Upgrade Infrastructure and Server Firmware in Intersight Managed Mode for Intersight Private Virtual Appliance.

Contents

Introduction

This document describes the upgrade process for a UCS domain and server on a Private Virtual Appliance (PVA).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- General knowledge and understanding of Intersight Managed Mode (IMM).
- Understanding of Intersight Private Virtual Appliance (PVA).

Components used

The information in this document is based on these software and hardware versions:

- Cisco UCS 6454 54-Port Fabric Interconnect, Firmware 4.2.3(d)
- Cisco UCS B200 M5 Blade Server, Firmware 4.2.1(a)

The information in this document was created from the devices in a specific lab environment. All the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

A Private Virtual Appliance (PVA) is an on-premises version of the Cisco Intersight platform encapsulated in a virtual machine. It provides the same features and benefits as the cloud-based Intersight service, including infrastructure management and automation, but within a private network. This meets the needs of organizations that require a high level of data security, such as those with strict compliance and regulatory requirements.

Software bundle packages for PVA environments are stored in Intersight and are available for download through the Intersight Appliance account.

Configure

Before you begin

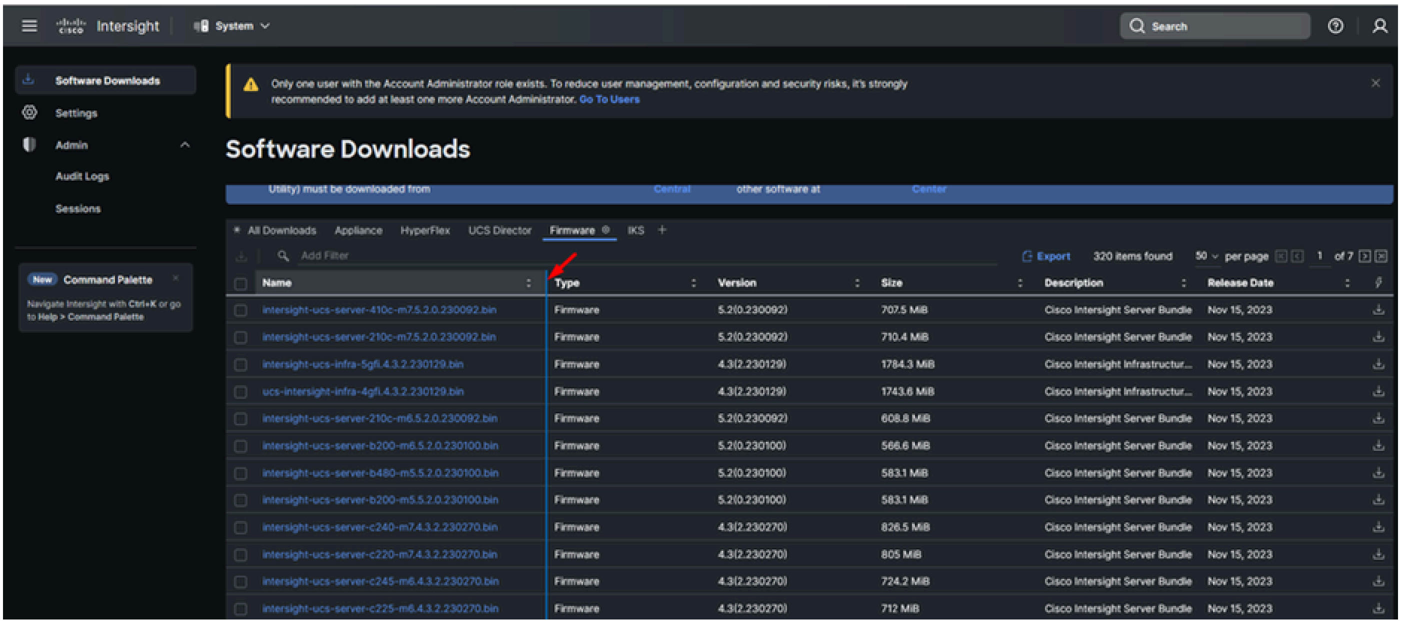
Navigate to this link to set up your account: Creating an Appliance Account.
Follow the steps, accept the license agreement, and create an account name for it.

Fabric Interconnect Upgrade

Step 1. Once the Appliance Account it is created, navigate to **Software Downloads** > **Software Catalog** > **Firmware**.

Look for the firmware version to want to go to. Click its name.

Tip: Expand the name column to see the model of the device and the version.



Only one user with the Account Administrator role exists. To reduce user management, configuration and security risks, it's strongly recommended to add at least one more Account Administrator. Go To Users

Navigate Intersight with Ctrl+K or go to Help > Command Palette

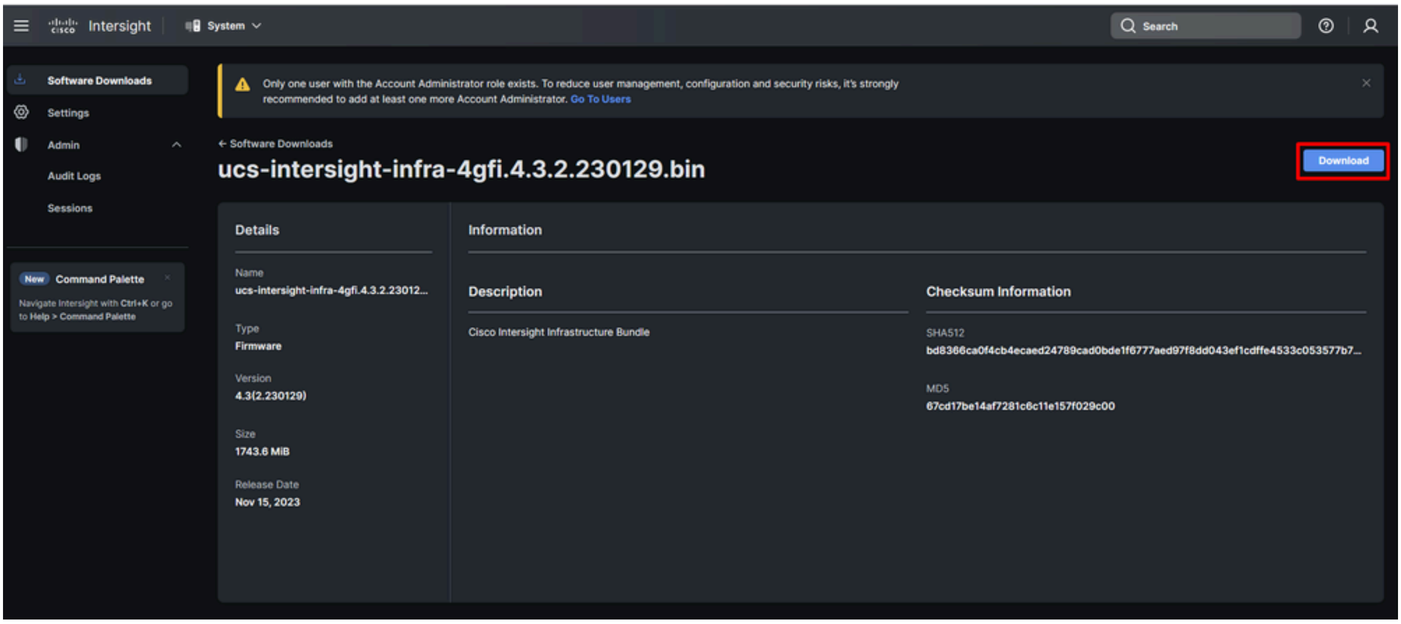
Software Downloads

Utility) must be downloaded from Central other software at Center

320 items found 50 per page 1 of 7

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

Step 2. In the new window, you can see some more detailed information about the package. Ensure this is the one you need. Click the **Download** button. For this example, the Fabric upgrade is for 4.3.2.



Only one user with the Account Administrator role exists. To reduce user management, configuration and security risks, it's strongly recommended to add at least one more Account Administrator. Go To Users

ucs-intersight-infra-4gfi.4.3.2.230129.bin

Details

Name: ucs-intersight-infra-4gfi.4.3.2.23012...

Type: Firmware

Version: 4.3(2.230129)

Size: 1743.6 MiB

Release Date: Nov 15, 2023

Information

Description: Cisco Intersight Infrastructure Bundle

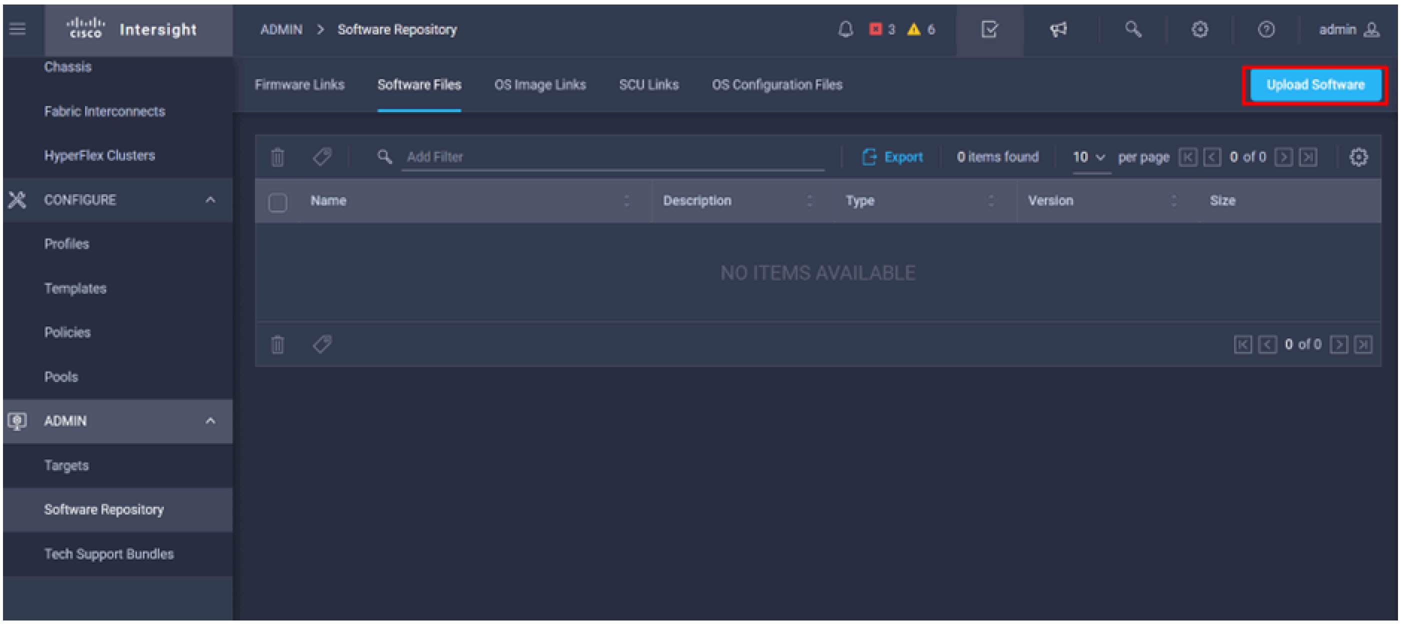
Checksum Information

SHA512: bd8366ca0f4cb4ecaed24789cad0bde1f6777aed97f8dd043ef1cdffe4533c053577b7...

MD5: 67cd17be14af7281c6c11e157f029c00

Step 3. When the download is complete, open a tab in your browser and Log In to your Private Virtual Appliance.

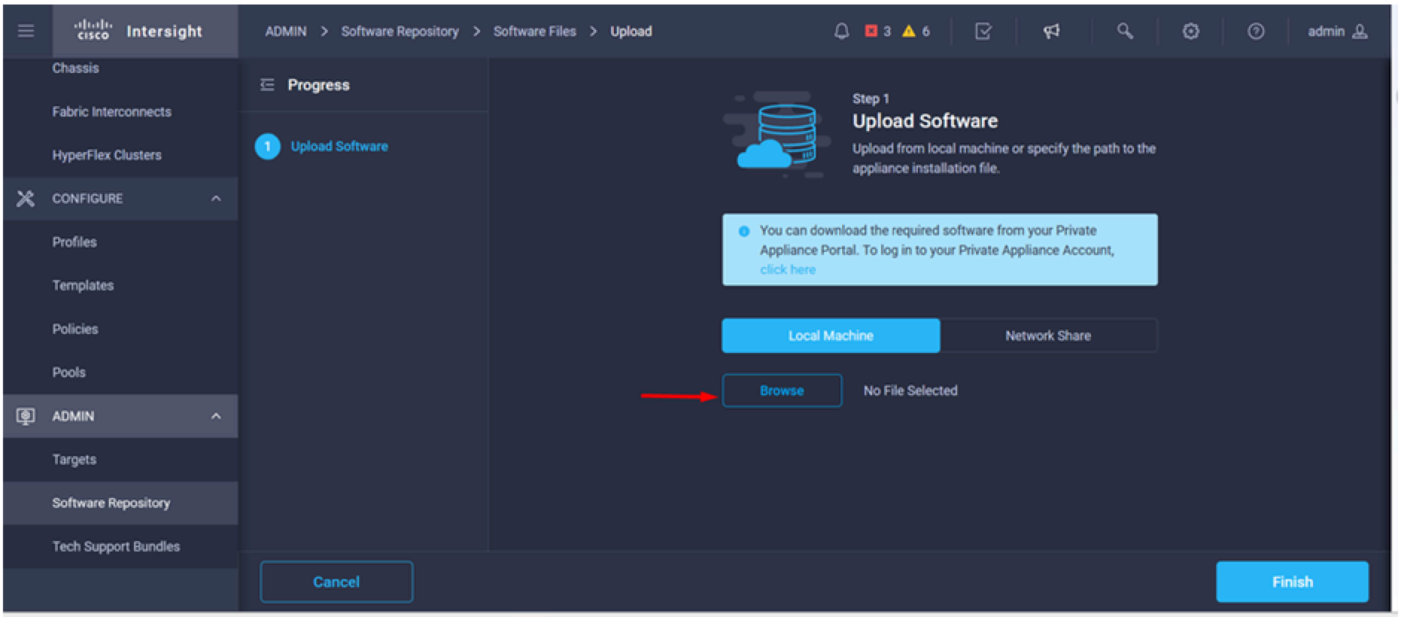
Navigate to **Admin** > **Software Repository** > **Software Files**. In this tab, you can see the list of packages available for upgrade and click **Upload Software**.



Name	Description	Type	Version	Size

NO ITEMS AVAILABLE

Step 4. Browse for the package for your Fabric Interconnect and upload it.

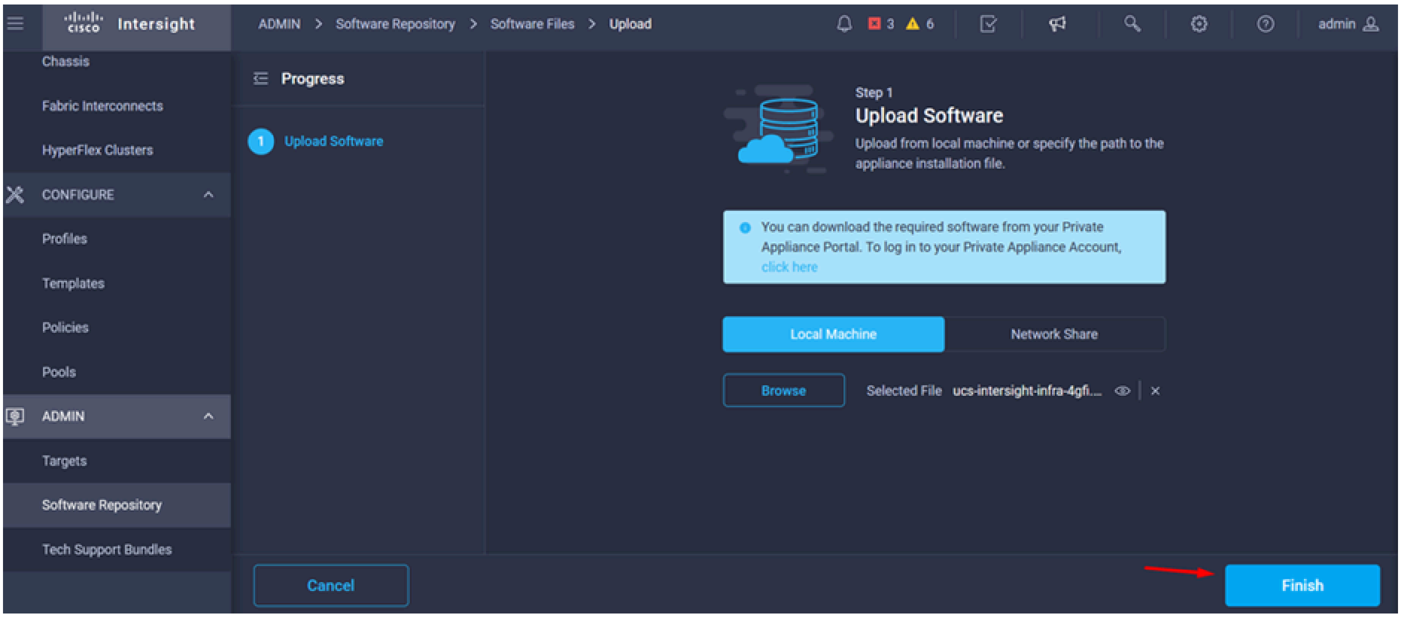


Upload from local machine or specify the path to the appliance installation file.

You can download the required software from your Private Appliance Portal. To log in to your Private Appliance Account, click here

No File Selected

Step 5. Once it has been mapped, click the **Finish** button.



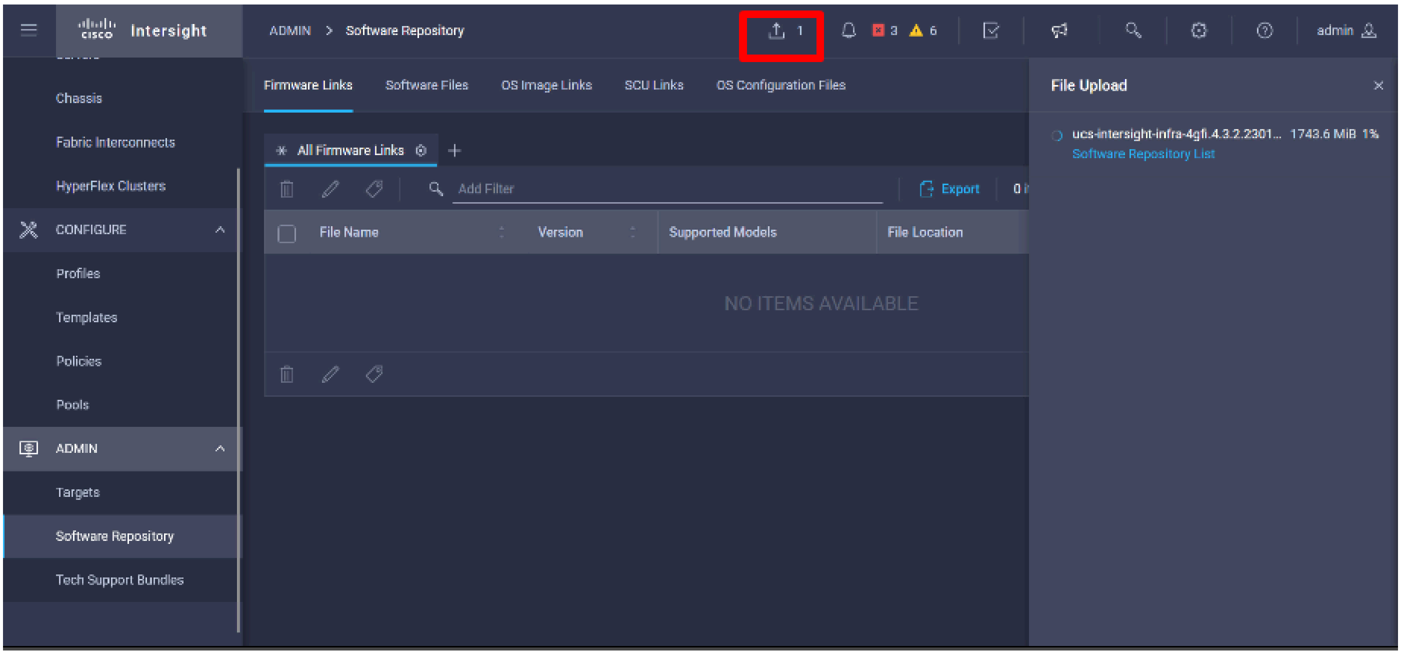
Upload from local machine or specify the path to the appliance installation file.

You can download the required software from your Private Appliance Portal. To log in to your Private Appliance Account, click here

Selected File ucs-intersight-infra-4gfi....

Step 6. You can see the progress in the icon to the left of the Alert button.

On the Software Files tab, confirm that your downloads are ready to use. Refresh the page if necessary.



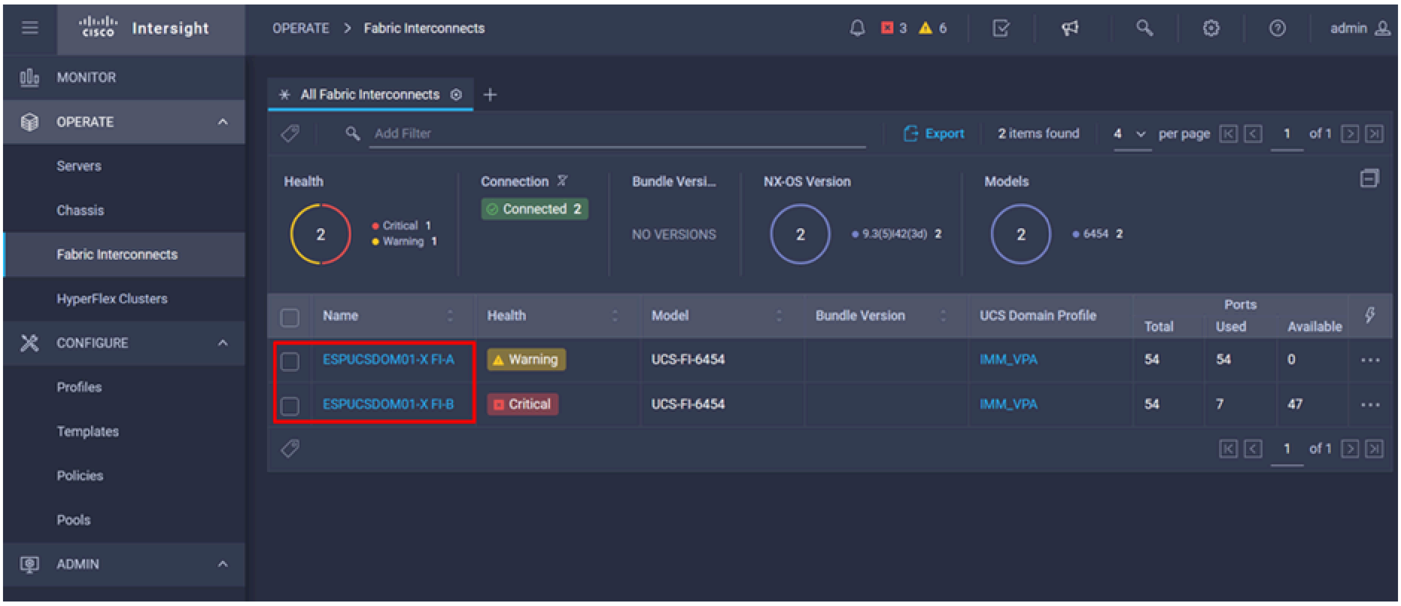
File Name	Version	Supported Models	File Location

NO ITEMS AVAILABLE

File Upload

ucs-intersight-infra-4gfi.4.3.2.2301... 1743.6 MiB 1%
Software Repository List

Step 7. Navigate to **Operate > Fabric Interconnects**. Select the device you need to upgrade. Click on any Fabric Interconnect (FI) that belongs to the cluster you need to upgrade.

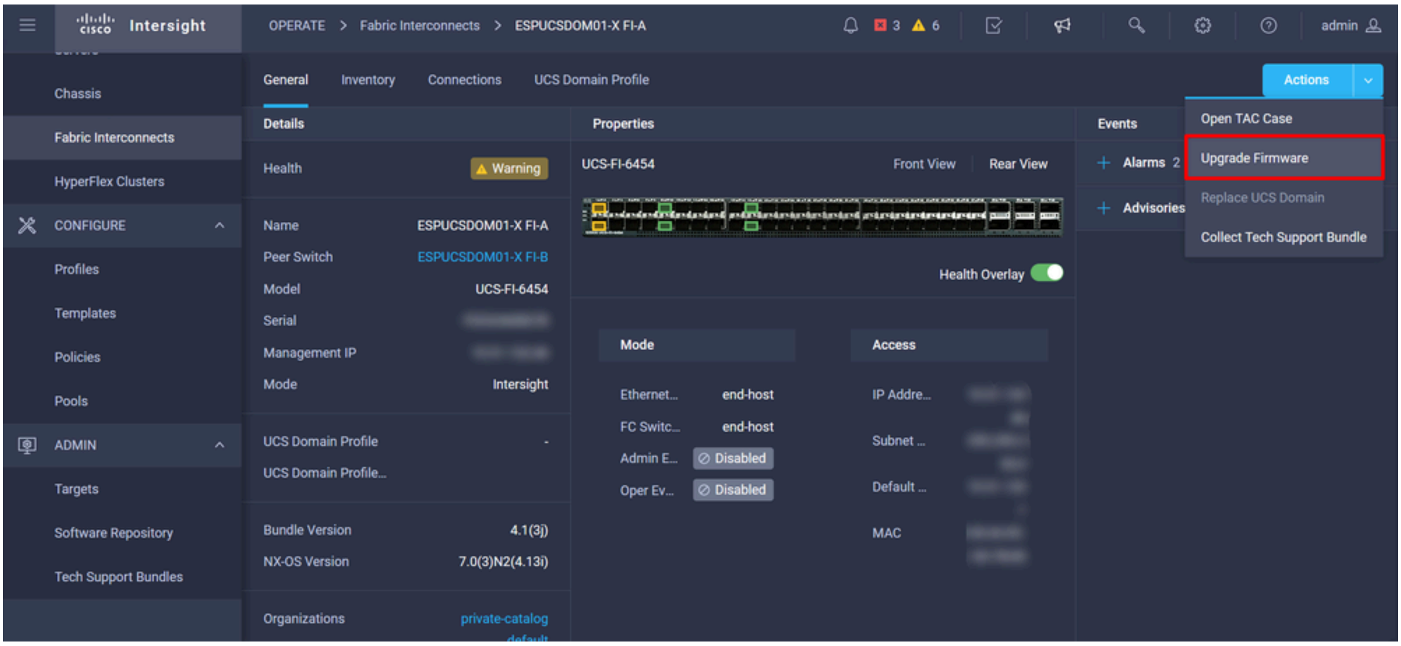


Name	Health	Model	Bundle Version	UCS Domain Profile	Ports Total	Ports Used	Ports Available
ESPUCSDOM01-X FI-A	Warning	UCS-FI-6454		IMM_VPA	54	54	0
ESPUCSDOM01-X FI-B	Critical	UCS-FI-6454		IMM_VPA	54	7	47

Step 8. Ensure you have selected the correct Fabric Interconnect.

On the Details tab, you can review general information such as the peer switch, management IP and current version.

Step 9. Navigate to **Action** button. Click on it, it displays a few options, choose **Upgrade firmware**.



Details

Health	Warning
Name	ESPUCSDOM01-X FI-A
Peer Switch	ESPUCSDOM01-X FI-B
Model	UCS-FI-6454
Serial	[redacted]
Management IP	[redacted]
Mode	Intersight
UCS Domain Profile	-
UCS Domain Profile...	
Bundle Version	4.1(3j)
NX-OS Version	7.0(3)N2(4.13i)
Organizations	private-catalog default

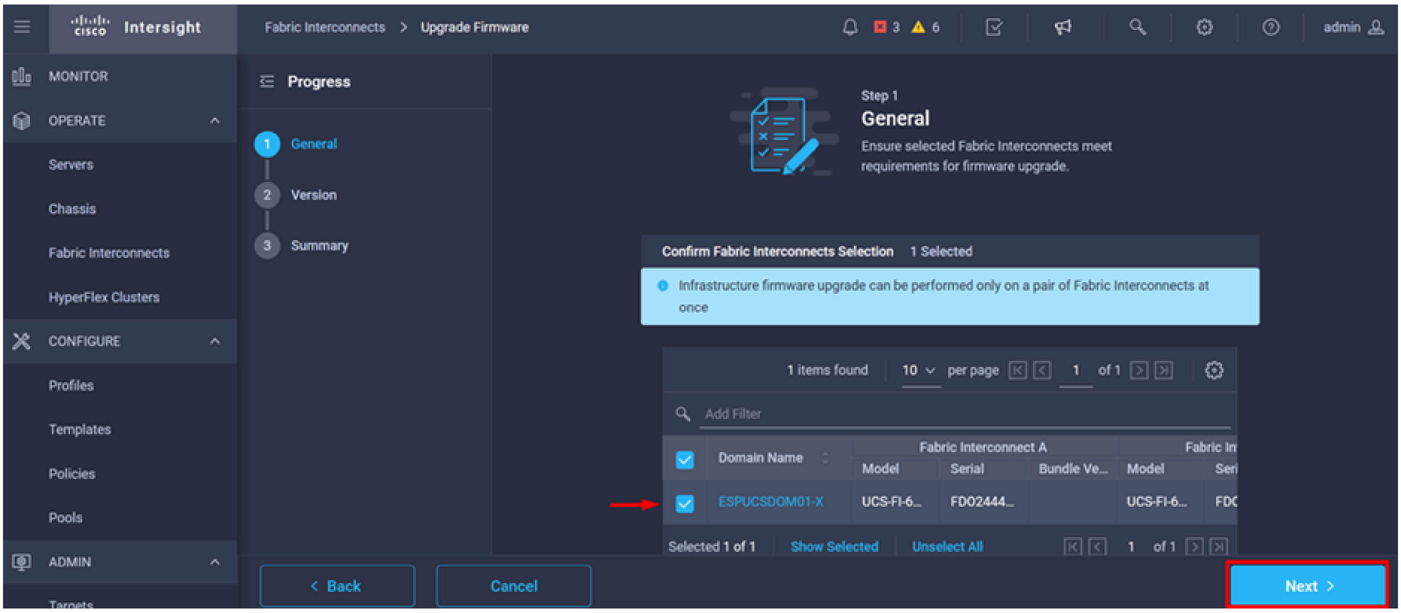
UCS-FI-6454

Mode	
Ethernet...	end-host
FC Switc...	end-host
Admin E...	Disabled
Oper Ev...	Disabled

Access	
IP Addre...	[redacted]
Subnet ...	[redacted]
Default ...	[redacted]
MAC	[redacted]

Step 10. A window appears with basic instructions on how to perform the upgrade. Click **Start**.

Step 11. You can see the list of Fabrics Interconnect that are claimed by Intersight. The domain you clicked on earlier is automatically selected.



Step 1

General

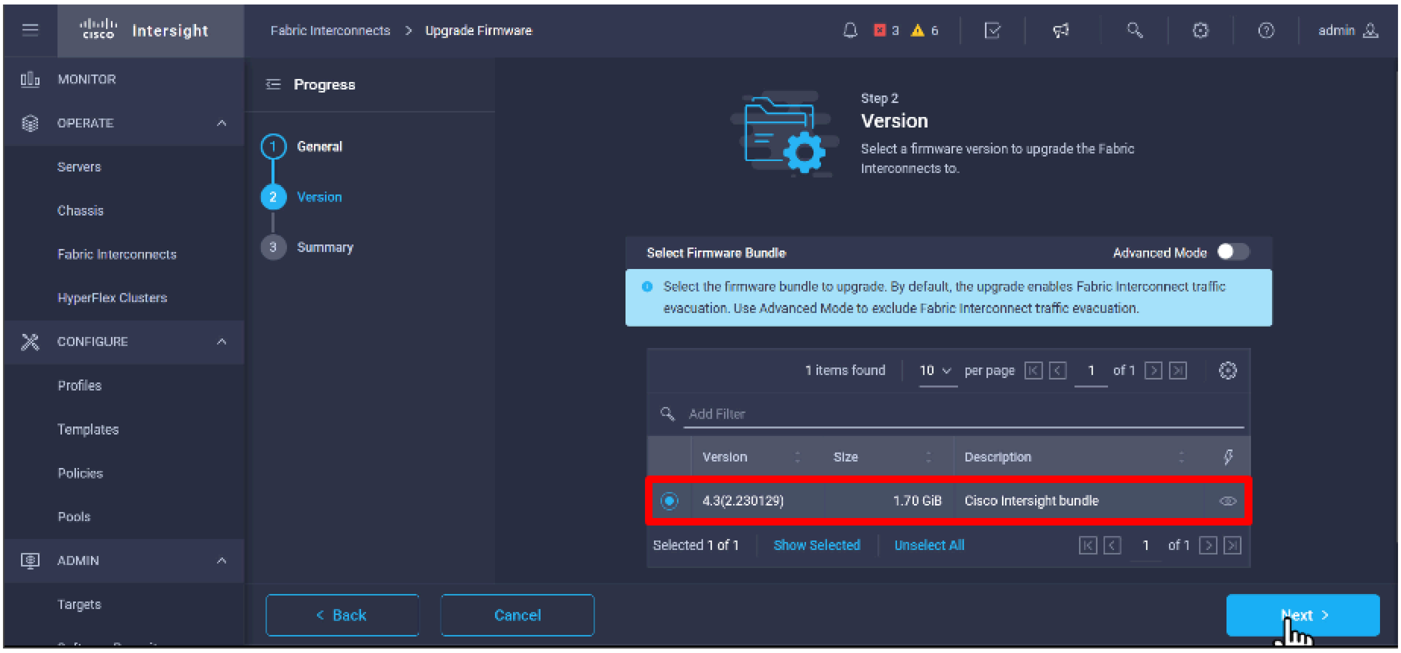
Ensure selected Fabric Interconnects meet requirements for firmware upgrade.

Confirm Fabric Interconnects Selection 1 Selected

Infrastructure firmware upgrade can be performed only on a pair of Fabric Interconnects at once

		Fabric Interconnect A			Fabric In	
☑	Domain Name	Model	Serial	Bundle Ve...	Model	Seri
☑	ESPUCSDOM01-X	UCS-FI-6...	FDO2444...		UCS-FI-6...	FDC

Step 12. For this example, package version 4.3.2 is available. Select your version and click the **Next** to continue.



Step 2

Version

Select a firmware version to upgrade the Fabric Interconnects to.

Select Firmware Bundle | Advanced Mode

Select the firmware bundle to upgrade. By default, the upgrade enables Fabric Interconnect traffic evacuation. Use Advanced Mode to exclude Fabric Interconnect traffic evacuation.

1 items found | 10 per page | 1 of 1

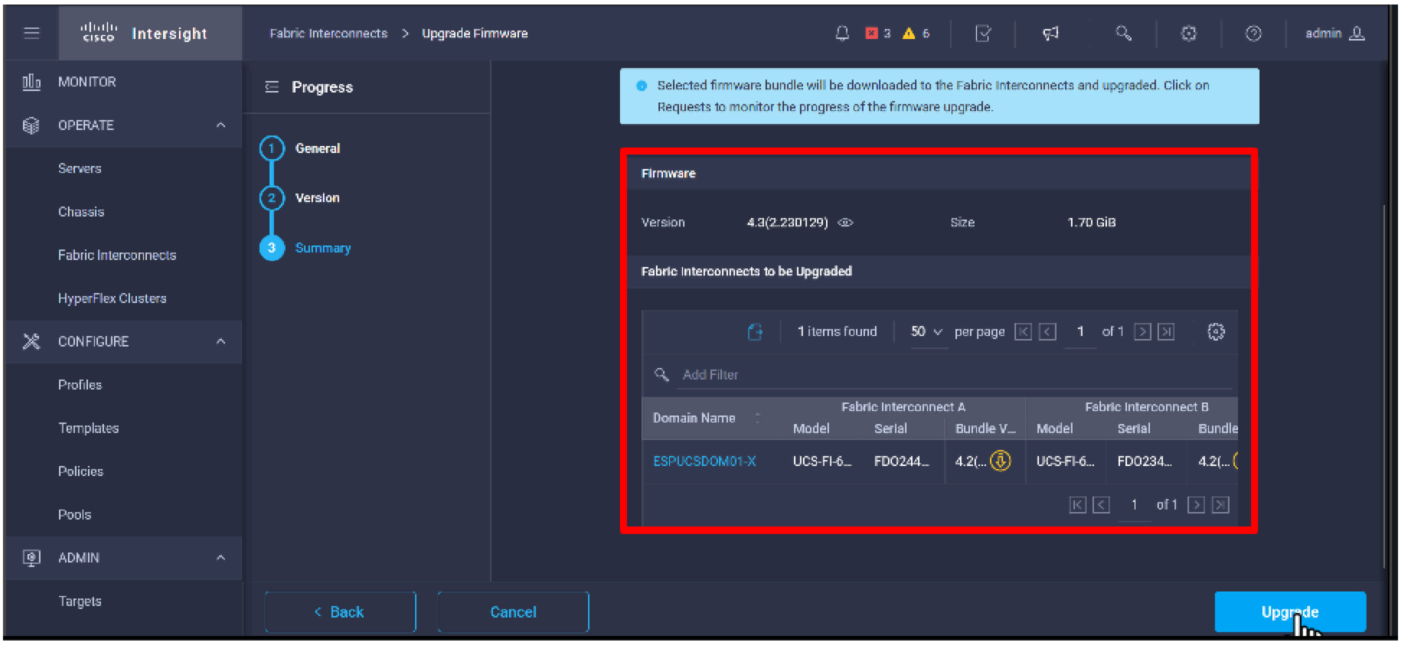
Add Filter

	Version	Size	Description
●	4.3(2.230129)	1.70 GiB	Cisco Intersight bundle

Selected 1 of 1 | Show Selected | Unselect All | 1 of 1

Step 13. It shows a summary of your upgrade: the domain name, serial number, model, and firmware version.

Confirm that this is the correct domain and click **Upgrade**.



Selected firmware bundle will be downloaded to the Fabric Interconnects and upgraded. Click on Requests to monitor the progress of the firmware upgrade.

Firmware

Version 4.3(2.230129) | Size 1.70 GiB

Fabric Interconnects to be Upgraded

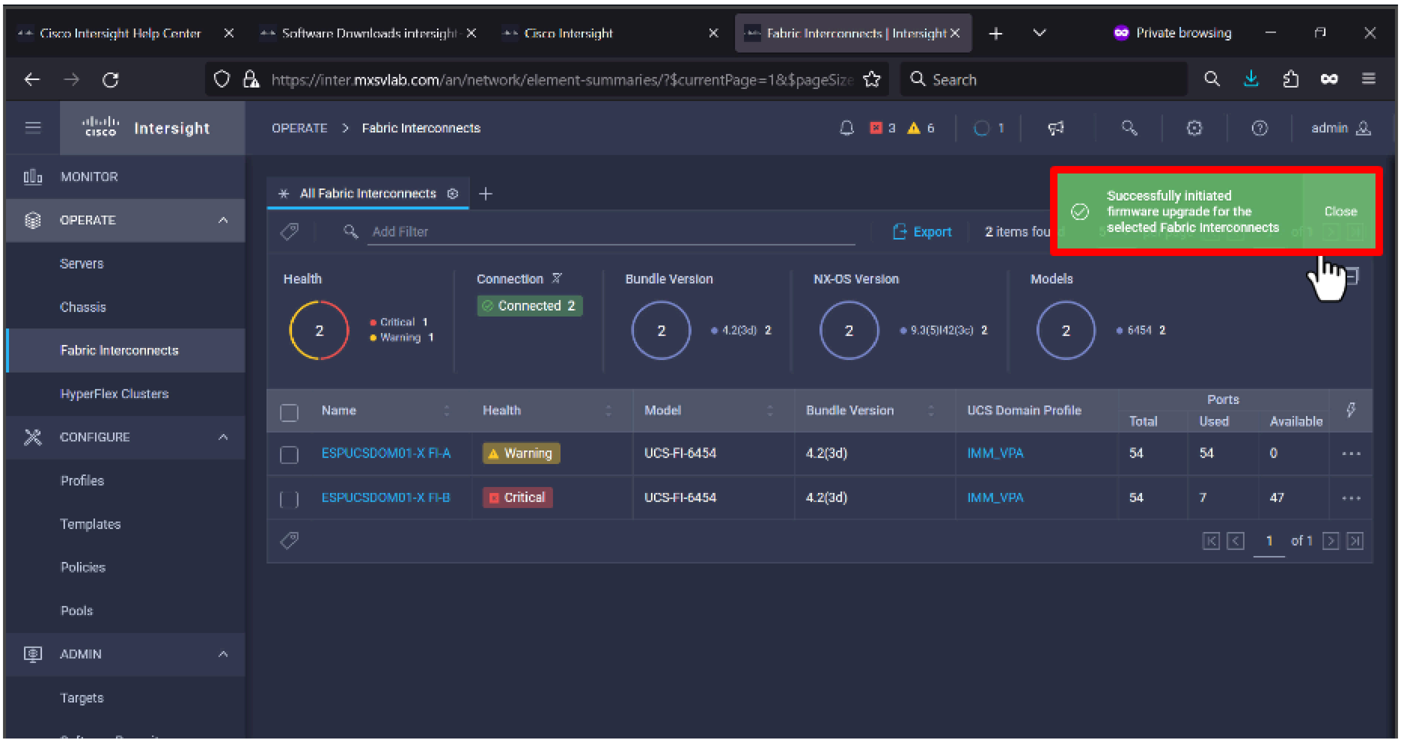
1 items found | 50 per page | 1 of 1

Add Filter

Domain Name	Fabric Interconnect A			Fabric Interconnect B		
	Model	Serial	Bundle V...	Model	Serial	Bundle
ESPUCSDOM01-X	UCS-FI-6...	FDO244...	4.2(...	UCS-FI-6...	FDO234...	4.2(...

1 of 1

Step 14. A green box appears in the upper right corner if the upgrade action was successful.

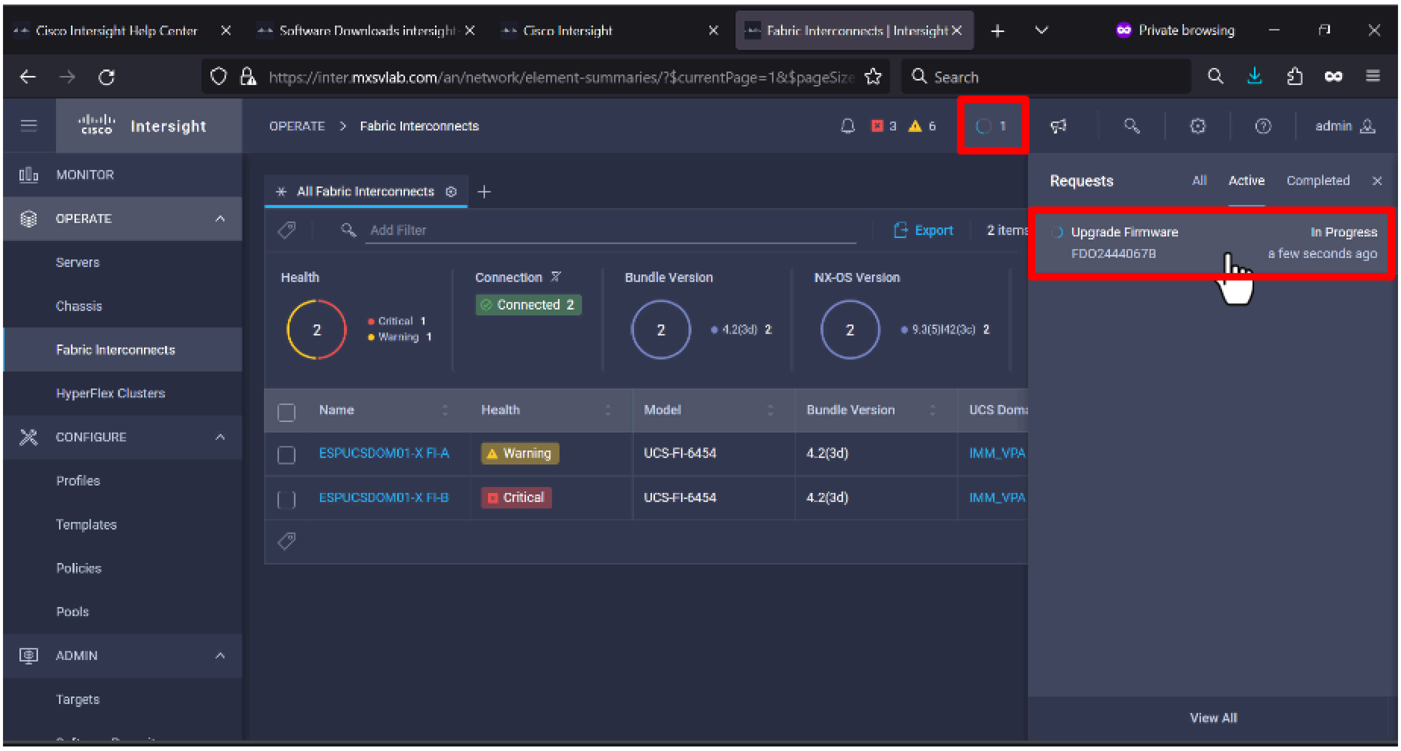


Successfully initiated firmware upgrade for the selected Fabric Interconnects

Close

Name	Health	Model	Bundle Version	UCS Domain Profile	Ports Total	 Used	 Available
ESPUCSDOM01-X FI-A	Warning	UCS-FI-6454	4.2(3d)	IMM_VPA	54	54	0
ESPUCSDOM01-X FI-B	Critical	UCS-FI-6454	4.2(3d)	IMM_VPA	54	7	47

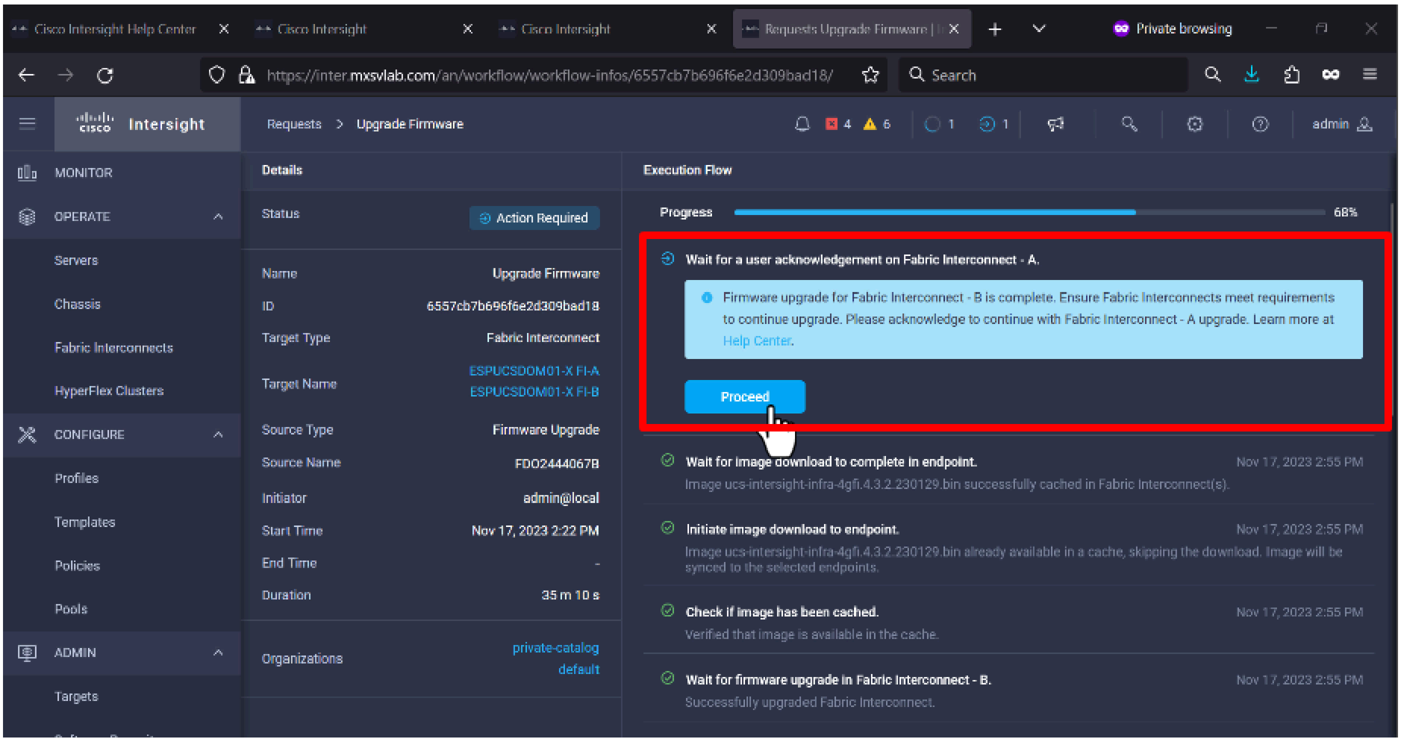
Step 15. Press the icon next to the alarm button to check the progress of the upgrade.



Name	Health	Model	Bundle Version	UCS Doma
ESPUCSDOM01-X FI-A	Warning	UCS-FI-6454	4.2(3d)	IMM_VPA
ESPUCSDOM01-X FI-B	Critical	UCS-FI-6454	4.2(3d)	IMM_VPA

Upgrade Firmware — In Progress
FDO2444067B — a few seconds ago

Step 16. It requires an acknowledge for the reboot of the Fabric. Click **Proceed** to continue with the upgrade.



Requests > Upgrade Firmware

Details

Status	Action Required
Name	Upgrade Firmware
ID	6557cb7b696f6e2d309bad18
Target Type	Fabric Interconnect
Target Name	ESPUCSDOM01-X FI-A ESPUCSDOM01-X FI-B
Source Type	Firmware Upgrade
Source Name	FDO2444067B
Initiator	admin@local
Start Time	Nov 17, 2023 2:22 PM
End Time	-
Duration	35 m 10 s
Organizations	private-catalog default

Execution Flow

Progress 68%

Wait for a user acknowledgement on Fabric Interconnect - A.

Firmware upgrade for Fabric Interconnect - B is complete. Ensure Fabric Interconnects meet requirements to continue upgrade. Please acknowledge to continue with Fabric Interconnect - A upgrade. Learn more at Help Center.

Proceed

Wait for image download to complete in endpoint. Nov 17, 2023 2:55 PM
Image ucs-intersight-infra-4gfi.4.3.2.230129.bin successfully cached in Fabric Interconnect(s).

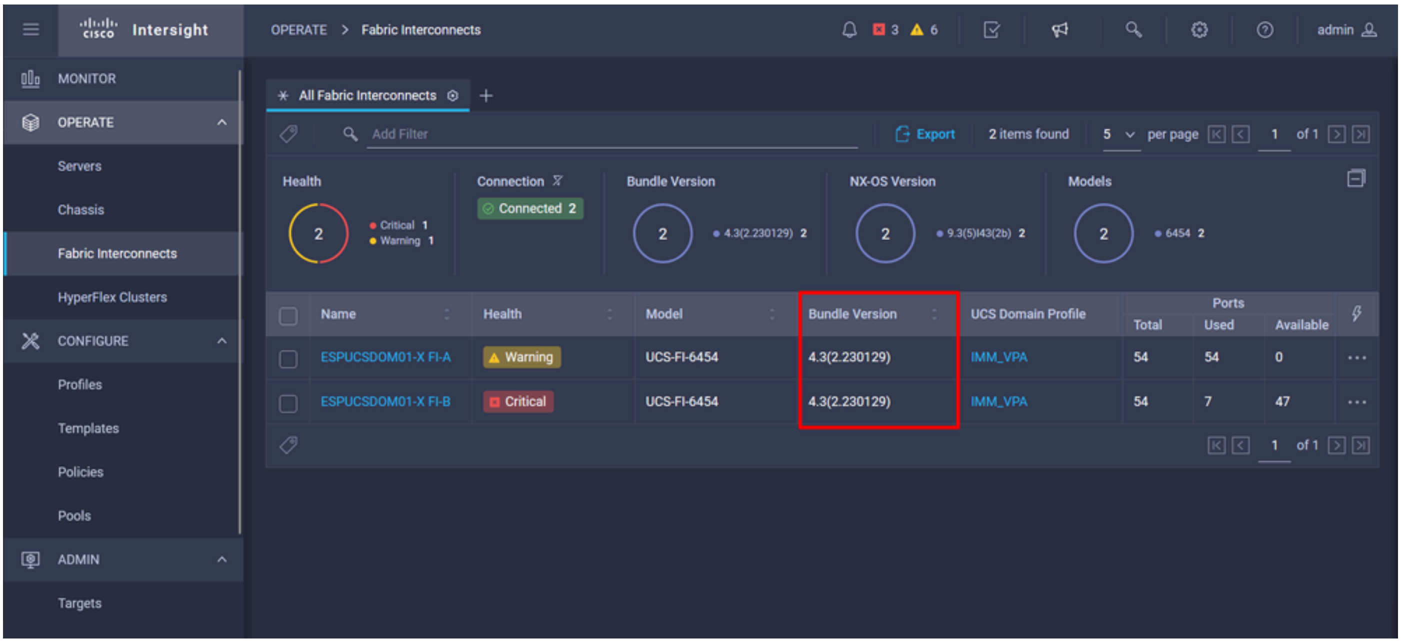
Initiate image download to endpoint. Nov 17, 2023 2:55 PM
Image ucs-intersight-infra-4gfi.4.3.2.230129.bin already available in a cache, skipping the download. Image will be synced to the selected endpoints.

Check if image has been cached. Nov 17, 2023 2:55 PM
Verified that image is available in the cache.

Wait for firmware upgrade in Fabric Interconnect - B. Nov 17, 2023 2:55 PM
Successfully upgraded Fabric Interconnect.

Step 17. Verify that the upgrade completed successfully in the Bundle Version column of the Fabric Interconnects tab.

Both FIs are now at version 4.3.2.



OPERATE > Fabric Interconnects

All Fabric Interconnects — 2 items found — 5 per page — 1 of 1

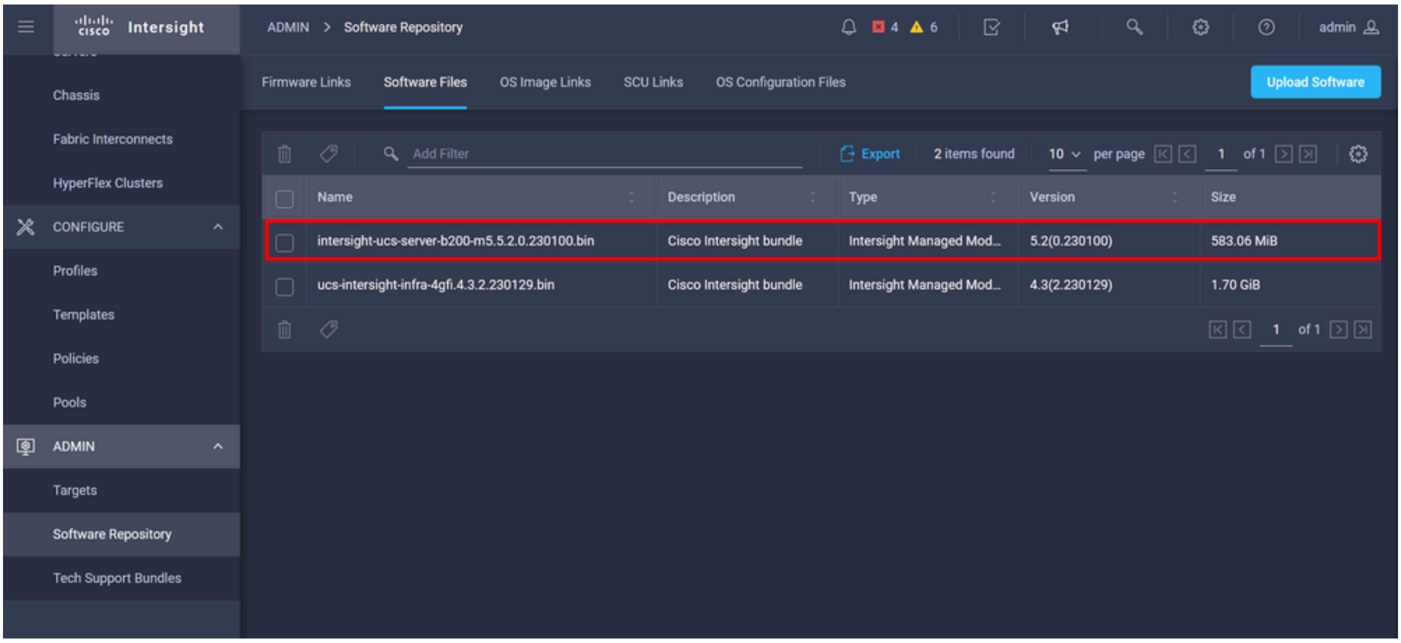
Health: 2 (Critical 1, Warning 1) · Connection: Connected 2 · Bundle Version: 2 (4.3(2.230129) 2) · NX-OS Version: 2 (9.3(5)I43(2b) 2) · Models: 2 (6454 2)

Name	Health	Model	Bundle Version	UCS Domain Profile	Ports Total	Ports Used	Ports Available
ESPUCSDOM01-X FI-A	Warning	UCS-FI-6454	4.3(2.230129)	IMM_VPA	54	54	0
ESPUCSDOM01-X FI-B	Critical	UCS-FI-6454	4.3(2.230129)	IMM_VPA	54	7	47

Server Upgrade

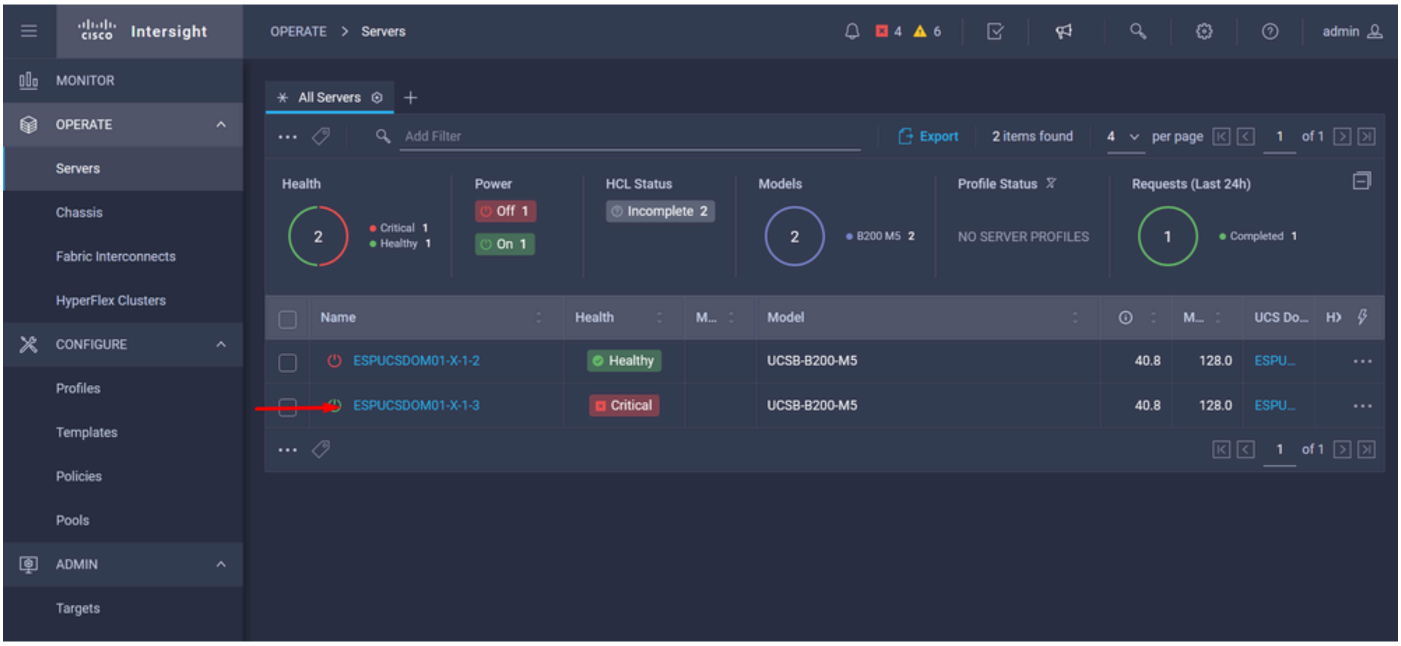
Step 1. Upload the firmware package for the server on **Admin > Software Repository > Software Files > Upload Software**.

Verify that it is listed when the upload is complete.



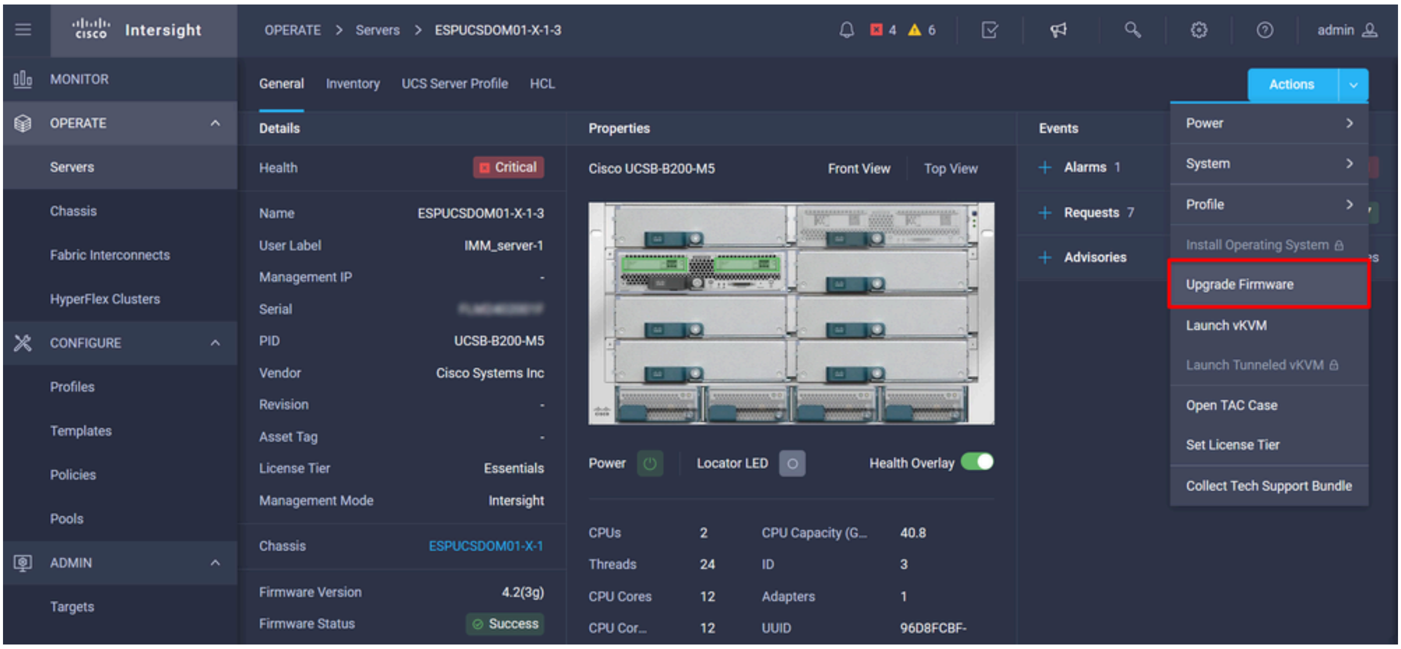
Name	Description	Type	Version	Size
intersight-ucs-server-b200-m5.5.2.0.230100.bin	Cisco Intersight bundle	Intersight Managed Mod...	5.2(0.230100)	583.06 MiB
ucs-intersight-infra-4gfi.4.3.2.230129.bin	Cisco Intersight bundle	Intersight Managed Mod...	4.3(2.230129)	1.70 GiB

Step 2. Navigate to **Operate** > **Server**. Select the server you want to upgrade. For this example, server 1/3.



Name	Health	M...	Model		M...	UCS Do...	H›
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...	...

Step 3. Navigate to the **Action** button and click it, it shows some options, select **Upgrade firmware**.



Details

Health	Critical
Name	ESPUCSDOM01-X-1-3
User Label	IMM_server-1
Management IP	-
Serial	[redacted]
PID	UCSB-B200-M5
Vendor	Cisco Systems Inc
Revision	-
Asset Tag	-
License Tier	Essentials
Management Mode	Intersight
Chassis	ESPUCSDOM01-X-1
Firmware Version	4.2(3g)
Firmware Status	Success

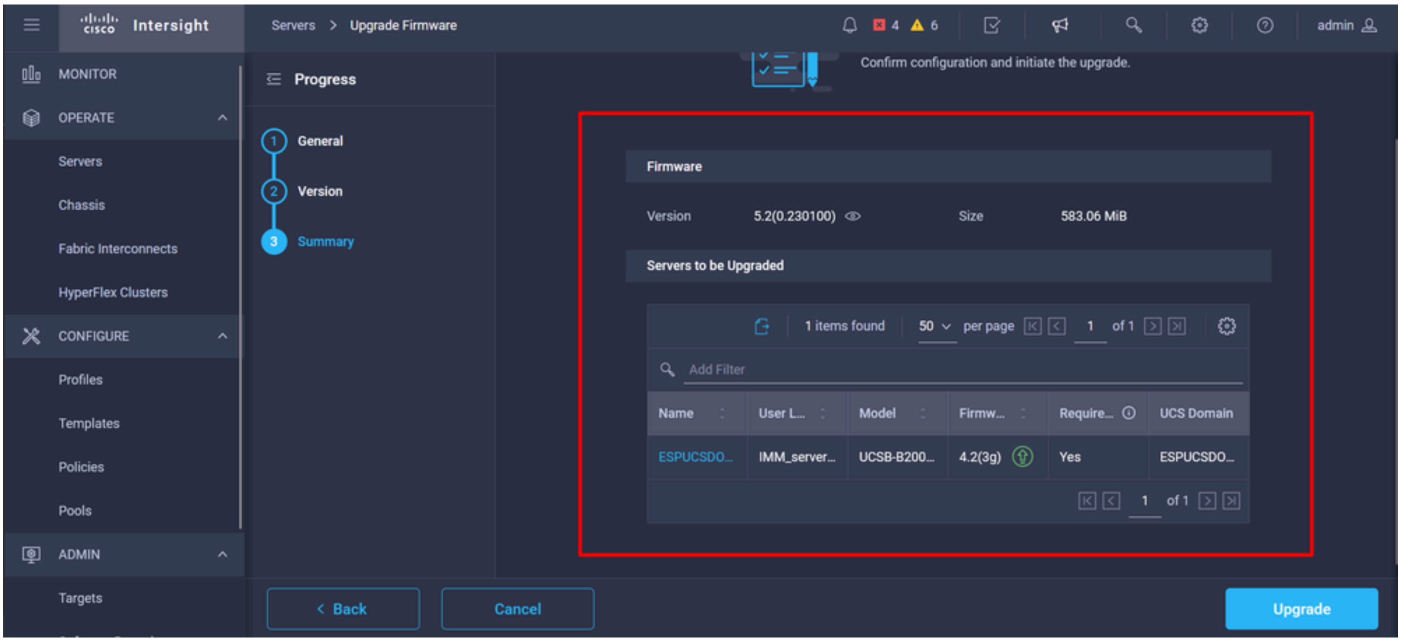
Properties

Cisco UCSB-B200-M5

CPUs	2	CPU Capacity (G...	40.8
Threads	24	ID	3
CPU Cores	12	Adapters	1
CPU Cor...	12	UUID	96D8FCBF-

Step 4. Verify that you have selected the correct server and click **Next**. Select the firmware version to upgrade.

A summary of the upgrade is displayed. Make sure the server and firmware version are correct.



Confirm configuration and initiate the upgrade.

Firmware

Version 5.2(0.230100) Size 583.06 MiB

Servers to be Upgraded

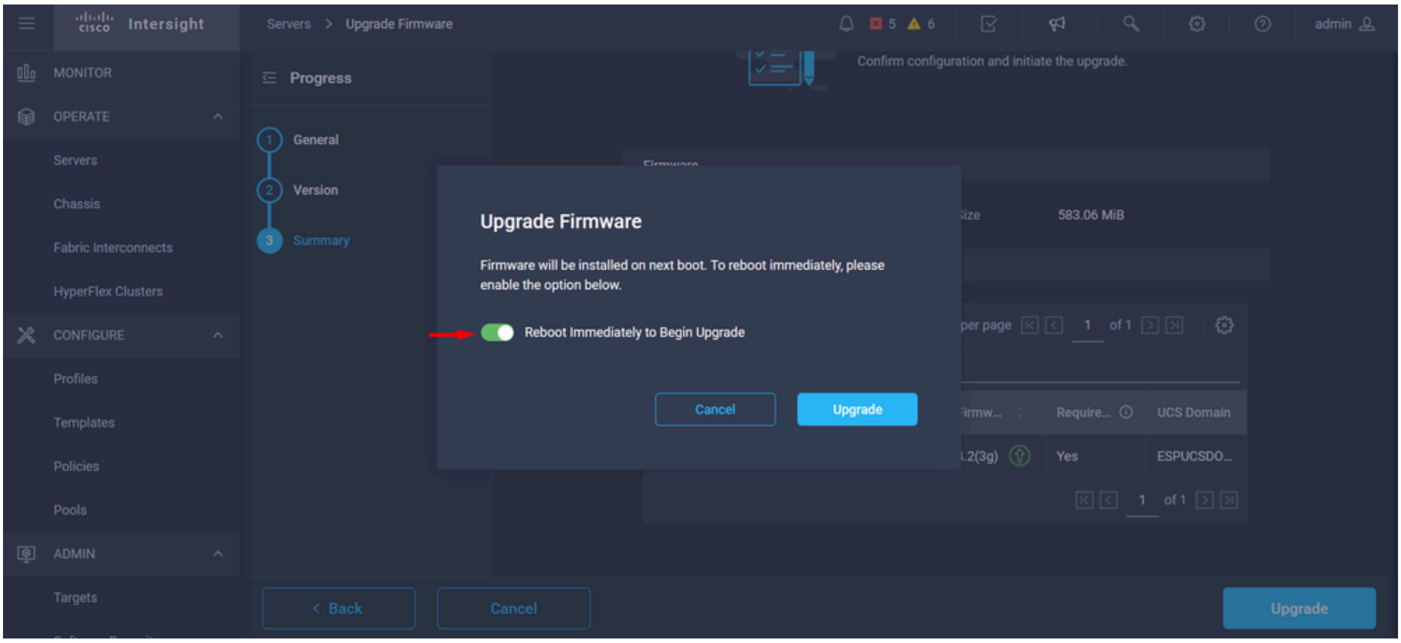
1 items found 50 per page 1 of 1

Add Filter

Name	User L...	Model	Firmw...	Require...	UCS Domain
ESPUCSDO...	IMM_server...	UCSB-B200...	4.2(3g)	Yes	ESPUCSDO...

Step 5. It displays a new window. Enable **Reboot Immediately to Begin Upgrade** and click on **Upgrade**.

Note: If you do not enable, the server does not get upgraded immediately. Server is upgraded until next reboot.



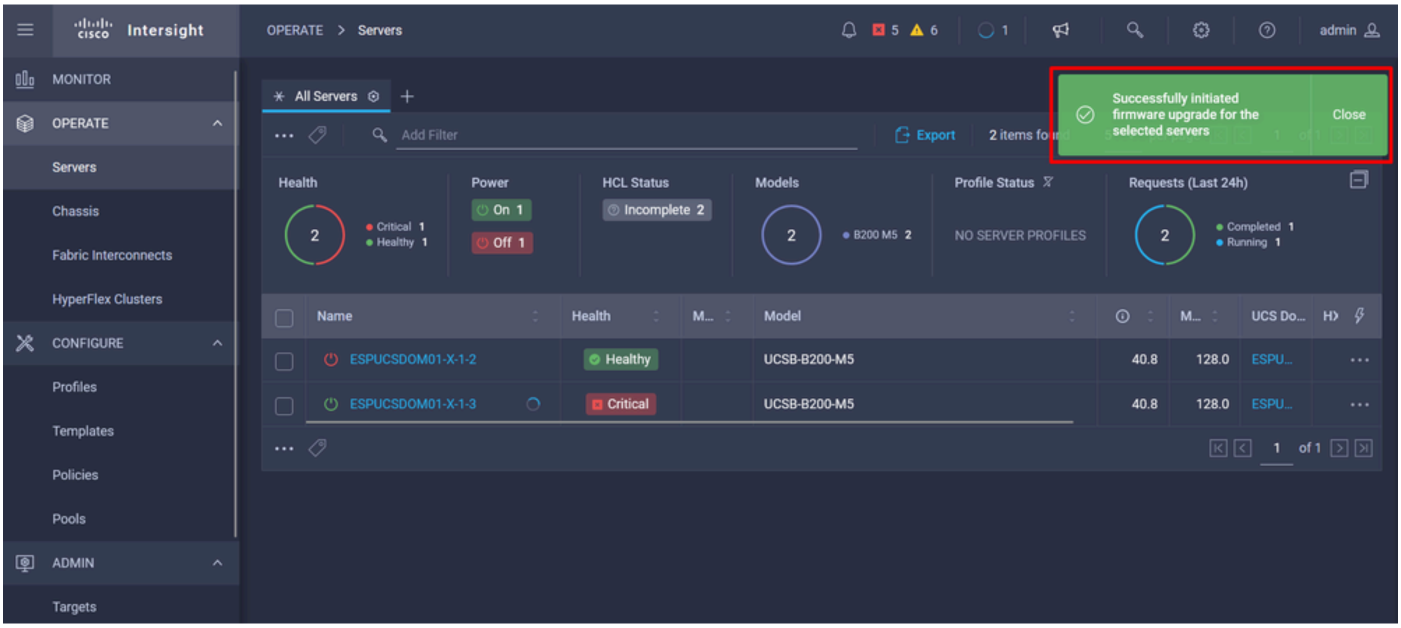
Upgrade Firmware

Firmware will be installed on next boot. To reboot immediately, please enable the option below.

● Reboot Immediately to Begin Upgrade

Cancel Upgrade

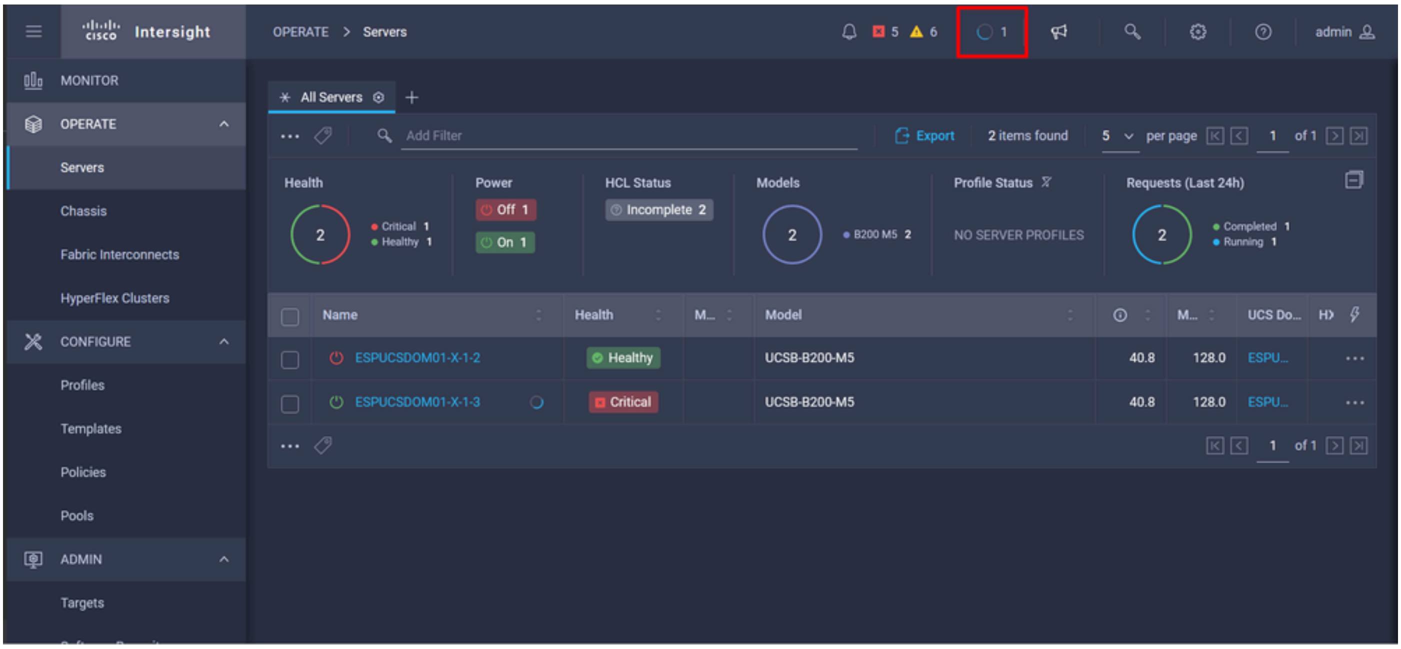
Step 6. A green box appears in the upper right corner if the upgrade action was successful.



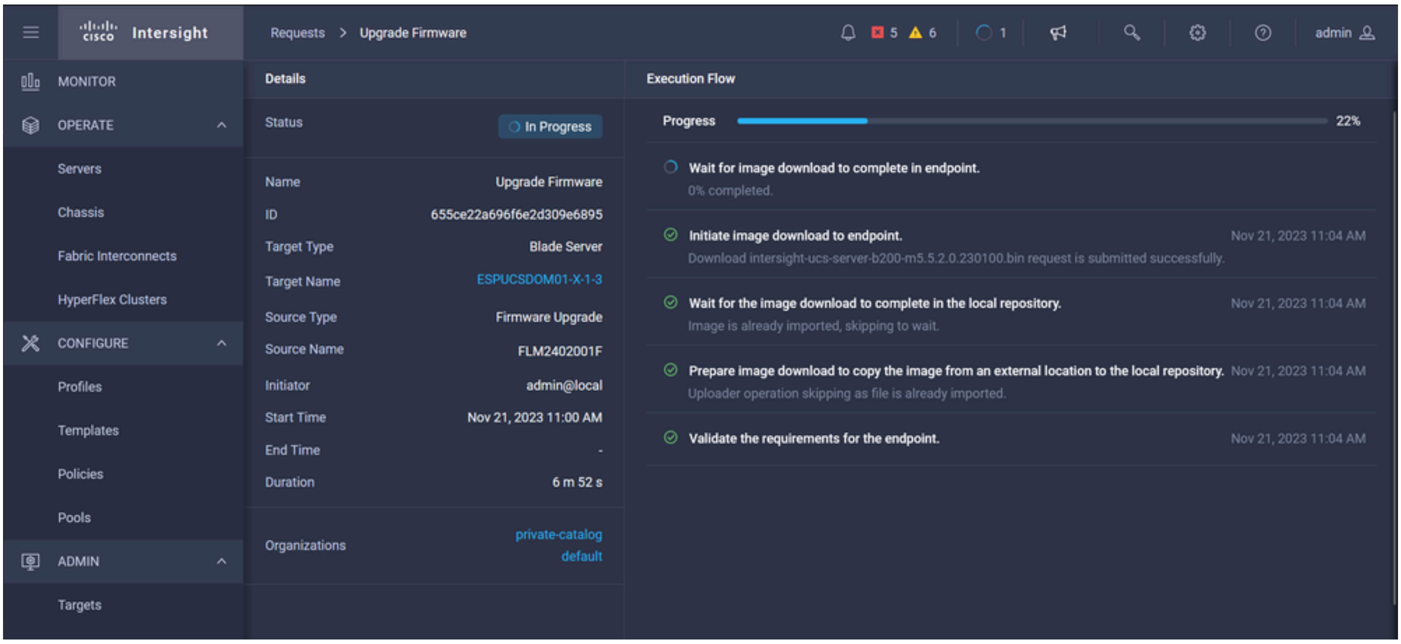
Successfully initiated firmware upgrade for the selected servers Close

Name	Health	M...	Model		M...	UCS Do...
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...

Step 7. Press the icon next to the alarm button to check the progress of the upgrade.



Name	Health	M...	Model		M...	UCS Do...
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.

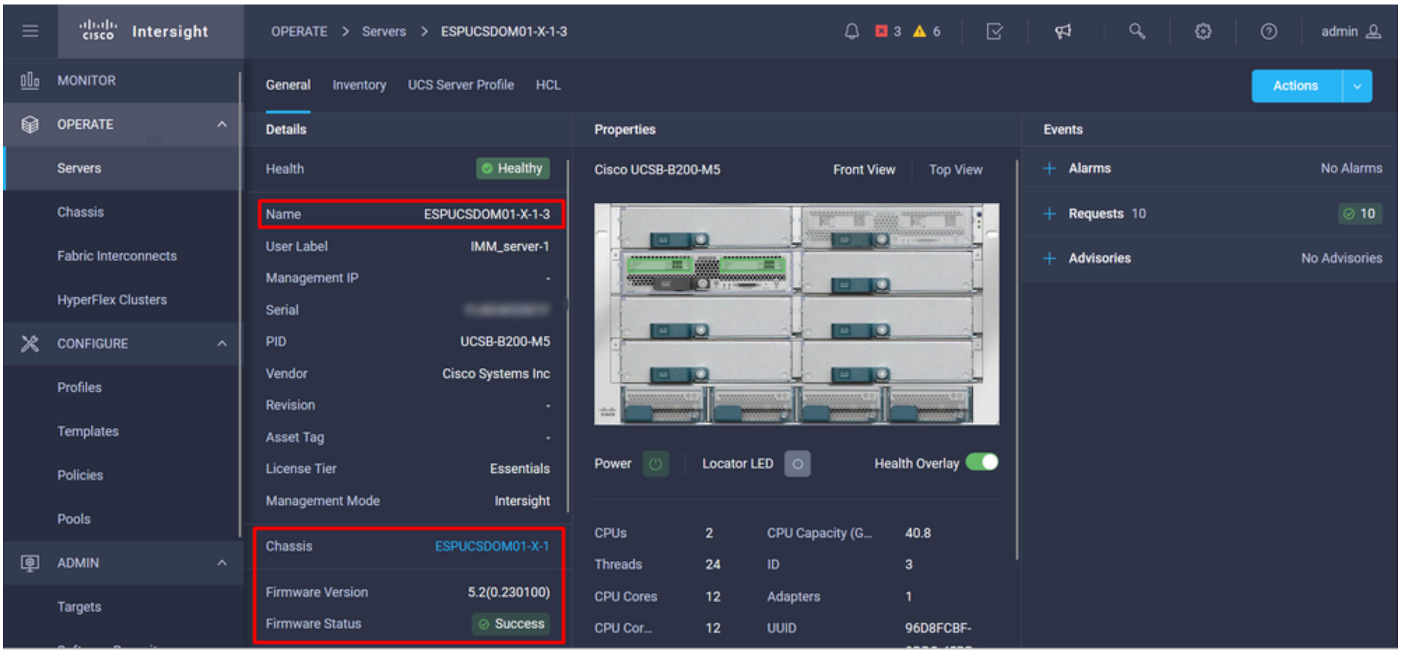
Initiate image download to endpoint. Nov 21, 2023 11:04 AM
Download intersight-ucs-server-b200-m5.5.2.0.230100.bin request is submitted successfully.

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

Step 8. Once complete, verify the new firmware version for the server on the General tab. This server now has firmware version 5.2(0.23).



Details

Health: Healthy
Name: ESPUCSDOM01-X-1-3
User Label: IMM_server-1
Management IP: -
Serial: [redacted]
PID: UCSB-B200-M5
Vendor: Cisco Systems Inc
Revision: -
Asset Tag: -
License Tier: Essentials
Management Mode: Intersight
Chassis: ESPUCSDOM01-X-1
Firmware Version: 5.2(0.230100)
Firmware Status: Success

Properties

Cisco UCSB-B200-M5

CPUs	2	CPU Capacity (G...	40.8
Threads	24	ID	3
CPU Cores	12	Adapters	1
CPU Cor...	12	UUID	96D8FCBF-

Events

Alarms: No Alarms
Requests 10: 10
Advisories: No Advisories

Verify

```
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
```

Related Information

[Cisco Intersight Virtual Appliance and Intersight Assist Getting Started Guide]()