

# Cisco UCS X-Series Quick Start Guide



# Contents

Introduction..... 3

Site planning checklist..... 4

Setup and Install..... 8

Topology diagrams..... 15

Starting the X-Series configuration ..... 16

Starting the X-Series server configuration ..... 27

Final thoughts ..... 35

Appendix and reference guides ..... 36

---

## Introduction

The purpose of this document is to assist with the basic installation and configuration of the X-Series solution. Much of the content in this guide was copied directly from several sources, including but not limited to the following:

- [Cisco UCS X9508 Server Chassis Installation Guide](#)
- [Cisco UCS 6400 Series Fabric Interconnect Hardware Installation Guide](#)
- [Getting Started with Intersight](#)
- Cisco Intersight Handbook
- [Deploy Cisco UCS X210c Compute Node with Cisco Intersight Management Mode for VDI](#)

## Intended audience

This guide is intended primarily for data center administrators with responsibilities and expertise in one or more of the following:

- Server administration
- Storage administration
- Network administration
- Network security

## Site planning checklist

Planning the location and layout of your equipment is essential for successful network operation, ventilation, and accessibility. Consider heat dissipation when sizing the air-conditioning requirements for an installation.

**Table 1.** Site Planning Checklist

Task #:	Planning Activity:	Verified By:	Time:	Date:
1	<b>Space evaluation:</b> <ul style="list-style-type: none"><li>• Space and layout</li><li>• Floor covering</li><li>• Impact and vibration</li><li>• Lighting</li><li>• Maintenance access</li></ul>			
2	<b>Environmental evaluation:</b> <ul style="list-style-type: none"><li>• Ambient temperature</li><li>• Humidity</li><li>• Altitude</li><li>• Atmospheric contamination</li><li>• Air flow</li></ul>			
3	<b>Power evaluation:</b> <ul style="list-style-type: none"><li>• Input power type</li><li>• Power receptacles</li><li>• Receptacle proximity to the equipment</li><li>• Dedicated circuit for power supply</li><li>• Dedicated (separate) circuits for redundant power supplies</li><li>• UPS for power failures</li></ul>			
4	<b>Grounding evaluation:</b> <ul style="list-style-type: none"><li>• Circuit breaker size</li><li>• CO ground (AC- powered systems)</li></ul>			
5	<b>Cable and interface equipment evaluation:</b> <ul style="list-style-type: none"><li>• Cable type</li><li>• Connector type</li><li>• Cable distance limitations</li><li>• Interface equipment (transceivers)</li></ul>			
6	<b>EMI evaluation:</b> <ul style="list-style-type: none"><li>• Distance limitations for signaling</li><li>• Site wiring</li><li>• RFI levels</li></ul>			

**Note:**

- Verify that the power supply installed in the chassis has a dedicated AC source circuit.
- UPS: uninterruptible power supply.
- EMI: electromagnetic interference.
- RFI: radio frequency interference

## X-Series customer-provided configuration information

It is recommended to gather the following information prior to setup and configuration to serve as a reference for both physical and logical setup.

**Table 2.** Fabric Interconnect Domain and Server Policy network information

Customer Provided Information			
Item	Description		Comment
Mgt IP addresses/netmask	FI-A	<IP/Netmask>	No VIP for IMM
	FI-B	<IP/Netmask>	
	<gateway>		
KVM - IPMI address range	<Start IP/Netmask/Gateway>	<count>	
DNS server	1: <IP>	2: <IP>	
NTP server	<IP or FQDN>		
VLANs	Mgmt.: <VLAN> <add rows as needed>		Annotate native VLAN
VSANs	A: VSAN-ID: <VSAN>	FCOE-VLAN: <VLAN>	
	B: VSAN-ID: < VSAN >	FCOE-VLAN: <VLAN>	
VNICs	<vNIC>: <IP/netmask> <VLAN> <add rows as needed>		Set adapter policy based on planned OS
SAN boot target WWNs	<add rows as needed>		
ID pool ranges for MAC, WWNN, WWPN	<Start value> <add rows as needed>	count	
ISO media server	<protocol>	<IP/URL/path>	NFS, CIFS, or HTTPS source for OS and other images
Cisco Intersight account for testing	<Account ID>	<login>	

**Table 3.** Fabric Interconnect physical cabling configuration information

Fabric Interconnect:		Connected to:			Fabric Interconnect:		Connected to:		
Number	FI Port	IFM Port	Port Type (FC/Eth Up/Server)	Connection notes	Number	FI Port	IFM Port	Port Type (FC/Eth Up/Server)	Connection notes
1	1				2	1			
	2					2			
	3					3			
	4					4			
	5					5			
	6					6			
	7					7			
	8					8			
	9					9			
	10					10			
	11					11			
	12					12			
	13					13			
	14					14			
	15					15			
	16					16			
	17					17			
	18					18			
	19					19			
	20					20			
	21					21			
	22					22			
	23					23			
	24					24			
	25					25			
	26					26			

Fabric Interconnect:		Connected to:			Fabric Interconnect:		Connected to:		
	27					27			
	28					28			
	29					29			
	30					30			
	31					31			
	32					32			
	33					33			
	34					34			
	35					35			
	36					36			
	37					37			
	38					38			
	39					39			
	40					40			
	41					41			
	42					42			
	43					43			
	44					44			
	45					45			
	46					46			
	47					47			
	48					48			
	49					49			
	50					50			
	51					51			
	52					52			
	53					53			
	54					54			

## Setup and Install

Before you begin the installation, ensure that you have the following items:

- Scissor jack or other lift device capable of bearing the weight of a fully loaded chassis, which is 400 lb (163.29 kg).
- Number 1 and number 2 Phillips-head screwdrivers with torque-measuring capabilities
- Flat-head screwdriver
- Tape measure and level
- ESD wrist strap or other grounding device
- Antistatic mat or antistatic foam

### Cisco UCS 6454 Fabric Interconnect

Cisco UCS X9508 Chassis can be connected to Cisco UCS 6400 Series Fabric Interconnects provide a single point of connectivity for the system. When supporting the Cisco UCS X-Series, the fabric interconnects run in Intersight Managed Mode.

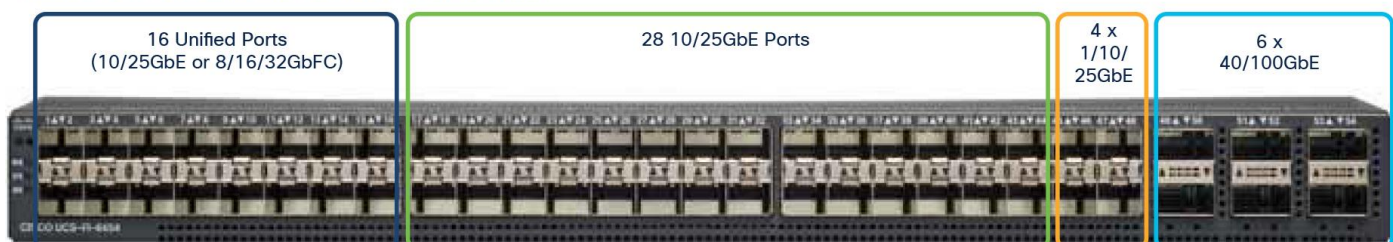
- **Cisco UCS 6454 Fabric Interconnect:** This 1RU 10/25/40/100 Gigabit Ethernet, FCoE, and Fibre Channel switch includes 28x 10/25-Gbps Ethernet ports, 4x 1/10/25-Gbps Ethernet ports, 6x 40/100-Gbps Ethernet uplink ports, and 16 unified ports that can support 10/25 Gigabit Ethernet or 8/16/32-Gbps Fibre Channel depending on the SFP connector used.
- **Cisco UCS 64108 Fabric Interconnect:** This 2RU 10/25/40/100 Gigabit Ethernet, FCoE, and Fibre Channel switch includes 72x 10/25-Gbps Ethernet ports, 8x 1/10/25-Gbps Ethernet ports, 12x 40/100-Gbps Ethernet uplink ports, and 16 unified ports.

This document provides example of UCS 6454 Fabric Interconnect. Please refer to [Cisco UCS 6400 Series Fabric Interconnect Hardware Installation Guide](#) for details on hardware setup for both UCS 6454 and UCS 64108 fabric interconnect.

Cisco UCS 6454 Fabric Interconnect Front View



Cisco UCS 6454 Fabric Interconnect Rear/Port View





## Environmental specifications

Below is specification for Cisco UCS 6454 FI

**Table 4.** Cisco UCS 6454 FI

Description	Specification
Dimensions (H x W x D)	1.72 in. x 17.3 in x 22.5 in (4.4 cm x 43.9 cm x 57.1 cm)
Weight (with two power supplies and fans installed)	22.24 lb (10.10 kg)
Temperature, operating	32 to 104° F (0 to 40° C)
Temperature, non-operating	-40 to 158° F (-40 to 70° C)
Humidity (RH), non-condensing	5 to 95%
Altitude	0 to 13,123 ft (0 to 4000 m)

## Rack and space requirements

This section provides the requirements for the following types of cabinets and racks, assuming an external ambient air temperature range of 0 to 104° F (0 to 40° C):

- Standard perforated cabinets (60-percent or greater perforation front and back is required)
- Standard open racks

### General requirements for cabinets and racks

The cabinet or rack must meet the following requirements:

- The minimum vertical rack space per Cisco Unified Computing System™ (Cisco UCS®) 6454 Fabric Interconnect must be 1 rack unit (1RU), equal to 1.75 in. (4.4 cm). The minimum vertical rack space per Cisco UCS 64108 Fabric Interconnect must be 2RUs, equal to 3.5 in. (8.8 cm).
- Use standard 19-in. (48.3-cm), four-post EIA cabinet or rack, with mounting rails that conform to English universal hole spacing per section 1 of ANSI/EIA-310-D-1992.
- The width between the rack-mounting rails must be at least 17.72 in. (45.0 cm) if the rear of the Fabric Interconnect is not attached to the rack. For four-post EIA racks, this is the distance between the two front rails.
- For four-post EIA cabinets (perforated):
  - The minimum spacing for the bend radius for fiber-optic cables should have the front-mounting rails of the cabinet offset from the front door by a minimum of 3 in. (7.6 cm), and a minimum of 5 in. (12.7 cm) if cable management brackets are installed on the front of the Fabric Interconnect.
  - The distance between the outside face of the front mounting rail and the outside face of the back mounting rail should be 23.5 to 34.0 in. (59.7 to 86.4 cm) to allow for rear-bracket installation.
  - A minimum of 2.5 in. (6.4 cm) of clear space should exist between the side edge of the Fabric Interconnect and the side wall of the cabinet. No sizeable flow obstructions should be immediately in the way of Fabric Interconnect air intake or exhaust vents.

### Requirements specific to perforated cabinets

A perforated cabinet is defined here as a cabinet with perforated front and rear doors and solid side walls. In addition to the requirements listed in the “General requirements for cabinets and racks” section, perforated cabinets must meet the following requirements:

- The front and rear doors must have at least a 60-percent open-area perforation pattern, with at least 15 square inches of open area per rack unit of door height.
- The roof should be perforated with at least a 20-percent open area.
- The cabinet floor should be open or perforated to enhance cooling.

**Note:** If you are using an enclosed cabinet, we recommend one of the thermally validated types: standard perforated or solid-walled with a fan tray.

**Note:** Do not use racks that have obstructions (such as power strips), because the obstructions could impair access to field-replaceable units (FRUs). The Cisco RP-Series PDUs, when mounted in a Cisco R-Series Rack, must not obstruct FRU replacement.

### Fabric Interconnect Installation guidelines

When installing the Cisco UCS Fabric Interconnect, follow these guidelines:

- Prepare the site as described in the “site preparation checklist” section of this document.
- Plan your site configuration and prepare the site before installing the Fabric Interconnect. The site preparation checklist lists the recommended site planning tasks.
- Record the information listed in the site preparation checklist as you install and configure the Fabric Interconnect.
- Ensure that there is adequate space around the Fabric Interconnect to allow for servicing and for adequate airflow. The site preparation checklist lists airflow requirements.
- Ensure that the air conditioning meets the heat dissipation requirements listed in site preparation checklist.
- Ensure that the Fabric Interconnect is adequately grounded. If the Fabric Interconnect is not mounted in a grounded rack, Cisco recommends connecting both the system ground on the Fabric Interconnect and the power supply ground to an Earth ground.
- Ensure that the site power meets the power requirements listed in power specifications in the “Power connectivity specifications” section. If available, you can use an uninterruptible power supply (UPS) to protect against power failures.

Avoid UPS types that use ferroresonant technology. These UPS types can become unstable with systems such as the Cisco UCS Fabric Interconnect, which can have substantial current draw fluctuations because of fluctuating data traffic patterns.

- Ensure that circuits are sized according to local and national codes. For North America, the power supply requires a 15-A or 20-A circuit.

To prevent loss of input power, ensure that the total maximum loads on the circuits supplying power to the Fabric Interconnect are within the current ratings for the wiring and breakers.

- Use the following screw torques (listed in Newton-meters [Nm]) when installing the Fabric Interconnect:
  - Captive screws: 4 in-lb (0.45 Nm)
  - M3 screws: 4 in-lb (0.45 Nm)
  - M4 screws: 12 in-lb (1.36 Nm)
  - 10-32 screws: 20 in-lb (2.26 Nm)
  - 12-24 screws: 30 in-lb (3.39 Nm)

### Power supply specifications (up to 2 per Fabric Interconnect)

Cisco UCS Fabric Interconnect supports AC or DC power supplies. You must use identical power supplies—either two AC or two DC power supplies with the fabric interconnect. .

**Note:** You cannot mix power supply types in a Cisco UCS Fabric Interconnect.

**Note:** The Cisco UCS 6454 FI and the UCS 6300 Series FIs use the same 650 W AC power supplies, so the ordering PIDs are the same.

**Table 5.** UCS 6454 FI Only: 650 W AC Power Supply Specifications (UCS-PSU-6332-AC)

AC Power Supply Properties	Specification
Maximum output per power supply	650 W
Input voltage	100 to 240 VAC
Maximum AC input current	7.6 A @ 100 VAC 3.65 A @ 208 VAC
Maximum holdup time	12 ms @50% load
Power supply output voltage	12 VDC
Power supply standby voltage	12 VDC
RoHS compliance	Yes
Hot swappable	Yes
Efficiency rating	Climate Savers Platinum Efficiency (80Plus Platinum Certified)

**Note:** The Cisco UCS 6400 Series FIs and the UCS 6300 Series FIs use the same 930 W DC power supplies, so the ordering PIDs are the same.

**Table 6.** UCS 6400 Series FIs: 930 W DC Power Supply Specifications (UCS-PSU-6332-DC)

DC Power Supply Properties	Specification
Maximum output per power supply	930 W

DC Power Supply Properties	Specification
Input voltage	-48 VDC
Maximum HVDC input current	23 A maximum @ -48 VDC
Maximum holdup time	8 ms @ 50% load
Power supply output voltage	12 VDC
Power supply standby voltage	12 VDC
RoHS compliance	Yes
Hot swappable	Yes
Efficiency rating	Climate Savers Platinum Efficiency (80Plus Platinum Certified)

## Cisco UCS X9508 chassis



### Environmental specifications

**Table 7.** Physical dimensions

Description	Specification
Height x Width x Depth	12.04 in. (30.6 cm) x 17.55 in. (44.6 cm) x 34.81 in. (88.4 cm)
Compute node slots	8
IFM slots	2
Fan module bays	4
Power supply bays	6

**Table 8.** Weight of the chassis components

Description	Specification
Empty chassis	95 lb. (43.09 kg)
IFM	8.5 lb. (3.85 kg)

Description	Specification
Fan module	3.4 lb. (1.54 kg)
Cisco UCS X210c M6 Compute Node	13 to 25 lb. (5.9 to 11.3 kg) depending on hardware options.
Fully Populated Cisco UCS X9508 Chassis	Approximately 400 lb. (163.29 kg) depending on models and options selected

The system weight listed here is an estimate for a fully configured system and will vary depending on the devices installed.

**Note:** Because of the chassis weight, a lift is recommended to install the chassis into a rack.

### Airflow considerations

Airflow through the chassis is from front to back. Air enters the chassis through the compute nodes and power supply grills at the front of the chassis and exits through the fan modules on the back of the chassis. To ensure proper airflow, follow these guidelines:

- Maintain ambient airflow throughout the data center to ensure normal operation.
- Consider the heat dissipation of all equipment when determining air-conditioning requirements. Do not allow the exhaust of one system to be the intake for another system.
- When evaluating airflow requirements, consider that the hot air generated by equipment at the bottom of the rack can be drawn in the intake of the equipment above.
  - Make sure that the exhaust at the rear of the chassis is unobstructed for at least 24 in. (61 cm), including obstruction due to messy cabling practices.
  - If you use an enclosed rack, the front door must be 65-percent perforated to ensure adequate airflow to the servers.

### Chassis rack requirements

This section provides the requirements for installing in a standard open rack, assuming an external ambient air temperature range of 41 to 95° F (5 to 35° C):

**Note:** Do not use racks that have obstructions. These obstructions could impair access to field-replaceable units (FRUs).

Cisco UCS is compliant with any EIA-310-D/E compliant rack. Your equipment racks must also be compliant with the EIA-310-D/E standard.

Also, be aware of these additional requirements:

- The tool-less rack-mount kits (either Type 1 or Type 2) shipped with the chassis are required. The adjustable rack rails shipped with each enclosure extend from 29 inches (73.66 cm) to 35 inches (88.9 cm)
- Front and rear doors: If your server rack includes closing front and rear doors, the doors must have a 65-percent open perforated area evenly distributed from top to bottom to permit adequate airflow.

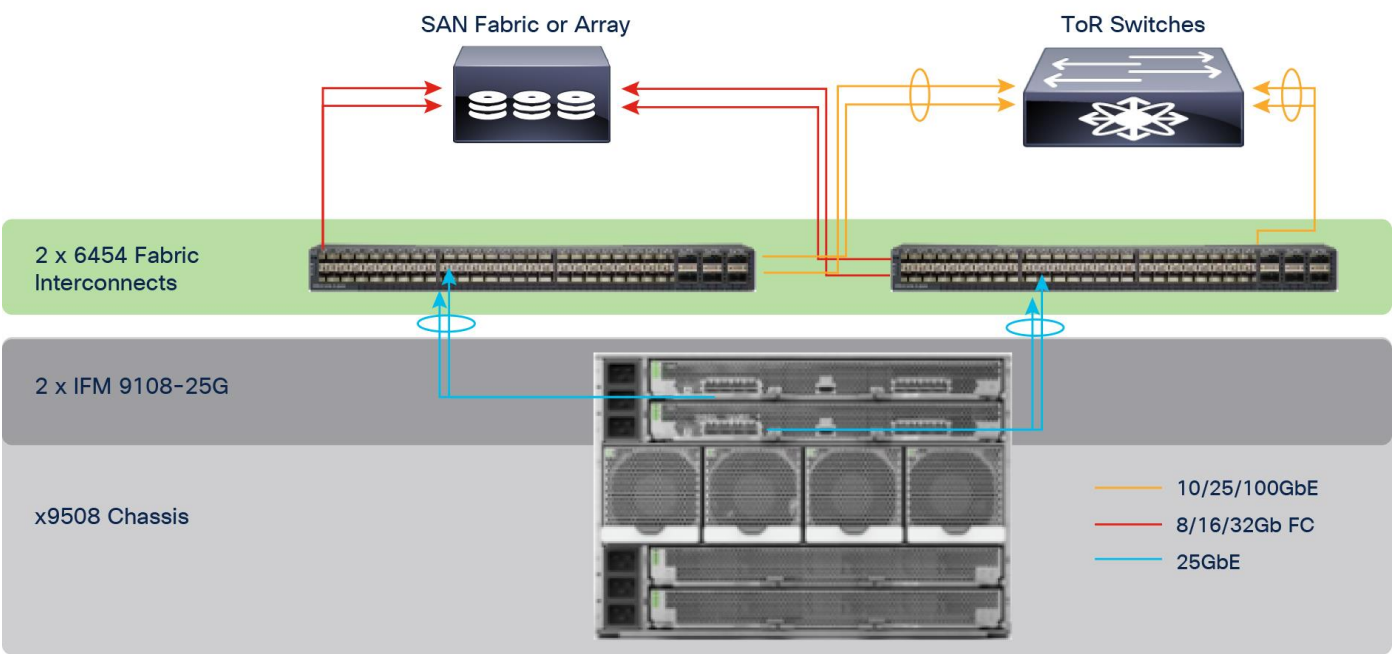
**Caution:** Always use blanking panels to fill all remaining empty front panel U-spaces in the rack. This arrangement helps ensure proper airflow. Using a rack without blanking panels results in improper cooling that can lead to thermal damage.

## Specifications for the Cisco UCS X9508 Chassis power supply units

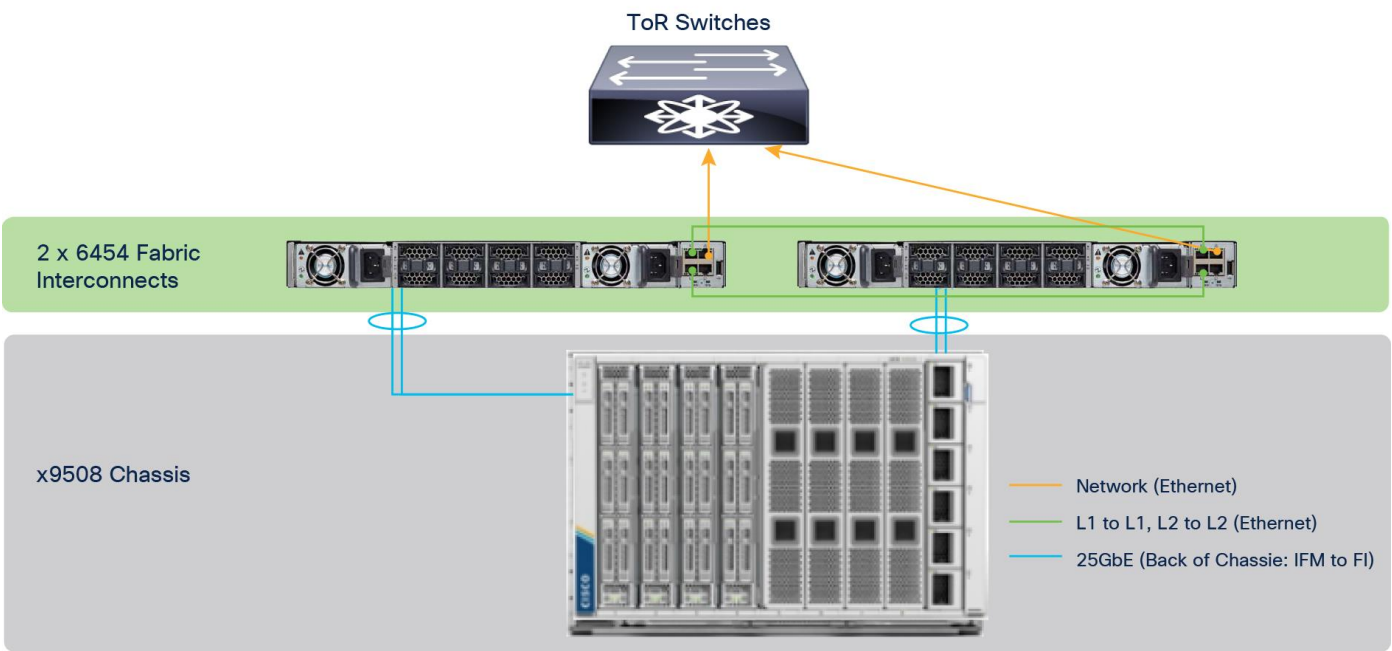
**Table 9.** Specifications for the Cisco UCS X9508 Chassis power supply units

Description	Specification
AC-input voltage	Voltage Range 100–127 VAC, 200–240 VAC nominal (range: 90–140 VAC, 180–264 VAC)
AC-input frequency	50 to 60 Hz nominal (range: 47 to 63 Hz)
Maximum AC-input current	18A @ 90 VAC 18A @ 180 VAC
Maximum input VA	3200 VA at 230 VAC
Maximum output power per power supply	2800W @ 200–240 VAC nominal 1400W @ 100–127 VAC nominal
Maximum inrush current	35A (sub cycle duration)
Minimum hold up time	10 ms @ 1400W 10 ms @ 2800W
Power supply main output voltage	54 VDC
Power supply standby voltage	3.4V
Efficiency rating	80+ Titanium Certified
Input connector	IEC320 C20  System input power connectors are located in the chassis PEMs, not on the power supply.

# Topology diagrams



**Figure 1.**  
Rear/port view cabling example (guidance on choosing ports)



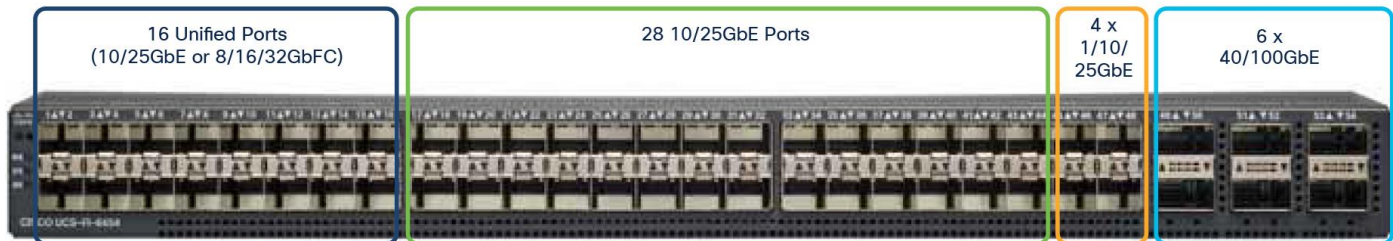
**Figure 2.**  
Front view cabling example



### Cisco UCS 6454 Fabric Interconnect Front View



### Cisco UCS 6454 Fabric Interconnect Rear/Port View



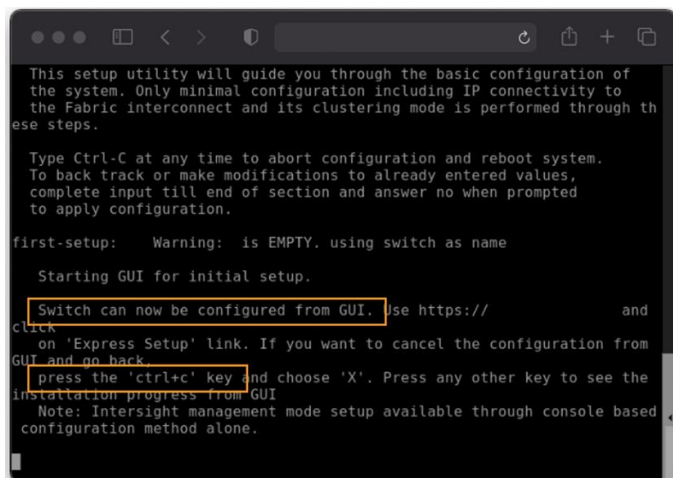
**Figure 3.**  
Fabric Interconnect port overview

## Starting the X-Series configuration

Using the data from the “X-Series customer-provided configuration information” table, do the following to configure the environment:

### Configure the first Fabric Interconnect for Cisco Intersight management.

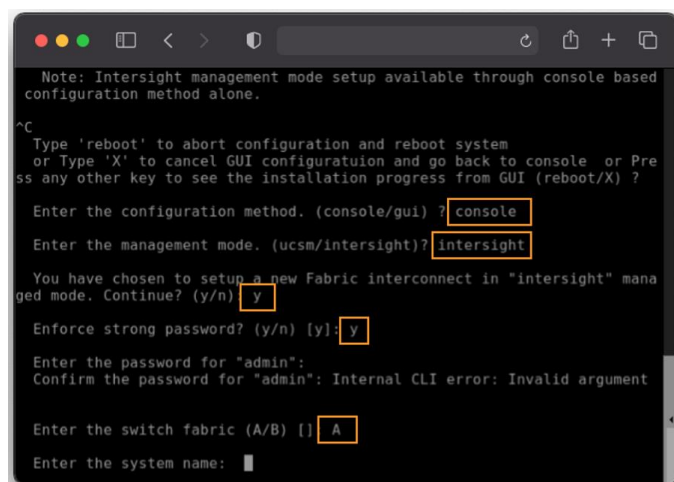
Depending on the state of each Fabric Interconnect, this first set of steps may not be necessary. If you see a message “Switch can now be configured from GUI” as shown in the following image, you must follow these steps:



1. Press **CTRL-c** as instructed on the screen to halt the GUI configuration process. You can configure Cisco Intersight mode only through the console. (Note: This step is typically seen if the management network is DHCP enabled)
2. Type “X” followed by Enter. Because of screen wrapping, you may not be able to see the “X” that you typed, but don’t worry about that.



Refer to the following image for the next steps:



```
Note: Intersight management mode setup available through console based
configuration method alone.

^C
Type 'reboot' to abort configuration and reboot system
or Type 'X' to cancel GUI configuratuion and go back to console or Pre
ss any other key to see the installation progress from GUI (reboot/X) ?

Enter the configuration method. (console/gui) ? console
Enter the management mode. (ucsm/intersight)? intersight

You have chosen to setup a new Fabric interconnect in "intersight" mana
ged mode. Continue? (y/n) y
Enforce strong password? (y/n) [y]: y
Enter the password for "admin":
Confirm the password for "admin": Internal CLI error: Invalid argument

Enter the switch fabric (A/B) [] A
Enter the system name: 
```

3. You will be asked to enter the configuration method. Remember that you can configure Cisco Intersight mode only through the console, so type **console**.
4. For the management mode, type **Intersight**.
5. The wizard will ask you to confirm that you are setting up a new Fabric Interconnect in Intersight Managed Mode. Type “y” to confirm.
6. You will be asked whether or not to enforce strong passwords. Obviously, strong passwords are encouraged.
7. For the switch fabric (A or B), choose A.
8. Name the system.
9. Enter the IP address for FI-A.
10. Enter the netmask for the management network.
11. Enter the default gateway.
12. Enter the IP address of the Domain Name System (DNS) servers.
13. Configure the default domain name.
14. The last step is to confirm all of your settings. Verify your settings are correct and type “yes” to continue.

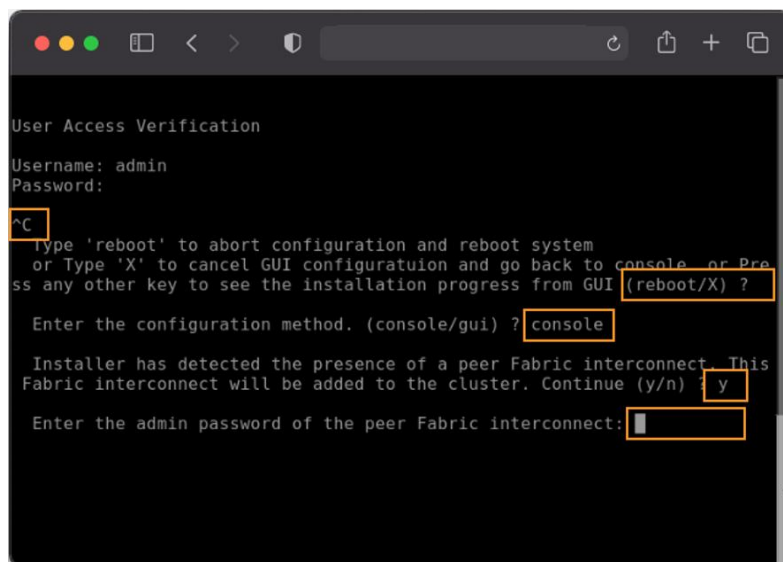
Congratulations. You have configured Fabric Interconnect A in Intersight Managed Mode. It will take several minutes for the Fabric Interconnect to reboot. Proceed to the next section to configure the second Fabric Interconnect.

## Configure the second Fabric Interconnect for Intersight management

Configuring the second Fabric Interconnect is much faster because it obtains most of its configuration from Fabric Interconnect A. These first few steps of the configuration are represented in the image following step 7 below:

1. You may need to hit the Enter key to wake up the console for FI-B. If you see nothing on the screen, the Fabric Interconnect might be in the mode where it is waiting for you to either configure it from the GUI or press **CTRL-c** to interrupt the process. Just like you did for the FI-A setup, press **CTRL-c**.

2. Like you did for the FI-A setup, press “x” and then Enter. As with FI-A, you may not actually see the “x” when you type it.
3. For the configuration method, enter console. Remember that you can configure Intersight mode only through the console.
4. FI-B should detect that its peer (FI-A) is already configured and will ask if it should attempt to join that cluster. Type “y” and hit Enter.
5. Enter the password you used for FI-A.
6. At this point, FI-B will pull the networking configuration from its peer. You only need to provide FI-B with an IP address. Use the IP address provided to you.
7. Type “yes” to save the configuration and restart the Fabric Interconnect.



```
User Access Verification
Username: admin
Password:
^C
Type 'reboot' to abort configuration and reboot system
or Type 'X' to cancel GUI configuratuion and go back to console or Pre
ss any other key to see the installation progress from GUI (reboot/X) ?
Enter the configuration method. (console/gui) ? console
Installer has detected the presence of a peer Fabric interconnect. This
Fabric interconnect will be added to the cluster. Continue (y/n) ? y
Enter the admin password of the peer Fabric interconnect:
```

Congratulations. You have configured Fabric Interconnect B in Cisco Intersight Managed Mode. It will take several minutes for the FI to reboot. Proceed to the next section to claim the Fabric Interconnect pair into the Cisco Intersight platform.

## Claim the Fabric Interconnects in Cisco Intersight platform

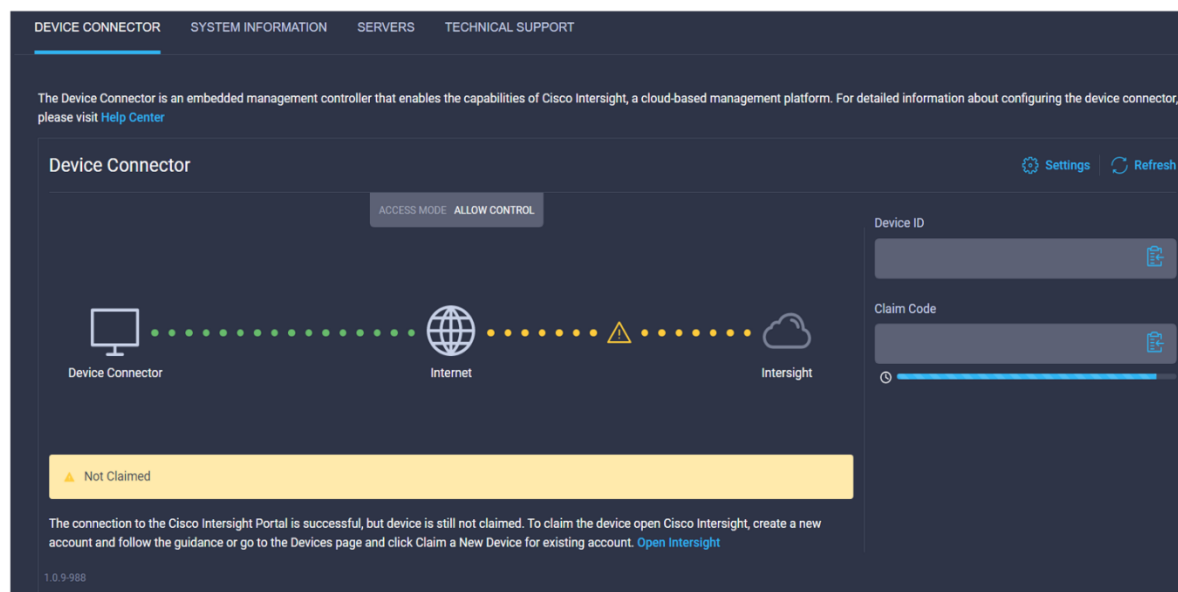
For this step, you will connect to the **Device Console** on the Fabric Interconnect pair. There is no longer an instance of Cisco UCS Manager, and when you browse to one of the Fabric Interconnects, you will be prompted to log into the Device Console instead. This console is where you obtain a Device ID and Claim Code in order to claim this new domain into the Cisco Intersight platform.

**Note:** Intersight is available as a cloud based SaaS service or as a locally deployed appliance. This section provides instructions based on a SaaS deployment. If you are using an appliance please refer to the [Intersight Appliance Deployment Guide](#).

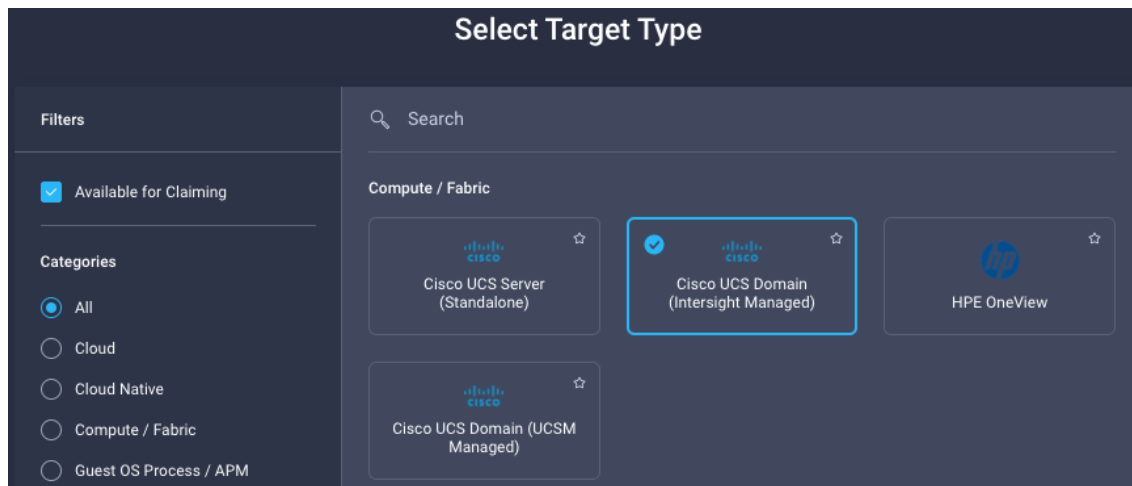
1. Using one of the supported browsers (found in section 6), connect the IP address of Fabric Interconnect A (you should see the Device Connector login screen like the one shown in the following image). Ensure that **HTTPS** is used or you will not be able to connect to the Device Console.
2. Use the credentials you configured earlier during Fabric Interconnect setup to log in.



3. Go the Device Connector tab. If there is an error on this page saying “*Some unknown internal error has occurred*”, it is likely because this domain has been claimed in Cisco Intersight already. Please **click the refresh button in the device connector view**, but if the problem persists, reach out to the Cisco Technical Assistance Center (TAC) to address this problem. If instead you see a screen awchich shows that the Fabric Interconnect can connect to Cisco Intersight but is not yet claimed, then proceed to the next step.



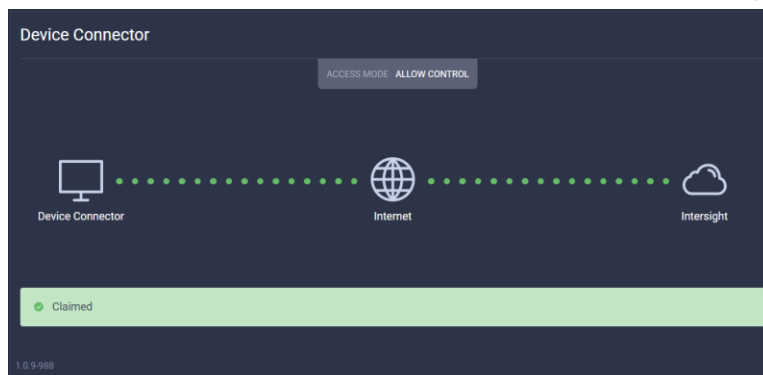
4. Browse to intersight.com from your computer. Use Cisco Intersight credentials for an account that has at least the **Device Technician** role. The roles Device Technician and Device Administrator allow you to claim and unclaim devices but do little else.
5. Click the blue **Claim Target** button in the Cisco Intersight.
6. For target type, select **Cisco UCS Domain (Intersight Managed)** as follows and click the **Start** button.



- You'll need the Device ID and Claim Code from the Device Console. Try copying those values into Cisco Intersight.

The screenshot shows the 'Cisco UCS Domain (Intersight Managed)' claim form. It includes a gear icon and the text 'To claim your target, you must have the Device ID and Claim Code.' Below this are two input fields: 'Device ID \*' and 'Claim Code \*'. At the bottom are three buttons: '< Previous', 'Cancel', and 'Claim'.

- Click the blue **Claim** button. Shortly after the claim succeeds, the Fabric Interconnect Device Connector should show a status of "Claimed" as shown in the following image:



- Although the Device Technician can claim a target, the Device Technician cannot put that target into the right organization. Currently, only an Account Administrator can do that. If your credentials don't have that privilege level, please reach out to someone within the organization with Account Administrator credentials.

Congratulations. You have claimed a domain in Intersight

After the domain is claimed to Intersight, all configuration of servers, chassis, and Fabric Interconnects is initiated with Intersight. For more information about Intersight managed domains, refer to the [Cisco Intersight Managed Mode Configuration Guide](#).

## Upgrade Fabric Interconnect firmware

Before discovering what hardware is connected to the Fabric Interconnects, you must upgrade the Fabric Interconnect firmware to the latest recommended version.

<input type="checkbox"/>	Name	Health	Management IP	Model	Firmware Version	
<input type="checkbox"/>	A	Healthy		UCS-FI-6454		...
<input type="checkbox"/>	B	Healthy		UCS-FI-6454		

☐ Upgrade Firmware

1. In Intersight, browse to OPERATE > Fabric Interconnects.
2. As shown in the previous image, click the three dots at the end of the row for either of the Fabric Interconnects and select “**Upgrade Firmware**”.
3. Click “**Start**” to bypass the first screen of the firmware upgrade.
4. Step 1 of the upgrade shows you the current running version for each Fabric Interconnect. Click “**Next**”.

Confirm Fabric Interconnects Selection 1 Selected

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

1 Items found 10 per page 1 of 1

Domain Name	Model	Fabric Interconnect A	Fabric Interconnect B
		Serial	Serial
		Firmware Version	Firmware Version
<input checked="" type="checkbox"/>	UCS-FI-6454		

Selected 1 of 1 Show Selected Unselect All 1 of 1

5. Step 2 of the upgrade allows you to select a different version of firmware. Fabric Interconnects in this state (with no discovered chassis) do not need to evacuate server traffic. *You must select Advanced Mode and uncheck “Fabric Interconnect Traffic Evacuation” as shown in the following image.* Do not do this for domains with discovered chassis.

Step 2  
**Version**

Select a firmware version to upgrade the Fabric Interconnects to.

Select Firmware Bundle Advanced Mode ☒

The selected firmware bundle will be downloaded from intersight.com. By default, the upgrade enables Fabric Interconnect traffic evacuation. Use Advanced Mode to exclude Fabric Interconnect traffic evacuation.

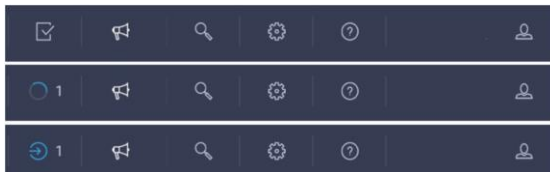
☐ Fabric Interconnect Traffic Evacuation

34 items found 10 per page 1 of 4

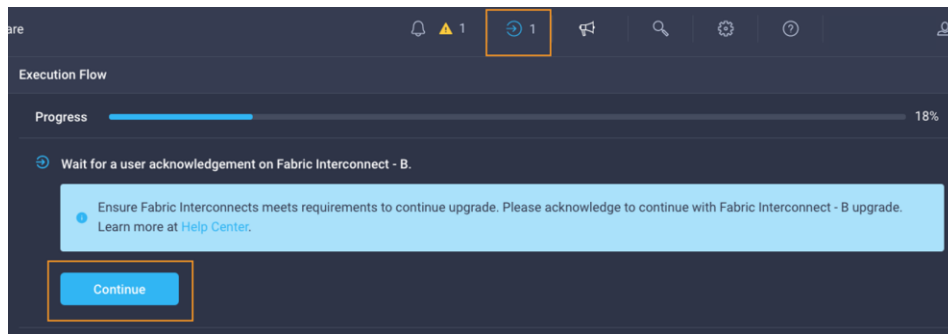
6. Step 3 of the upgrade is simply a confirmation screen that should show both Fabric Interconnects with their current firmware version and an icon showing the intended firmware version as shown in the following image. Click “Upgrade”.

The Intersight Requests icon will help you keep track of long-running tasks such as firmware updates. It is the left-most icon shown in the following image where three different states for the icon are shown.

- Rectangle with a check mark: All user requests have been completed. You can click this icon to view completed tasks.
- Spinning blue icon: The number shown is the number of user requests currently being worked on by Intersight. You can click this icon to view active tasks.
- Blue circle with arrow: The number shows the number of tasks that require user action or intervention. You can click the icon to view these actions and then act on them.



7. You will be required to confirm that it is okay to start upgrading the first Fabric Interconnect as shown in the following image. Click the “Continue” button and click “Continue” again on the popup. At this point, the firmware has been downloaded and you just approved the process to begin updating the firmware on the first Fabric Interconnect.



8. It will take about 15 to 20 minutes for the first Fabric Interconnect to complete its upgrade. You will be required to confirm that it is okay to start upgrading the second Fabric Interconnect, much like you did in the previous step. Watch for the spinning blue circle to change to a circle with an arrow to indicate that your action is required. Click Continue and click Continue again on the popup.
9. It will take about 15 to 20 minutes for the second Fabric Interconnect to complete its upgrade. If you browse away from the firmware upgrade status, you can always get back to it by clicking the spinning blue circle in the Intersight task bar to see current or completed tasks. Browse to OPERATE → Fabric Interconnects to confirm that both Fabric Interconnects are now running the correct version of firmware.

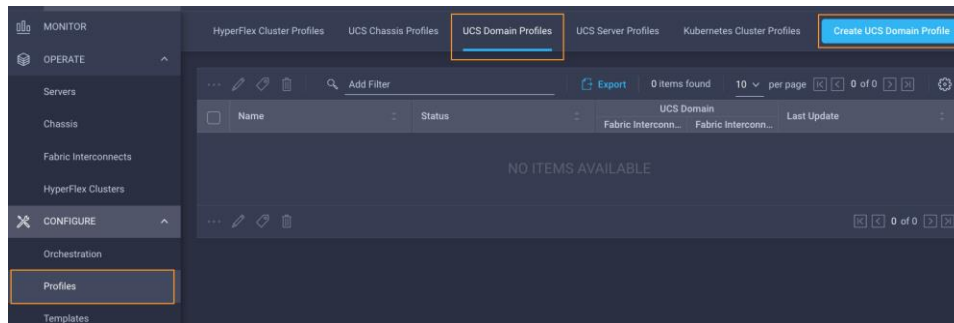
Congratulations. You have performed a Fabric Interconnect firmware update through Intersight. Proceed to the next section to discover what hardware is connected to that domain.

## Create a UCS Domain Profile

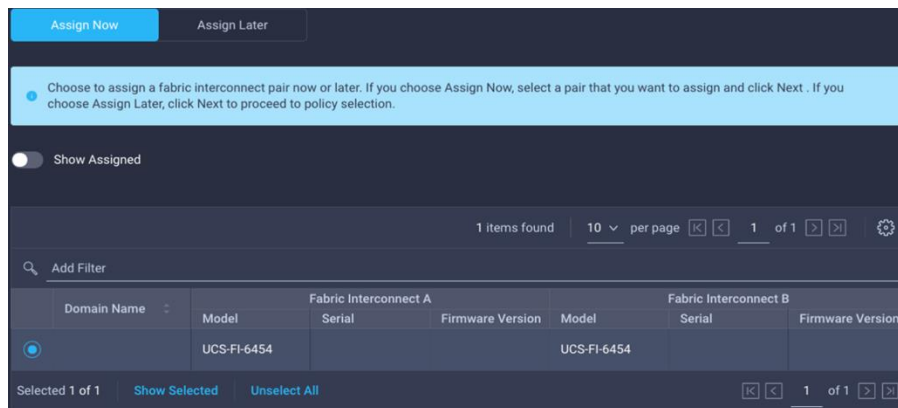
In this section, you will create a domain profile for the newly claimed domain. Intersight cannot discover any hardware connected to the Fabric Interconnects until its ports are configured, and that is done through a domain profile. You can create each of the policies the profile will use before you create it, or you can create the policies while creating the profile. We will do the latter in this guide.

The following reference details the policies involved in creating a domain profile. Not all policies are required. Please refer to [Domain Policies](#) for more details about each domain policy type.

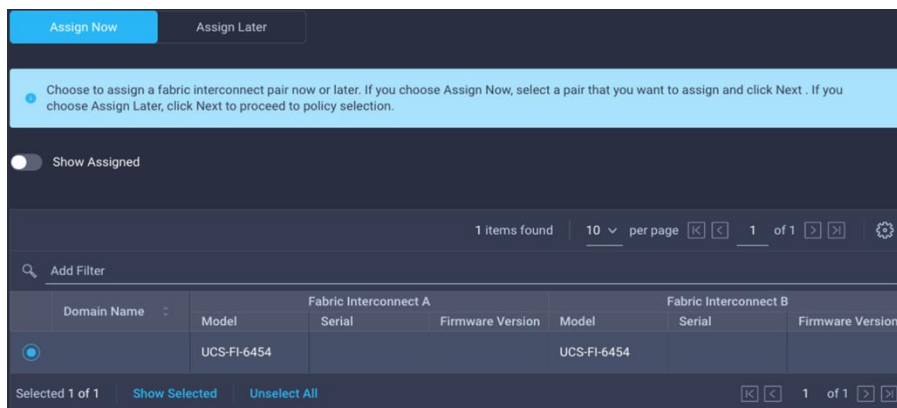
1. While logged in to Intersight, choose CONFIGURE > Profiles > UCS Domain Profiles > Create UCS Domain Profile as shown here:



2. At the intro screen for the wizard, click “**Start**”.
3. Give the profile a name (you can name it after yourself if you like), a description, and any tags you want to apply to it. Click “**Next**”.



4. Step 2 of the domain creation wizard is domain assignment. You should see the domain you created. Select that domain and click “**Next**”:



5. Step 3 of the domain creation wizard is VLAN and VSAN configuration. Notice that you can apply a different policy to the A and B fabrics. It is recommended that you click “**Create New**” rather than use the existing policy so you can learn the process. Add VLANs/VSANs documented in the “**X-Series Customer Provided Configuration Information**” table to your policy.
6. Create a new multicast policy. Creating a multicast policy involves selecting the snooping and querier state. Both settings have a tooltip next to them describing their function.



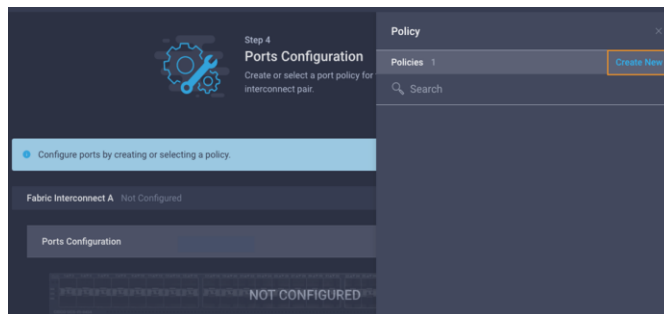
7. Create a VLAN policy (if using the same VLANs on Fabric A and B, you can use the same policy for both).
8. If connecting to a SAN, create a VSAN configuration policy.

**Note:** It is best practice for VSAN IDs to be different for each fabric, so you should create two policies.

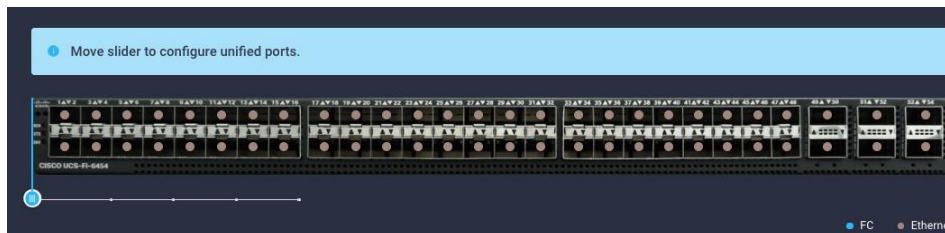
9. Click **“Next”**.

The next part of creating the Domain Profile is to create a port policy. If you follow internal standards for cabling Cisco UCS domains, you can create this port policy once and reuse it for every new domain, saving significant setup time. You will use the data gathered in the Site Planning Checklist on port cabling to match the policy to the physical deployment. If you use fiber channel storage with separate VSANs for the A and B fabrics you will need to create separate policies for each fabric. You can use a single port policy for deployments without VSANs.

10. On the ports configuration screen that shows an image of a 6454 Fabric Interconnect, click **“Select Policy”**.
11. Click **“CreateNew”** to create a new policy rather than select an existing policy:



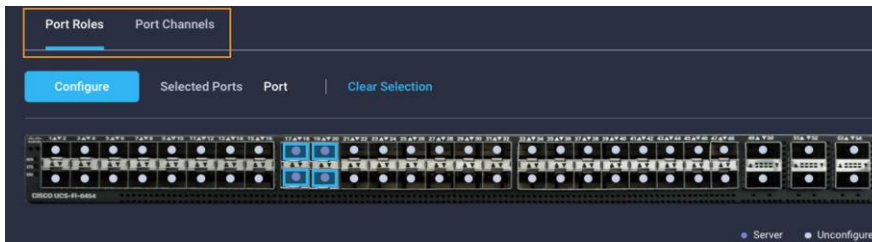
12. In the first step of creating the port policy, give the policy a name and select **UCS-FI-6454** for the switch model. You can optionally give the profile a description and any tags you like.
13. In the second step of creating a port policy, you have the option to set some number of the unified ports to Fibre Channel by moving the slider. Note that in firmware 4.1(3c) and later, you can change the position of the slider after deploying the domain profile, but it will require rebooting both Fabric Interconnects. Changing any of the unified ports between Ethernet and Fibre Channel is a hardware change and requires a reboot. Click **“Next”**.



14. In the third and final step of creating the port policy, you must change the role of ports connected to the chassis to be Server Ports. While on the Port Roles tab (tabs are shown in the image that follows), select ports that are cabled to chassis IFMs and click **“Configure”** to select Server Ports.
15. Click the Port Channels tab shown in the following image and click **“CreatePort Channel”**. Add the ports connecting to the switch if using 10-/25-Gigabit Ethernet (GbE) cables or the ports cabled to the switch using 100-GbE cables to an Ethernet Uplink Port Channel with a port channel ID and admin speed of Auto. If you need to define additional details for flow control, link aggregation, and link control



policies, please review additional information about these policies at:  
[https://intersight.com/help/features - domain\\_policies](https://intersight.com/help/features - domain_policies).



16. Repeat steps 14 and 15 for each set of cabled ports and their roles (server, uplink, or fiber channel), either individual or in port channels.
17. Click **“Save”** to save the port policy. You now have defined a reusable port policy and should be returned to step 4 of the domain profile configuration.
18. Click **“Select Policy”** to choose a port policy for the second Fabric Interconnect and choose the port policy that you just created or create a new one if needed for a unique VSAN configuration. Click **“Next”** to move to step 5 of domain profile configuration.

Step 5 of the domain profile configuration involves creating several policies. This guide covers the steps for creating the Network Time Protocol (NTP), Network Connectivity (DNS) and System quality-of-service (QoS) policies, but you should familiarize yourself with the capabilities of the other policies as well. Consult the online Intersight help.

19. Create a new NTP policy that specifies the NTP servers from the site planning checklist and choose the appropriate time zone.
20. Create a new Network Connectivity policy that specifies the primary DNS and the alternate DNS.
21. Create a System QoS policy. This step is required for domain profile creation.
22. Syslog, Simple Network Management Protocol (SNMP), and Switch Control policies are optional. You can explore and create them if you choose. Click **“Next”** when you are ready to move to the next step.
23. Click **“Deploy”** (and then click Deploy again in the popup) to apply this UCS domain profile. You can watch the status of the tasks associated with this action by clicking any of the requests. These tasks will complete quickly and chassis discovery will begin.

Congratulations, you have created and applied a UCS domain profile in Intersight. This step had many tasks, but fewer than are required for configuring a traditional UCS domain. Additionally, you can reuse many of the policies you created to deploy a second domain in Intersight Managed Mode much faster.

## Verify discovered chassis

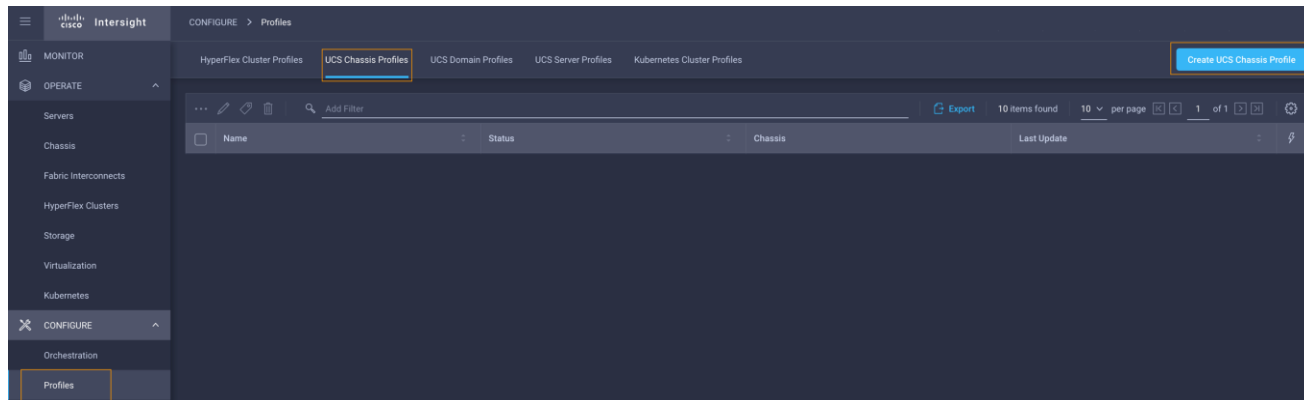
The chassis will be discovered almost immediately, but it will take longer for the compute node(s) to be discovered. In Intersight, browse to OPERATE → Chassis to see the newly discovered chassis. The chassis will likely show up empty because it is still performing discovery. Now is a good time to start creating pools and profiles. Proceed to the next section.

## Create a Chassis profile

In this section, you will create a **chassis profile** for each discovered chassis. The primary goal is to set the power policy as appropriate for the deployed power configuration.

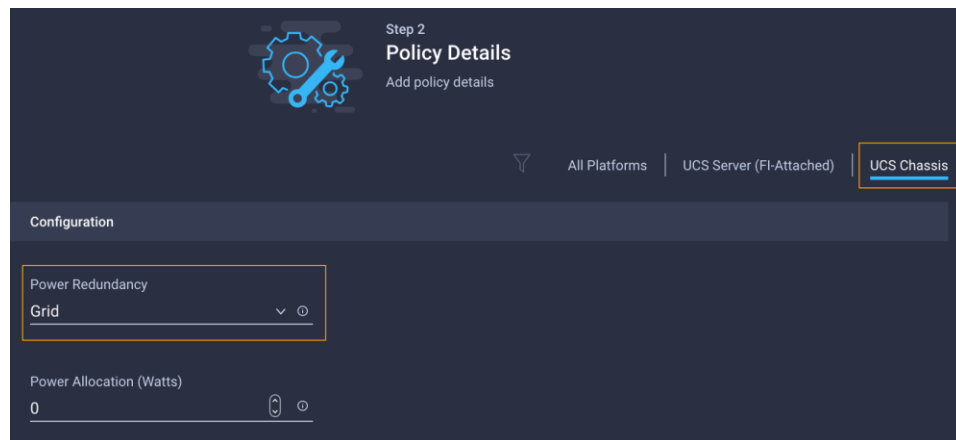
The following reference details the policies involved in creating a chassis profile. Not all policies are required. Please refer to [Chassis Policies](#) for more details about each chassis policy type.

1. While logged in to Intersight, choose CONFIGURE → Profiles → UCS Chassis Profiles → Create UCS Chassis Profile as shown here:



2. At the intro screen for the wizard, click “**Start**”.
3. Give the profile a name (you can name it after yourself if you like), a description, and any tags you want to apply to it. Click “**Next**”.
4. Step 2 of the chassis profile creation wizard is chassis assignment. You should see the discovered chassis. Select a chassis and click “**Next**”:
5. For this purpose we will define a power policy. Click on Power and then Create New.
6. Make sure “UCS Chassis” is selected for the policy target.
7. Select the Power Redundancy mode supported by the chassis power configuration. Our example uses the Grid policy, where the first 3 power supplies are connected to a single power source and power supplies 4–6 are connected to a second power source.

**Note:** This policy is also where a power limit can be specified for the chassis if the power source cannot support the maximum draw possible with the chassis power supply configuration. This is an advanced topic. Consult with your facilities power team and appropriate documentation if you need assistance with this setting.



**Note:** Chassis Profiles also support a Thermal Policy where a specific fan mode can be selected. This is an advanced topic. Consult appropriate documentation before using this policy.

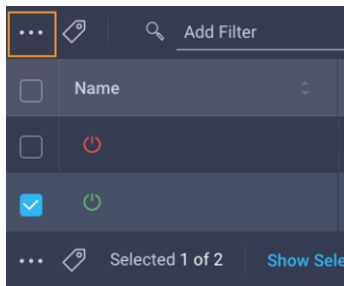
8. Click “**Create**” to finish creation of the power policy.
9. Click “**Next**” and review the profile settings.
10. Click “**Deploy**” and click again on the popup to complete profile creation and assignment.
11. Repeat for additional chassis in the domain.

## Starting the X-Series server configuration

### Update server firmware

Intersight allows for upgrading firmware on multiple servers at once. At this point, any blades attached to the domain should have completed discovery. If blades are still discovering you can proceed with creating the server profile templates while they complete and then come back to this step to upgrade firmware.

1. In Intersight, browse to OPERATE -> Servers. Intersight should have discovered the servers in the domain. If you don’t see them, hit the refresh button in your browser.
2. Select all the discovered servers that are of the same type by clicking the checkbox next to each one. Bulk firmware upgrade operations are supported on only similar servers. You can sort the servers table by **Model** if there is any confusion.
3. With one or more servers selected, click the ellipses (...) at the top or bottom of the server table and choose **Upgrade Firmware**. The ellipses are highlighted here:



4. The first step of the firmware upgrade process introduces the firmware upgrade wizard and allows you to change your mind about which servers you want to upgrade. Press “**Next**” to proceed.
5. The second step of the firmware upgrade process allows you to select the upgrade firmware version. Select the latest firmware version and click through the remaining screens to initiate the upgrade. This process takes roughly 30 minutes.

### Create Server Profile Template

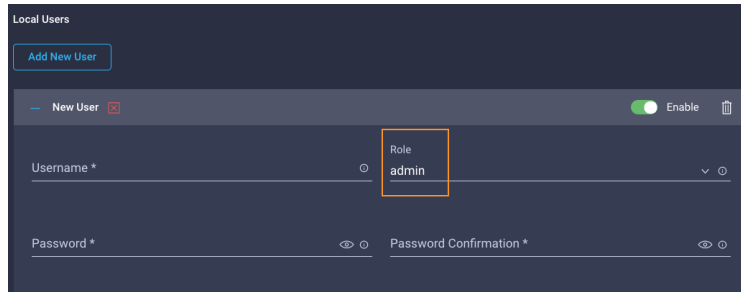
In this step, you will create a server profile template. Intersight allows converting a server profile to a template, but let’s just create a template directly instead. Just know that you can take any server profiles that you have already created in your own Intersight account and convert them into templates.

The following reference details the policies involved in creating a server profile and server profile template. Not all policies are required. Please refer to [Server Policies](#) for more details about each server policy type.

#### Before creating the profile, create some of the policies that you will need:

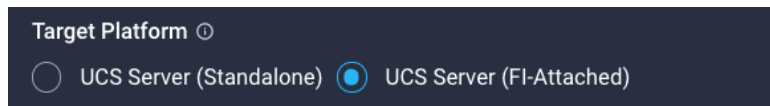
1. In Intersight, browse to CONFIGURE -> Policies and click “**Create Policy**”. Select a **local user** policy. The local user will be the user whom you use to connect to KVM.

2. Give the local user policy any name, description, and tags that you like. Click “**Next**”
3. Choose “**Add New User**” and set that user to a role of **admin** as shown in the image that follows. Give the user a username and password. You can create multiple user accounts with this policy. **Use something unique for the local user account.**



Next, you will create a LAN Connectivity policy. This policy specifies the number and mapping of virtual network interface cards (vNICs). It takes several steps, so this guide will walk you through building this policy prior to building a server profile rather than building the policy in line with creating the profile.

4. In Intersight, browse to CONFIGURE -> Policies.
5. Click **Create Policy** and choose LAN Connectivity policy.
6. In step 1 of the LAN Connectivity policy creation, it is important to select **FI-Attached** for the target platform: You can give the policy any name you like.

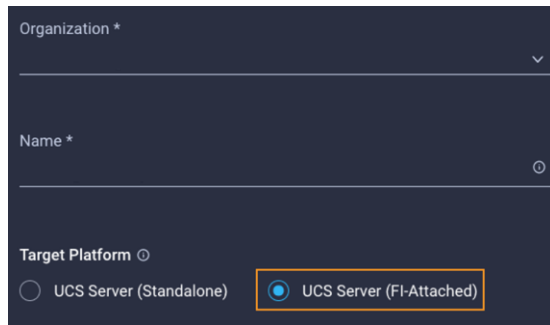


During step 2 of the LAN Connectivity policy creation, you will create two vNICs and assign a Media Access Control (MAC) pool and policies to each vNIC. The policies have been left at their default values, but you should understand the purpose of these policies before installation. The next few numbered steps in this guide will help you complete step 2.

7. For *iSCSI Initiator* (IQN), leave this set to None.
8. For vNIC placement, choose **Auto vNICs Placement**.
9. Click add vNIC.
10. Give the vNIC a name such as vNIC0 or Eth0.
11. Click **Select Pool** for the MAC Address Pool.
12. For Switch ID, choose switch **A**.
13. Create an Ethernet Group Policy, Ethernet Network Control Policy, Ethernet QoS, and Ethernet Adapter policy according to customer configuration requirements.
14. Click **Add** to complete the creation of the first vNIC. You should follow these steps again to create a second vNIC on fabric **B** with a name similar to vNIC1 or Eth1.
15. After you have created the correct number of vNICs, click **Create** to complete the creation of the LAN Connectivity policy.

Now that you have completed some of the initial work, it is time to create the server profile template.

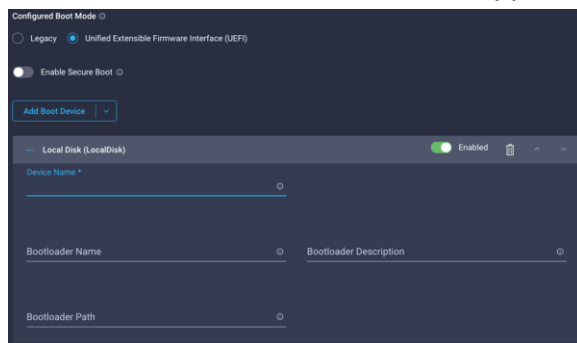
16. In Intersight, browse to CONFIGURE -> Templates and click “**Create UCS Server Profile Template**”.
17. Give the template a name and be sure to select **FI-Attached** for the target platform:



The screenshot shows a configuration form for a UCS Server Profile Template. It includes fields for 'Organization \*' and 'Name \*'. Below these is the 'Target Platform' section with two radio buttons: 'UCS Server (Standalone)' and 'UCS Server (FI-Attached)'. The 'UCS Server (FI-Attached)' option is selected and highlighted with an orange box.

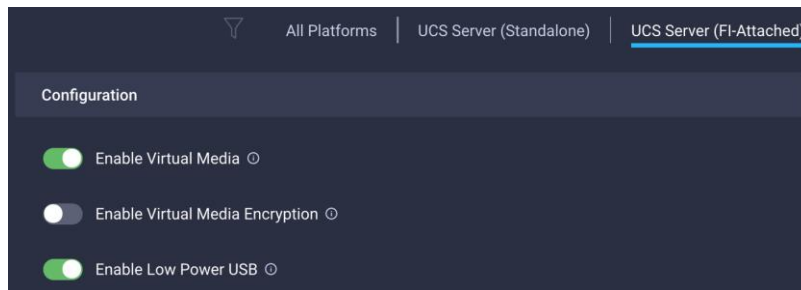
18. In step 2, you will set the boot order. The goal is to create a policy that attempts to boot first from virtual media and second from the local disk. When creating a boot policy:

- Add Local Disk.
- Add the virtual media with CIMC-mapped DVD sub-type.
- Add the virtual media with KVM-mapped DVD sub-type.



The screenshot shows the 'Configured Boot Mode' settings. It has two radio buttons: 'Legacy' and 'Unified Extensible Firmware Interface (UEFI)'. The 'UEFI' option is selected. Below this is a toggle for 'Enable Secure Boot'. There is an 'Add Boot Device' button. A list of boot devices is shown, with 'Local Disk (LocalDisk)' selected and marked as 'Enabled'. Below the list are fields for 'Device Name \*', 'Bootloader Name', 'Bootloader Description', and 'Bootloader Path'.

19. Also, in step 2, you will set the Virtual Media policy to enable virtual media. Unlike traditional UCS servers, even KVM-mapped virtual media will not work if it is not enabled by policy.



The screenshot shows the 'Configuration' section of the UCS Server (FI-Attached) template. It has three toggle switches: 'Enable Virtual Media' (checked), 'Enable Virtual Media Encryption' (unchecked), and 'Enable Low Power USB' (checked).

20. If you choose to use standard basic input/output system (BIOS) settings, you can skip that policy. Click **Next** to proceed.
21. Step 3 of the server profile template configuration allows you to configure multiple management policies. Start with **local user** and select the policy you created earlier.
22. Create a SAN Connectivity Policy (requires server pools and sub-policies).
- Create the WWNN pool.
  - Create the WWPN pool for each fabric (fabric A pool and fabric B pool)

- Add and name virtual host bus adapters (vHBAs) from the WWPN pool created earlier and select the switch ID.
- Create a FC Network Policy and make sure the VSAN IDs match the fabric (A or B) being configured.
- Create the Fibre Channel QoS Policy.
- Create the Fiber Channel Adapter Policy.

23. For the **IMC Access** policy, note that the purpose of this policy is to define an IP pool for IMC as well as VLAN, gateway, and DNS information.

24. For the virtual **KVM policy**, simply use the default settings. Click **Next** to proceed.

25. Step 4 of the server profile template configuration allows you to configure storage-related policies. Configure either of these policies. SD-Cards are only supported with M5 servers. The following image shows a storage policy which includes an M.2 Boot Optimized RAID1 drive and two MRAID volumes (one RAID1 and one RAID5) intended for use as VMDK partitions for ESXi storage. When creating a disk group specify the Span field as a comma or hyphen separated list of drive slots, as shown in the second image. Click **Next** to proceed.

The screenshot displays the 'General Configuration' tab of a server profile template configuration. It includes sections for 'Unused Disks State', 'M.2 Configuration', and 'Drive Group Configuration'. The 'M.2 Configuration' section is enabled, showing 'MSTOR-RAID-1' as the slot of the M.2 RAID controller. The 'Drive Group Configuration' section is also enabled, showing 'Global Hot Spares' as an option. Below these sections are two tables: 'Add Drive Group' and 'Add Virtual Drive'.

**Add Drive Group Table:**

Drive Group Name	RAID Level	Number of Spans	Dedicated Hot Spares	Drive Array Spans
vmdk-raid1	RAID1			{1,2}
vmdk-raid5	RAID5			{3,4,5,6}

**Add Virtual Drive Table:**

Virtual Drive Name	Drive Group	Size (MiB)	Expand to Available	Set as Boot Drive
vmdk2	vmdk-raid1	-	Yes	No
vmdk	vmdk-raid5	-	Yes	No

**Edit Drive Group**

**Configuration**

Drive Group Name \*  RAID Level

**Drive Selection**

Drive Array Span 0  Dedicated Hot Spares

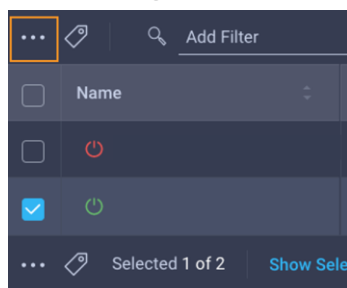
26. Step 5 of the server profile template configuration allows you to configure network policies. For the **LAN connectivity** policy, choose the policy you built earlier in the guide.
27. The final step of the server profile template configuration is to either exit (**Close**) or Derive Profiles. You will derive the profiles later, so for now, click **Close**.

Congratulations. You have created a server profile template and will soon get a chance to use it. First you must update the firmware on your server(s).

## Update server firmware

Intersight allows for upgrading firmware on multiple servers at once. At this point, any blades attached to the domain should have completed discovery.

1. In Intersight, browse to OPERATE -> Servers. Intersight should have discovered the servers in the domain. If you don't see them, hit the refresh button in your browser.
2. Select all of the discovered servers that are of the same type by clicking the checkbox next to each one. Bulk firmware upgrade operations are supported on only similar servers. You can sort the servers table by **Model** if there is any confusion.
3. With one or more servers selected, click the ellipses (...) at the top or bottom of the server table and choose **Upgrade Firmware**. The ellipses are highlighted here:

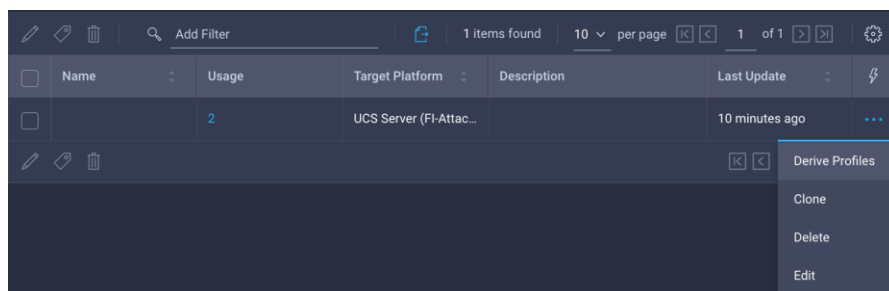


4. The first step of the firmware upgrade process introduces the firmware upgrade wizard and allows you to change your mind about which servers you want to upgrade. Press "**Next**" to proceed.
5. The second step of the firmware upgrade process allows you to select the upgrade firmware version. Select the latest firmware version and click through the remaining screens to initiate the upgrade. This process takes roughly 30 minutes.

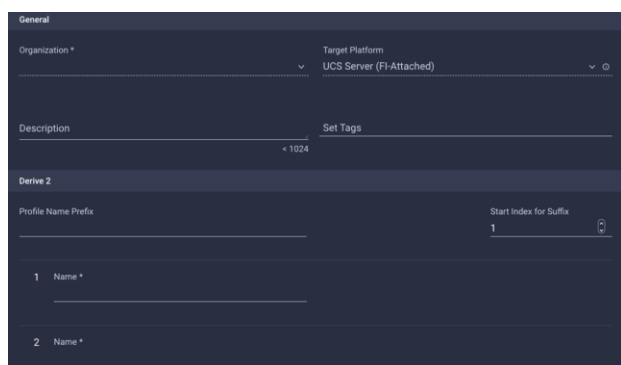
## Assign profiles to servers

After you have completed the firmware update, you can assign profiles to the servers.

1. In Intersight, browse to CONFIGURE -> Templates.
2. From the table of templates (you likely have only one), click the ellipses to the right of the template you created and choose **Derive Profiles**:

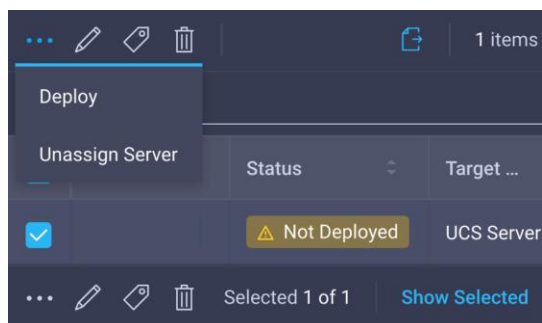


3. You can select server(s) to which to assign the derived profiles. Select all available servers and choose **Next** to proceed.
4. Intersight lets you set a prefix and suffix for all derived profile names, and also lets you customize each one. You can also add a description and tags that will be applied to all profiles derived in this step (refer to image that follows). Feel free to rename the profiles if you don't like seeing "DERIVED" in the profile name.
5. Click **Derive**.



6. The assignment process is immediate. The profiles are **assigned** to the servers, but no configuration changes happen yet.
7. In Intersight, browse to CONFIGURE -> Profiles and you will see that your profile(s) has been assigned to a server but shows a status of **Not Deployed**. You can select multiple profiles in this state and click the ellipses at the top of the table to deploy them all in bulk (refer to image that follows). When you **Deploy** a profile, Intersight will create a Request that you can monitor. Every time you make a change to a profile or a policy associated with that profile, its state will change from **Deployed** to a state indicating changes that have not been pushed to the server yet were made within Intersight. Each time, you will have to come back to this screen and **Deploy** the profile. This behavior is different from that of Cisco UCS Manager, so if you are unfamiliar, you can read more about the various states at: [https://intersight.com/help/features#server\\_profiles](https://intersight.com/help/features#server_profiles).





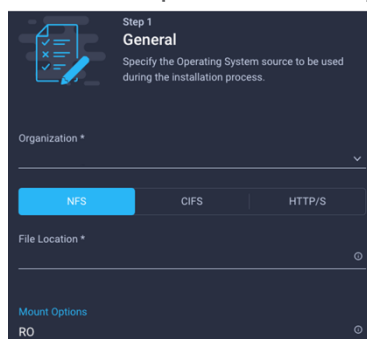
Congratulations. You have assigned a profile to a server in Intersight Now imagine an environment where you have multiple UCS domains. You can move that profile between any of those domains.

## Install an operating system with Software Repository

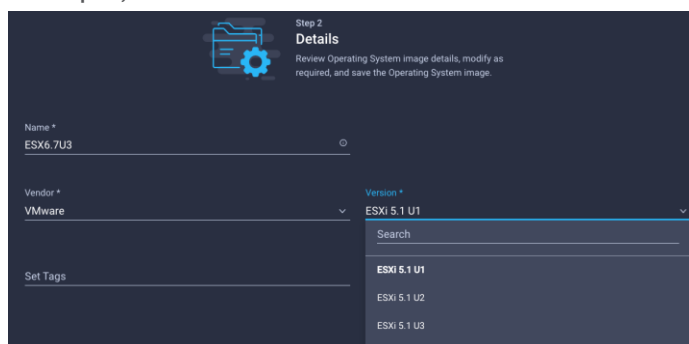
You can install an operating system by a traditional method of mapping the operating system install media via KVM and walking through the installation manually. Intersight provides the capability of automated operating system installation. This section guides you through that process. If you prefer to install via KVM, proceed to the next section. **Proceed to the next step.**

Normally the software repository used to install an operating system would be already configured. This section shows you how to set up an operating system image in the software repository and install an OS using that repository. Obviously, the process of automated OS installation for future OS installs will run faster after you do the initial work of setting up the repository.

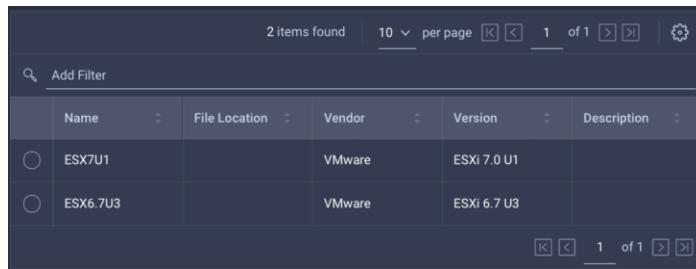
1. In Intersight, browse to ADMIN -> Software Repository.
2. On the Operating Systems Images tab, click the blue button Add Operating System Image.
3. Add the file path via the **NFS, CIFS, or HTTP/S** protocol with mount options RO:



4. Add details for the operating system image as shown in the following image. You can give the image any **Name** that you choose, but the vendor and version must match the contents of the ISO image. For this example, it is **VMware ESXi 6.7 U3**. Click the **Add** button.

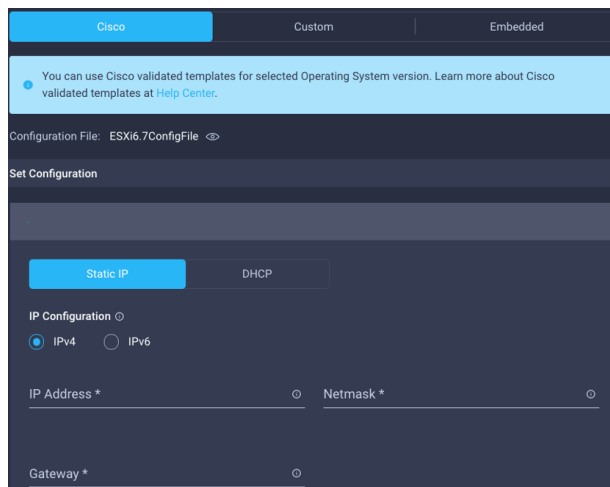


5. We also need to map the Server Configuration Utility SCU in the software repository.
6. Now that you have an OS image in your software repository, you can install that OS on your server(s). Browse to OPERATE -> Servers.
7. Choose one or more servers on which to install the OS.
8. Click the ellipses at the top or bottom of the servers table and choose **Install Operating System**.
9. As you step through the wizard, you will see familiar screens like the one that lets you change your mind about which servers you want to affect. Step 2 of the process lets you choose from the images available in your local software repository:



2 items found					10 per page	1 of 1
Add Filter						
	Name	File Location	Vendor	Version	Description	
<input type="radio"/>	ESX7U1		VMware	ESXi 7.0 U1		
<input type="radio"/>	ESX6.7U3		VMware	ESXi 6.7 U3		

10. Step 3 of the OS install lets you choose a config file. When selecting a valid config file, you will also see the option to provide variables such as IP addresses for each server on which you are installing an OS:



Cisco Custom Embedded

You can use Cisco validated templates for selected Operating System version. Learn more about Cisco validated templates at [Help Center](#).

Configuration File: ESXi6.7ConfigFile

Set Configuration

Static IP DHCP

IP Configuration

☒ IPv4 ☐ IPv6

IP Address \* Netmask \*

Gateway \*

11. Choose either Static IP or DHCP and click **Next**.
12. Select the Server Configuration Utility that you added to the software repository. Click **Next**.
13. Choose the installation target (which disk) for the operating system. Click **Next**.
14. On the final confirmation screen, choose **Install**. You can monitor the status of the installation the same way you monitored the status of firmware upgrades earlier in this guide.

Congratulations. You have installed an operating system using Intersight's automated OS installation feature.

---

## Install an operating system with KVM-attached virtual media

In this section, you will install an operating system using KVM-attached virtual media. The Cisco Intersight supports OS install through a more automated process if desired. Additionally, it is unlikely you will have the OS images staged in the Intersight software repository.

1. In Intersight, browse to OPERATE -> Servers and locate your server.
2. Click the ellipses next to your server and select **Launch vKVM**.
3. In the tab that pops up for KVM, select **Activate Virtual Devices** from the Virtual Media menu. If you get an error message on this step, you likely did not attach the proper Virtual Media policy to the server profile. There should be a Virtual Media policy that enables virtual media. Go back and correct this problem. Don't forget to **Deploy** the profile after making changes.
4. Select **Map CD/DVD** from the Virtual Media menu.
5. Attach the desired image and boot the server.
6. The remainder of the installation process should proceed like installing ESXi on any UCS server. Use the IP addresses provided to you for the OS management addresses.

## Final thoughts

### Intersight Organizations

In this guide, you may have had access to a single organization within an Intersight account that has several organizations. When you started, your user role could have had visibility to only a single server. This construct is powerful in that it allowed you to create policies and profiles that others could neither see nor modify using this Intersight account. Talk to your Cisco account team about using organizations effectively.

Every device that is claimed in Intersight is added to the **default** organization. When starting to use Intersight, it is tempting to use default as the one and only organization. As your environment grows, it will become problematic. Talk to your Cisco account team about how businesses or operations are organized so you can help them identify the partitions they need to establish to run the business effectively.

### Intersight User Roles

In this guide, you may have had access to a built-in role (Device Technician) for claiming targets and a **custom** role for creating pools, policies, and profiles. The custom role could grant you administrative capabilities *within one organization*. Roles are a powerful construct that can provide an individual user or group of users the granular level of privileges needed. Talk to your Cisco account team about using roles effectively to enable team members.

## Appendix and reference guides

### Appendix A

#### AC power cords and plugs for Cisco UCS X9508 Chassis

The AC power connectors on the chassis PEM use an IEC 320 C20 socket. Each chassis power supply has a separate power cord. The power cord that you use to connect the power supply units to an AC power source has an IEC 320 C19 plug on one end and on the other end one that conforms to the AC power outlet specifications for your country. Refer to the following table to determine which cord to order for your chassis power supply units. When you determine which power cord you need to order, you can verify that its plugs conform to the power outlets for your facility by clicking its reference link.

The jumper power cords, for use in racks, are available as an optional alternative to the standard power cords.

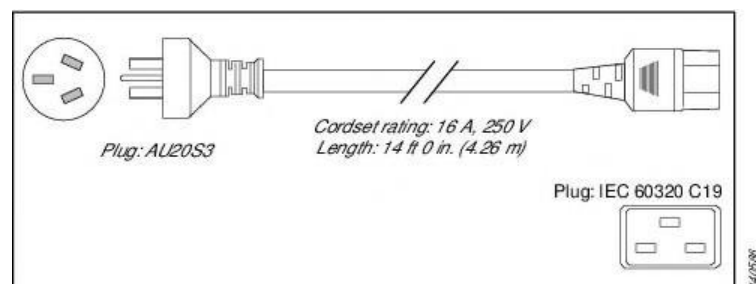
The optional jumper power cords have an IEC C19 connector (such as a Cisco RP-Series PEM) on the end that plugs into the chassis PEM and an IEC C20 connector on the end that plugs into an IEC C19 outlet receptacle. For more information, contact your Cisco Systems representative.

**Note:** Only the regular power cords or jumper power cords provided with the chassis are supported.

#### Australia and New Zealand

Power Cord Part Number—CAB-AC-16A-AUS

Cord Set Rating—16A, 250 VAC

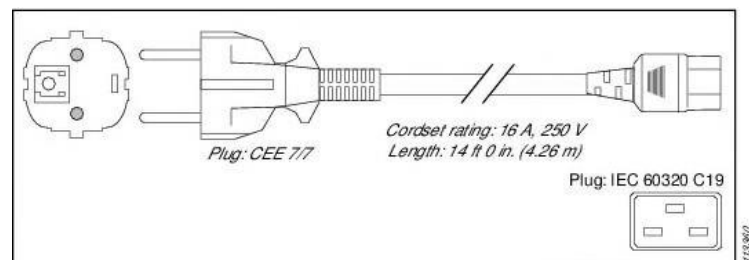


**Figure 4.**  
CAB-AC-16A-AUS Power Cord for the Cisco UCS X9508 Chassis

#### Continental Europe

Power Cord Part Number—CAB-AC-2800W-EU

Cord Set Rating—16A, 250 VAC

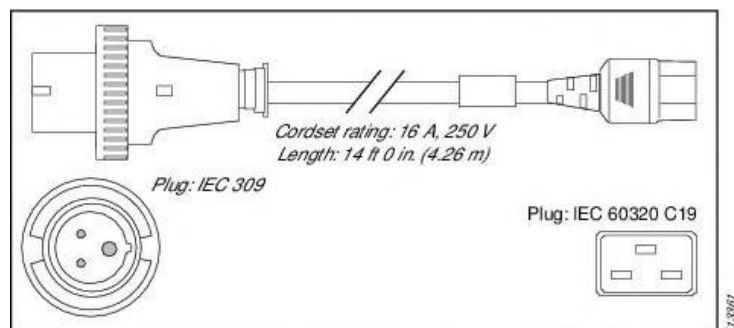


**Figure 5.**  
CAB-AC-2800W-EU Power Cord for the UCS X9508 Chassis

## International

Power Cord Part Number—CAB-AC-2800W-INT

Cord Set Rating—16A, 250 VAC



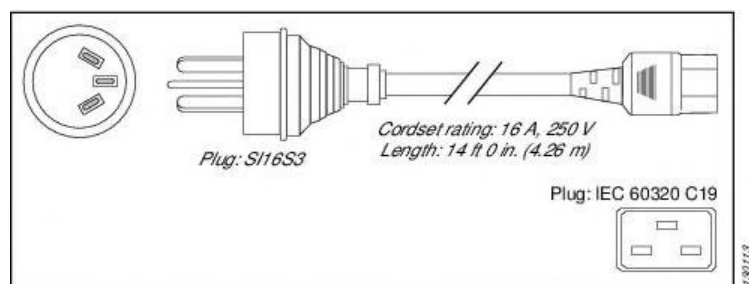
**Figure 6.**

CAB-AC-2800W-INT Power Cord for the UCS X9508 Chassis

## Israel

Power Cord Part Number—CAB-AC-2800W-ISRL

Cord Set Rating—16A, 250 VAC



**Figure 7.**

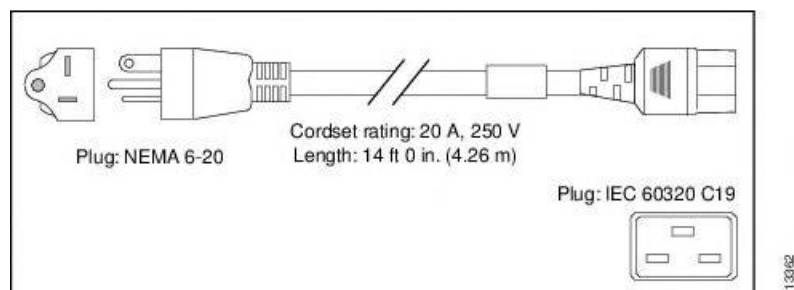
CAB-AC-2800W-ISRL Power Cord for the UCS X9508 Chassis

## Japan and North America

### **Non-Locking 200 to 240 VAC operation**

Power Cord Part Number—CAB-AC-2800W-US1

Cord Set Rating—16A, 250 VAC



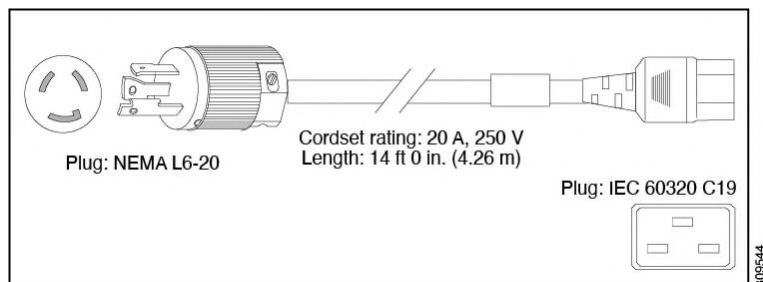
**Figure 8.**

CAB-AC-2800W-US1 Power Cord for the UCS X9508 Chassis

### Locking 200 to 240 VAC Operation

Power Cord Part Number—CAB-AC-C6K-TWLK

Cord Set Rating—16A, 250 VAC



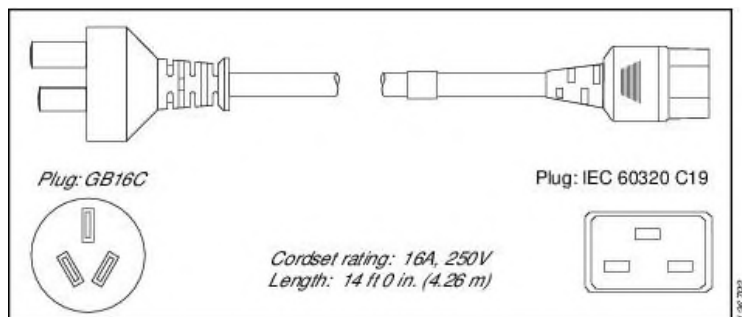
**Figure 9.**

CAB-AC-C6K-TWLK Power Cord for the UCS X9508 Chassis

### Peoples Republic of China

Power Cord Part Number—CAB-AC-16A-CH

Cord Set Rating—16A, 250 VAC



**Figure 10.**

CAB-AC-16A-CH Power Cord for the Cisco UCSX X9508 Chassis

### Taiwan

Power Cord—CAB-AC-C19-TW

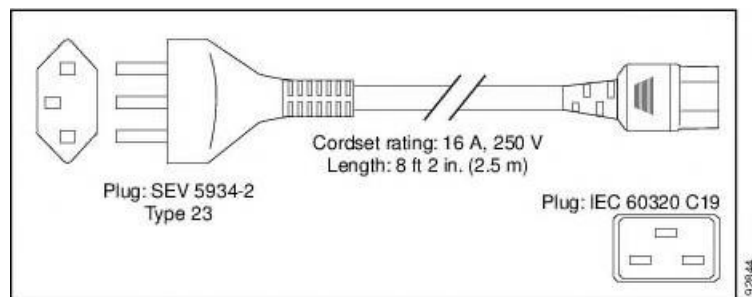
Plug—250 VAC 16 A, C19

Length—7.5 feet / 2.3 meters

## Switzerland

Power Cord Part Number—CAB-ACS-16

Cord Set Rating—16A, 250 VAC



**Figure 11.**

CAB-ACS-16 Power Cord for the UCS X9508 Chassis

## Appendix B

### Earth ground considerations for Cisco UCS X9508 Chassis

**Warning:** This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available. Statement 1024

**Warning:** For Nordic countries (Norway, Finland, Sweden, and Denmark) this system must be installed in a Restricted Access Location, where the voltage of the main ground connection of all equipment is the same (equipotential earth) and the system is connected to a grounded electrical outlet. Statement 328

**Warning:** High leakage current: Earth connection is essential before connection to the system power supply. Statement 342

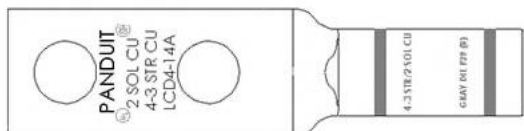
**Warning:** This equipment must be externally grounded using a customer-supplied ground wire before power is applied. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available. Statement 366

#### Customer-supplied ground lug

Connecting the chassis to Earth ground is completed by installing a grounding bracket, assembling the ground wire and ground lug, and then screwing a ground lug and ground wire to the grounding bracket.

Cisco does not supply the ground lug, so before beginning the installation procedure, you must obtain one. The grounding lug is available through third-party retailers, such as Panduit.

**Note:** The following information is for standard AC power installations in North America. Your location might require different specifications. Make sure that you are using the correct ground lug and ground cable for your location.



---

**Note:** The positive and negative wires can be installed pointing either to the right or to the left as long as the terminal cover is used.

Panduit LCD4-14A-L connectors (or equivalent) may be used supply and return wires, and Panduit LCD4-14A or equivalent connectors may be used for the 90-degree ground lug wire. Both connections have double lugs with .25-inch holes measuring .625 inches from center to center.

## Appendix C

Cisco Intersight runs on the following minimum supported browser versions:

- Google Chrome 62.0.3202.94
- Mozilla Firefox 57.0.1
- Apple Safari 10.1.1
- Microsoft Edge (Chromium) Beta and later versions

**Americas Headquarters**  
Cisco Systems, Inc.  
San Jose, CA

**Asia Pacific Headquarters**  
Cisco Systems (USA) Pte. Ltd.  
Singapore

**Europe Headquarters**  
Cisco Systems International BV Amsterdam,  
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at <https://www.cisco.com/go/offices>.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)