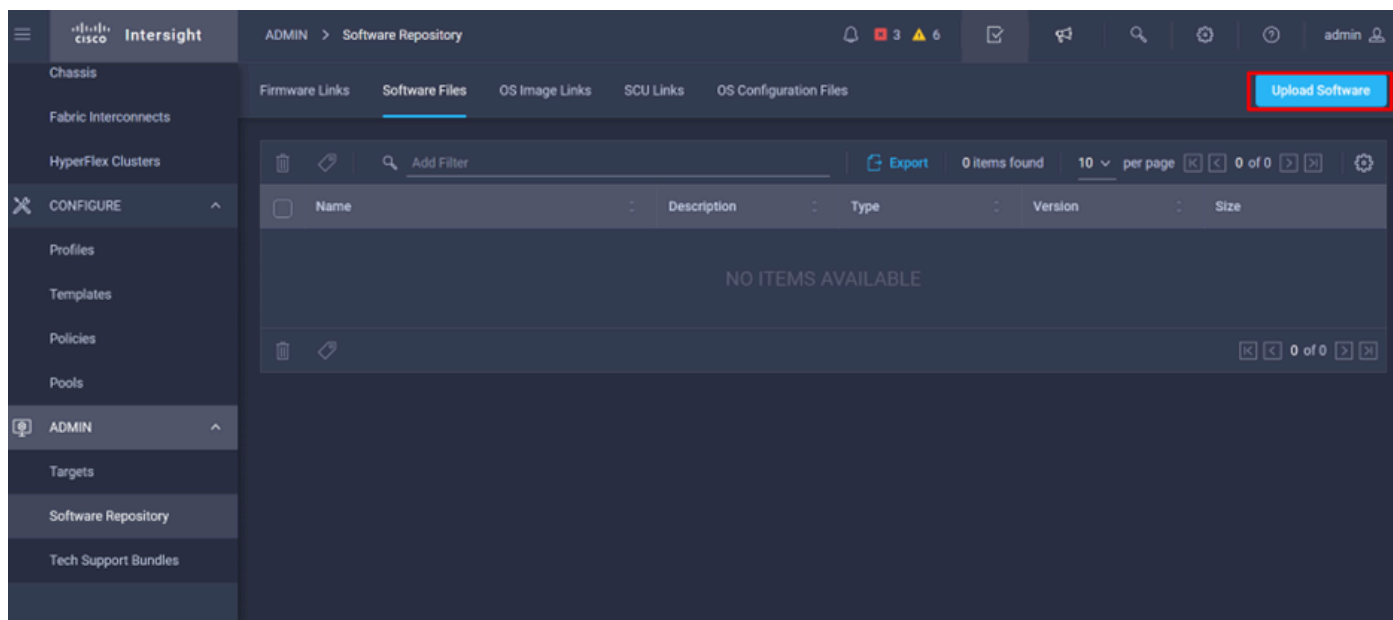
Etapa 2. Na nova janela, você pode ver algumas informações mais detalhadas sobre o pacote.

Certifique-se de que é o que você precisa. Clique no botão Download. Para este exemplo, a atualização da estrutura é para 4.3.2.

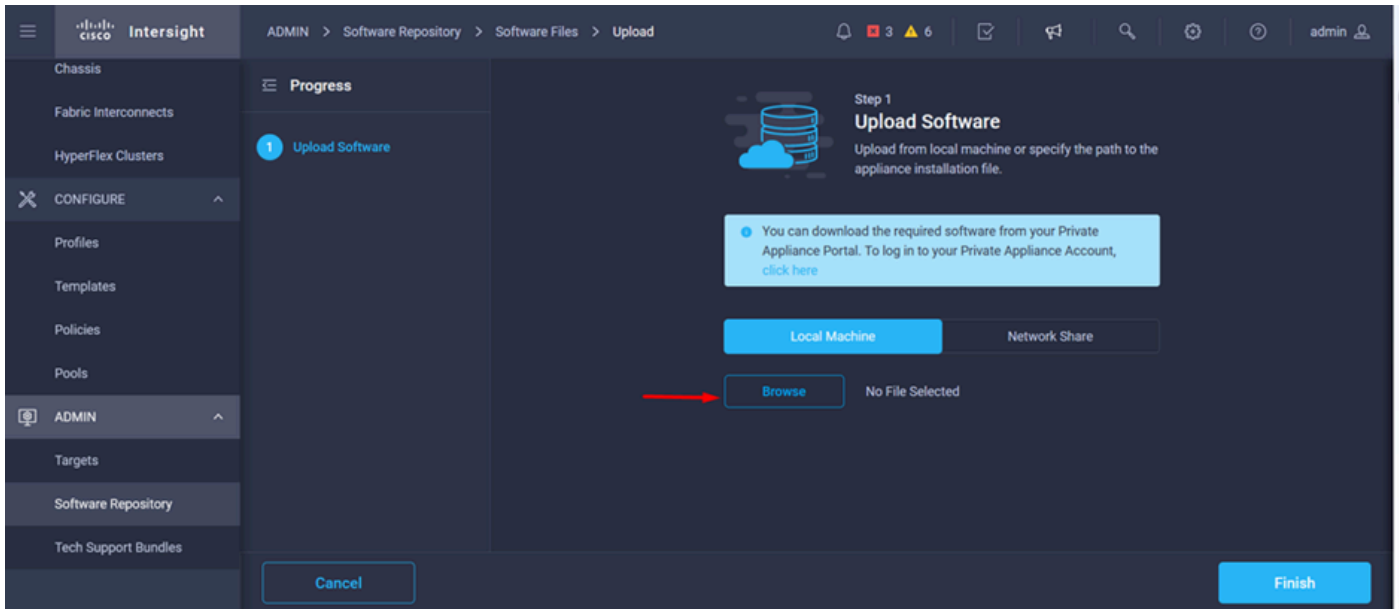


Etapa 3. Quando o download estiver concluído, abra uma guia no navegador e faça login no dispositivo virtual privado.

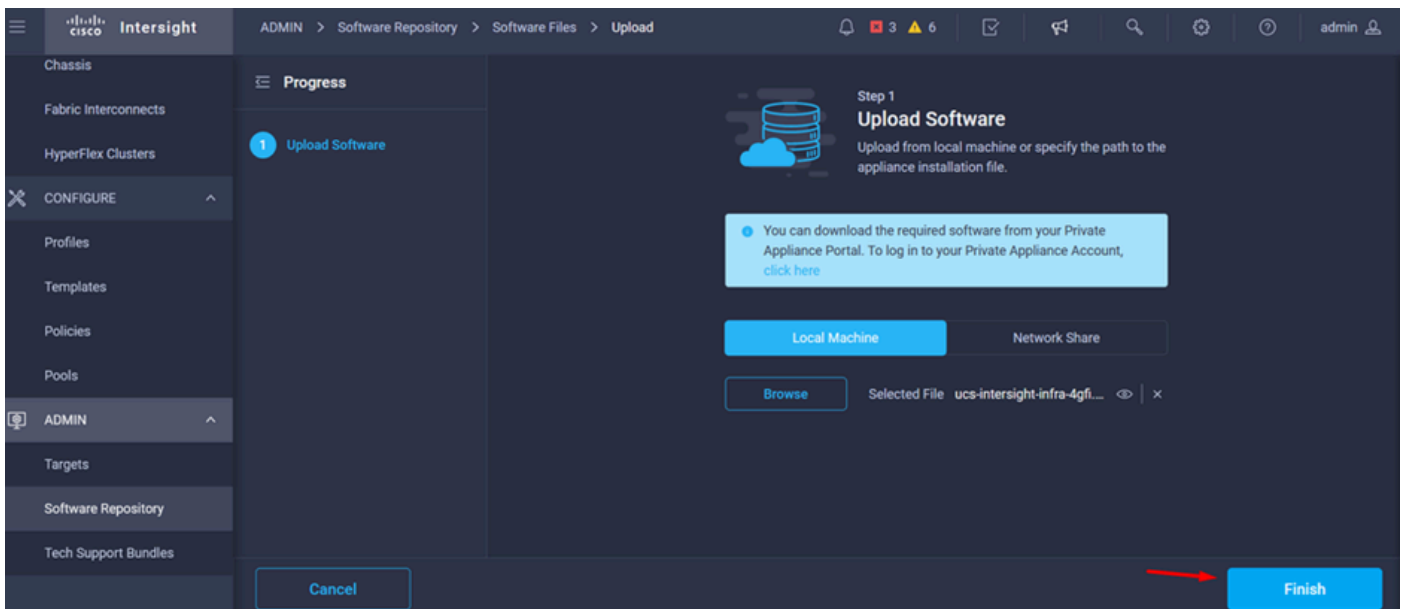
Navegue até Admin > Repositório de software > Arquivos de software. Nessa guia, você pode ver a lista de pacotes disponíveis para atualização e clicar em Carregar software.



Etapa 4. Procure o pacote para sua Interconexão de estrutura e carregue-o.

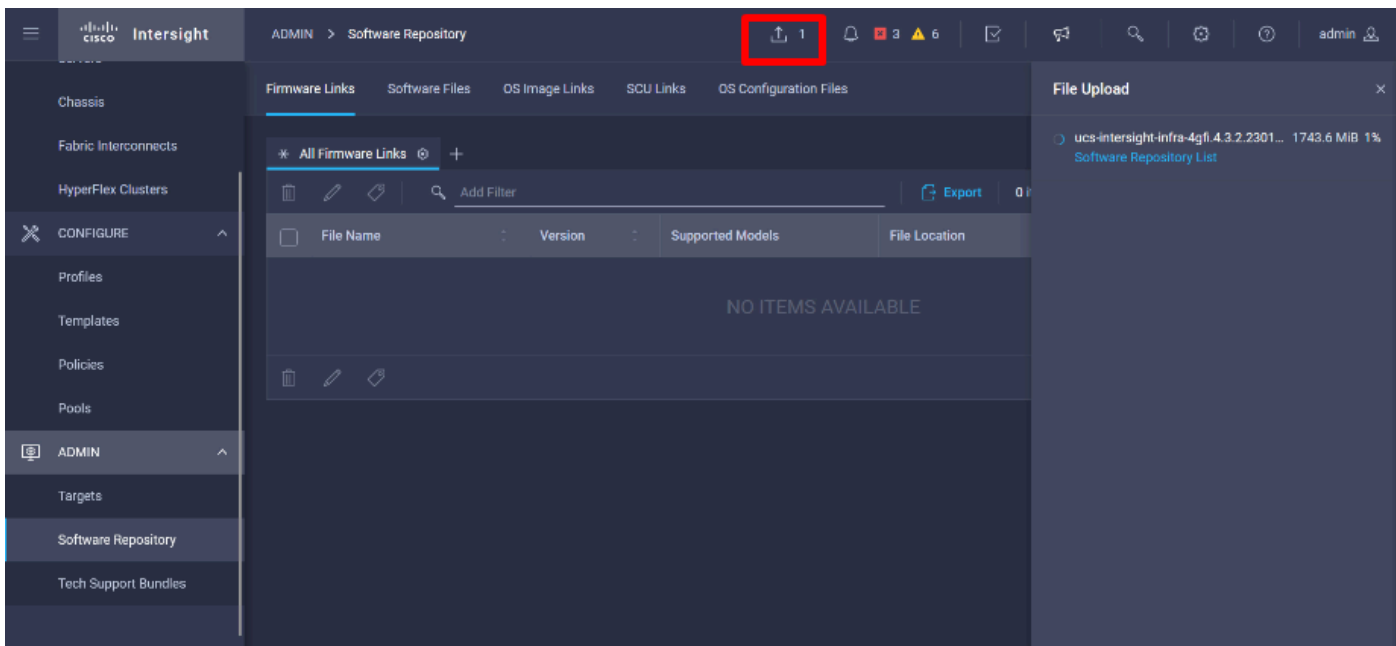


Etapa 5. Depois de mapeada, clique no botão Finish.

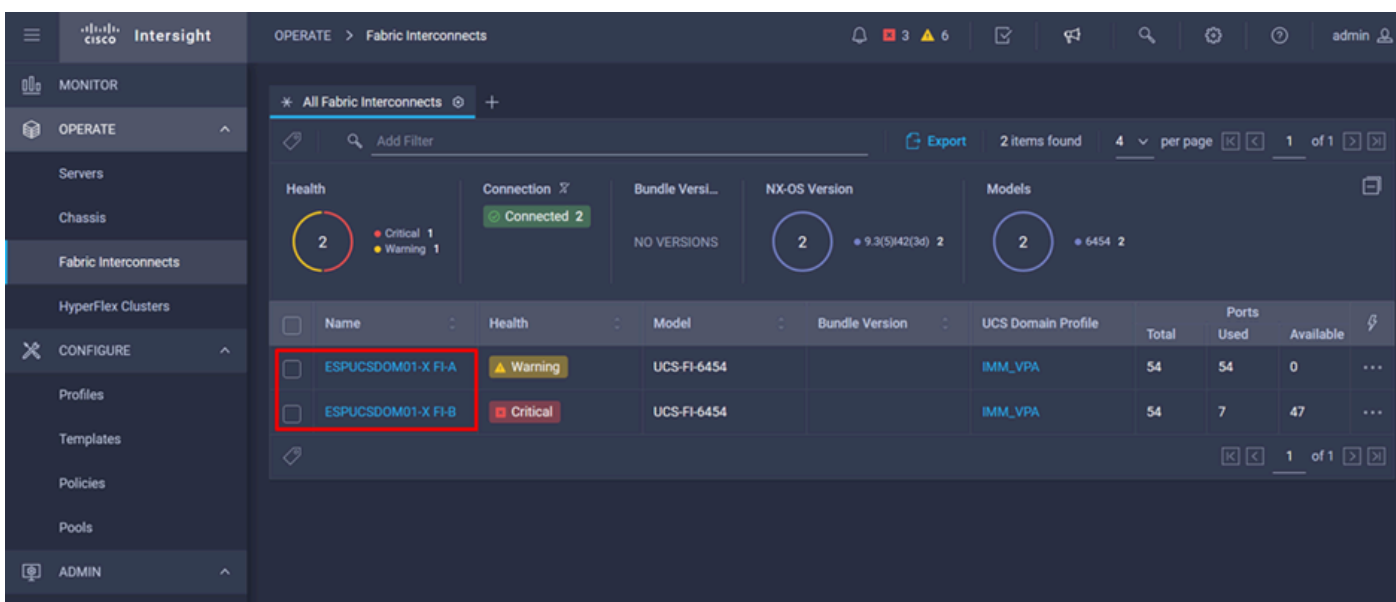


Etapa 6. Você pode ver o progresso no ícone à esquerda do botão Alerta.

Na guia Arquivos de software, confirme se seus downloads estão prontos para uso. Atualize a página, se necessário.



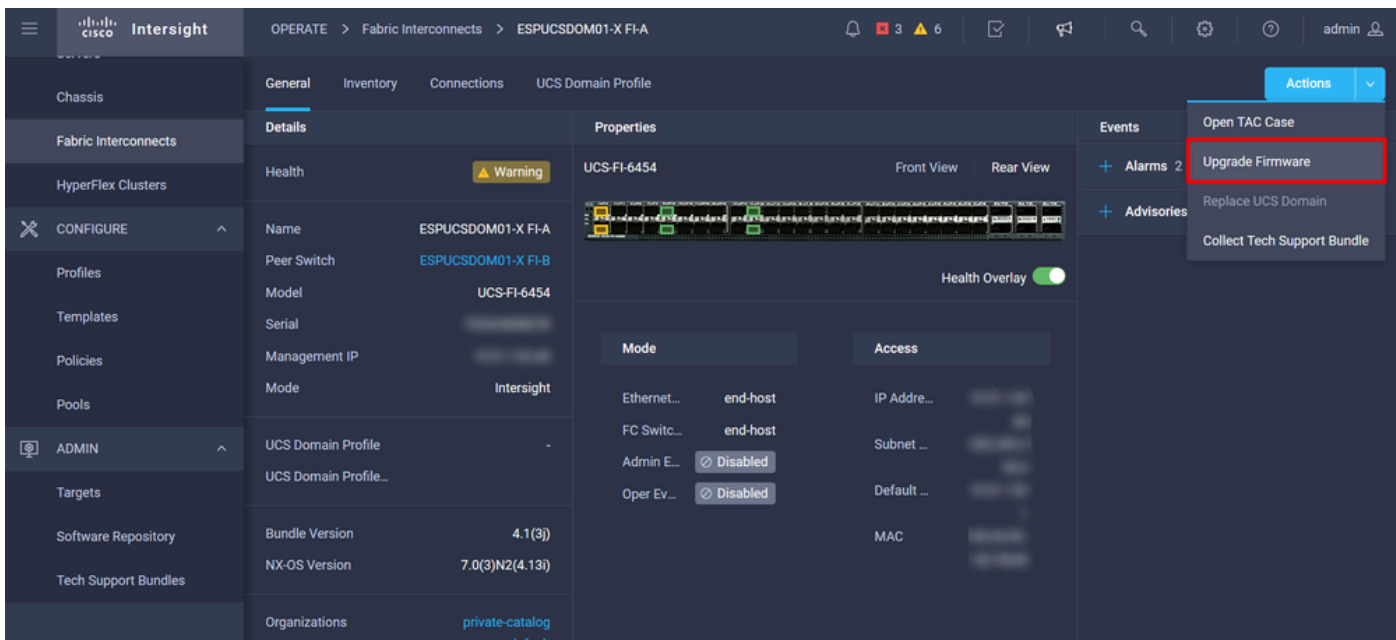
Passo 7. Navegue até Operate > Fabric Interconnects. Selecione o dispositivo que você precisa atualizar. Clique em qualquer Interconexão de estrutura (FI) que pertença ao cluster que você precisa atualizar.



Etapa 8. Verifique se você selecionou a Interconexão de estrutura correta.

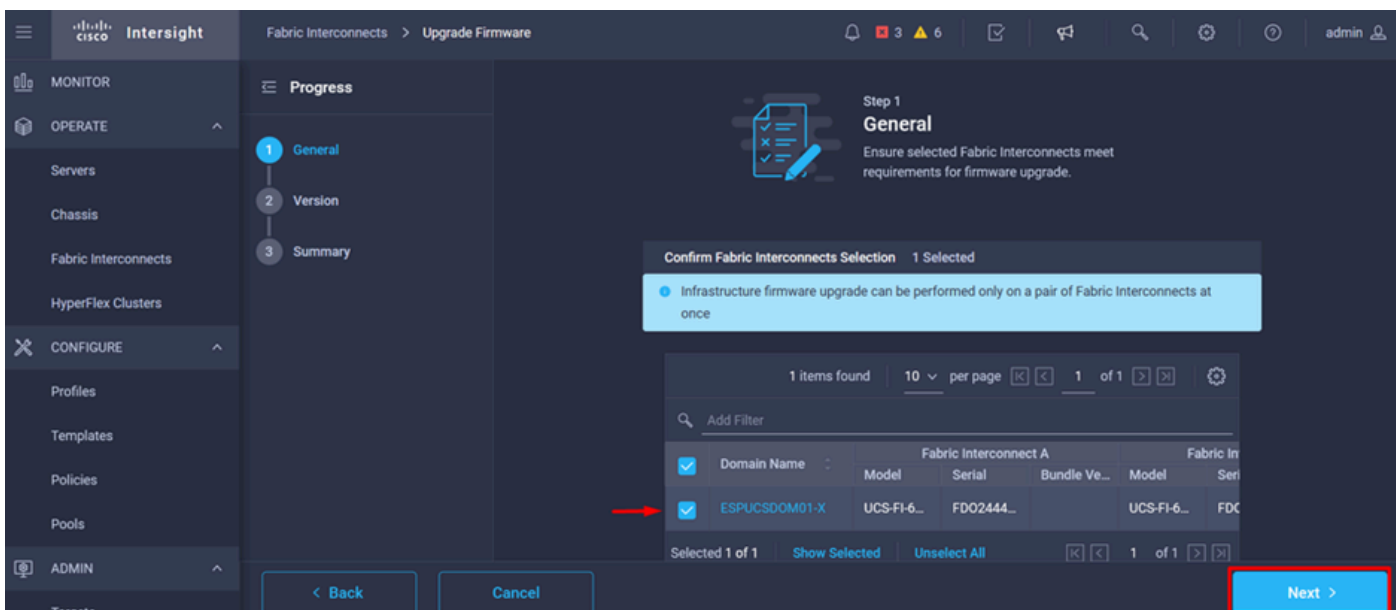
Na guia Detalhes, você pode revisar informações gerais como o switch peer, o IP de gerenciamento e a versão atual.

Etapa 9. Navegue até o botão Ação. Clique nele, ele exibe algumas opções, escolha Atualizar firmware.

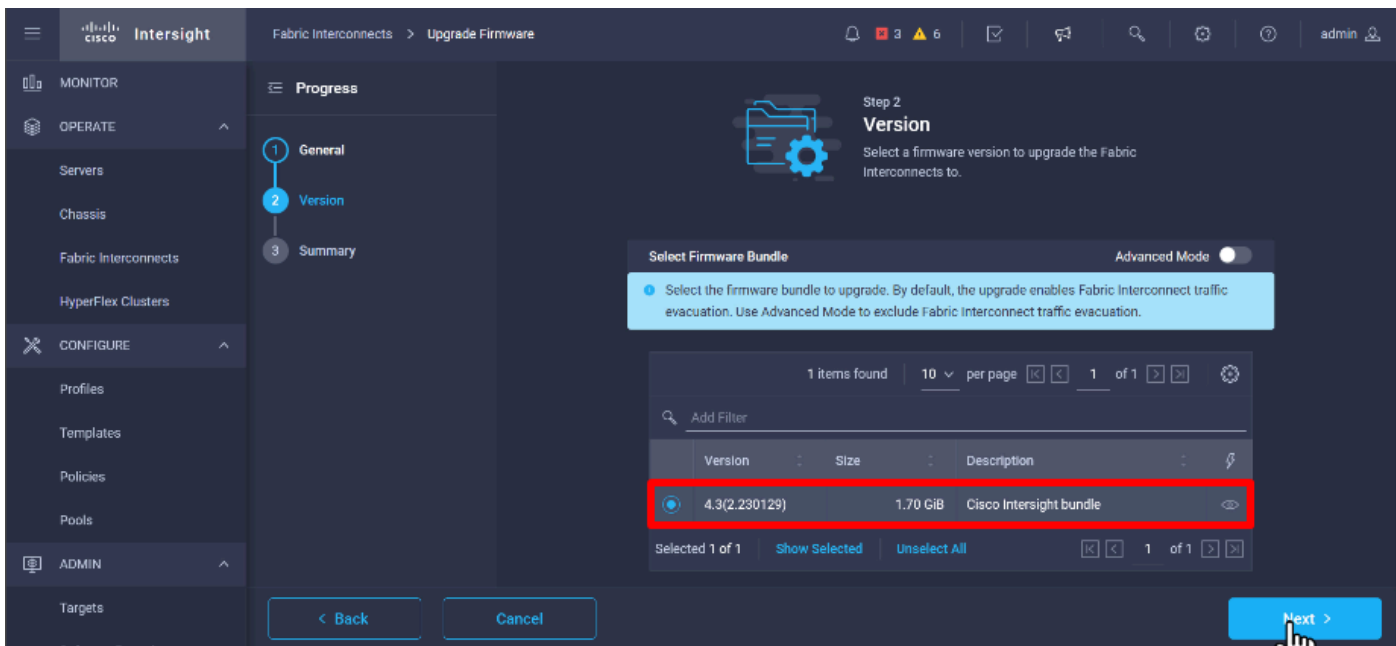


Etapa 10. Uma janela é exibida com instruções básicas sobre como executar a atualização. Clique em Iniciar.

Etapa 11. Você pode ver a lista de Interconexão de estrutura reivindicada pela Intersight. O domínio no qual você clicou anteriormente é selecionado automaticamente.

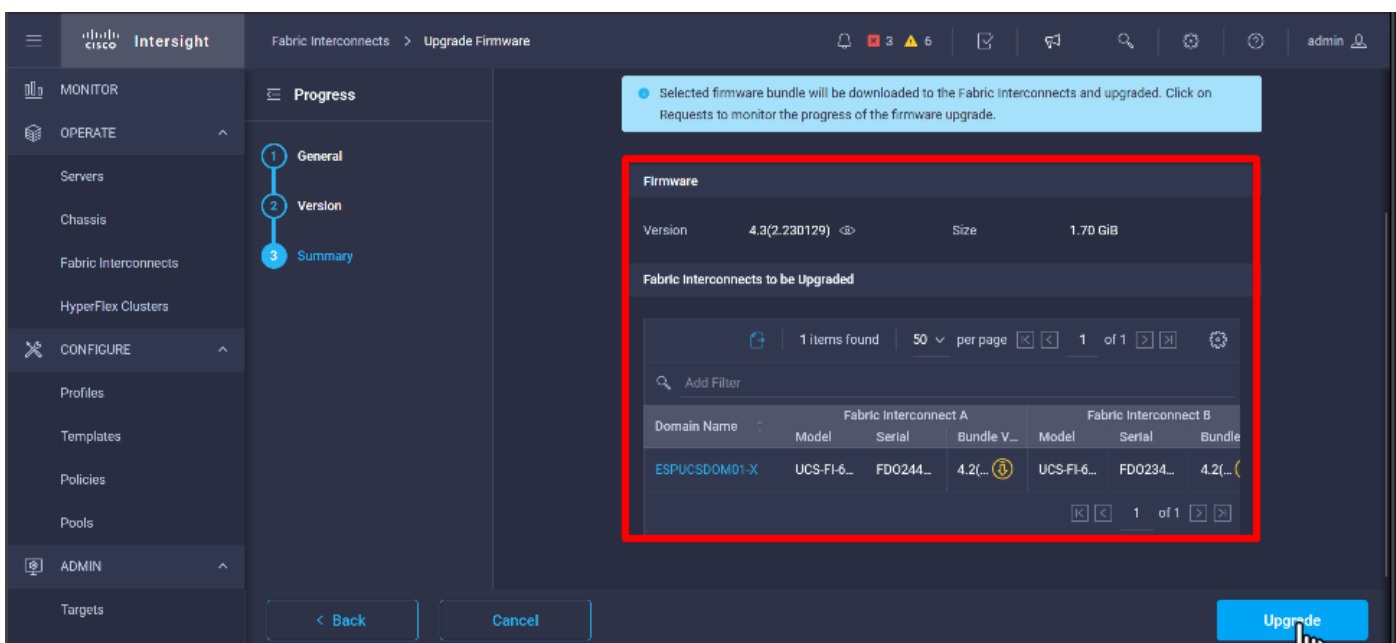


Etapa 12. Para este exemplo, a versão do pacote 4.3.2 está disponível. Selecione sua versão e clique em Avançar para continuar.

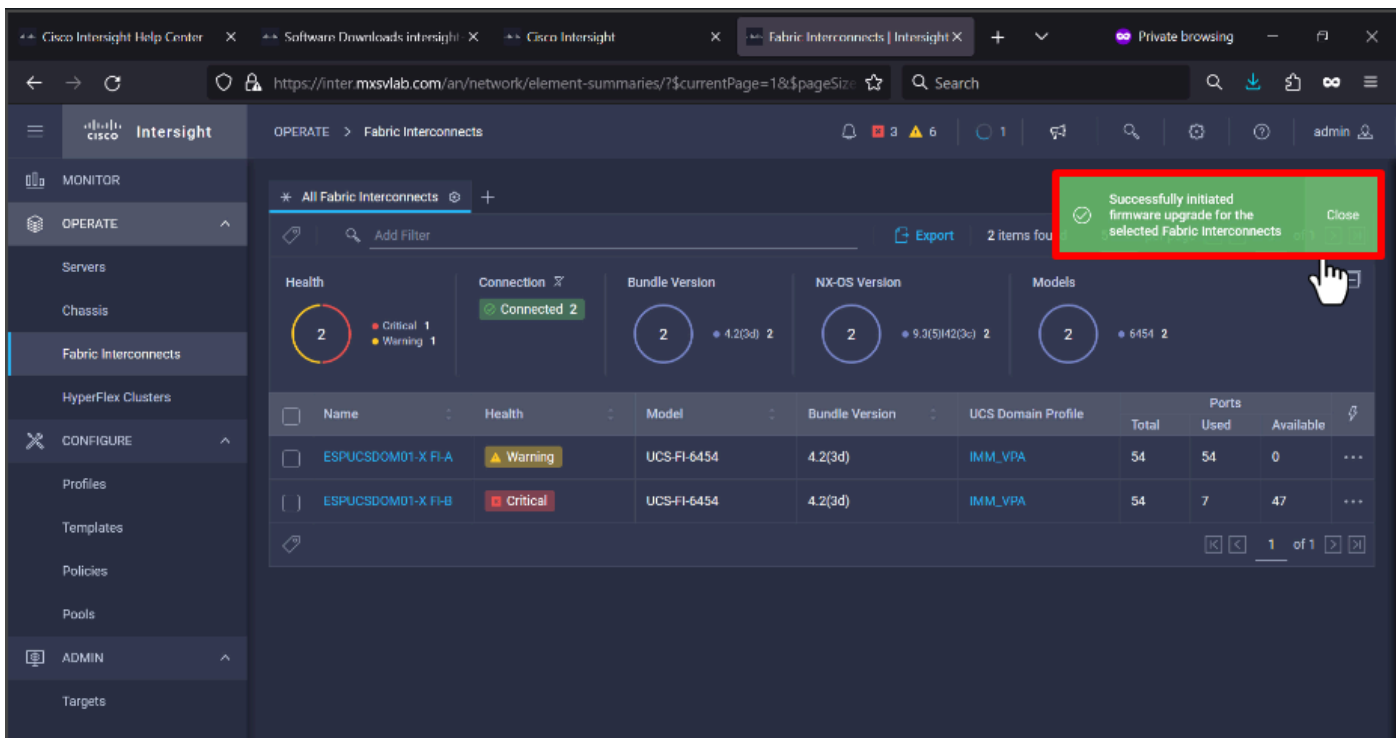


Etapa 13. Ele mostra um resumo da sua atualização: o nome de domínio, o número de série, o modelo e a versão do firmware.

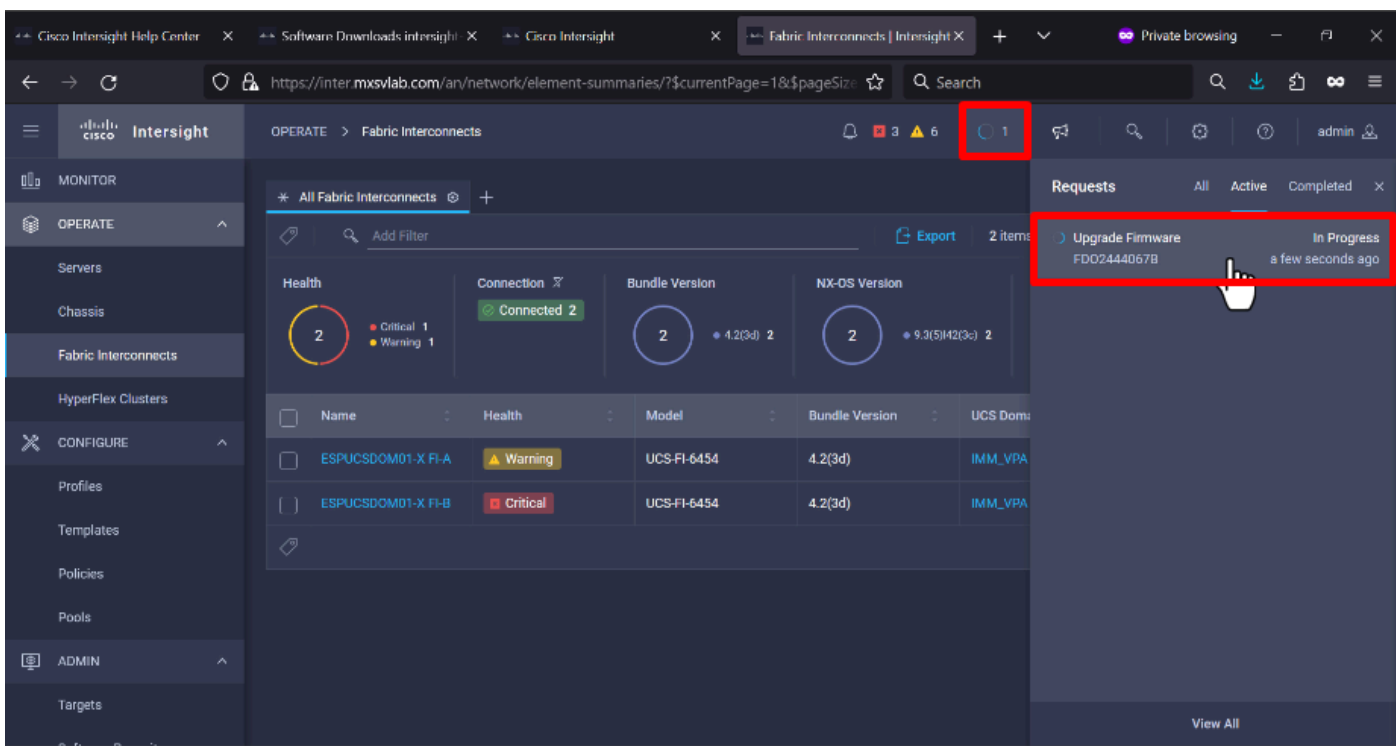
Confirme se este é o domínio correto e clique em Upgrade.



Etapa 14. Uma caixa verde aparecerá no canto superior direito se a ação de atualização tiver sido bem-sucedida.

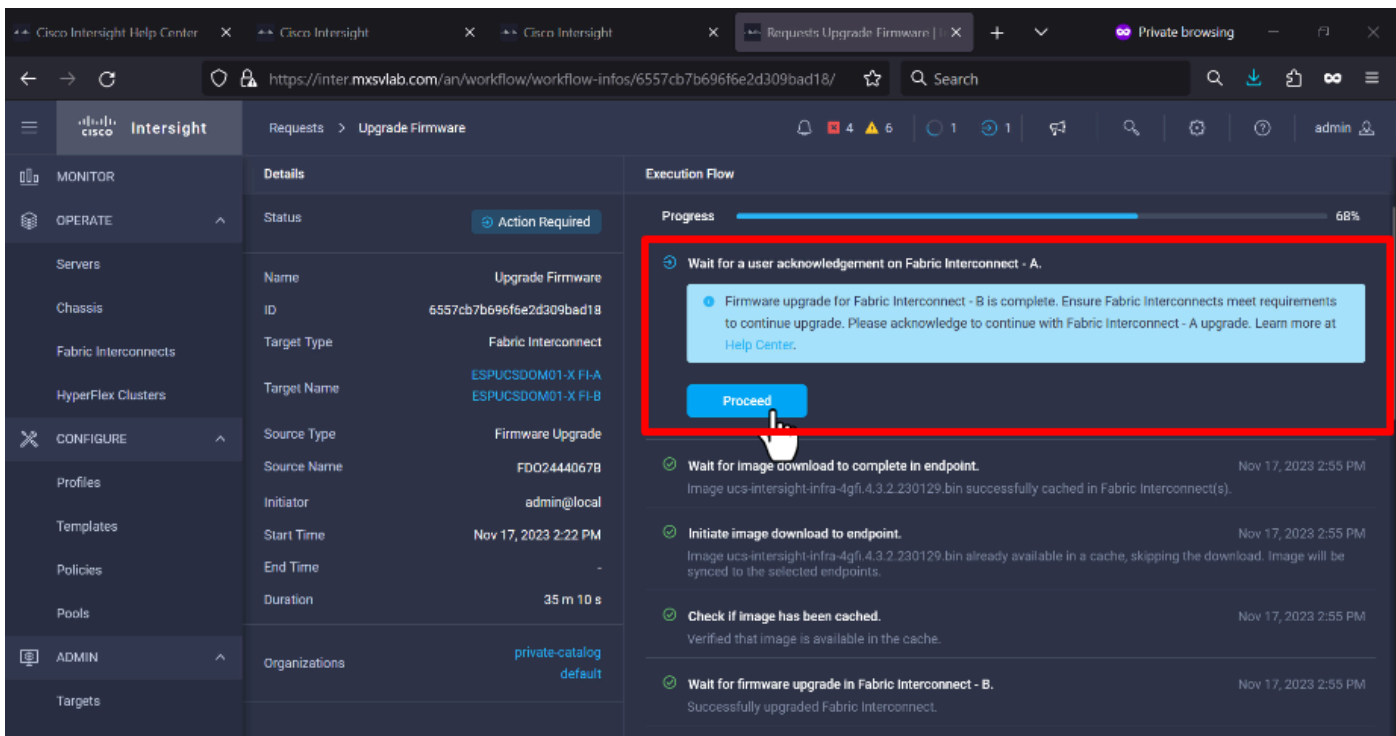


Etapa 15. Pressione o ícone ao lado do botão de alarme para verificar o progresso da atualização.



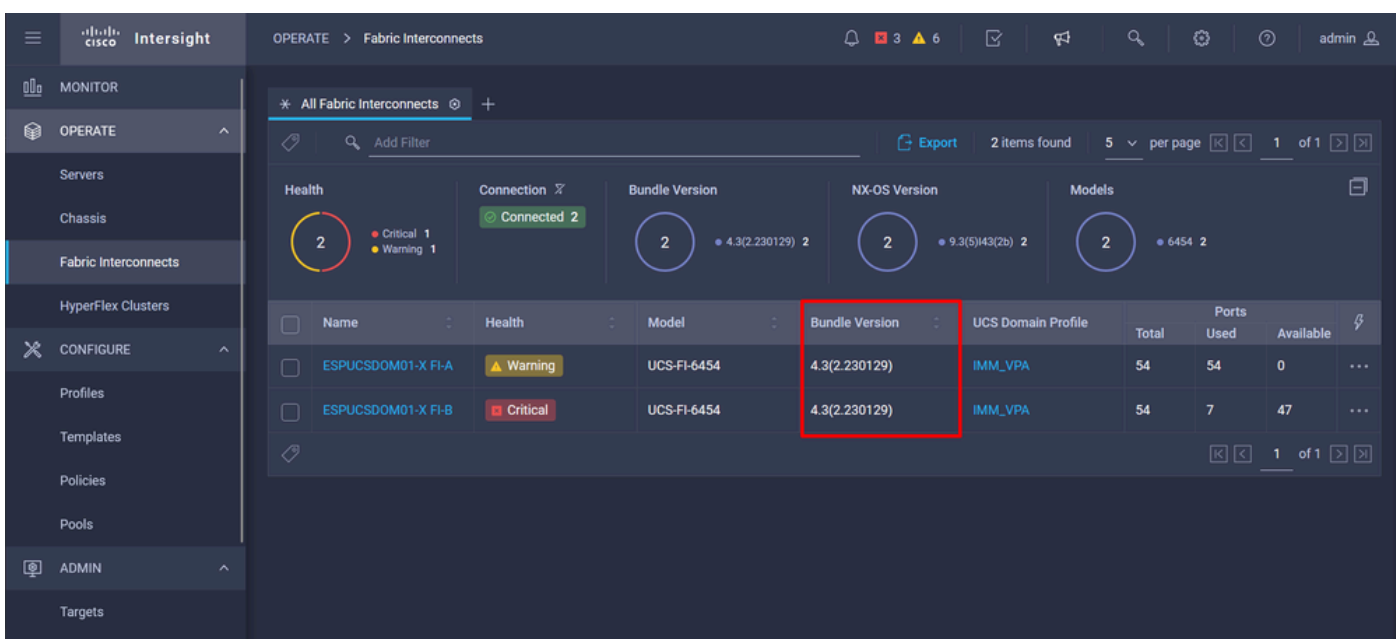
Etapa 16. Requer uma confirmação para a reinicialização da malha. Clique em Continuar para continuar com a atualização.





Etapa 17. Verifique se a atualização foi concluída com êxito na coluna Versão do pacote da guia Interconexões de estrutura.

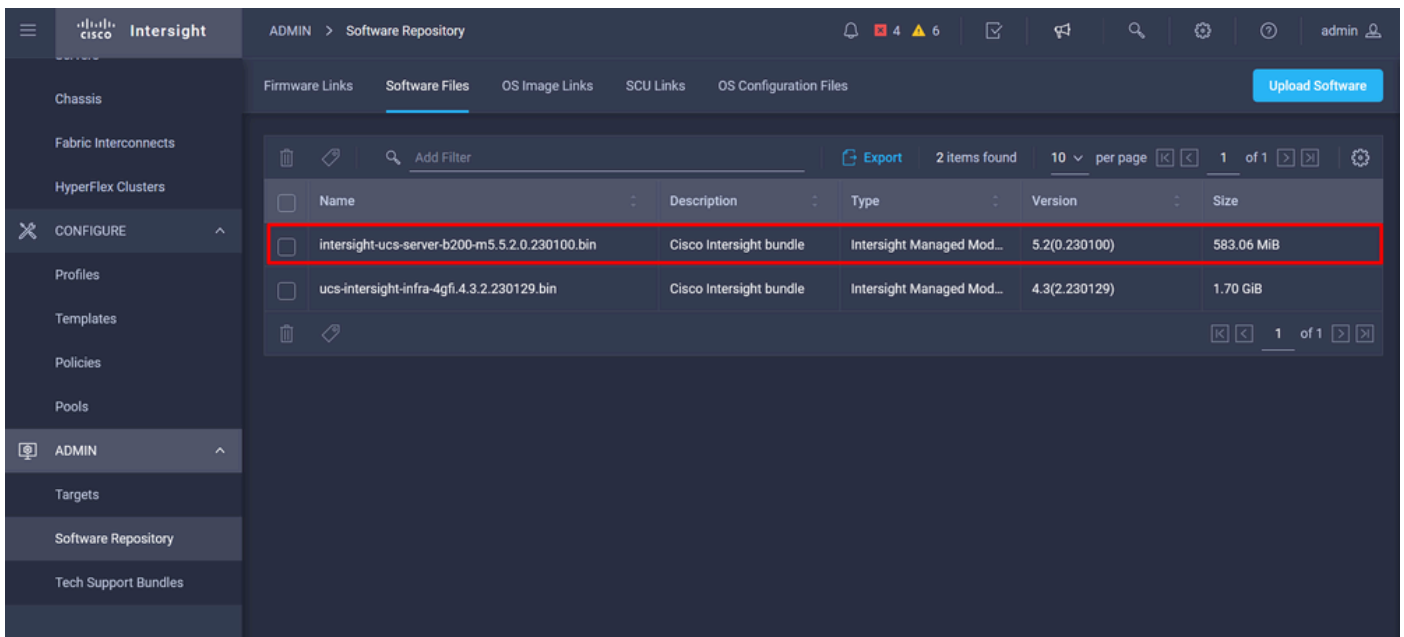
Ambos os FIs estão agora na versão 4.3.2.



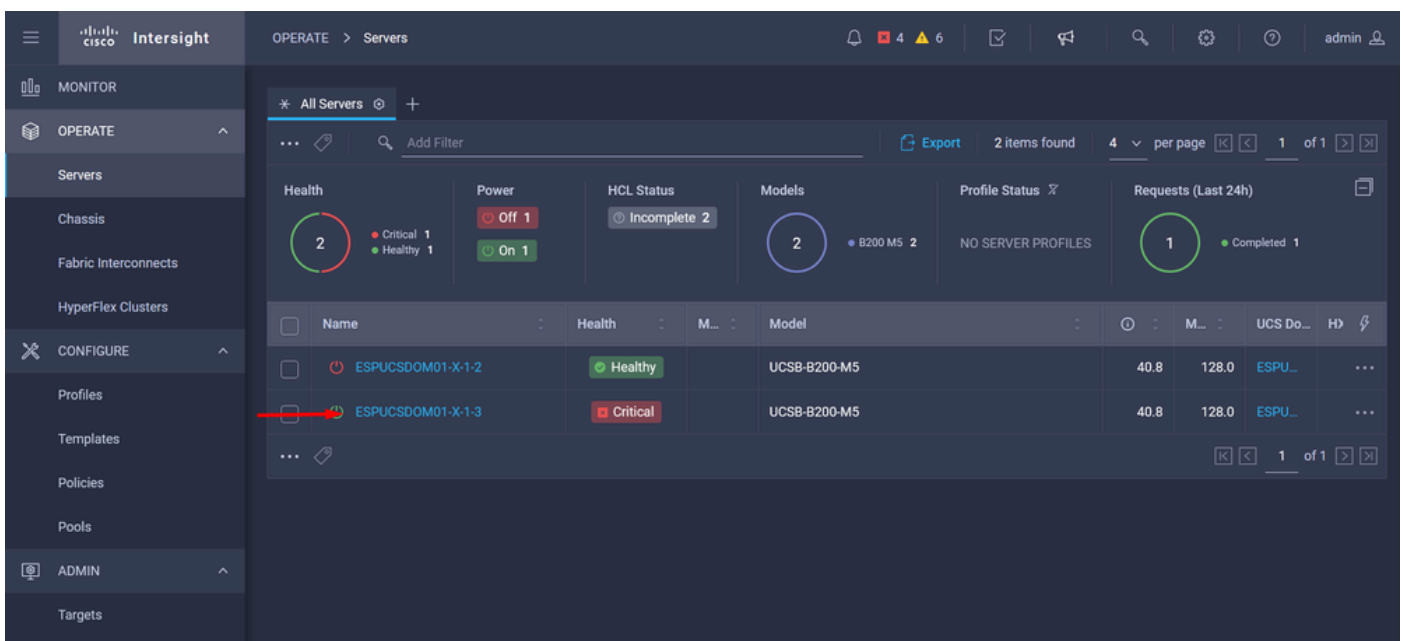
## Atualização do servidor

Etapa 1. Carregue o pacote de firmware para o servidor em Admin > Repositório de software > Arquivos de software > Carregar software.

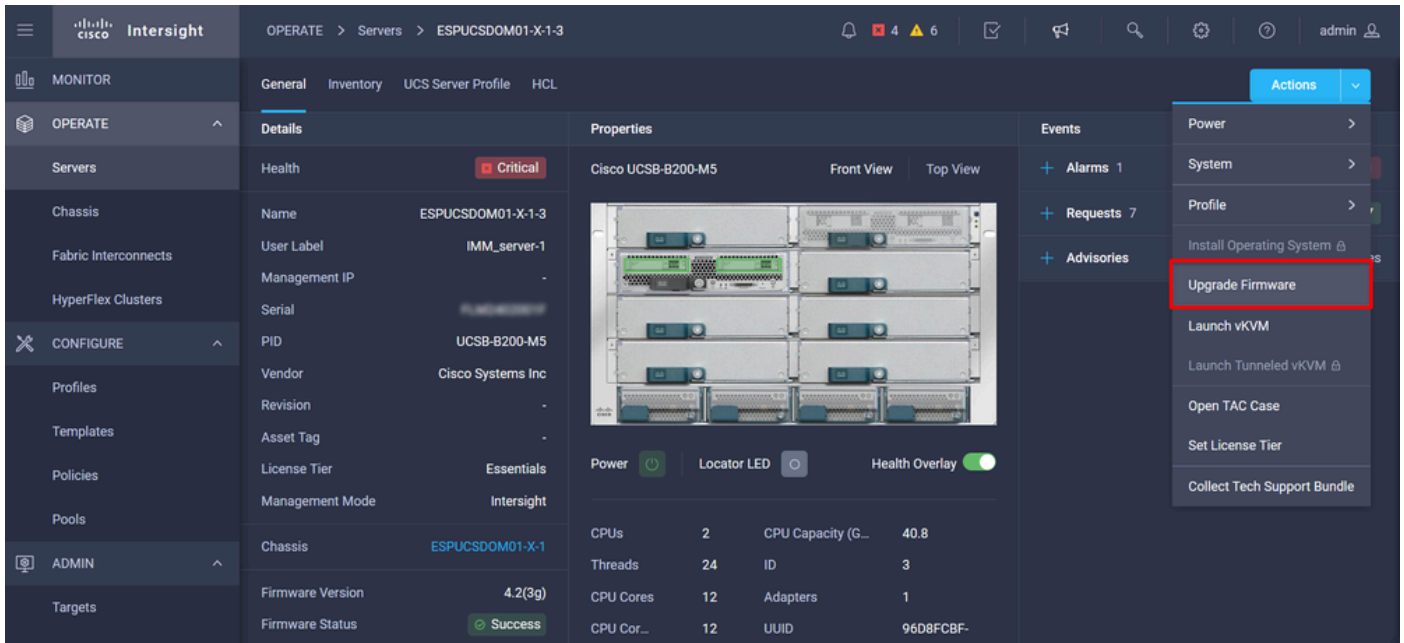
Verifique se ele está listado quando o carregamento for concluído.



Etapa 2. Navegue até Operar > Servidor. Selecione o servidor que deseja atualizar. Para este exemplo, servidor 1/3.

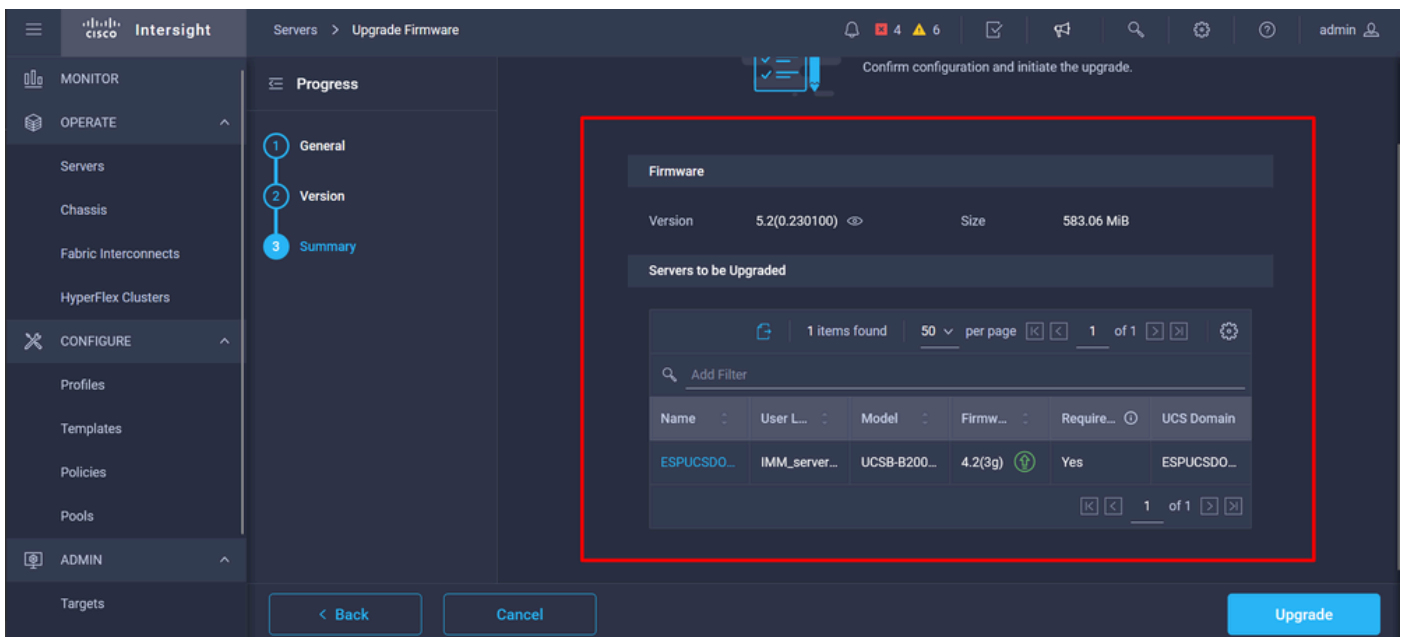


Etapa 3. Navegue até o botão Action e clique nele, ele mostra algumas opções, selecione Upgrade firmware.




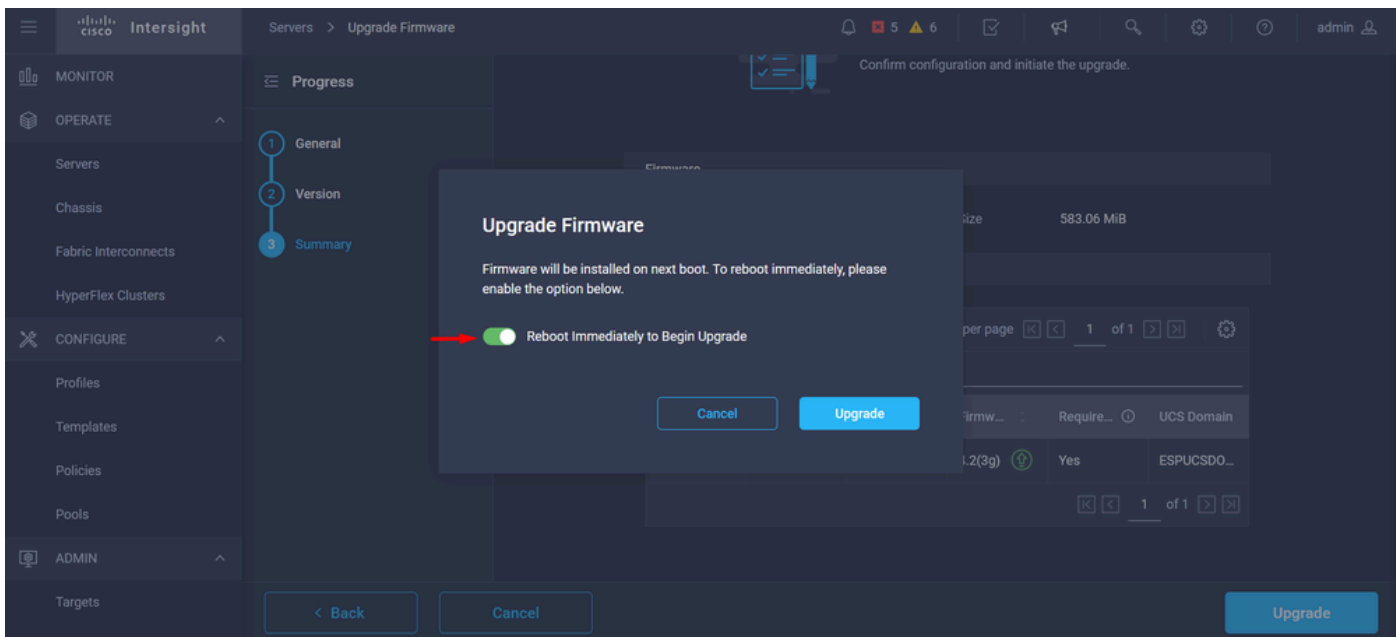
Etapa 4. Verifique se você selecionou o servidor correto e clique em Avançar. Selecione a versão do firmware a ser atualizada.

Um resumo da atualização é exibido. Verifique se a versão do servidor e do firmware estão corretas.

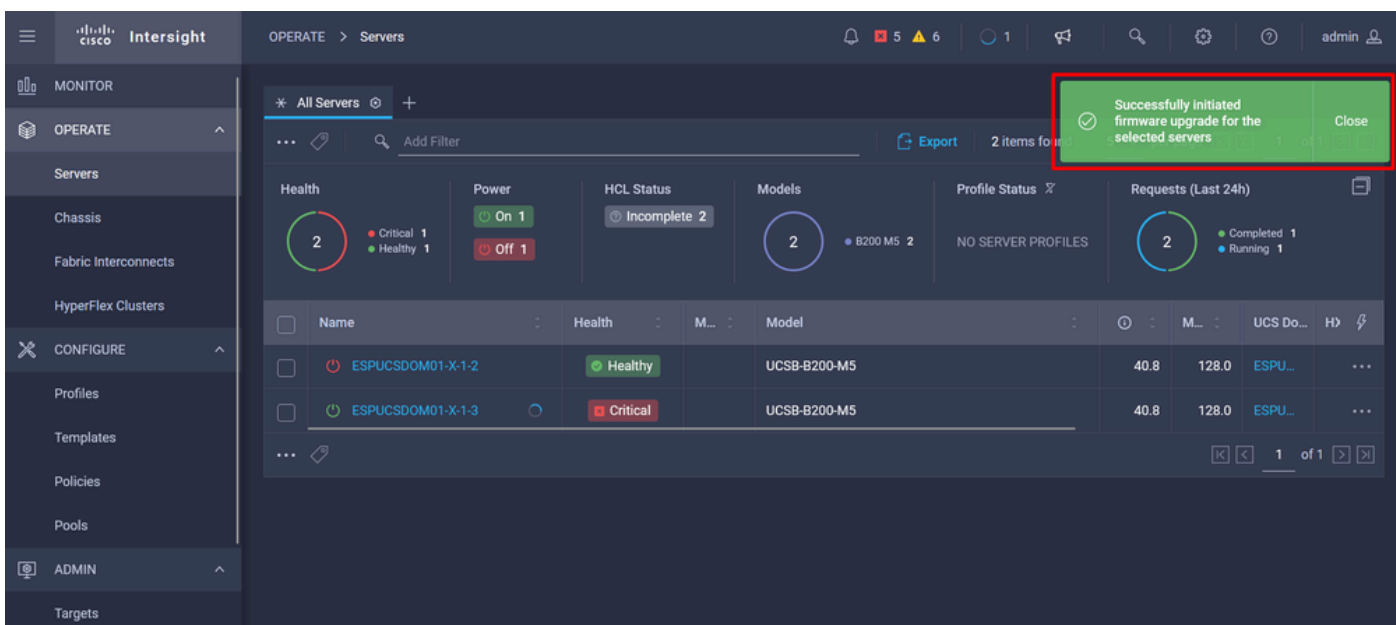


Etapa 5. Ele exibe uma nova janela. Ative Reboot Immediately para iniciar a atualização e clique em Upgrade.

 Observação: se você não ativar, o servidor não será atualizado imediatamente. O servidor é atualizado até a próxima reinicialização.



Etapa 6. Uma caixa verde aparecerá no canto superior direito se a ação de atualização tiver sido bem-sucedida.



Passo 7. Pressione o ícone ao lado do botão de alarme para verificar o progresso da atualização.

Name	Health	M...	Model		M...	UCS Do...	HD
ESPUCSDOM01-X-1-2	Healthy		UCSB-B200-M5	40.8	128.0	ESPU...	...
ESPUCSDOM01-X-1-3	Critical		UCSB-B200-M5	40.8	128.0	ESPU...	...

**Details**

Status: In Progress

Name: Upgrade Firmware

ID: 655ce22a696f6e2d309e6895

Target Type: Blade Server

Target Name: ESPUCSDOM01-X-1-3

Source Type: Firmware Upgrade

Source Name: FLM2402001F

Initiator: admin@local

Start Time: Nov 21, 2023 11:00 AM

End Time: -

Duration: 6 m 52 s

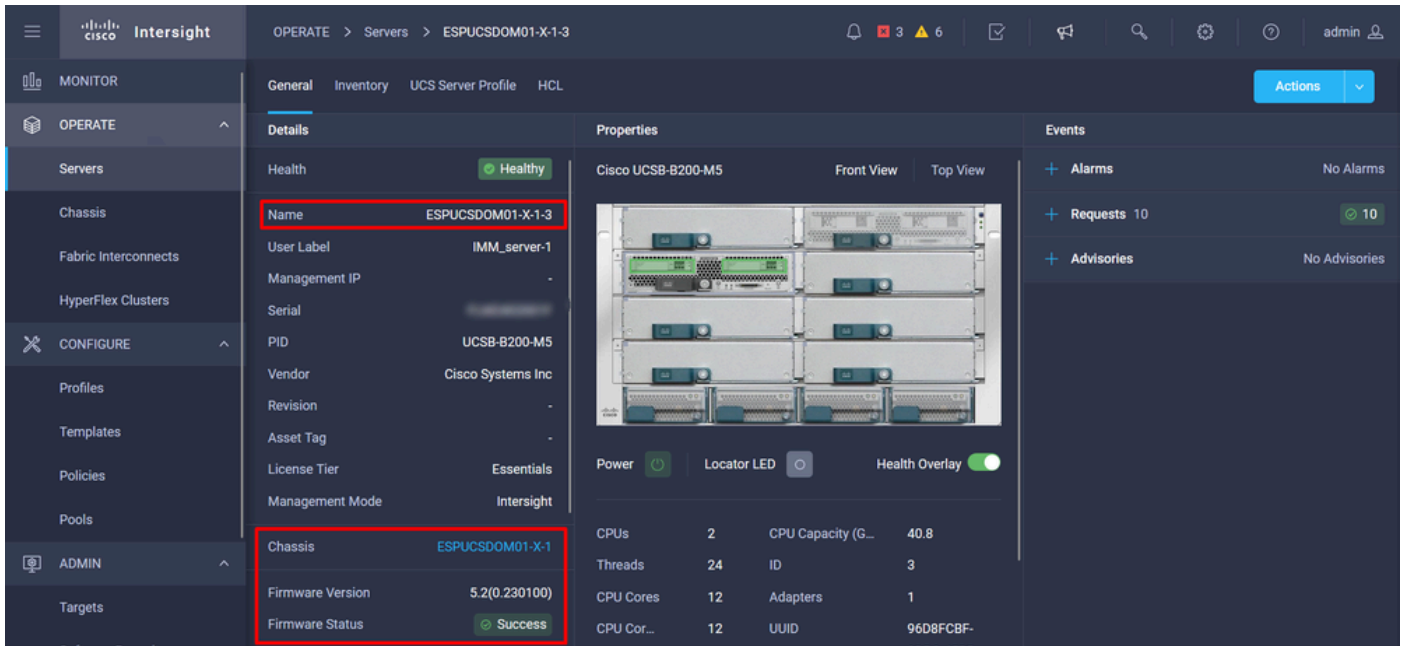
Organizations: private-catalog, default

**Execution Flow**

Progress: 22%

- Wait for image download to complete in endpoint. 0% completed.
- Initiate image download to endpoint. Nov 21, 2023 11:04 AM  
Download intersight-ucs-server-b200-m5.5.2.0.230100.bin request is submitted successfully.
- Wait for the image download to complete in the local repository. Nov 21, 2023 11:04 AM  
Image is already imported, skipping to wait.
- Prepare image download to copy the image from an external location to the local repository. Nov 21, 2023 11:04 AM  
Uploader operation skipping as file is already imported.
- Validate the requirements for the endpoint. Nov 21, 2023 11:04 AM

Etapa 8. Quando terminar, verifique a nova versão do firmware para o servidor na guia Geral. Este servidor agora tem a versão do firmware 5.2(0.23).



## Verificar

FOR FABRIC INTERCONNECT

```
ESPUCSDOM01-X-A# connect nxos
ESPUCSDOM01-X-A(nx-os)#show version | egrep NXOS
NXOS: version 9.3(5)I43(2b) <<<<
NXOS image file is: bootflash:///ucs-6400-k9-system.9.3.5.I43.2b.bin
NXOS compile time: 10/23/2023 15:00:00 [10/23/2023 18:26:58]
```

FOR SERVER

```
ESPUCSDOM01-X-A# connect cimc 1/3
[ help ]#version
ver: 5.2(0.230100) <<<<
Build Time: Wed Nov 1 17:14:35 2023
Build Sha: 7e4aab46a4c04c403b3a2ae380572c38c3c4ef18
Build Tools: armv7-cortex_a9_v011-linux-gnueabi
```

## Informações Relacionadas

[Guia de introdução do Cisco Intersight Virtual Appliance e do Intersight Assist](#)

## 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.