

Table of Contents

About this Lab	2
Requirements	2
About This Solution	3
Tasks	4
Task 1 - Claiming the UCS Domain (Review-Only(Do Not Attempt))	5
Task 2 – Intersight Dashboard Overview.....	11
Task 3 – Add and Remove a Dashboard Widget	15
Task 4 – Activate Trial Essentials License (Review-Only(Do Not Attempt))	17
Task 5 – Domain Policy Creation	19
Task 6 – Domain Profile Deployment (Review-Only(Do Not Attempt))	41
Task 7 – Updating Firmware (Review-Only(Do Not Attempt))	45
Task 8 – Creating Server Pools.....	49
Task 9 – Server Policy Creation.....	56
Task 10 – Server Profile Deployment	68
Task 11 – Server Profile Template Deployment	74
Task 12 – Virtual Media Using OS Links.....	78
Task 13 – Installing VMware ESXi	79
Task 14 – Accessing the KVM and Installing an Operating System(Do Not Attempt).....	83
Task 15 – Server Profile Deployment(Do Not Attempt).....	92
Task 16 – Submitting Feedback and Further Information.....	99
What’s Next.....	100

About this Lab

This lab provides an overview of Cisco UCS management via Cisco Intersight, and the embedded analytics that allow organizations to analyze, simplify, and automate their environments.

This Cisco Intersight™ environment is Read/Write and provides Administrator access to an emulated UCS infrastructure. This lab walks users through creating a Cisco Intersight account and using the functionality provided as part of the Cisco Intersight Essentials licensing within the account.

Requirements

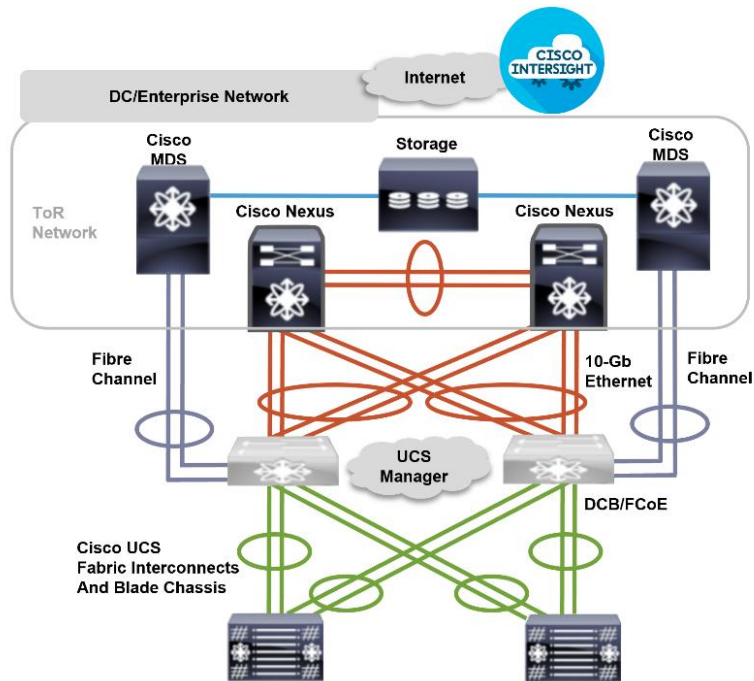
The table below outlines the requirements for performing the steps in this preconfigured lab.

Required	Optional
Personal Computer	Cisco AnyConnect® (required only for task 1)
Supported Web Browser*	
Cisco CCO account	

*See the Supported Browsers section at https://Cisco Intersight.com/help/getting_started.

About This Solution

Cisco Intersight™ provides intelligent cloud-based infrastructure management with embedded analytics for the Cisco Unified Computing System X™ (Cisco UCS X-Series®) and Cisco HyperFlex® platforms.



Tasks

This lab will walk you through viewing or performing the following tasks related to managing a UCS-X Series environment through Cisco Intersight.

1. [Claiming the UCS Domain \(Review-Only\(Do Not Attempt\) \)](#)
2. [Intersight Dashboard Overview](#)
3. [Add and Remove a Dashboard Widget](#)
4. [Activate Trial Essentials License \(Review-Only\(Do Not Attempt\) \)](#)
5. [Domain Policy Creation](#)
6. [Domain Profile Deployment \(Review-Only\(Do Not Attempt\) \)](#)
7. [Updating Firmware \(Review-Only\(Do Not Attempt\) \)](#)
8. [Creating Server Pools](#)
9. [Server Policy Creation](#)
10. [Server Profile Deployment](#)
11. [Server Profile Template Deployment](#)
12. [Virtual Media Using OS Links](#)
13. [Installing VMware ESXi](#)
14. [Accessing the KVM and Installing an Operating System \(Do Not Attempt\)](#)
15. [Server Profile Deployment \(Do Not Attempt\)](#)
16. [Submitting Feedback and Further Information](#)

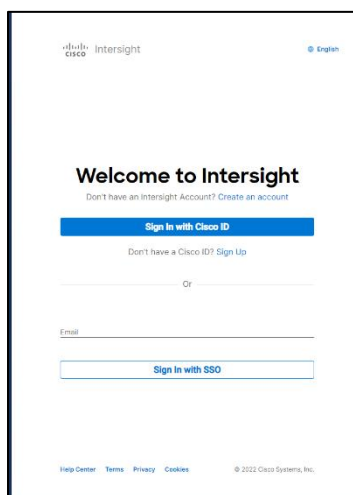
Task 1 - Claiming the UCS Domain (Review-Only)

In this task, the instructor will walk through the steps needed to claim your UCS domain in Cisco Intersight. Claiming the domain sets up the connection between your domain and Intersight so that you can manage the domain through Intersight.

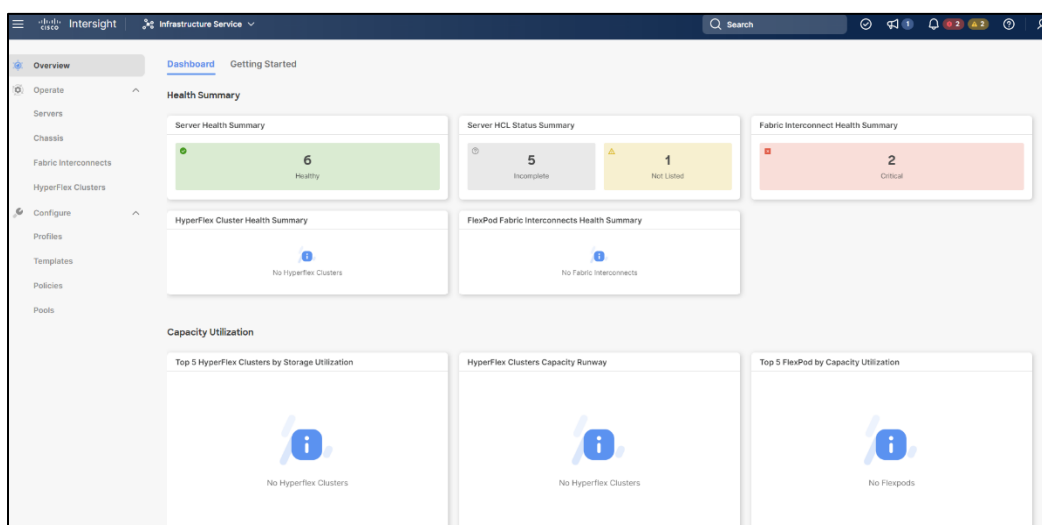
Note: Since this lab uses a shared UCS domain, claiming the domain in Intersight can be performed a single time. You may follow along with the instructor, but you will not be able to perform the claiming yourself.

Procedure

- Step 1** Open one of the supported browsers indicated in the [Requirements](#) section above.
- Step 2** In the address bar, enter the URL <https://intersight.com>
- Step 3** Click the **Sign In with Cisco ID** button.



- Step 4** Log in to Intersight using the credentials provided to you by the lab administrator.
- Step 5** Verify that you can now view the Intersight dashboard. The screen will say **OVERVIEW** at the top left, like the graphical view below.



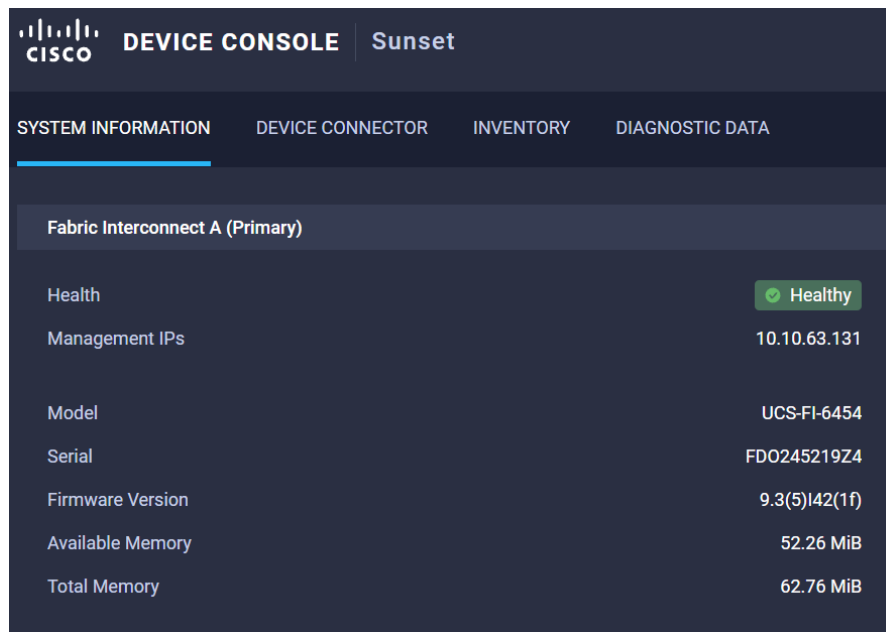
Note: To perform the steps in the remainder of this task, ensure you are connected to the SLI VPN using Cisco AnyConnect. If you are not able to connect, please read the remaining steps or follow along as the instructor performs the demonstration.

Step 6 Open a second browser tab and navigate to the UCS Fabric Interconnect at <https://10.10.63.131>

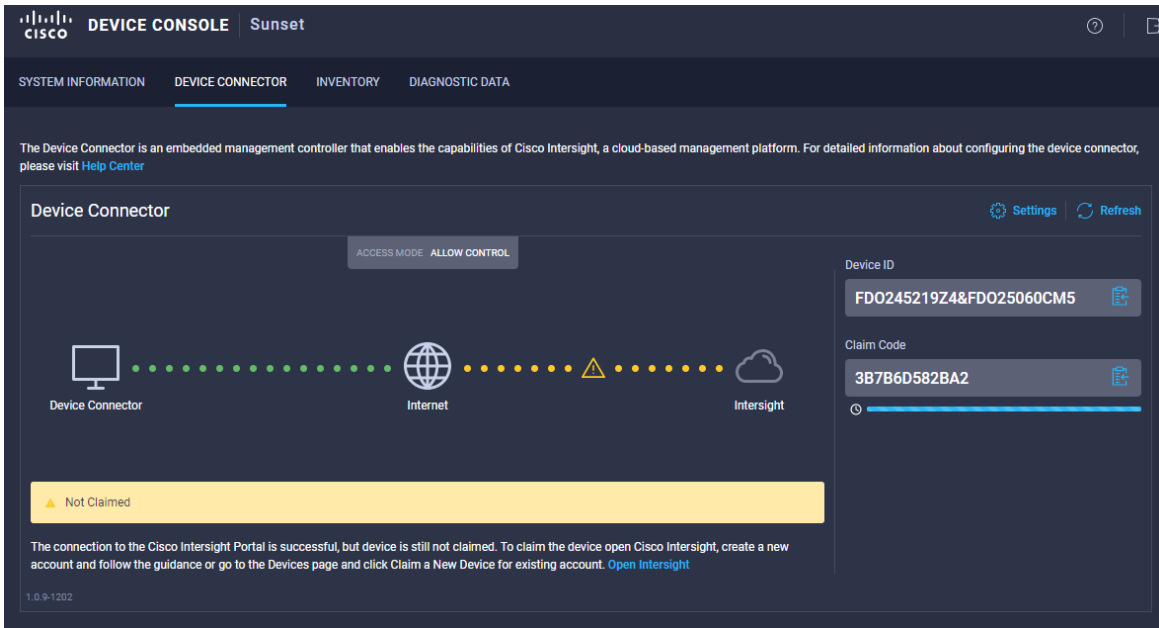
Note: If you receive security warnings, proceed past the warnings to connect to the system.

Step 7 Log in to the Fabric Interconnect using the credentials provided to you by the lab administrator.

Step 8 Verify that you can now view the DEVICE CONSOLE (like the graphic below).

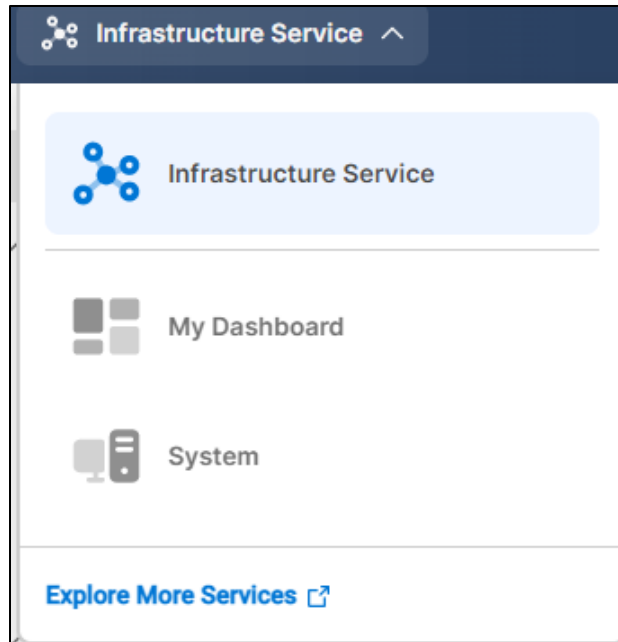


Step 9 In your Device Console, click on **Device Connector**. Your screen should look like The one below:

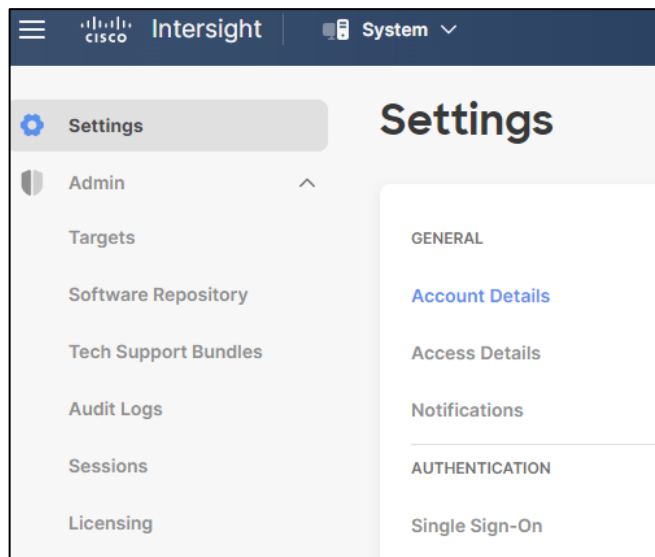


Step 10 Copy and save the **Device ID** and **Claim ID** to a notepad document.

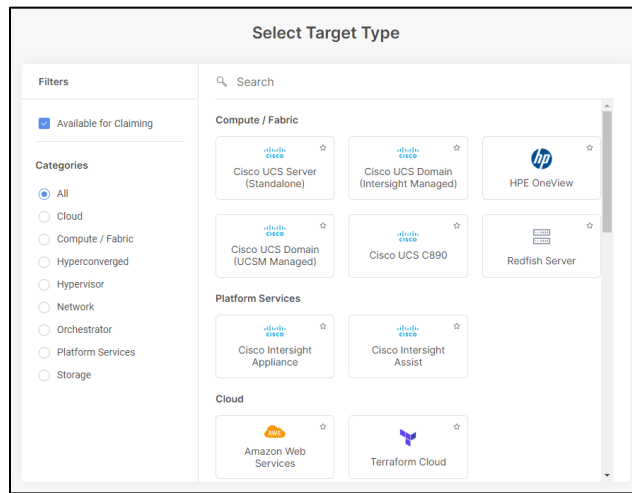
Step 11 At the top of the screen, select **System** from the dropdown. Return to the **Intersight** tab on your browser and click on **Targets** under the **Admin** tab on the left-hand side of the Intersight screen.



Step 12 Click on the **Claim Target** button to start the Claim Wizard.

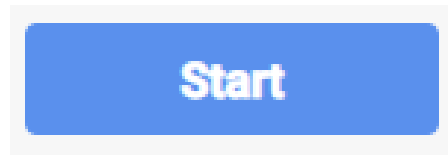


Step 13 Click on the **Cisco UCS Domain (Cisco Intersight Managed)** selection box.

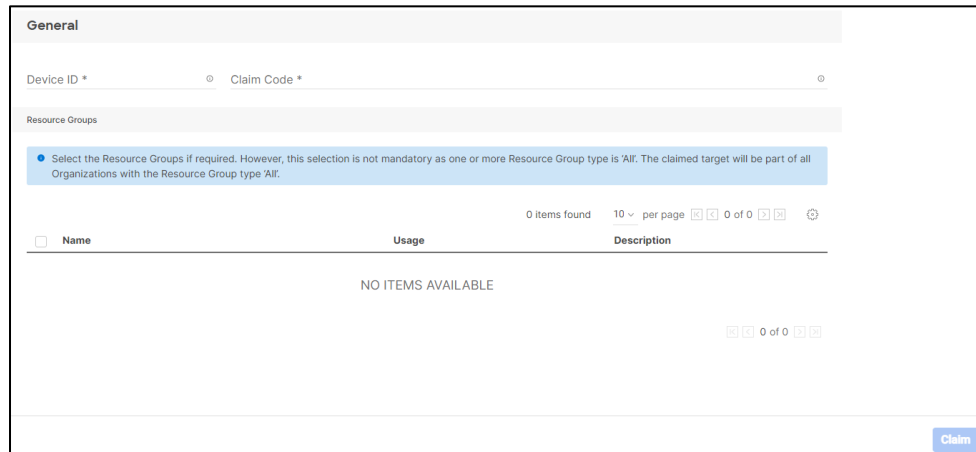


Note: Be careful not to select the **UCS Domain (UCSM Managed)** box by mistake.

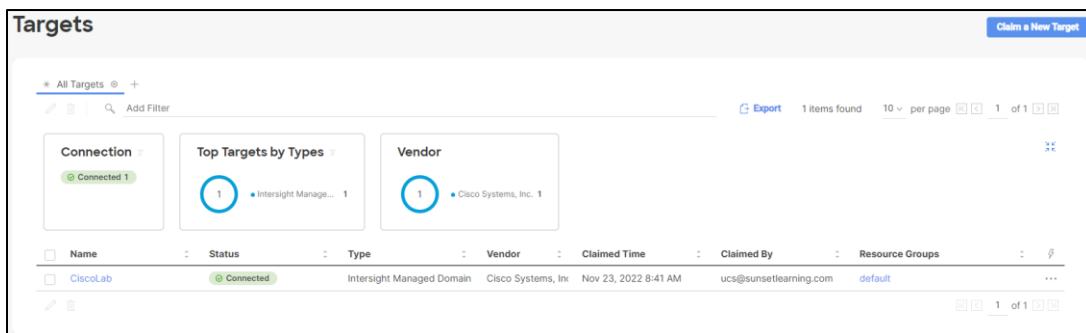
Step 14 Click the **Start** button at the bottom right of the screen to start the claiming process.



Step 15 Paste the **Domain ID** and **Claim Code** from notepad to the respective line and then click the **Claim** button at the bottom right of the screen.



Step 16 Verify that the target has been claimed in the next window.



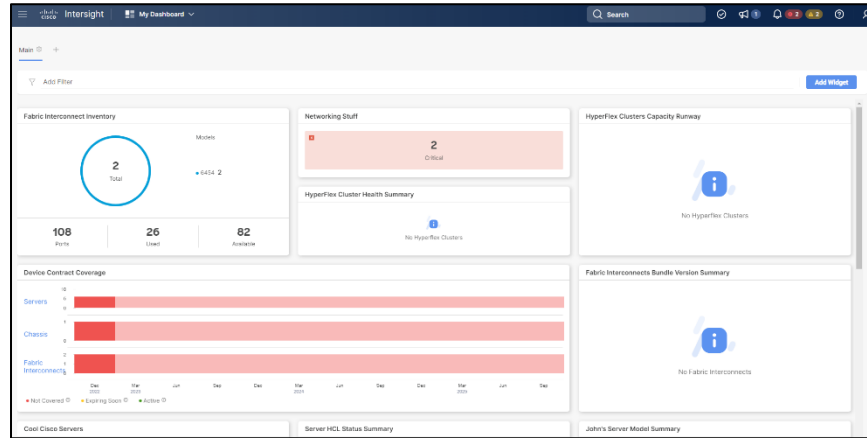
Name	Status	Type	Vendor	Claimed Time	Claimed By	Resource Groups
CiscoLab	Connected	Intersight Managed Domain	Cisco Systems, Inc	Nov 23, 2022 8:41 AM	ucs@sunsetlearning.com	default

Task 1 has been completed!

Note: A connection to the SLI VPN (via AnyConnect) is not required for the remaining tasks in this lab guide. If you had connected to the SLI VPN, you may now disconnect.

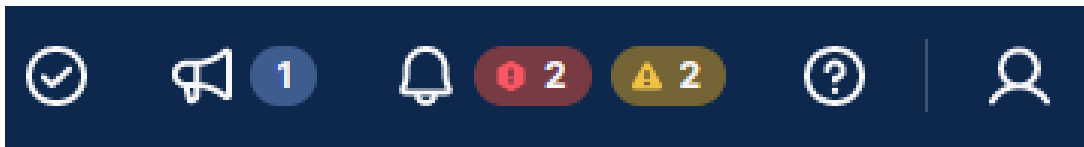
Task 2 – Intersight Dashboard Overview

The Cisco Intersight dashboard displays information about the claimed UCS Domains. In a production environment, the dashboard would show all Fabric Interconnects, Servers, and HyperFlex Clusters that have been registered and are currently under management by Cisco Intersight, as well as high-level information about alarms.

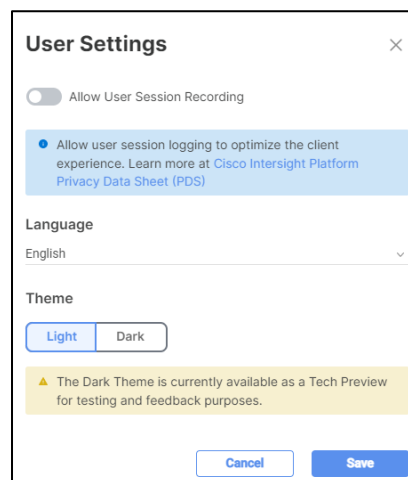


Procedure

Step 1 Click the **Profile Menu** in the upper right corner of the top toolbar.




Step 2 Click **User Settings** in the resulting menu to see how the new features are controlled.

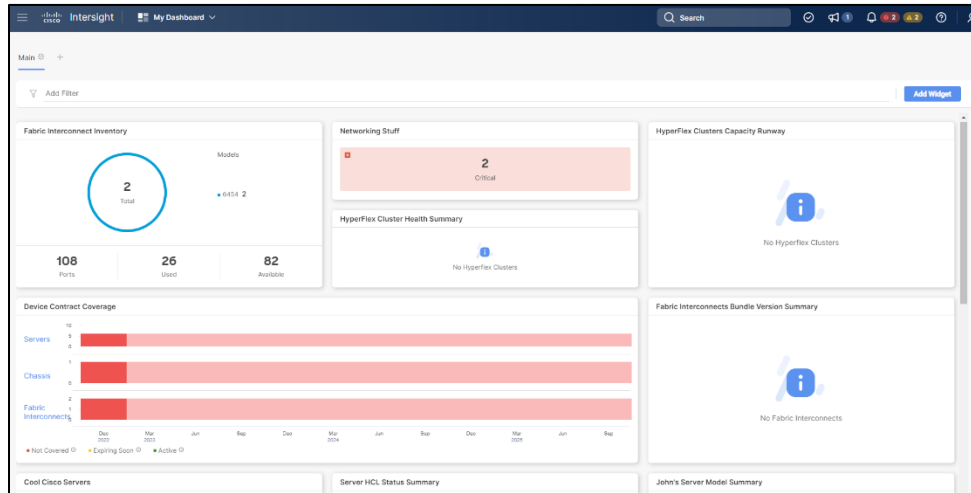


Step 3 Click the **Language** drop-down to show the language option for the Cisco Intersight dashboard.

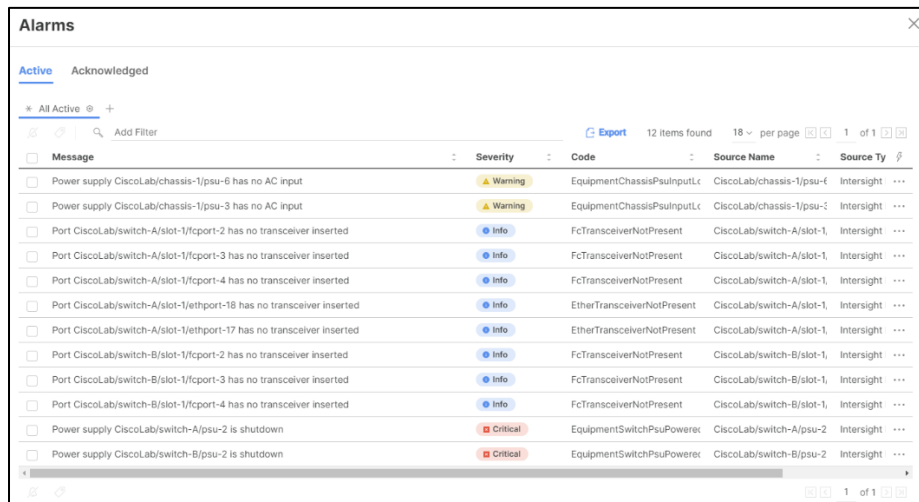
Step 4 If desired, change the theme from **Dark** to **Light** to show the difference.

Step 5 Click **Save** to save the changes or **Cancel** to discard them.

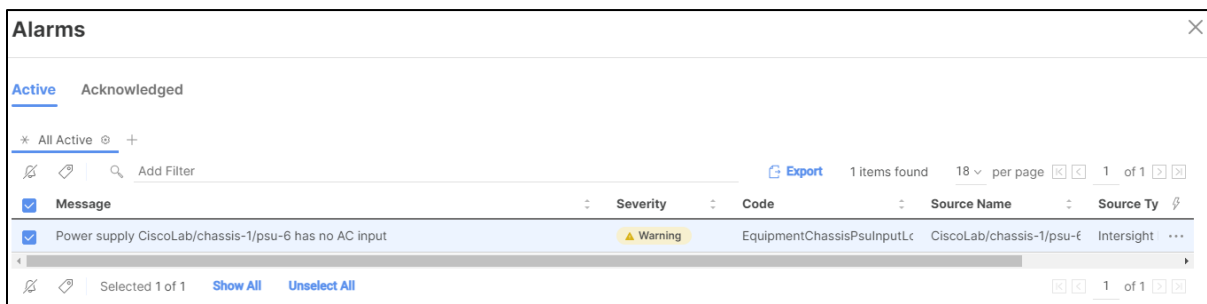
Step 6 Click the **OVERVIEW** tab to return to the Intersight dashboard. Note the overall health bars for the currently managed UCS servers and Fabric Interconnects. Also, note the alarm indicators in the top toolbar. Then click the **alarm** () icon.



Step 7 Click the **All** tab at the top or the **View All** button at the bottom of the list of alarms to open a full list of the alarms in the workspace.



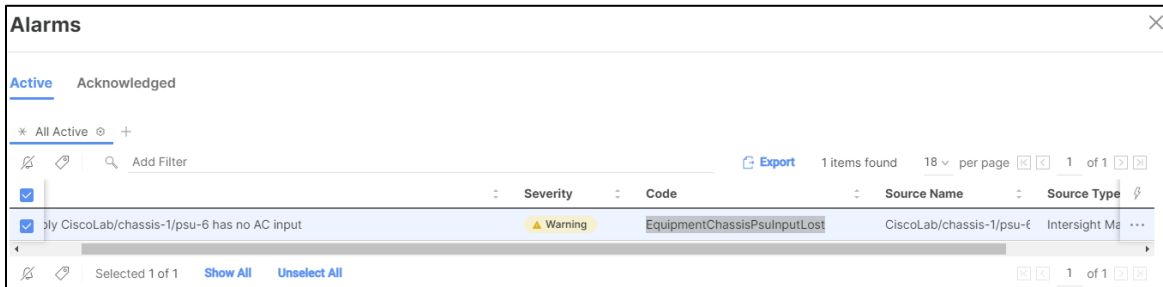
Step 8 Choose one alarm code from the list and click on it.



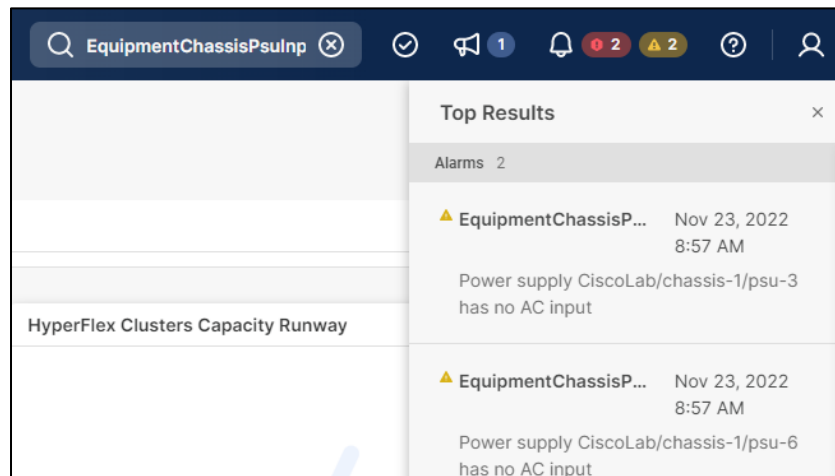
Step 9 Observe that you are taken to the **Alarms** page and the source of the alarm code is shown.



Step 10 You may also search the system for a specific alarm code. Copy the **alarm code** from the **Alarms** list. In this example, the alarm code is **EquipmentChassisPSUInput**.

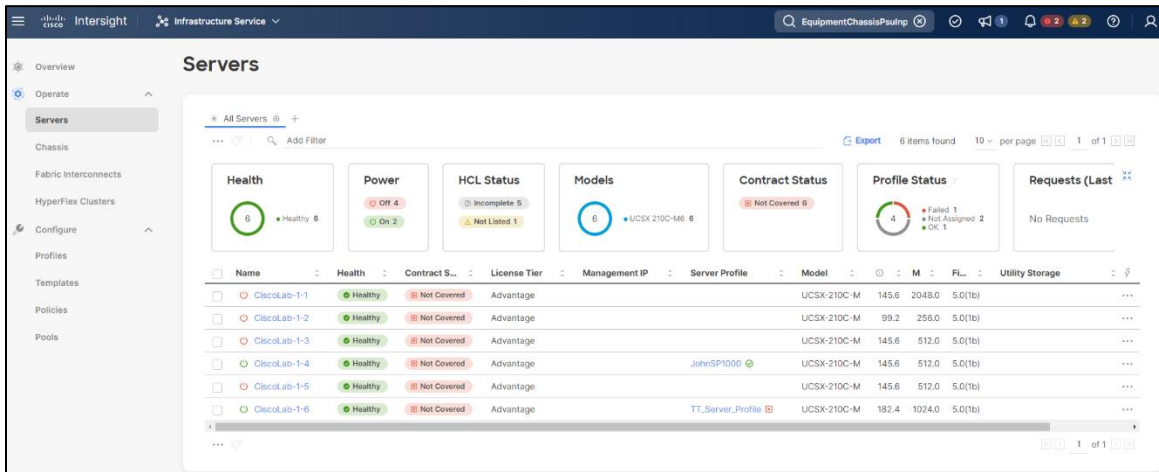


Step 11 Enter the alarm code into the search field on the toptoolbar, to see a list of all the occurrences of that alarm code. As before, you can click on any occurrence in the list to locate the source of that code.

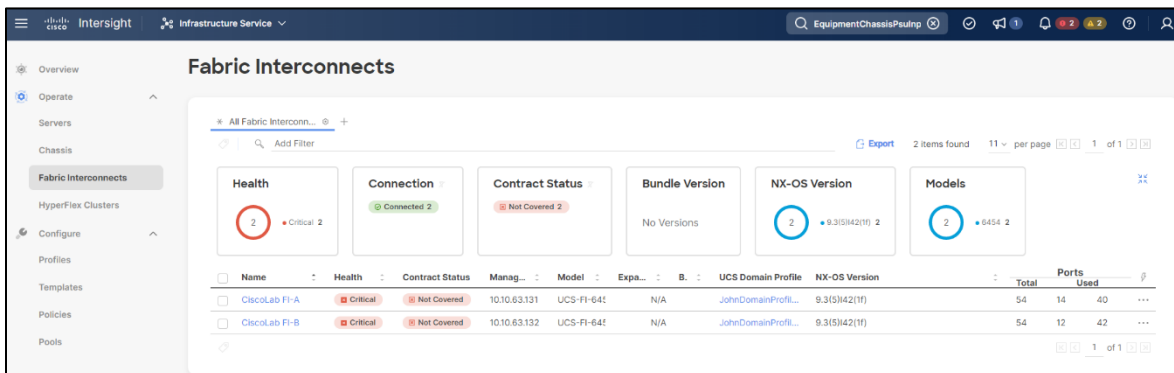


Step 12 Close the search results window.

Step 13 In the navigation pane on the left, click the **Servers** tab located underneath **OPERATE** to show the list of currently managed UCS servers, which includes a health indicator, Model, the License Tier, and other helpful information.



Step 14 Click the **Fabric Interconnects** tab to show the currently managed live physical Fabric Interconnects running, including a health indicator, the management IP, and available and used ports.



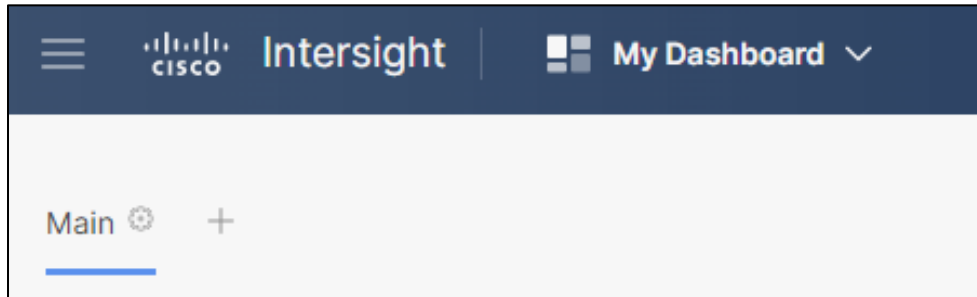
Task 2 has been completed!

Task 3 – Add and Remove a Dashboard Widget

The purpose of this section is to understand how to add, configure, and remove a personal dashboard.

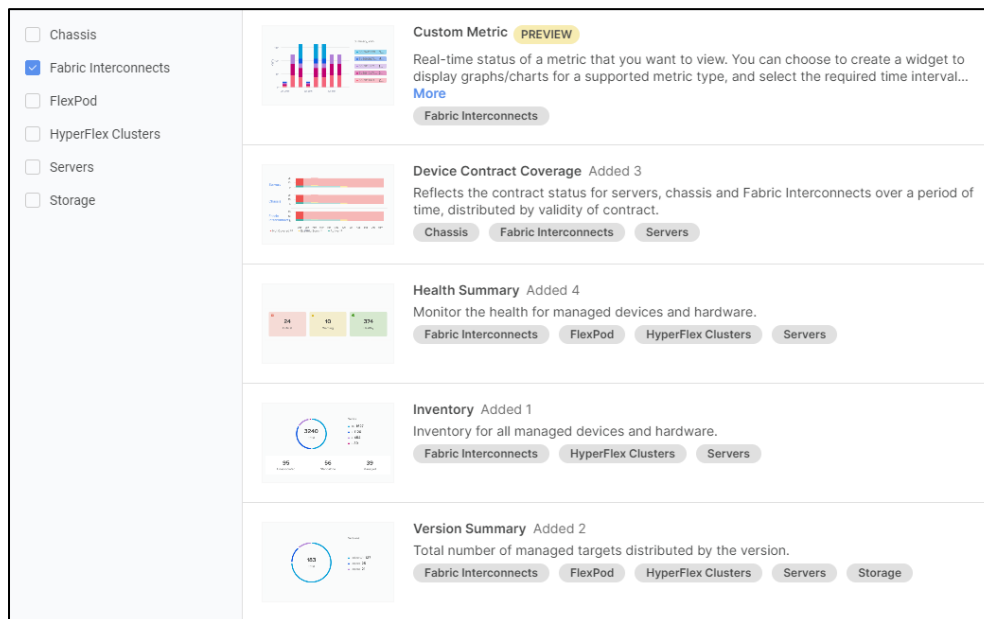
Procedure

Step 1 At the top of the page, from the dropdown, select **My Dashboard**. Then click the plus sign (+) along the tabs at the top of the dashboard to add a new dashboard tab.

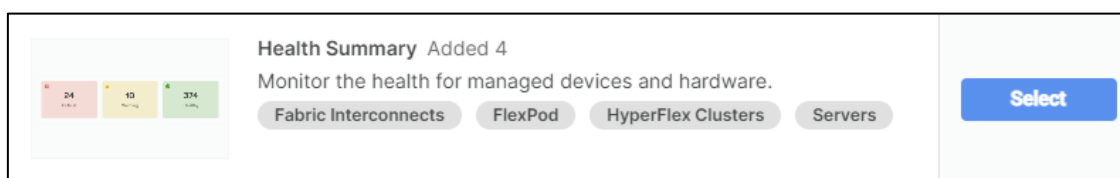


The **Widget Library** automatically opens in the work pane after adding a new dashboard.

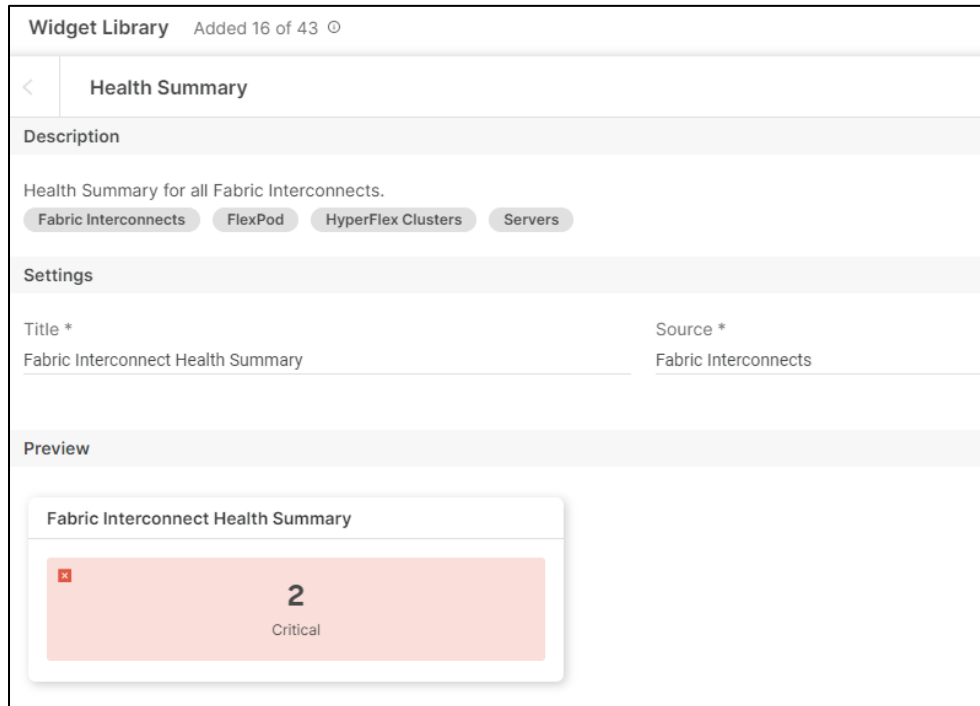
Step 2 Use the **Filters** list to limit the widgets shown to only be widgets for **Fabric Interconnects**.



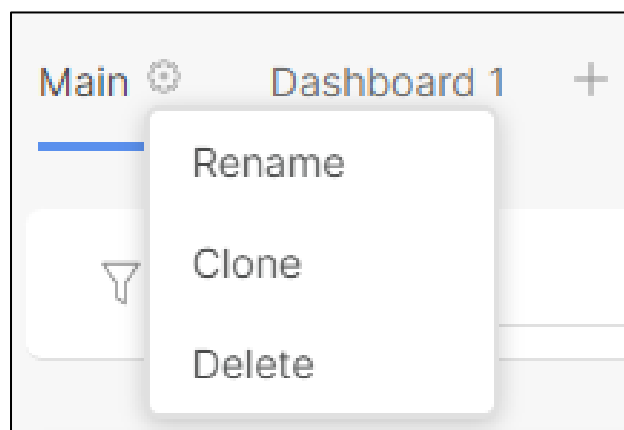
Step 3 Choose a widget in the Widget Library list by hovering over it and then clicking **Select**. In the example below, the **Health Summary** widget was selected.



- Step 4** The **Settings** menu appears for the selected widget. Here, the title for the selected widget can be customized, if desired. If the widget supports other sources, you may also choose to select a different source. Scroll down and select **Add Widget** to add the widget to the new dashboard.



- Step 5** Repeat the above three steps for the desired number of widgets and when you have created enough widgets, click **X** to close the **Widget Library**.
- Step 6** Your new dashboard tab will be given a default name. In the example below, the default name is **Dashboard1**. Click the **Edit** icon next to the dashboard title name in the work pane and then, select **Rename**.
- Step 7** Give the dashboard a name in the **Rename Dashboard** screen and then, click **Rename**.
- Step 8** If desired, move the widgets around or delete one or two to show the functionality.
- Step 9** Click the **Edit** icon next to the new dashboard name again then, select **Delete** from the drop-down menu and delete the new dashboard.




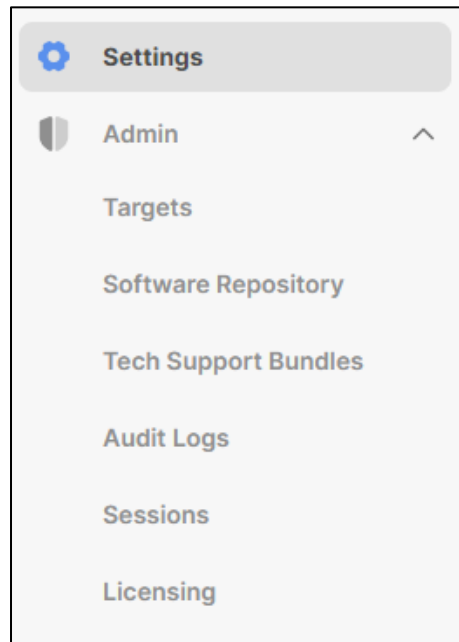
Task 3 has been completed!

Task 4 – Activate Trial Essentials License (Review-Only)

This lab uses features of Cisco Intersight that require at a minimum, a **Cisco Intersight Essentials** license. The instructor will demonstrate how to verify licensing. You may follow along, but please do not modify anything in the lab environment as part of this task.

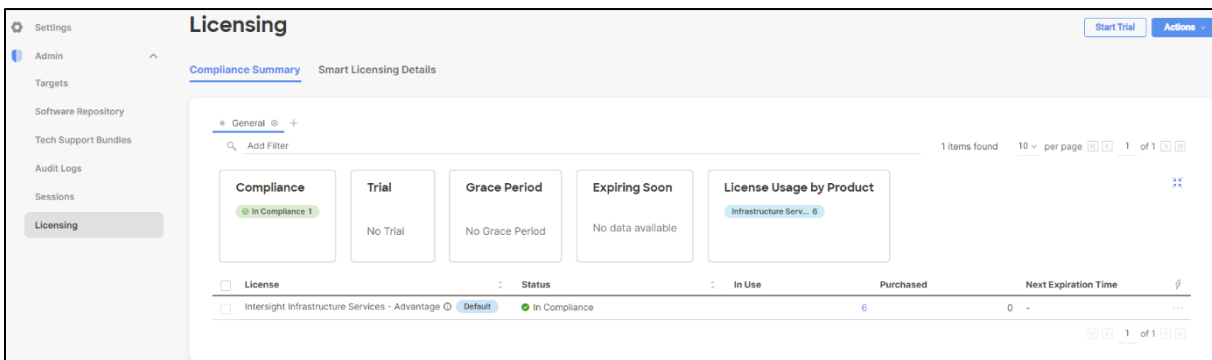
Procedure

Step 1 On the top left ,Next to the Intersight , Choose **SYSTEM** from the drop down. Now on the top left of the system page, click the Admin drawer just below the settings () icon, and then select **Licensing** .



Note: As a new Intersight user, you can evaluate Intersight for a period of 90 days without a registered license. During this Trial period, the premium features of Intersight are available without a registered license.

Step 2 To use the trial license, in the next screen, select **Start Trial**.



Step 3 Check the box for **Intersight** and then click the **Start** button on the confirmation box to start the trial license. The evaluation period is 90 days, and an Essentials (or higher level) license can be registered anytime during the trial period.

Start Trial

Select the Intersight Service to request trial.

Infrastructure Service & Cloud Orchestrator

Trial option is not available as you are currently registered with Smart Licensing. If trial is needed, please contact your Cisco representative for additional trial options.

Workload Optimizer Registration Required

45 days trial

Task 4 has been completed!

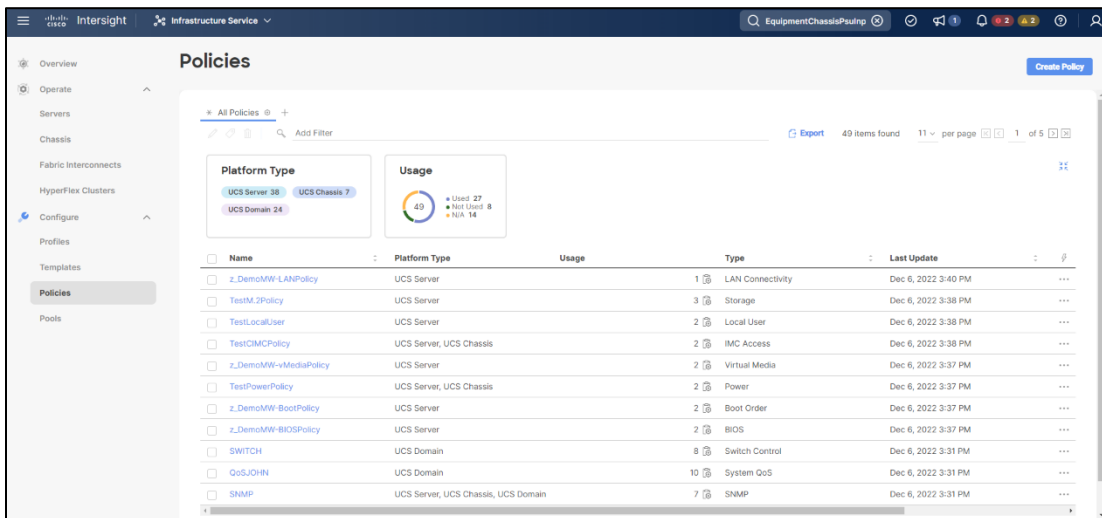
Task 5 – Domain Policy Creation

The purpose of this section is to create the policies needed to configure the Fabric Interconnects after being claimed. These policies will then be used in the Domain Profile to deploy those configurations. Afterwards, you will verify that the Fabric Interconnects are configured correctly for proper operation.

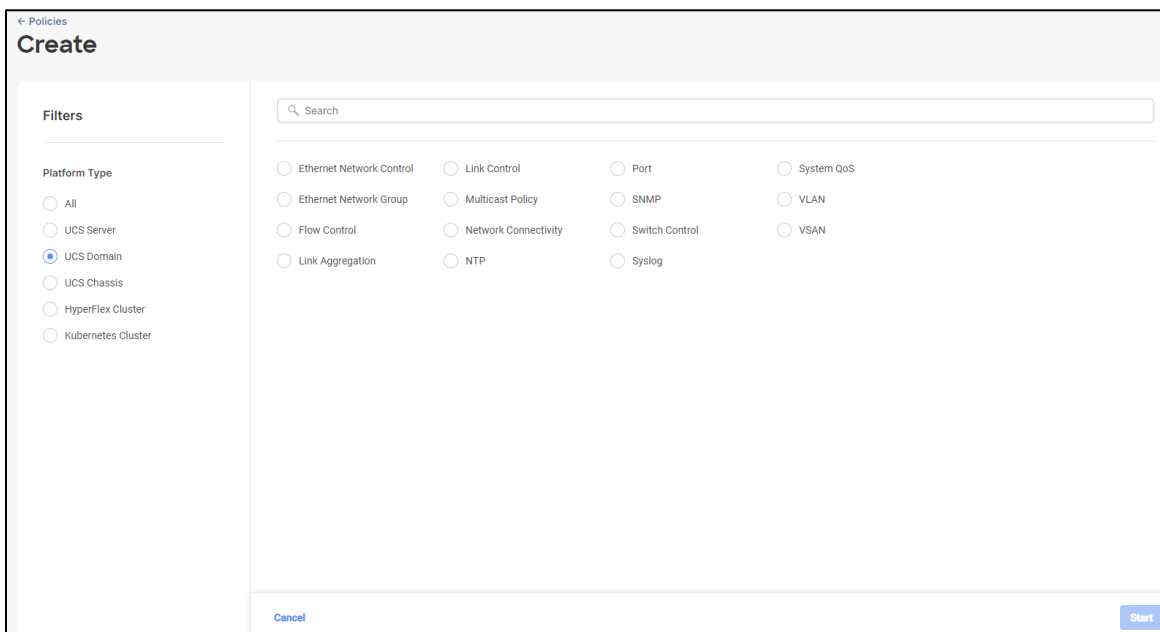
Procedure

CREATE A PORT POLICY

Step 1 In the left navigation pane of the **Cisco Intersight** home page, click **Policies** under **CONFIGURE**. Then select **Create Policy** in the top right-hand corner of your dashboard.



Step 2 Under the **Filters** column, click on the **UCS Domain** radio button.



NOTE: Familiarize yourself with steps 1 and 2 above. We will be repeating these steps and using the filter option throughout the remainder of this task.

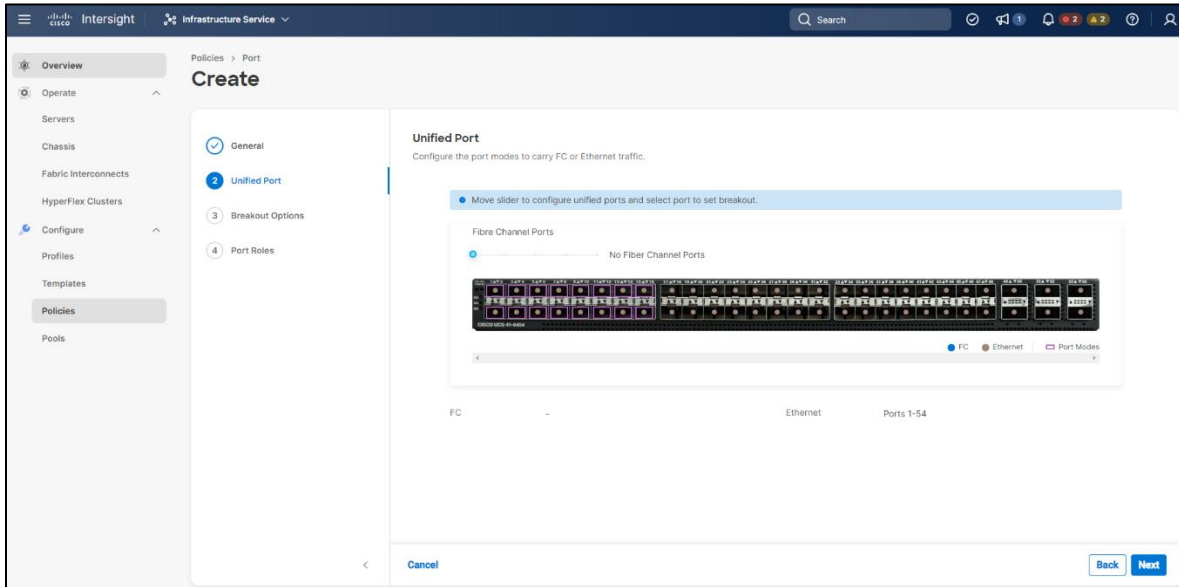
Step 3 Select the **Port** radio button and select **Start** to begin the Port Policy creation wizard.

The screenshot shows the 'Create' policy wizard interface. On the left, under 'Platform Type', the 'UCS Domain' radio button is selected. In the main area, the 'Port' radio button is selected among various policy types. At the bottom, there are 'Cancel' and 'Start' buttons.

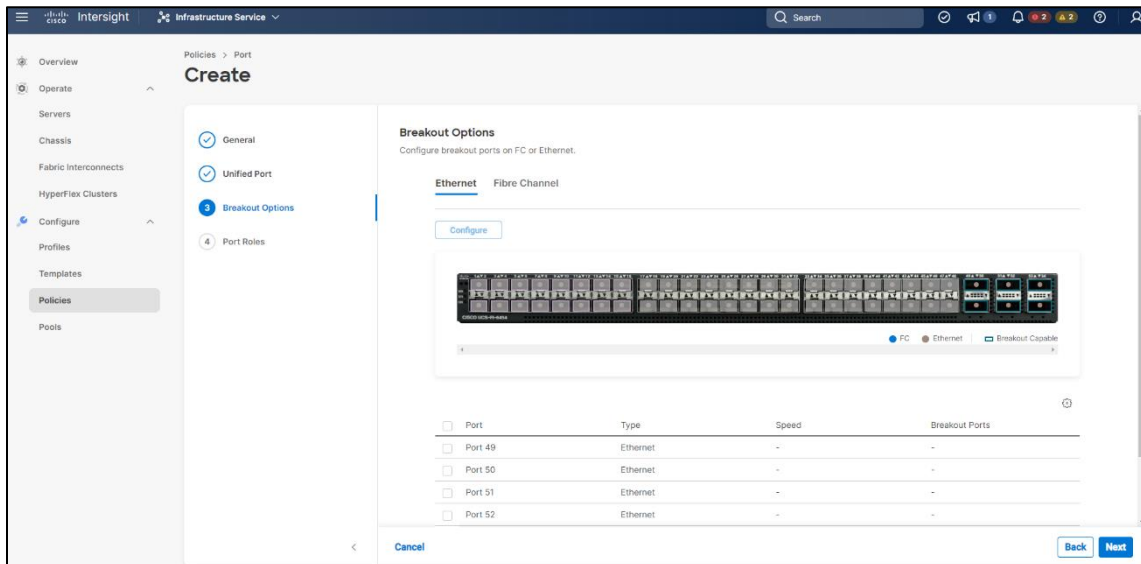
Step 4 Name the policy **PodX-PortPolicy**, where X is your assigned pod number and click **Next**.

The screenshot shows the 'General' configuration step of the 'Create' policy wizard. The 'Name' field is filled with 'Pod2-PortPolicy'. The 'Organization' is set to 'default' and the 'Switch Model' is 'UCS-FI-6454'. At the bottom, there are 'Cancel' and 'Next' buttons.

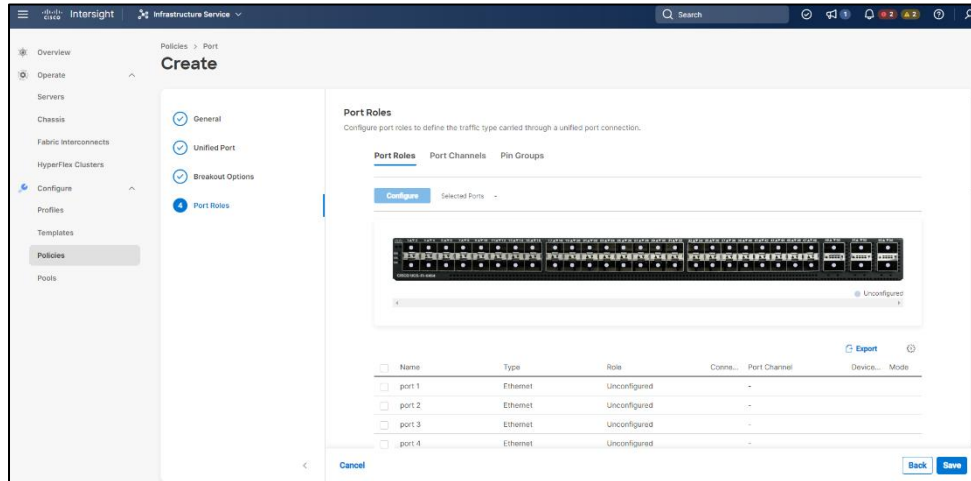
Step 5 We will not be using Fibre Channel ports, so all the Unified Ports will be left as Ethernet ports, click **Next** to continue.



Step 6 On the **Port Roles** page, **select ports 45 through 48** by either: scrolling down the list of ports and selecting ports 45 through 48; or by clicking on ports 45 through 48 on the switch image. If you scrolled down the list, scroll back up to the top of the page. Ensure that ports 45 through 48 show as selected and click the **Configure** button.

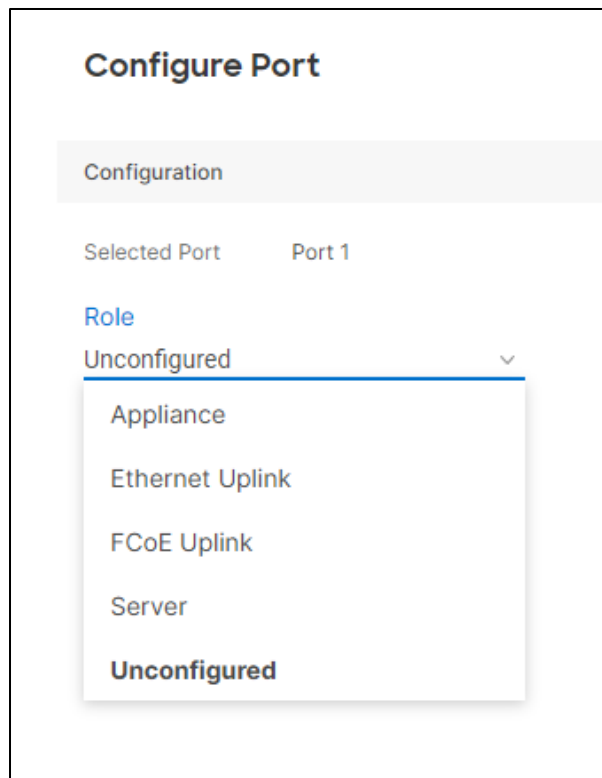


Step 7 In the drop-down under **Role**, select **Server** and click **Save**. This will enable Fabric Extension and allow the Fabric Interconnects to learn the Intelligent Fabric Modules (IFMs) and the Chassis/Servers.

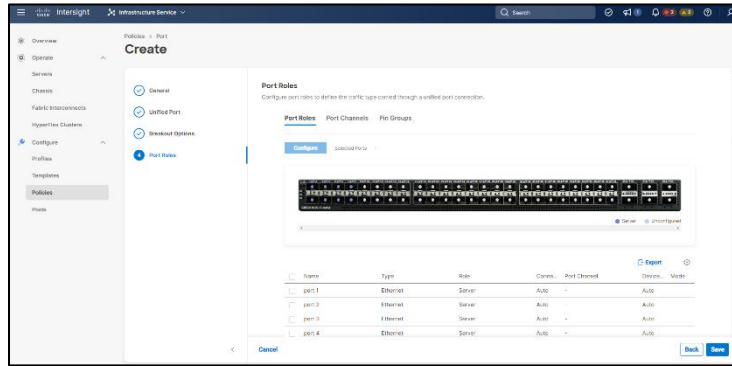


Step 8 Back on the **Port Roles** page, select ports **15 and 16**, then click the **Configure** button again.

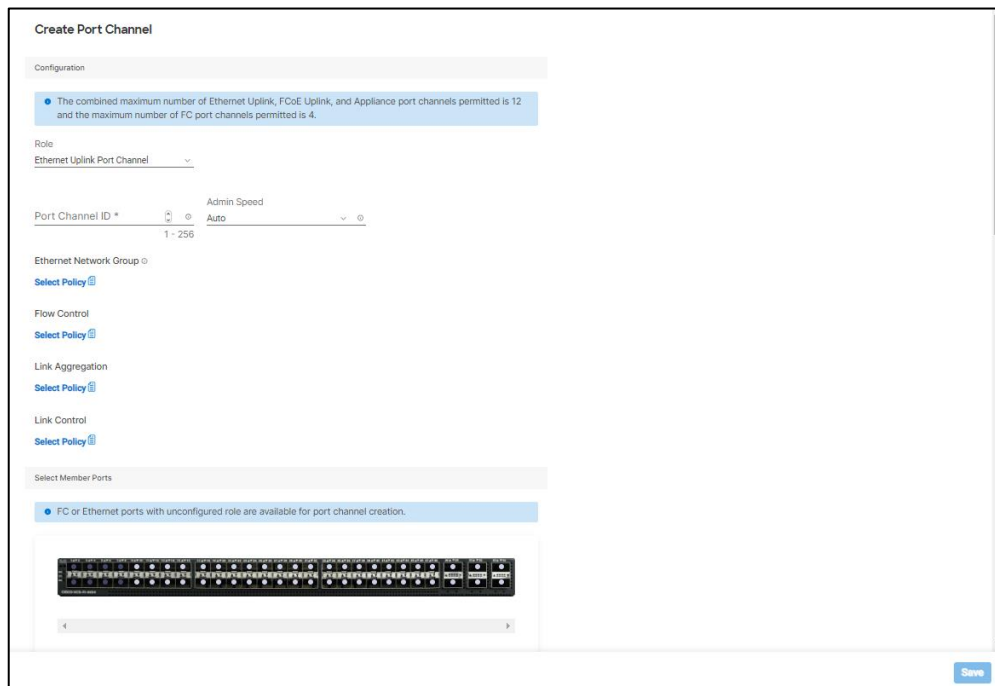
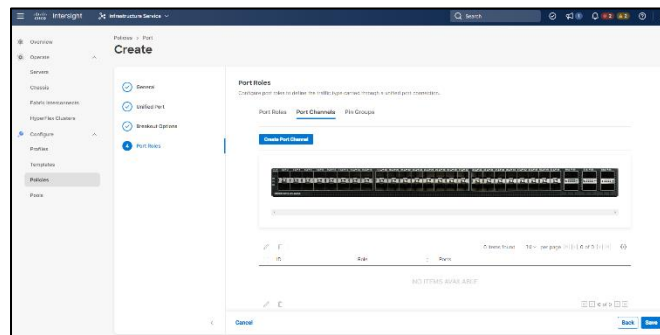
Step 9 These ports will be configured as Ethernet uplinks so you will need to select **Ethernet Uplink** in the **Role** drop-down menu. Leave the other settings at their default values and click **Save**.

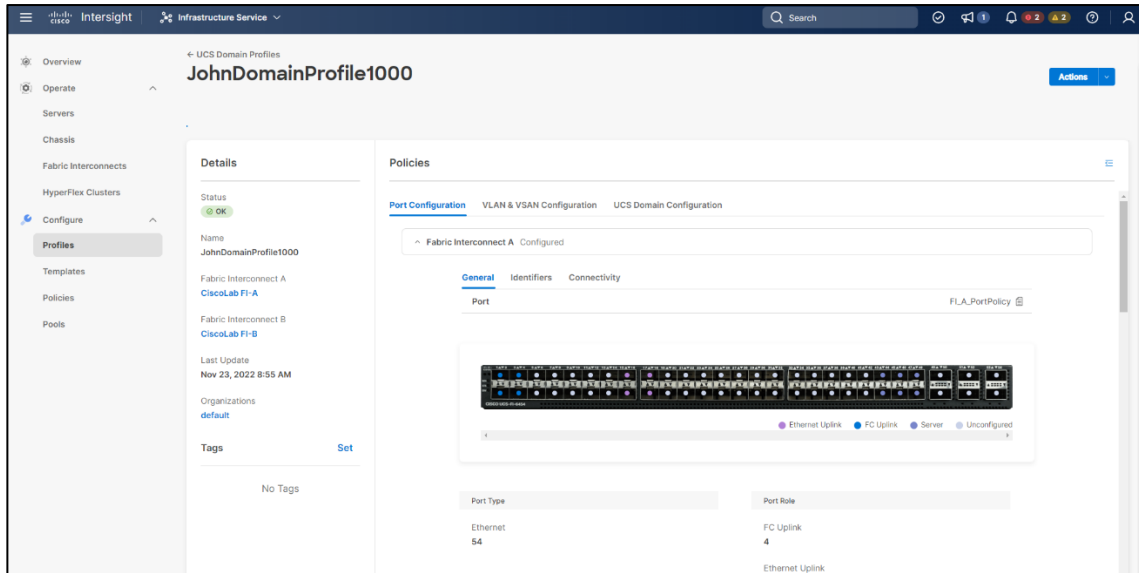
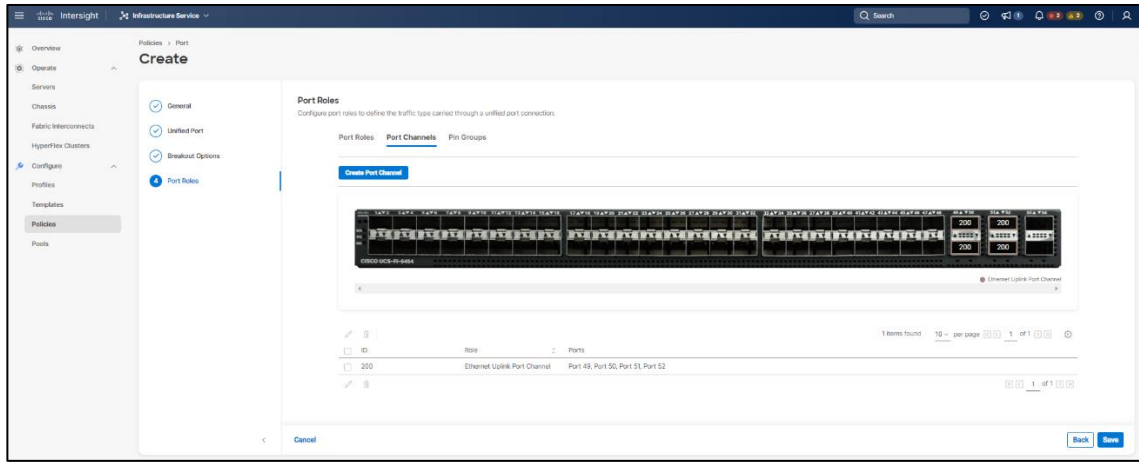


Step 10 Next, you will create Port Channels by selecting the **Port Channels** tab at the top of the content window.



Step 11 Click the **Create Port Channel** button and give the port channel a Port Channel ID of **X1**, where **X** is your pod number. Leave all other settings at their default values. Then click the **Save** button. Example of Pod 1's configuration:

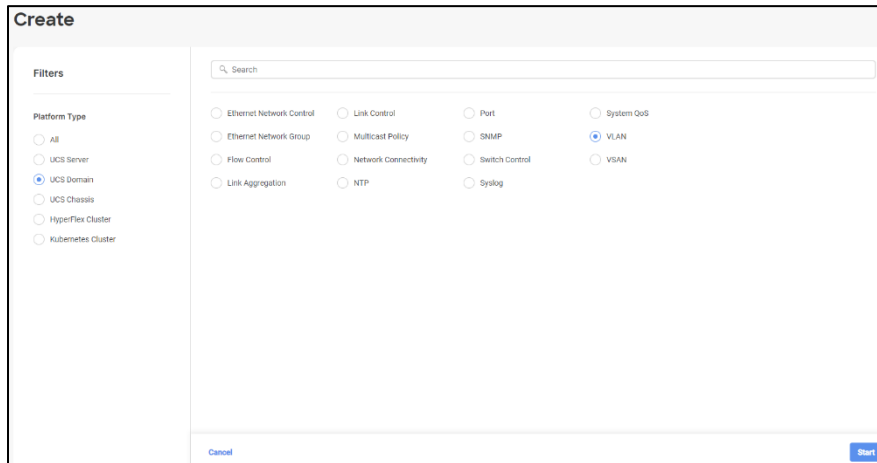




Step 12 Click the **Save** button on the **Port Roles** page to complete the Port Policy Configuration Wizard.

CREATE A VLAN POLICY

Step 13 Return to the **Policies** in the left navigation pane. Select **Create Policy**. Use the Filter to select the **UCS Domain** radio button again. In the list of policies, select the **VLAN** radio button and click **Start**.



Step 14 Name your VLAN **PodX-VLANPolicy**, where X is your pod number and click **Next**.

Create

1 General

2 Policy Details

General
Add a name, description and tag for the policy.

Organization *
default

Name *
Pod2-VLANPolicy

Set Tags

Description
<= 1024

Cancel Next

Step 15 Click on the **Add VLANs** button.

Create

Add VLANs
Add VLANs to the policy

▲ VLANs should have one Multicast policy associated to it

Configuration

Name / Prefix *	VLAN IDs *
Pod2VLAN	21

Auto Allow On Uplinks

Enable VLAN Sharing

Multicast Policy *

Select Policy

Cancel Add

Step 16 Name the VLAN **PodXVLAN** and use the use the VLAN ID of **X1**, where **X** is your pod number. The following graphic is an example using Pod 2:

Policies > VLAN

Create

Add VLANs
Add VLANs to the policy

▲ VLANs should have one Multicast policy associated to it

Configuration

Name / Prefix *	VLAN IDs *
Pod2VLAN	21

Auto Allow On Uplinks

Enable VLAN Sharing

Multicast Policy *

Select Policy

Select Policy

Policies 1 Create New

Search

MULTICAST

Step 17 You will also need to select a Multicast Policy. There is a **default** policy created by the lab administrator. Click on **Select Policy** and then click on the **default** policy to select it.

NOTE: Once the policy is selected, your screen should look like the following:

Create

Add VLANs

Add VLANs to the policy

▲ VLANs should have one Multicast policy associated to it

Configuration

Name / Prefix *	VLAN IDs *
Pod2VLAN	21

Auto Allow On Uplinks

Enable VLAN Sharing

Multicast Policy *

Selected Policy MULTICAST

Cancel Add

Step 18 Click the **Add** button.

Step 19 On the next screen verify that your VLAN has been added with the correct VLAN name and ID. Then select **Create** to complete the policy.

Create

General

Policy Details

Policy Details

Add policy details

● This policy is applicable only for UCS Domains

VLANs

Add VLANs

Show VLAN Ranges

2 items found 10 per page 1 of 1

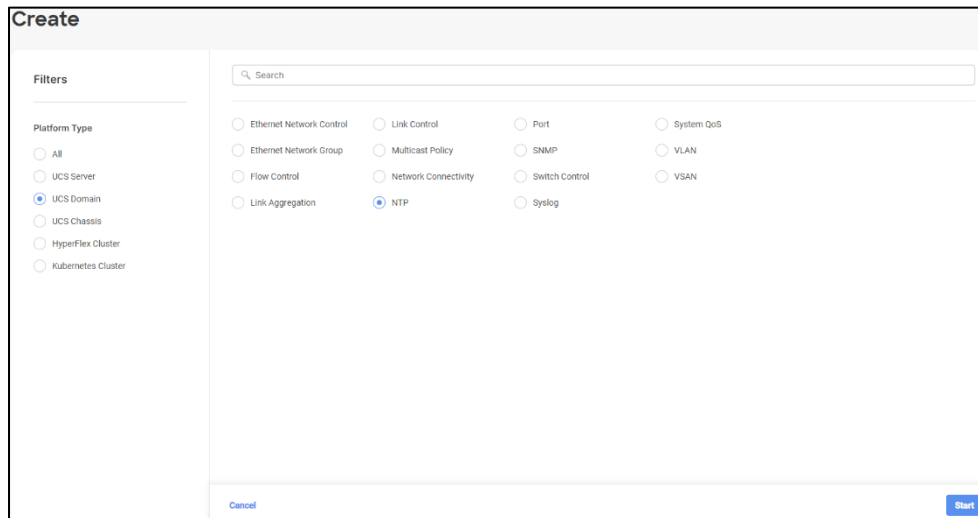
VLAN ID	Name	Sharing Type	Primary VLAN ID	Multicast Policy	Auto Allow On Uplinks
1	default	None			Yes
21	Pod2VLAN_21	None		MULTICAST	Yes

Set Native VLAN ID

Cancel Back Create

CREATE AN NTP POLICY

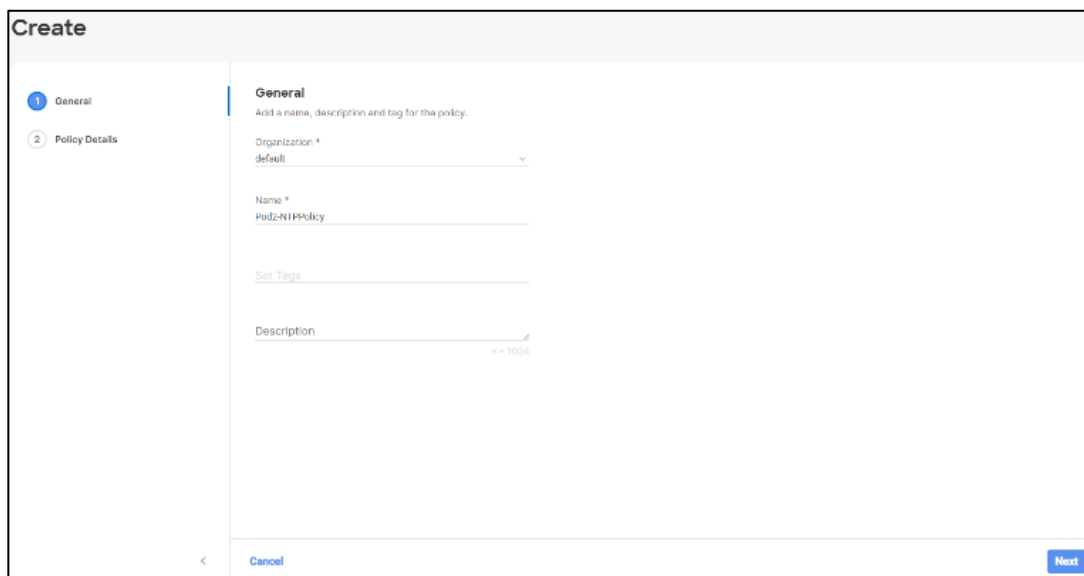
Step 20 Return to the **Policies** in the left navigation pane. Select **Create Policy**. Use the Filter to select the **UCS Domain** radio button again. In the list of policies, select the **NTP** radio button and click **Start**.



The screenshot shows the 'Create' dialog box in a web interface. On the left, under 'Filters', the 'Platform Type' section has 'UCS Domain' selected with a radio button. The main area contains a search bar and a grid of radio buttons for various policy types. 'NTP' is selected in the grid. At the bottom, there are 'Cancel' and 'Start' buttons.

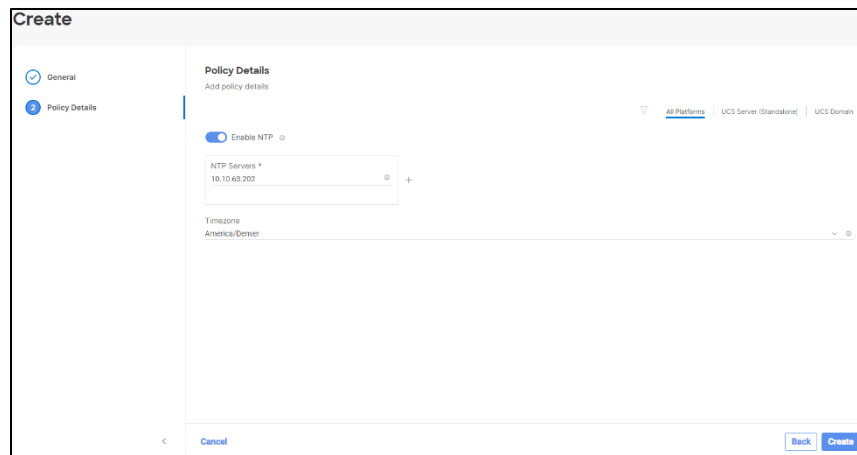
Step 21 Name your NTP policy **PodX-NTPPolicy**, where X is your pod number, and click **Next**.

Step 22 Next, you will need to create an NTP server for the devices in your UCSX deployment to use for time. In the **NTP Servers *** box, click in that box and enter the IP address of **10.10.63.202**. Next, you will need to select the time zone. Click on the **Time Zone** dropdown and type **Denver**. Then select the **America/Denver** option. Your policy should look like the following:



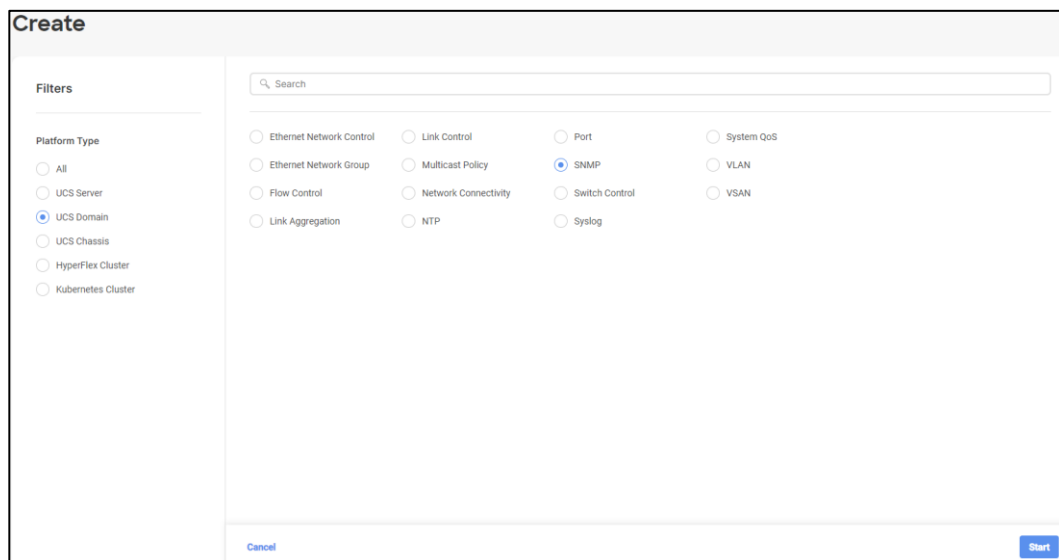
The screenshot shows the 'Create' dialog box in the 'General' tab. The 'Organization' dropdown is set to 'default'. The 'Name' field contains 'PodZ-NTPPolicy'. There are fields for 'Set Tags' and 'Description' (with a character count of 1024). At the bottom, there are 'Cancel' and 'Next' buttons.

Step 23 Click **Create** to complete the NTP policy creation wizard.



CREATE AN SNMP POLICY

Step 24 Return to the **Policies** in the left navigation pane. Select **Create Policy**. Use the Filter to select the **UCS Domain** radio button again. In the list of policies, select the **SNMP** radio button and click **Start**.



Step 25 Name your SNMP policy **PodX-SNMPPolicy**, where X is your pod number and click **Next**.

The screenshot shows a 'Create' configuration page for a policy. On the left, there is a navigation pane with two items: '1 General' (selected) and '2 Policy Details'. The main content area is titled 'General' and includes the instruction 'Add a name, description and tag for the policy.' Below this are four input fields: 'Organization *' with a dropdown menu showing 'default', 'Name *' with the text 'Pod2-SNMPPolicy', 'Set Tags' with a text input field, and 'Description' with a text area containing a character limit indicator '<= 1024'. At the bottom of the page, there is a left-pointing arrow, a 'Cancel' button, and a 'Next' button.

Step 26 Next, you will need to fill out the SNMP information. Please fill in the following:

- **System Contact** = Your Name
- **System Location** = Your Location
- **Access Community String** = Cisco123!!
- **SNMP Community Access** = Full
- **Trap Community String** = Cisco123!!

Below is an example:

The screenshot shows the 'Create' page for an SNMP policy in the Cisco UCS management console. The interface is divided into two main sections: 'General' and 'Policy Details'. The 'Policy Details' section is active and contains the following configuration options:

- Enable SNMP:** A toggle switch is turned on.
- SNMP Version:** Three radio buttons are present: 'v2c Only', 'v3 Only', and 'Both v2c and v3'. 'Both v2c and v3' is selected.
- Configuration Fields:**
 - SNMP Port *:** 161
 - System Contact *:** John Doe
 - System Location *:** San Jose
 - Access Community String:** Cisco123!!
 - SNMP Community Access:** Full
 - Trap Community String:** Cisco123!!
 - SNMP Engine Input ID:** (Empty)
- SNMP Users:** A section with an 'Add SNMP User' button.

At the bottom of the form, there are 'Cancel', 'Back', and 'Create' buttons.

Step 27 Scroll down past the **Add SNMP Users** section. **USE Auth Type as SHA (Auth Type MD5 is depreciated so choose SHA)**

Add SNMP User ✕

Name *
Pod2 ⊙

Security Level *
AuthPriv ▼ ⊙

Auth Type
MD5 ▼ ⊙

Auth Password *
..... 👁 ⊙

Auth Password Confirmation *
..... 👁 ⊙

Privacy Type
AES ▼ ⊙

Privacy Password *
..... 👁 ⊙

Privacy Password Confirmation *
..... 👁 ⊙

Cancel Add

Step 28 Click the **Add SNMP Trap Destination** button. In the **SNMP Version** drop-down, select **V2**. Then for the **Destination Address**, please type **10.10.63.202**. Click **Add**.

Add SNMP Trap Destination [X]

Enable [O]

SNMP Version *
V2 [v] [O]

Community String *
Cisco123!! [O]

Trap Type *
Trap [v] [O]

Destination Address *
10.10.63.202 [O]

Port *
162 [O] 1 - 65535

[Cancel] [Add]

Step 29 Finally, click the **Create** button to complete the SNMP policy creation wizard.

Create

General [✓]
Policy Details [2]

SNMP Engine Input ID [O]

SNMP Users

[Add SNMP User]

Name	Security Level	Auth Type	Privacy Type	
Pod2	AuthPriv	MDS	AES	...

SNMP Trap Destinations

[Add SNMP Trap Destination]

Enable	SNMP Version	Trap Type	User	Community String	Destination Address	Port	
<input checked="" type="checkbox"/>	V2	Trap	-	Cisco123!!	10.10.63.202	162	...

[Cancel] [Back] [Create]

CREATE A SYSLOG POLICY

Step 30 Return to the **Policies** in the left navigation pane. Select **Create Policy**. Use the Filter to select the **UCS Domain** radio button again. In the list of policies, select the **Syslog** radio button and click **Start**.

The screenshot shows a web interface titled "Create" for configuring a policy. On the left, under "Filters", the "Platform Type" section has several radio buttons: "All", "UCS Server", "UCS Domain" (which is selected), "UCS Chassis", "HyperFlex Cluster", and "Kubernetes Cluster". The main area contains a search bar and a grid of radio buttons for policy types: "Ethernet Network Control", "Link Control", "Port", "System QoS", "Ethernet Network Group", "Multicast Policy", "SNMP", "VLAN", "Flow Control", "Network Connectivity", "Switch Control", "VSAN", "Link Aggregation", "NTP", and "Syslog" (which is selected). At the bottom left is a "Cancel" button and at the bottom right is a "Start" button.

Step 31 Name your Syslog policy **PodX-SyslogPolicy**, where X is your pod number and click **Next**.

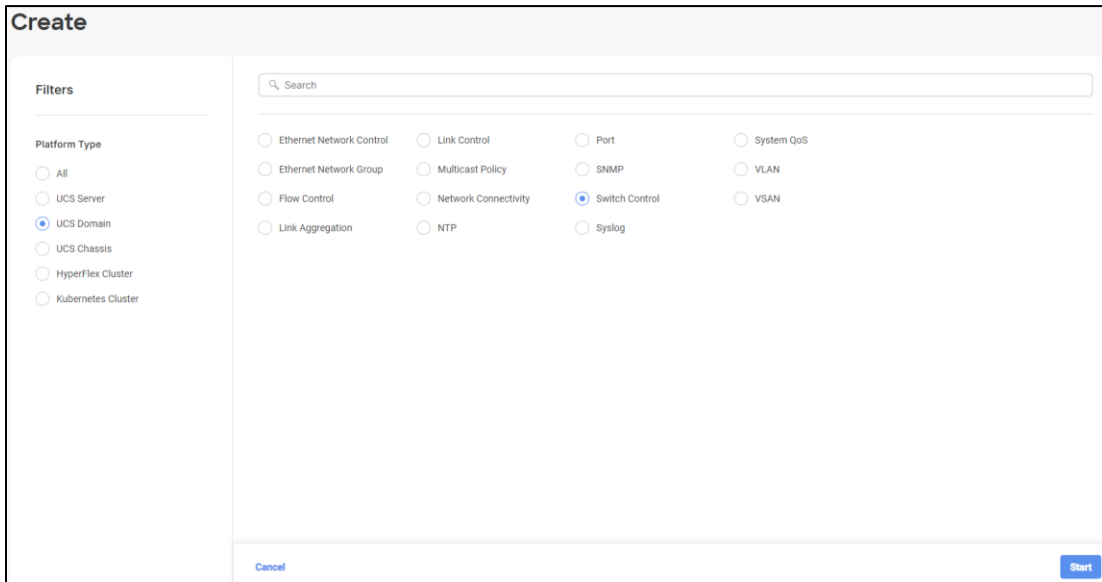
The screenshot shows the 'Create' wizard in the General tab. The left sidebar has '1 General' selected and '2 Policy Details' below it. The main area is titled 'General' and contains the following fields: 'Organization *' with a dropdown menu showing 'default'; 'Name *' with the text 'Pod2-SyslogPolicy' entered; 'Set Tags' with a link; and 'Description' with a text area and a character count '<= 1024'. At the bottom, there are 'Cancel' and 'Next' buttons.

Step 32 Keeping all other defaults, click on the + sign next to **Syslog Server 1** under **Remote Logging** and use IP address **10.10.63.202** for the **Hostname/IP Address**. Then click **Create** to complete the Syslog policy creation wizard.

The screenshot shows the 'Create' wizard in the Policy Details tab. The left sidebar has '1 General' and '2 Policy Details' selected. The main area is titled 'Policy Details' and contains the following sections: 'Local Logging' with a 'File' section and a 'Minimum Severity to Report *' dropdown set to 'Warning'; 'Remote Logging' with a 'Syslog Server 1' section. This section includes an 'Enable' toggle, a table with columns for 'Hostname/IP Address *', 'Port *', and 'Protocol *', and a 'Minimum Severity To Report *' dropdown. The table contains the values '10.10.63.202', '514', and 'UDP'. At the bottom, there are 'Cancel', 'Back', and 'Create' buttons.

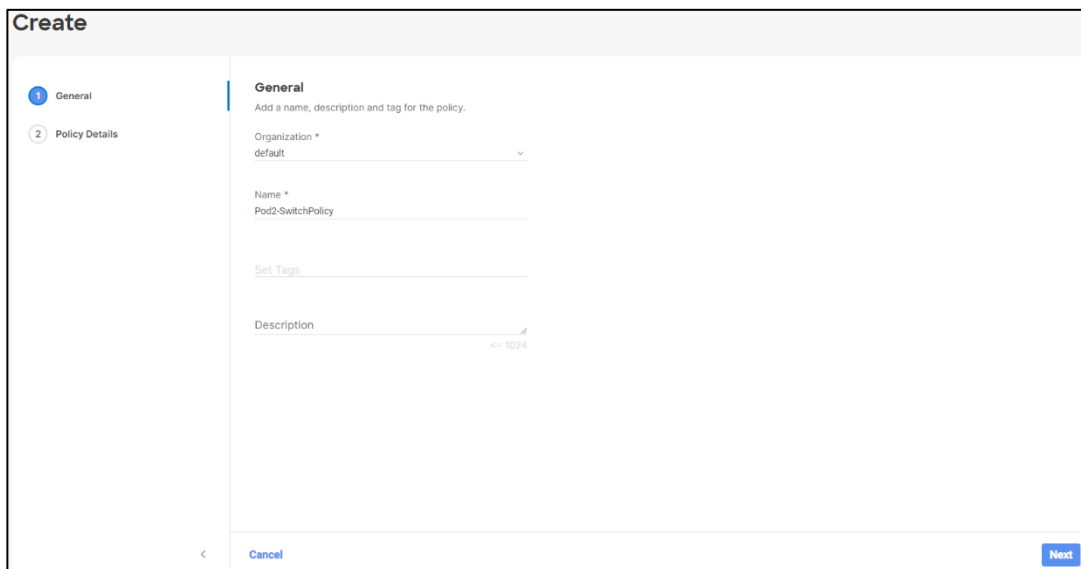
CREATE A SWITCH CONTROL POLICY

Step 33 Return to the **Policies** in the left navigation pane. Select **Create Policy**. Use the Filter to select the **UCS Domain** radio button again. In the list of policies, select the **Switch Control** radio button and click **Start**.



The screenshot shows the 'Create' policy interface. On the left, under 'Filters', the 'Platform Type' section has 'UCS Domain' selected. The main area contains a search bar and a grid of radio buttons for policy types. 'Switch Control' is selected. At the bottom, there are 'Cancel' and 'Start' buttons.

Step 34 Name your Switch Control policy **PodX-SwitchPolicy**, where X is your pod number and click **Next**.



The screenshot shows the 'Create' policy interface in the 'General' tab. The 'Name' field is filled with 'Pod2-SwitchPolicy'. The 'Organization' is set to 'default'. There is a 'Set Tags' link and a 'Description' field with a character count of '<= 1024'. At the bottom, there are '<', 'Cancel', and 'Next' buttons.

Step 35 Keeping the defaults, click **Create** to complete the Switch Control policy creation wizard.

The screenshot shows the 'Create' wizard for a Switch Control policy. The interface is divided into two main sections: a left sidebar and a main content area.

Left Sidebar:

- General (checked)
- Policy Details (active)

Main Content Area:

Policy Details
Add policy details

- This policy is applicable only for UCS Domains

Switching Mode

Ethernet FC

End Host Switch End Host Switch

VLAN Port Count

Enable VLAN Port Count Optimization

MAC Address Table Aging Time

Default Custom Never

This option sets the default MAC address aging time to 14500 seconds for the End Host mode.

Link Control Global Settings

Message Interval: 15 (range 7-90)

Recovery Action None Reset

Buttons: Cancel, Back, Create

CREATE NETWORK CONNECTIVITY POLICY

Step 36 Return to the **Policies** in the left navigation pane. Select **Create Policy**. Use the Filter to select the **UCS Domain** radio button again. In the list of policies, select the **Network Connectivity** radio button and click **Start**.

The screenshot shows the 'Create' policy configuration interface. On the left, under 'Filters', the 'Platform Type' section has 'UCS Domain' selected. The main area contains a search bar and a grid of policy categories. The 'Network Connectivity' category is selected. At the bottom, there are 'Cancel' and 'Start' buttons.

Step 37 Name your Network Connectivity policy **PodX-NetCon-Policy**, where X is your pod number. Click **Next**.

The screenshot shows the 'Create' policy configuration interface, 'General' tab. The 'Organization' is set to 'default', the 'Name' is 'Pod2-NetConPolicy', and the 'Description' field is empty. The 'Next' button is visible at the bottom right.

Step 38 For the **Preferred IPv4 DNS Server** use **10.10.63.202**. For the **Alternate IPv4 DNS Server** use **8.8.8.8**. Then click **Create** to complete the Network Connectivity policy creation wizard.

The screenshot shows the 'Create' wizard for a Network Connectivity policy. The interface is divided into two main sections: a left-hand navigation pane and a main content area.

Navigation Pane:

- General (checked)
- Policy Details (active)

Main Content Area:

- Policy Details:** Add policy details. Platform selection: [All Platforms](#) | [UCS Server \(Standalone\)](#) | [UCS Domain](#)
- Common Properties:** Enable Dynamic DNS
- IPv4 Properties:**
 - Obtain IPv4 DNS Server Addresses from DHCP
 - Preferred IPv4 DNS Server: 10.10.63.202
 - Alternate IPv4 DNS Server: 8.8.8.8
 - Enable IPv6

At the bottom of the wizard, there are three buttons: a back arrow, a 'Cancel' button, and a 'Create' button.

CREATE SYSTEM QoS POLICY

Step 39 Return to the **Policies** in the left navigation pane. Select **Create Policy**. Use the Filter to select the **UCS Domain** radio button again. In the list of policies, select the **System QoS** radio button and click **Start**.

The screenshot shows the 'Create' policy configuration interface. On the left, under 'Filters', the 'Platform Type' section has 'UCS Domain' selected. The main area contains a search bar and a grid of radio buttons for policy types. The selected options are 'UCS Domain' and 'System QoS'. The 'Start' button is visible in the bottom right corner.

Step 40 Name your System QoS policy **PodX-SysQoSPolicy**, where X is your pod number and click **Next**.

The screenshot shows the 'General' tab of the 'Create' policy configuration. The 'Name' field is filled with 'Pod2-QoSPolicy'. The 'Organization' dropdown is set to 'default'. The 'Description' field is empty. The 'Next' button is visible in the bottom right corner.

Step 41 Accepting all defaults, click on **Create** to complete the System QoS policy creation wizard.

The screenshot shows the 'Create' wizard interface for a System QoS policy. The left sidebar has two tabs: 'General' (selected) and 'Policy Details'. The main area is titled 'Policy Details' and contains the following elements:

- A blue banner: "This policy is applicable only for UCS Domains".
- A section titled "Configure Priorities" with four toggle switches: Platinum, Gold, Silver, and Bronze, all of which are turned off.
- Two active priority configurations:
 - Best Effort**: CoS Any, Weight 5 (range 0-10), Allow Packet Drops checked, MTU 1500 (range 1500-9216).
 - Fibre Channel**: CoS 3, Weight 5 (range 0-10), Allow Packet Drops unchecked, MTU 2240 (range 1500-9216).
- Navigation buttons at the bottom: a back arrow, a "Cancel" button, and "Back" and "Create" buttons.

Task 5 has been completed!

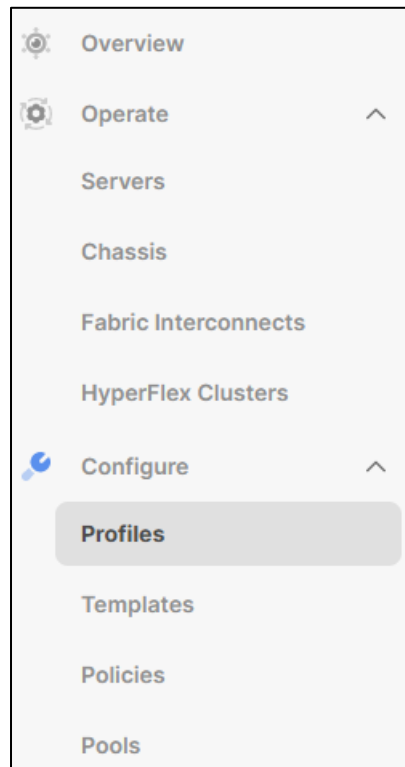
Task 6 – Domain Profile Deployment (Review-Only)

The purpose of this section is to show how to the policies created in the previous task in the form of a Domain Profile. We will start the Profile creation wizard and deploy a profile to the UCS Fabric Interconnects.

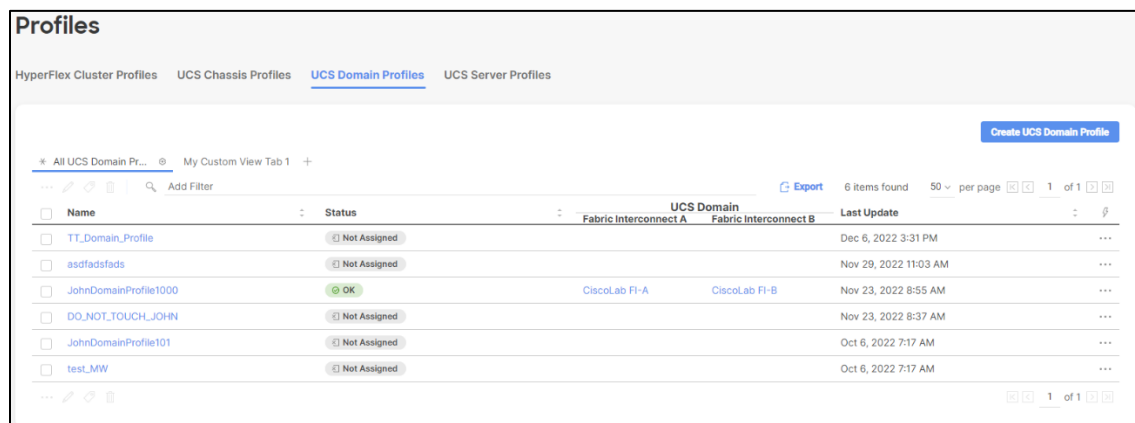
Note: Applying a domain profile affects the entire UCS domain. As a result, you may follow along as the instructor demonstrates this process, but please DO NOT DEPLOY your domain profile.

Procedure

Step 1 In the left-hand menu, select **Profiles** from under **CONFIGURE**.



Step 2 Ensure that you are in the sub-tab named **UCS Domain Profiles**. Then select the **Create UCS Domain Profile** button to start the wizard.



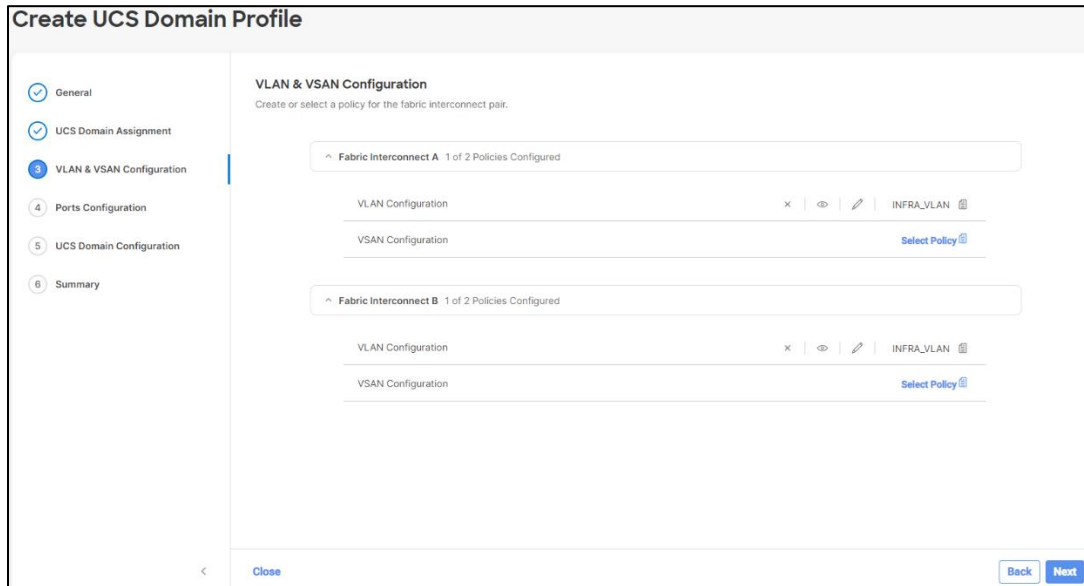
Step 3 In the **General** page, name the policy **Domain-Profile-XX** (use your initials in place of the XX) and click **Next**.

The screenshot shows the 'Create UCS Domain Profile' window with the 'General' tab selected. The left sidebar contains a navigation menu with six items: 1 General (selected), 2 UCS Domain Assignment, 3 VLAN & VSAN Configuration, 4 Ports Configuration, 5 UCS Domain Configuration, and 6 Summary. The main content area is titled 'General' and includes the instruction 'Add a name, description and tag for the UCS domain profile.' Below this, there are three input fields: 'Organization *' with a dropdown menu showing 'default', 'Name *' with a text input field containing 'Domain-Profile-JG', and 'Description' with a text area containing a slash icon and a character limit of '<= 1024'. At the bottom right, there are 'Back' and 'Next' buttons. At the bottom left, there is a 'Close' button and a back arrow.

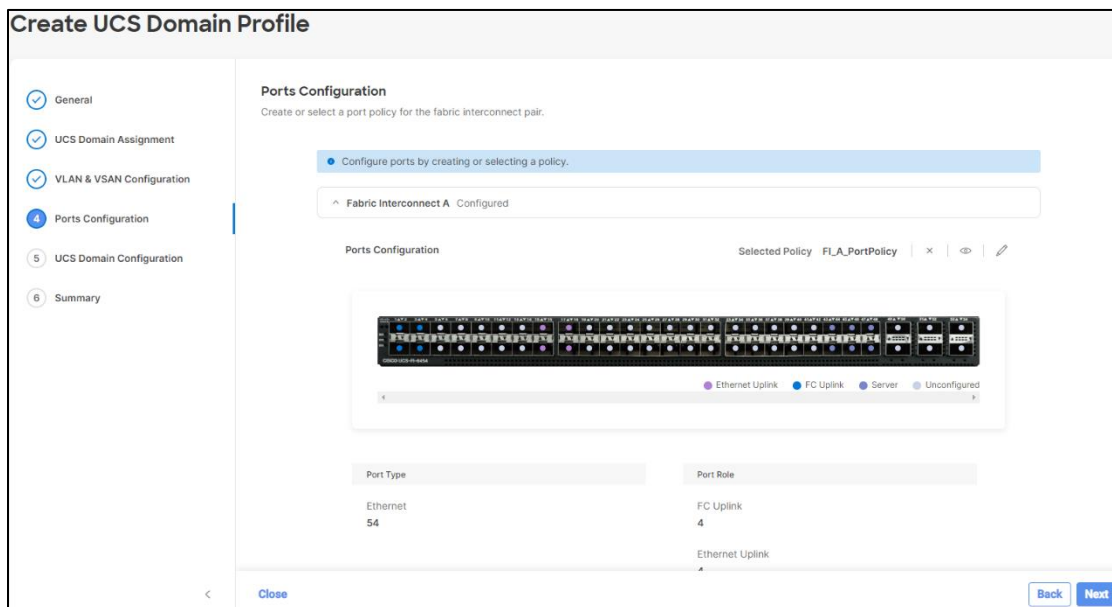
Step 4 In the **UCS Domain Assignment** window, verify the **Assign Now** button is selected. Then select the **Sunset** radio button and click **Next**.

The screenshot shows the 'Create UCS Domain Profile' window with the 'UCS Domain Assignment' tab selected. The left sidebar navigation menu is the same as in the previous screenshot, but 'General' is now marked with a checkmark and 'UCS Domain Assignment' is selected. The main content area is titled 'UCS Domain Assignment' and includes the instruction 'Choose to assign a fabric interconnect pair to the profile now or later.' Below this, there are two buttons: 'Assign Now' (selected) and 'Assign Later'. A blue information box contains the text: 'Choose to assign a fabric interconnect pair now or later. If you choose Assign Now, select a pair that you want to assign and click Next . If you choose Assign Later, click Next to proceed to policy selection.' At the bottom right, there are 'Back' and 'Next' buttons. At the bottom left, there is a 'Close' button and a back arrow.

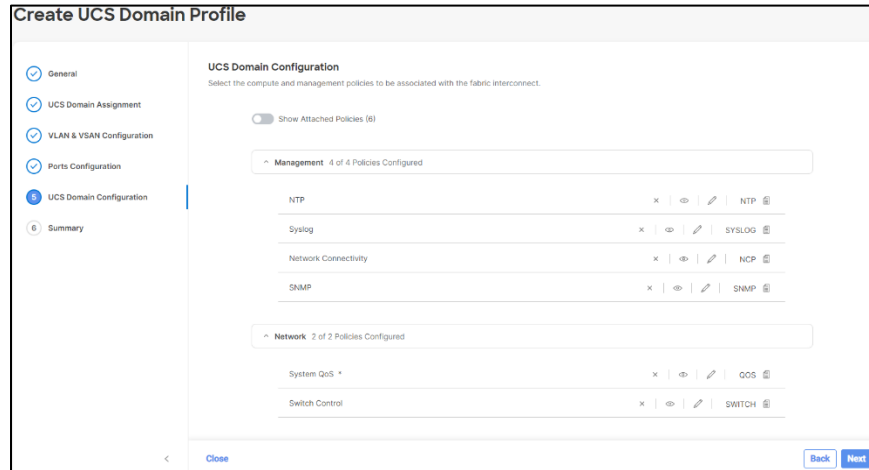
Step 5 In the **VLAN & VSAN Configuration** window, next to **VLAN Configuration** under **Fabric Interconnect A**, click on **Select Policy**. This will display all the available VLAN policies currently created on the dashboard on the right-hand side of the screen. Select **INFRA_VLAN**. Do the same for the **VLAN Configuration** under **Fabric Interconnect B**. Then click **Next**.



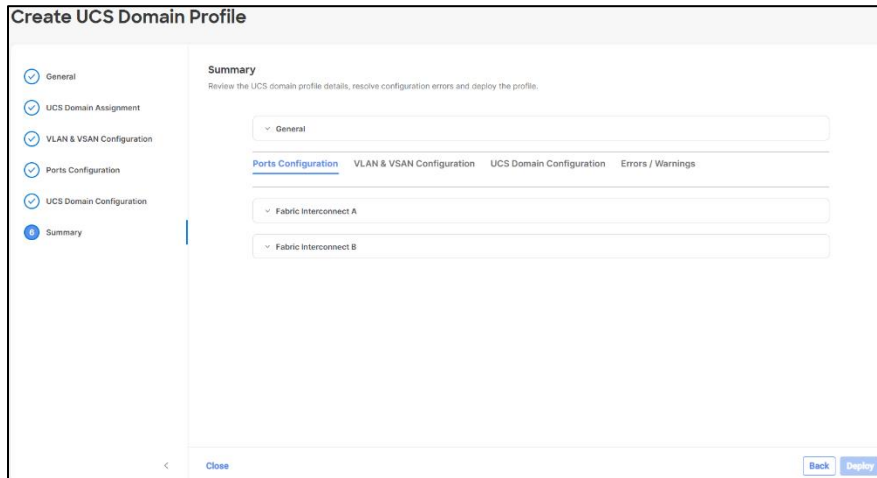
Step 6 Under both Fabric Interconnects, for the **Ports Configuration** Policy, click on **Select Policy**. Under the policy selection pane, select **FI_A_Policy** for Fabric Interconnect A and **FI_B_Policy** for Fabric Interconnect B and then click **Next**.



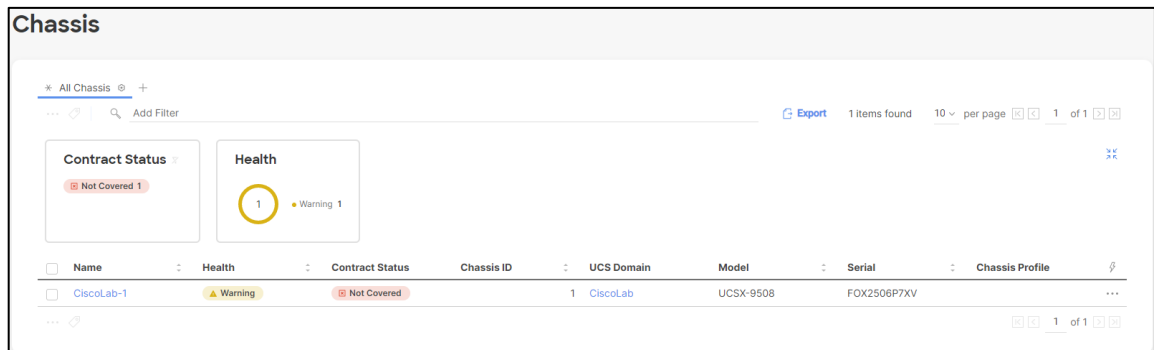
Step 7 In the UCS Domain Configuration window, select the **Sunset** policies for each of the **Management Policies** and **Network Policies** and click **Next**.



Step 8 Verify your configuration and select **Deploy**.



Step 9 Ensure that a Chassis is now displaying when you click on the **Chassis** menu. You should see something like the one shown below:



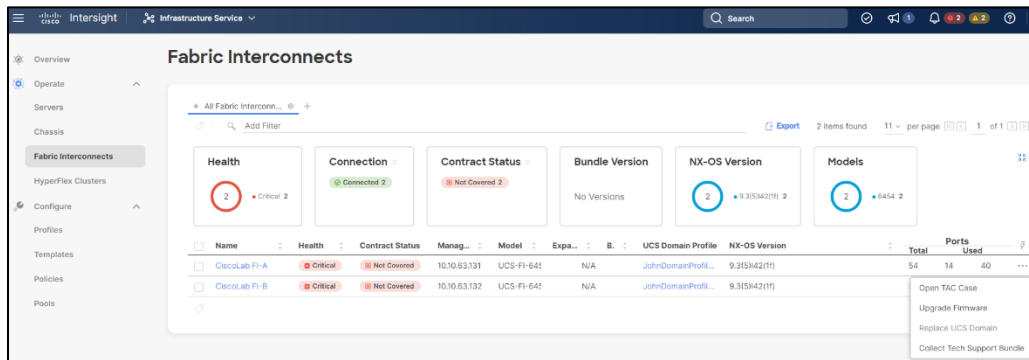
Task 6 has been completed!

Task 7 – Updating Firmware (Review Only)

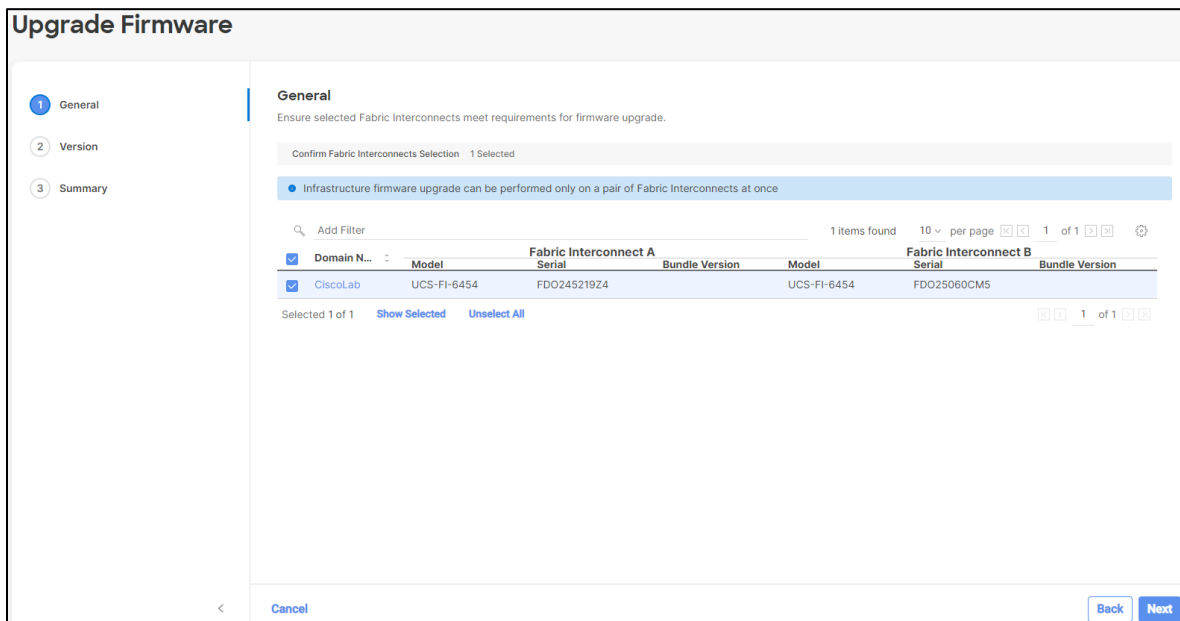
The purpose of this section is to show how to use the Intersight dashboard to update the Infrastructure Firmware and the Server Firmware. We will NOT be completing the firmware updates. But we will review the procedure of updating each firmware, respectively.

Procedure

Step 1 On the left-hand side of the screen, under **OPERATE**, click on **Fabric Interconnects**. On the right-hand side of the **CiscoLab FI-A** device, click on the ellipsis (...) to bring up the menu. Select **Upgrade Firmware**.



Step 2 On the next window, ensure that the **CiscoLab** is selected and click **Next**.



Step 3 Select the **4.2(1#)** firmware version, where # is provided to you by your instructor and click **Next**.

Upgrade Firmware

General
Version
Summary

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.

21 Items found 10 per page 1 of 3

Version	Size	Release ...	Description
<input type="radio"/> 4.2(2d)	1.69 GiB	Nov 28, 2022 2	Cisco Intersight Infrastructure Bundle
<input type="radio"/> 4.2(2c)	1.69 GiB	Sep 20, 2022 11	Cisco Intersight Infrastructure Bundle
<input type="radio"/> 4.2(2a)	1.69 GiB	Jul 14, 2022 9:5	Cisco Intersight Infrastructure Bundle
<input type="radio"/> 4.2(2.220314)	1.69 GiB	May 13, 2022 7:	Cisco Intersight Infrastructure Bundle
<input type="radio"/> 4.2(1n)	1.66 GiB	Aug 3, 2022 9:5	Cisco Intersight Infrastructure Bundle
<input checked="" type="radio"/> 4.2(1m)	1.66 GiB	May 19, 2022 9:	Cisco Intersight Infrastructure Bundle
<input type="radio"/> 4.2(1l)	1.66 GiB	Feb 15, 2022 11	Cisco Intersight Infrastructure Bundle
<input type="radio"/> 4.2(1i)	1.66 GiB	Oct 26, 2021 12	Cisco Intersight Infrastructure Bundle
<input type="radio"/> 4.2(1h)	1.66 GiB	Sep 16, 2021 10	Cisco Intersight Infrastructure Bundle
<input type="radio"/> 4.2(1f)	1.66 GiB	Aug 17, 2021 1:2	Cisco Intersight Infrastructure Bundle

Selected 1 of 21 [Show Selected](#) [Unselect All](#) 1 of 3

[Cancel](#) [Back](#) [Next](#)

Step 4 On the next screen, verify your settings **BUT DO NOT CLICK THE UPGRADE BUTTON**. Click **Cancel** to exit out of the upgrade wizard.

Upgrade Firmware

General
Version
Summary

Summary
Confirm configuration and initiate the 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	Size
4.2(1m)	1.66 GiB

Fabric Interconnects to be Upgraded

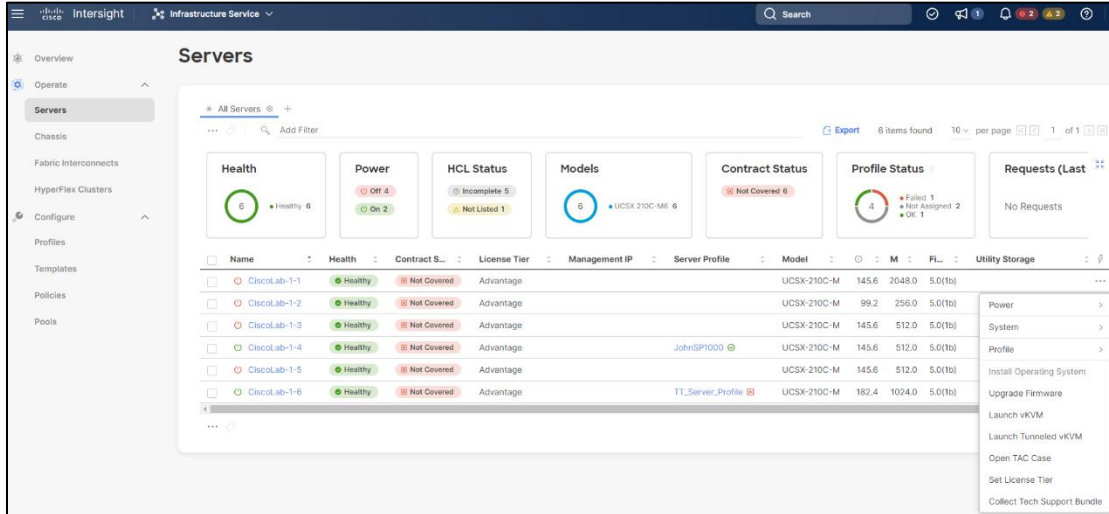
Export 1 items found 10 per page 1 of 1

Domain N...	Fabric Interconnect A			Fabric Interconnect B		
	Model	Serial	Bundle Version	Model	Serial	Bundle Version
CiscoLab	UCS-FI-6454	FDO245219Z4	4.2(1m)	UCS-FI-6454	FDO25060CM5	4.2(1m)

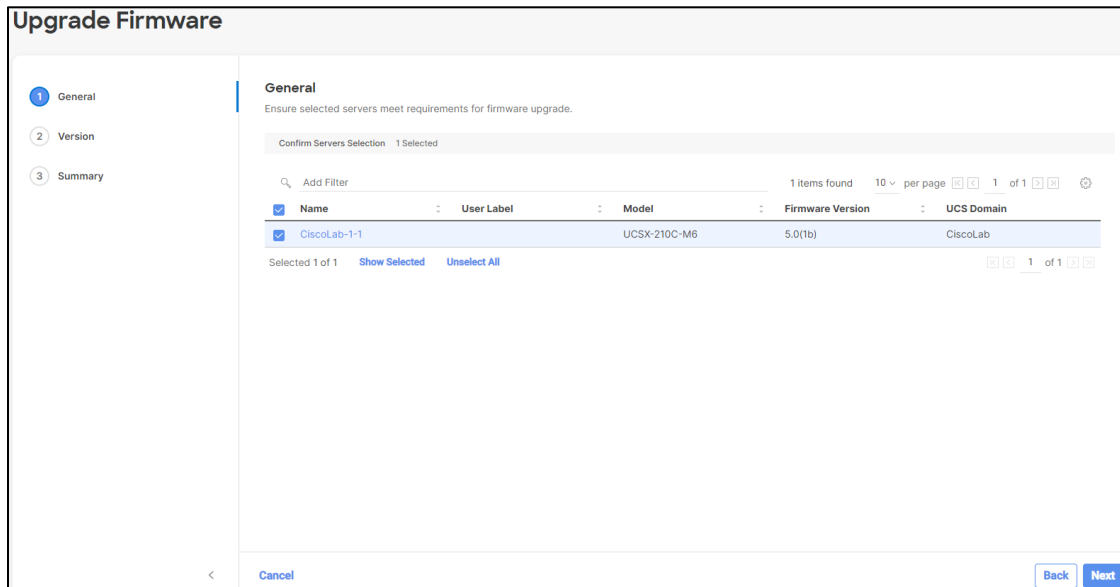
1 of 1

[Cancel](#) [Back](#) [Upgrade](#)

Step 5 On the left-hand side of the screen, under **OPERATE** select **Servers**. In the list of servers, next to the server that has been provided for your pod, click on the **ellipsis (...)** on the right-hand side of the screen and select **Upgrade Firmware**.



Step 6 In the server list, ensure that you pod's server is selected and click **Next**.



Step 7 In the list of the firmware versions, select the **5.0(2#)** version, where # is provided to you by your instructor and click **Next**.

Upgrade Firmware

Version
Select a firmware version to upgrade the servers to.

Select Firmware Bundle Advanced Mode

The selected firmware bundle will be downloaded from intersight.com. All the server components will be upgraded along with drives and storage controllers. Use Advanced Mode to exclude upgrade of drives and storage controllers.

Search: Add Filter 10 items found 10 per page 1 of 1

Version	Size	Release ...	Description
<input type="radio"/> 5.0(2e)	693.59 MIB	Nov 29, 2022 1'	Cisco Intersight Server Bundle
<input type="radio"/> 5.0(2d)	678.01 MIB	Sep 20, 2022 1'	Cisco Intersight Server Bundle
<input checked="" type="radio"/> 5.0(2b)	654.02 MIB	Jul 14, 2022 9:5	Cisco Intersight Server Bundle
<input type="radio"/> 5.0(2.220506)	654.04 MIB	May 16, 2022 6'	Cisco Intersight Server Bundle
<input type="radio"/> 5.0(1f)	464.34 MIB	Sep 1, 2022 11:2	Cisco Intersight Server Bundle
<input type="radio"/> 5.0(1e)	460.63 MIB	Jun 16, 2022 9'	Cisco Intersight Server Bundle
<input type="radio"/> 5.0(1c)	454.58 MIB	Feb 2, 2022 12'	Cisco Intersight Server Bundle
<input type="radio"/> 5.0(1b)	450.83 MIB	Sep 16, 2021 5:3	Cisco Intersight Server Bundle
<input type="radio"/> 5.0(1a)	451.00 MIB	Aug 4, 2021 6:5	Cisco Intersight Server Bundle
<input type="radio"/> 4.1(5h)	351.39 MIB	Jun 17, 2021 11:3	Cisco Intersight Server Bundle

Selected 1 of 10 [Show Selected](#) [Unselect All](#) 1 of 1

[Cancel](#) [Back](#) [Next](#)

Step 8 On the next screen, verify your settings **BUT DO NOT CLICK UPGRADE**. Click **Cancel** to exit the firmware upgrade wizard.

Task 7 has been completed!

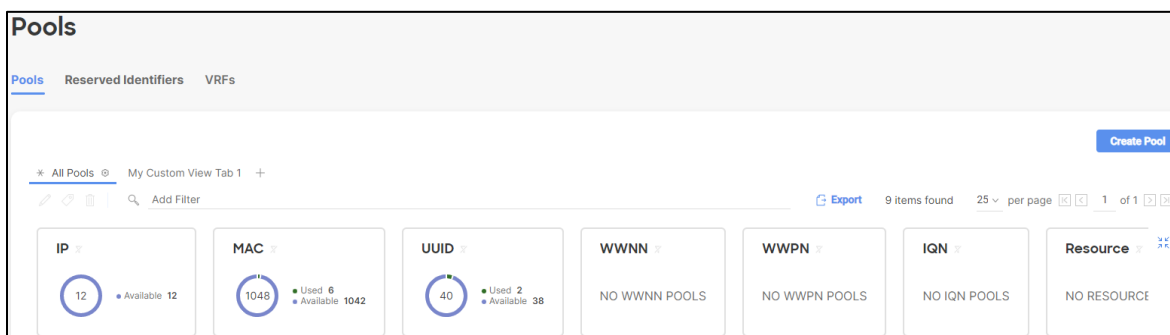
Task 8 – Creating Server Pools

The purpose of this section is to create the pools that are required to complete the Server Profile wizard. These pools will be used to assign identities to the compute nodes. We will create a MAC, UUID, WWNN/WWPN pool and assign them in the next section.

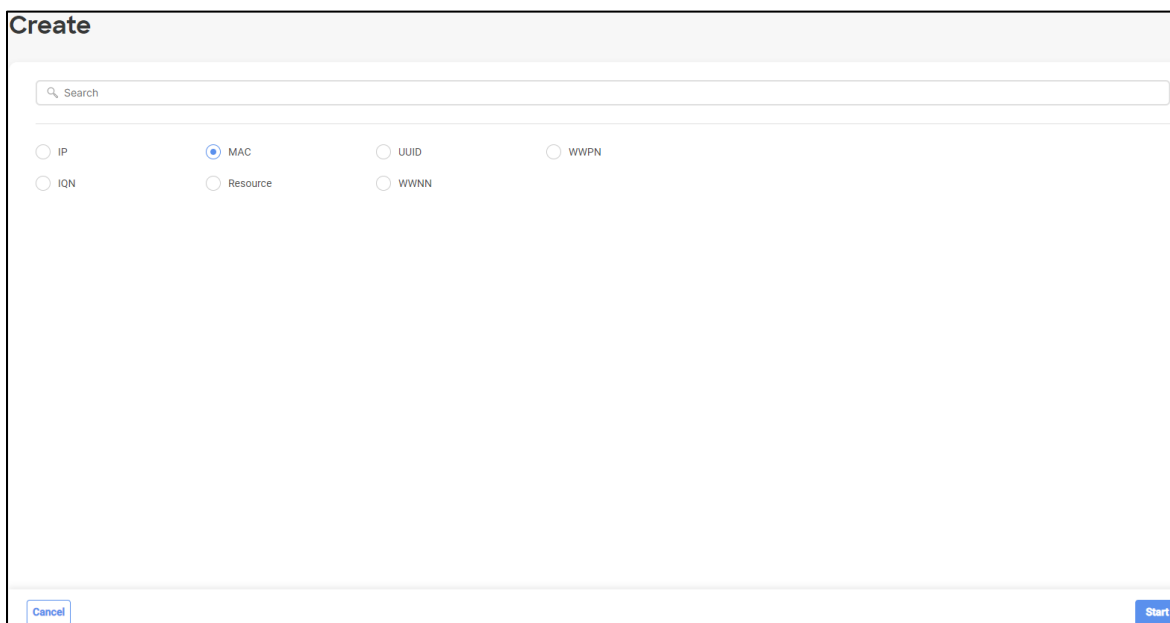
Procedure

CREATE A MAC POOL

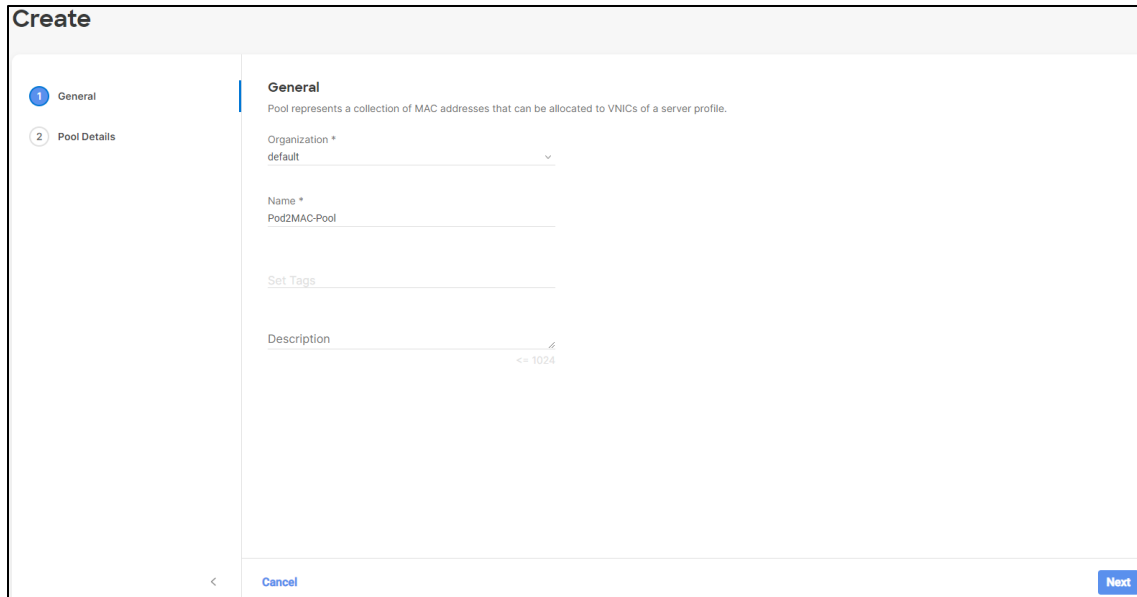
Step 1 On the left-hand side of the screen, under **CONFIGURE**, click on **Pools**. In the top right-hand corner click on **Create Pool**.



Step 2 Select the **MAC** radio button and click **Start**.

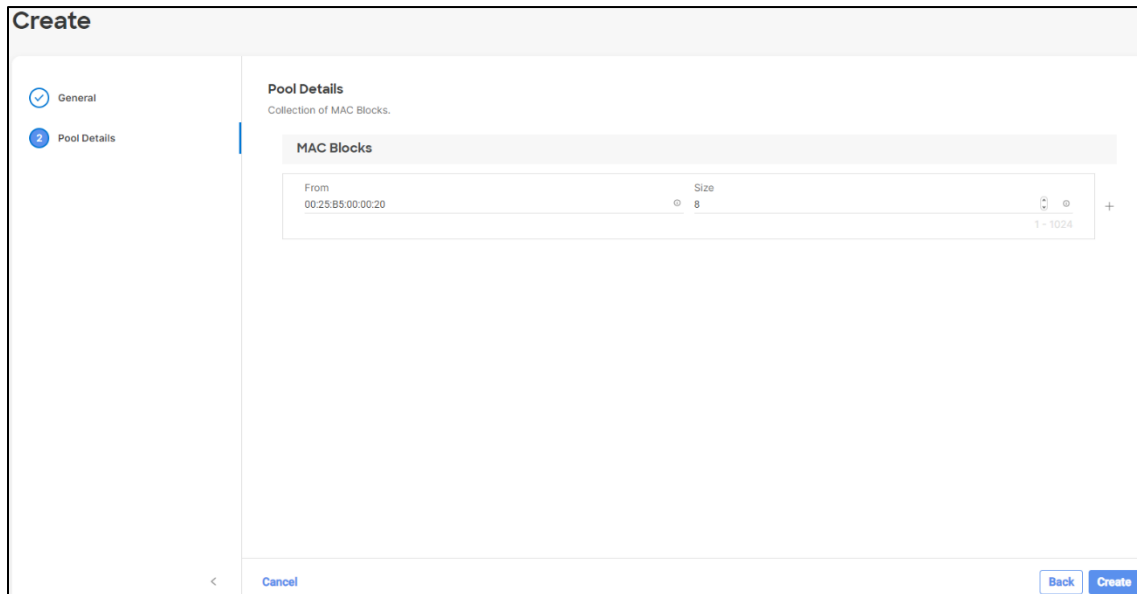


Step 3 Name the pool **PodXMAC-Pool**, where X is your pod number and click **Next**.



The screenshot shows the 'Create' wizard in the General tab. The left sidebar has 'General' selected with a blue circle containing the number 1, and 'Pool Details' is listed below it with a grey circle containing the number 2. The main content area is titled 'General' and includes a sub-header 'Pool represents a collection of MAC addresses that can be allocated to VNICs of a server profile.' Below this are several input fields: 'Organization *' with a dropdown menu showing 'default', 'Name *' with the text 'Pod2MAC-Pool' entered, 'Set Tags' with a plus icon, and 'Description' with a text area containing '<= 1024'. At the bottom left is a back arrow and a 'Cancel' button, and at the bottom right is a 'Next' button.

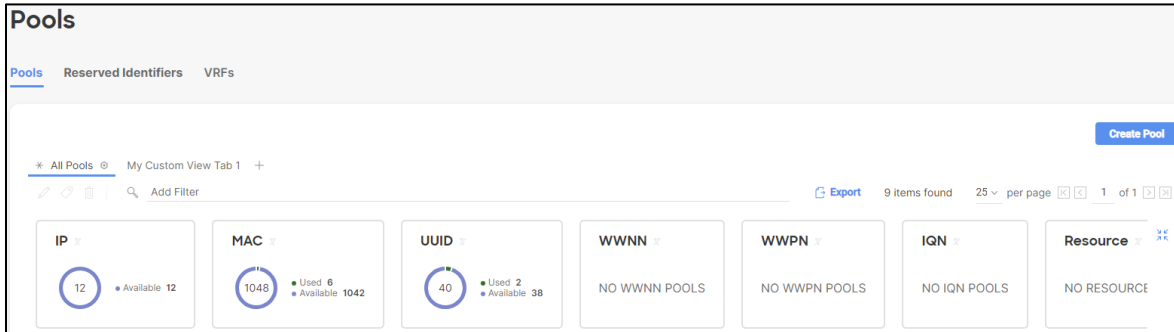
Step 4 For the block suffix use **00:00:X0**, where X is your pod number. For the **size**, use **8**. Then click **Create**.



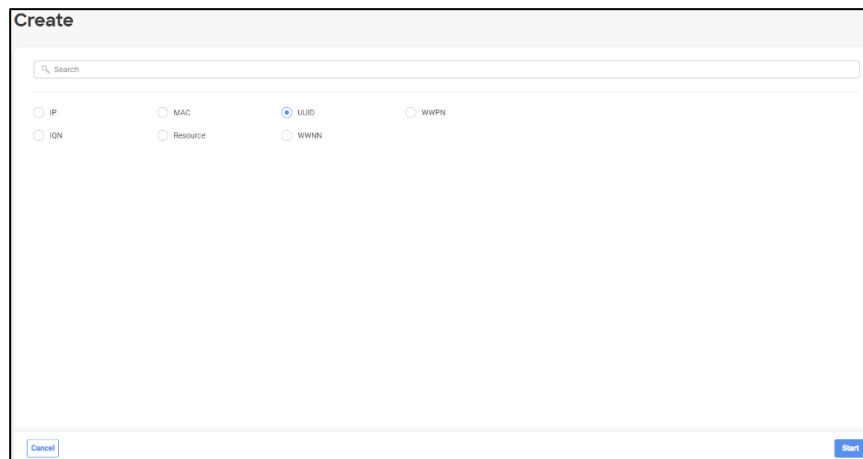
The screenshot shows the 'Create' wizard in the Pool Details tab. The left sidebar has 'General' with a checked checkbox and 'Pool Details' selected with a blue circle containing the number 2. The main content area is titled 'Pool Details' with a sub-header 'Collection of MAC Blocks.' Below this is a table titled 'MAC Blocks' with one row. The row has columns for 'From' (containing '00:25:B5:00:00:20'), 'Size' (containing '8'), and a plus sign icon. At the bottom right of the table is a range indicator '1 - 1024'. At the bottom left is a back arrow and a 'Cancel' button, and at the bottom right are 'Back' and 'Create' buttons.

CREATE A UUID POOL

Step 5 On the left-hand side of the screen, click on **Pools**. And in the top right-hand corner click on **Create Pool**.



Step 6 Select the **UUID** radio button and click **Start**.



Step 7 Name the pool **PodXUUID-Pool**, where X is your pod number and click **Next**. Fill out the following fields, where X is your pod number:

- Prefix = **0000000X-000X-000X**
- From = **000X-0000000000X0**
- Size = **8**

Below is an example from Pod 2:

Create

1 General

2 Pool Details

General

Pool represents a collection of UUID items that can be allocated to server profiles.

Organization *
default

Name *
Pod2UUID-Pool

Set Tags

Description
<= 1024

< Cancel Next

Step 8 Click the **Create** button to complete the pool creation wizard.

The screenshot shows the 'Create' wizard interface. On the left, there are two tabs: 'General' (checked) and 'Pool Details' (selected). The main area is titled 'Pool Details' and contains the following sections:

- Configuration**: A field for 'Prefix *' with the value '00000002-0002-0002'.
- UUID Blocks**: A table with columns 'From' and 'Size'. The first row shows 'From' as '0002-0000000000020' and 'Size' as '8'. There is a '+' button on the right to add more blocks.

At the bottom, there are buttons for '<', 'Cancel', 'Back', and 'Create'.

CREATE AN IP POOL

Step 9 On the left-hand side of the select **Pools** then click on the **Create Pool** button. Select the **IP** radio button and then click **Start**.

The screenshot shows the 'Create' wizard interface. At the top, there is a search bar with the text 'Search'. Below it, there are six radio buttons for selecting the pool type:

- IP
- MAC
- UUID
- WWPN
- IQN
- Resource
- WWNN

At the bottom, there are buttons for 'Cancel' and 'Start'.

Step 10 Name the pool **PodXIP-Pool**, where X is your pod number and click **Next**.

The screenshot shows a 'Create' form with three steps: 1. General, 2. IPv4 Pool Details, and 3. IPv6 Pool Details. The 'General' step is selected. The form contains the following fields:

- Organization *: default
- Name *: Pod2IP-Pool
- Set Tags
- Description: (with a character limit of 1024)

Navigation buttons: '<', 'Cancel', and 'Next'.

Step 11 Fill in the following information:

- Netmask = 255.255.255.0
- Gateway = 10.10.63.254
- Primary DNS = **10.10.63.202**
- Secondary DNS = **8.8.8.8**
- From = **10.10.63.14X**, where X is your pod number
- Size = **1**

Note: A pool size of 1 is not practical in a production environment, but in the lab, you will need only 1 IP address.

Step 12 Then click **Next**

Below is an example from Pod 2:

The screenshot shows the 'Create' wizard for an IPv4 Pool. The left sidebar has three steps: 'General' (checked), 'IPv4 Pool Details' (selected), and 'IPv6 Pool Details'. The main content area is titled 'IPv4 Pool Details' and includes a sub-header 'Network interface configuration data for IPv4 interfaces.' Below this is a toggle switch for 'Configure IPv4 Pool' which is turned on. There are two sections: 'Configuration' and 'IP Blocks'. The 'Configuration' section has four fields: 'Netmask *' (255.255.255.0), 'Gateway' (10.10.63.254), 'Primary DNS' (10.10.63.202), and 'Secondary DNS' (8.8.8.8). The 'IP Blocks' section has a table with 'From' (10.10.63.142) and 'Size' (1), with a range indicator '1 - 1024' and a plus sign. At the bottom right are 'Back' and 'Next' buttons.

Step 13 Click the **Configure IPv6 Pool** slider bar to disable IPv6. And then click the **Create** button to complete the pool creation wizard.

The screenshot shows the 'Create' wizard for an IPv6 Pool. The left sidebar has three steps: 'General' (checked), 'IPv4 Pool Details' (checked), and 'IPv6 Pool Details' (selected). The main content area is titled 'IPv6 Pool Details' and includes a sub-header 'Network interface configuration data for IPv6 interfaces.' Below this is a toggle switch for 'Configure IPv6 Pool' which is turned off. A blue message bar states: 'You can skip IPv6 Pool configuration for now and configure it later.' At the bottom right are 'Back' and 'Create' buttons.

Task 8 has been completed!

Task 9 – Server Policy Creation

The purpose of this section is to create policies required for creating a Server Profile.

Procedure

CREATE A BIOS POLICY

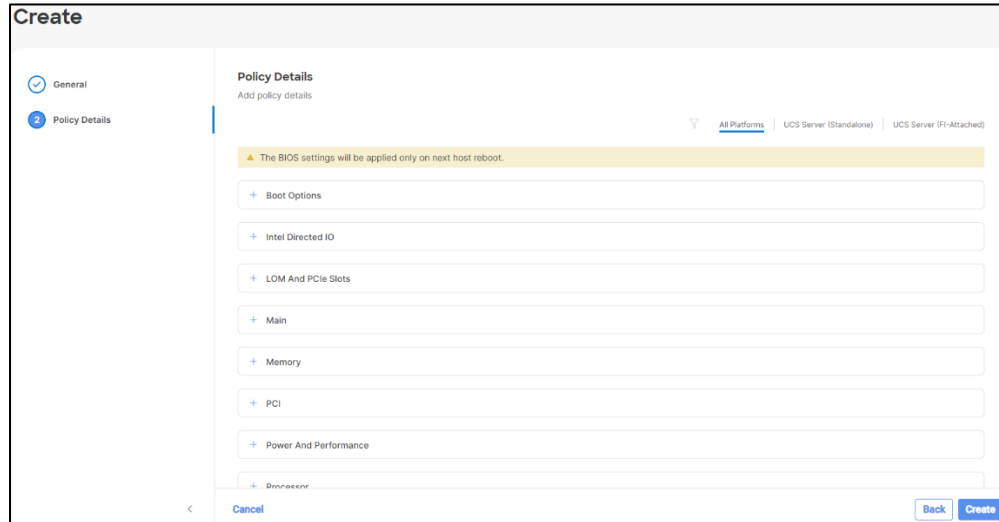
- Step 1** On the left-hand side of the screen, under **CONFIGURE**, select **Policies** and then the **Create Policy** button.
- Step 2** Under **Filters** select the **UCS Server** radio button, select the **BIOS** radio button and click **Start**.

The screenshot shows the 'Create' interface for a policy. On the left, under 'Filters', the 'Platform Type' section has 'UCS Server' selected. The main area contains a grid of radio buttons for various policy categories. The 'BIOS' radio button is selected. At the bottom, there are 'Cancel' and 'Start' buttons.

- Step 3** Name the Policy **PodXBIOS-Policy**, where X is your pod number and click **Next**.

The screenshot shows the 'Create' interface for a policy, specifically the 'General' tab. The 'Organization' is set to 'default', the 'Name' is 'Pod2BIOS Policy', and the 'Description' field is empty. The 'Next' button is visible at the bottom right.

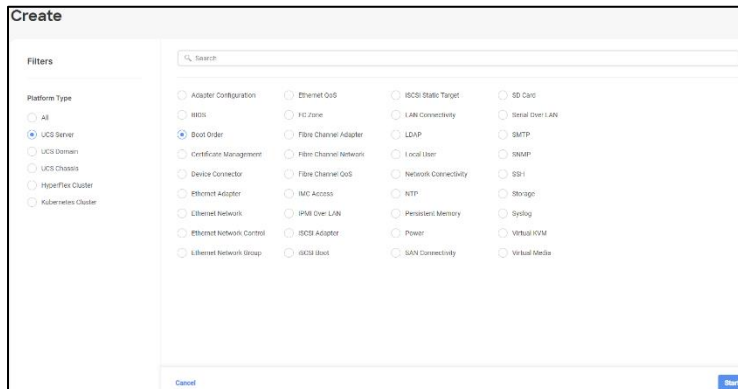
Step 4 Review the available options. Retain all defaults and click **Create** to complete the policy creation wizard.



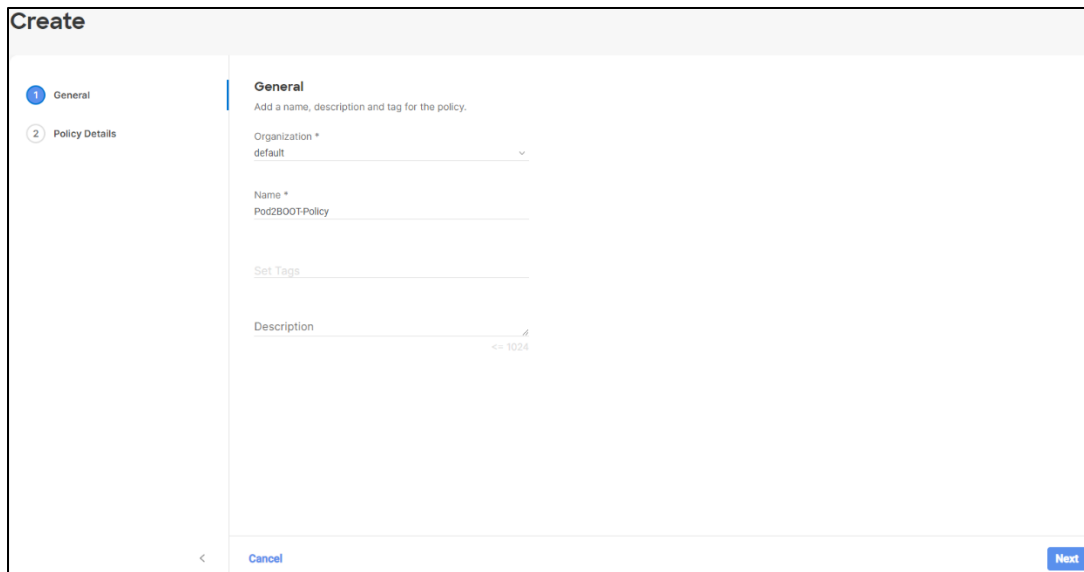
CREATE A BOOT POLICY

Step 5 From the left-hand side of the window, select **Policies** and then click the **Create Policy** button.

Step 6 Under **Filter**, select **UCS Server** and click on the **Boot Order** radio button.

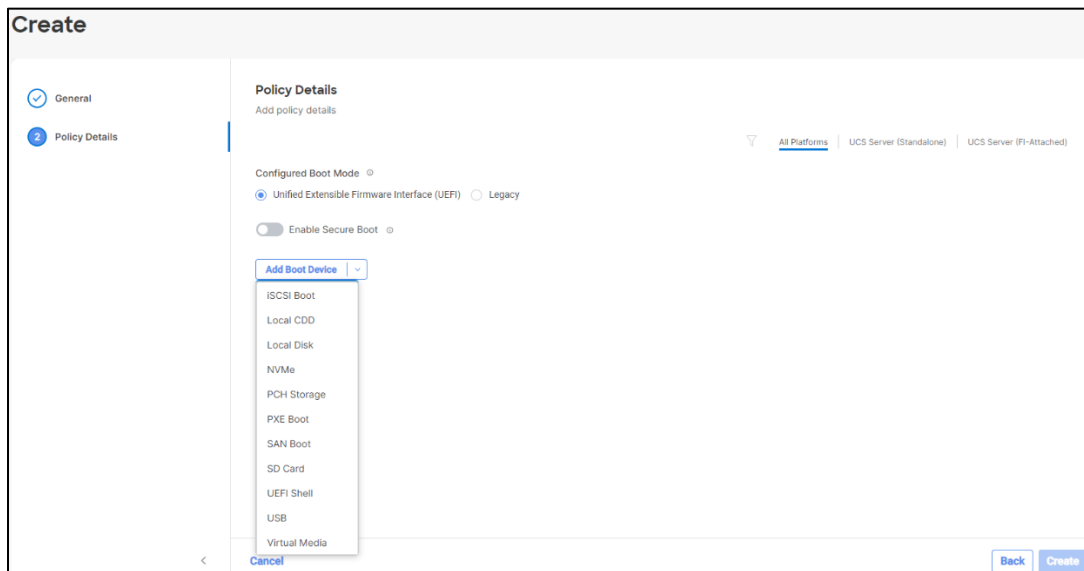


Step 7 Name the policy **PodXBOOT-Policy**, where X is your pod number and click **Next**.



The screenshot shows the 'Create' policy page with the 'General' tab selected. The 'Organization' dropdown is set to 'default'. The 'Name' field contains 'Pod2BOOT-Policy'. There is a 'Set Tags' link and a 'Description' field with a character count of '<= 1024'. At the bottom, there are 'Cancel' and 'Next' buttons.

Step 8 Click the **Add Boot Device** drop-down and select **Local Disk**.



The screenshot shows the 'Create' policy page with the 'Policy Details' tab selected. The 'Configured Boot Mode' is set to 'Unified Extensible Firmware Interface (UEFI)'. The 'Enable Secure Boot' toggle is off. The 'Add Boot Device' dropdown menu is open, showing options: ISCSI Boot, Local CDD, Local Disk, NVMe, PCH Storage, PXE Boot, SAN Boot, SD Card, UEFI Shell, USB, and Virtual Media. At the bottom, there are 'Cancel', 'Back', and 'Create' buttons.

Step 9 Use the following information to fill in the fields:

- Device Name: **OS-Disk**
- Slot: **1**

Step 10 Click the **Add Boot Device** drop-down again and click **Virtual Media**. Name this device **OS-Install**, and under Sub-Type, select **KVM MAPPED DVD**.

Step 11 Click **Create** to complete the policy creation wizard.

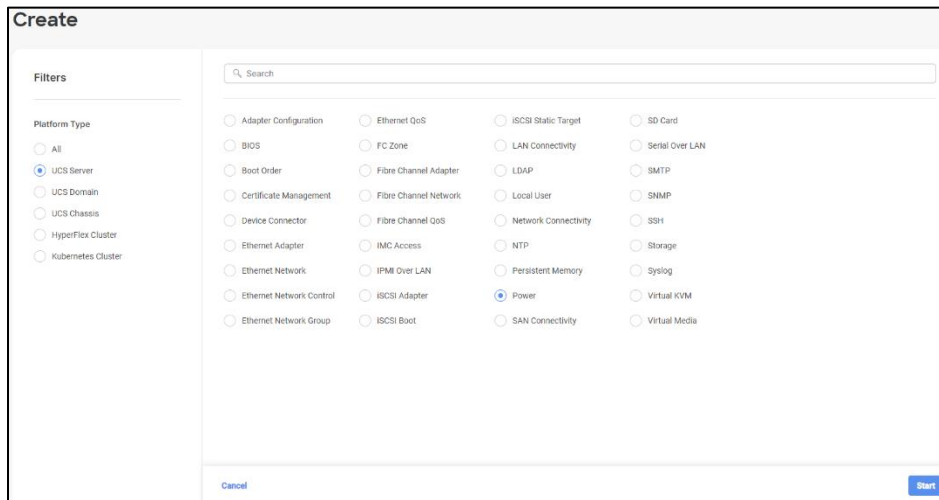
The screenshot shows the 'Create' policy creation wizard in the 'Policy Details' step. The interface is divided into a left sidebar and a main content area. The sidebar contains two tabs: 'General' (with a checkmark) and 'Policy Details' (with a blue circle). The main content area is titled 'Policy Details' and includes the following elements:

- A breadcrumb trail: 'Add policy details' > 'All Platforms' > 'UCS Server (Standalone)' > 'UCS Server (FI-Attached)'.
- 'Configured Boot Mode' section with radio buttons for 'Unified Extensible Firmware Interface (UEFI)' (selected) and 'Legacy'.
- 'Enable Secure Boot' section with a toggle switch that is currently turned off.
- 'Add Boot Device' section with a dropdown menu.
- A list of boot devices, each with a plus sign, a name, a status, and control icons:
 - 'Virtual Media (OS-Install)' with status 'Enabled'.
 - 'Local Disk (OS-Disk)' with status 'Enabled'.
- At the bottom, there are 'Cancel', 'Back', and 'Create' buttons.

CREATE A POWER POLICY

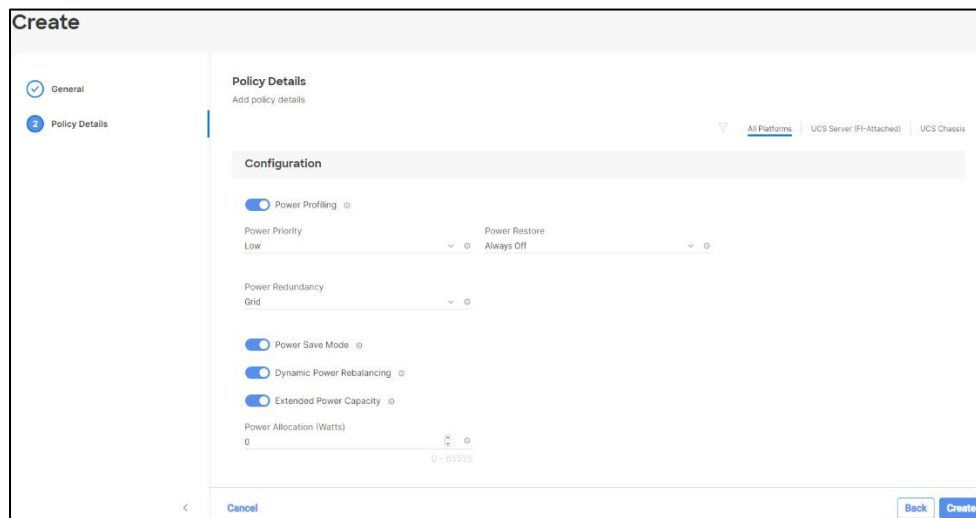
Step 12 On the left-hand side of the screen, select **Policies** and then click on the **Create Policy** button.

Step 13 Under the **Filter** option, highlight the **UCS Server** radio button and then select **Power**. Then click the **Start** button.



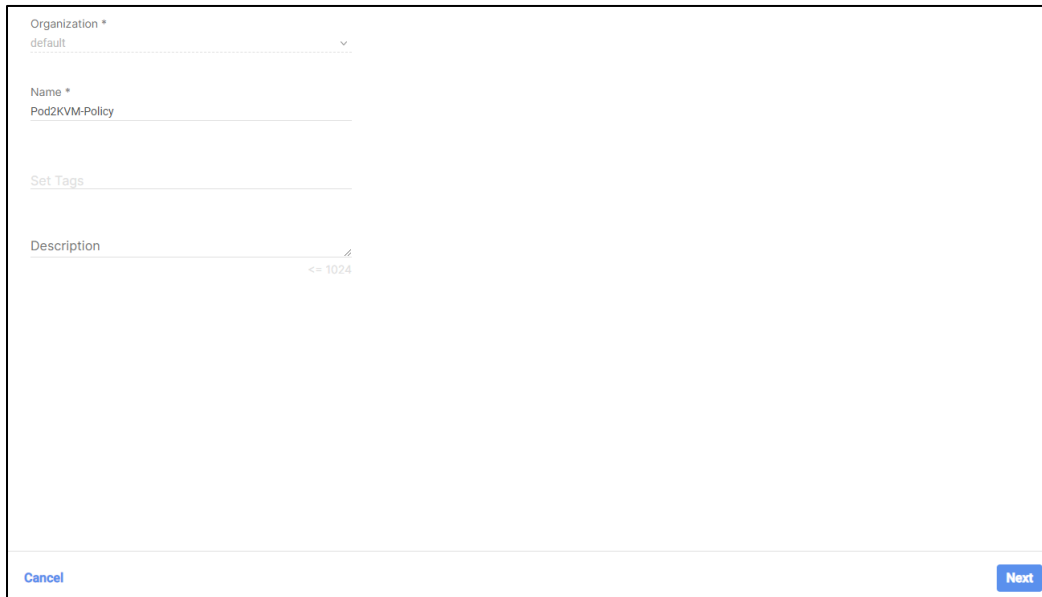
Step 14 Name the policy **PodXPOWER-Policy**, where X is your pod number and click **Next**.

Step 15 Review the available options and then click **Create** to complete the policy creation wizard.



CREATE A VIRTUAL KVM POLICY

- Step 16** Click on **Create Policy** again and then under the filter option select **UCS Server**. Scroll down the list of policies; select the **Virtual KVM** radio button and click **Start**.
- Step 17** Name the policy **PodXKVM-Policy**, where X is your pod number and click **Next**.



Organization *
default

Name *
Pod2KVM-Policy

Set Tags

Description
<= 1024

Cancel Next

- Step 18** Review the available options and then click **Create** to complete the policy creation wizard.



Policy Details
Add policy details

All Platforms | UCS Server (Standalone) | UCS Server (FI-Attached)

Enable Virtual KVM

Max Sessions *
4 1 - 4

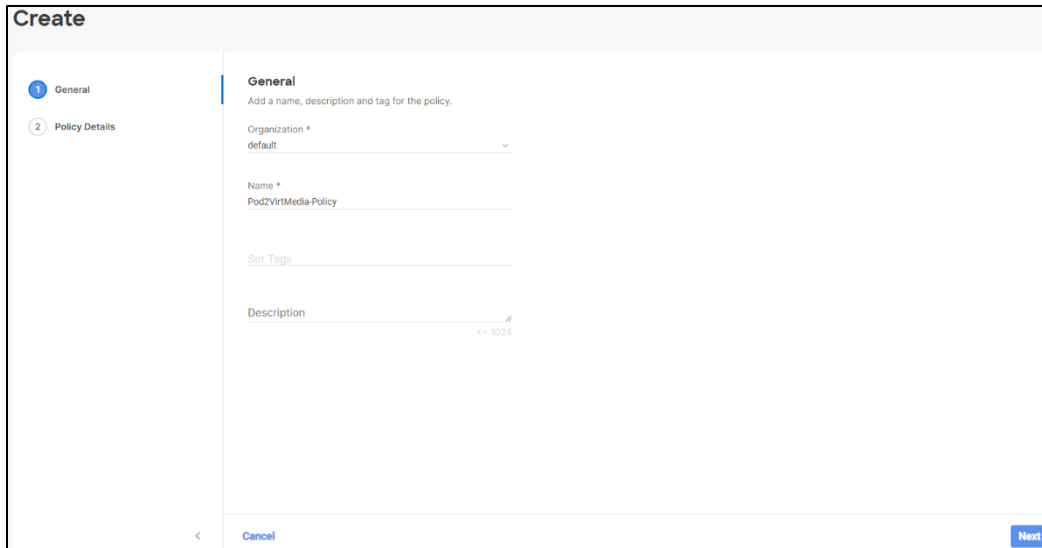
Enable Video Encryption

Allow Tunneled vKVM

Cancel Back Create

CREATE A VIRTUAL MEDIA POLICY

- Step 19** Click on **Create Policy** again and then under the filter option select **UCS Server**. Scroll down the list of policies; select the **Virtual Media** radio button and click **Start**.
- Step 20** Name the policy **PodXVirtMedia-Policy**, where X is your pod number and click **Next**.

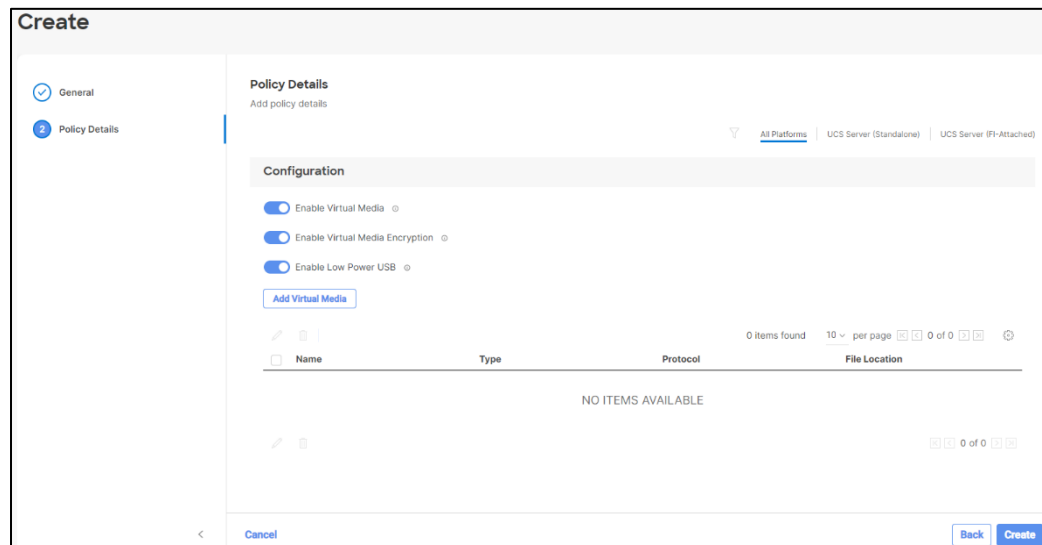


The screenshot shows the 'Create' wizard in the 'General' tab. The left sidebar has 'General' selected with a blue checkmark and 'Policy Details' with a blue circle and number '2'. The main content area is titled 'General' and contains the following fields:

- Organization *: default (dropdown menu)
- Name *: Pod2VirtMedia-Policy (text input)
- Set Tags (text input)
- Description (text area, limit 1024 characters)

At the bottom, there are 'Cancel' and 'Next' buttons.

- Step 21** Review the available options and then click **Create** to complete the policy creation wizard.



The screenshot shows the 'Create' wizard in the 'Policy Details' tab. The left sidebar has 'General' with a blue checkmark and 'Policy Details' with a blue circle and number '2'. The main content area is titled 'Policy Details' and contains the following configuration options:

- Configuration section with three toggle switches:
 - Enable Virtual Media (checked)
 - Enable Virtual Media Encryption (checked)
 - Enable Low Power USB (checked)
- An 'Add Virtual Media' button.
- A table with columns: Name, Type, Protocol, File Location. The table is empty and displays 'NO ITEMS AVAILABLE'.

At the bottom, there are 'Cancel', 'Back', and 'Create' buttons.

CREATE AN IMC ACCESS POLICY

Step 22 Click on the **Create Policy** button and under the filter option select **UCS Server**. Scroll down the list of policies; select **IMC Access** radio button and click **Start**.

The screenshot shows the 'Create' interface for selecting a policy. On the left, under 'Filters', 'UCS Server' is selected under 'Platform Type'. The main area contains a search bar and a grid of radio buttons for various policy types. 'IMC Access' is selected. At the bottom, there are 'Cancel' and 'Start' buttons.

Step 23 Name the policy **PodXIMC-Policy**, where X is your pod number and then click **Next**.

The screenshot shows the 'General' configuration tab for the policy. The 'Name' field is filled with 'Pod2IMC-Policy'. The 'Organization' is set to 'default'. There are fields for 'Set Tags' and 'Description' (with a character count of <= 1024). At the bottom, there are 'Cancel' and 'Next' buttons.

Step 24 For the **VLAN ID**, use vlan **63**. Then you will need to click on the **Select IP Pool** link to select the Pool you created earlier. Then click on the **Create** button to complete the policy creation wizard.

The screenshot shows the 'Create' wizard interface for a policy. The left sidebar has two tabs: 'General' (checked) and 'Policy Details' (active). The main area is titled 'Policy Details' with the subtitle 'Add policy details'. At the top right, there are filters for 'All Platforms', 'UCS Server (FI-Attached)', and 'UCS Chassis'. A blue warning banner states: 'A minimum of one configuration must be enabled. Policies like SNMP, vMedia and Syslog are currently not supported via Out-Of-Band and will require an In-Band IP to be configured. Check here for more info, Help Centre'. Below this, there are three configuration sections: 1. 'In-Band Configuration' with a toggle switch set to 'Enabled'. 2. 'VLAN ID' with a dropdown menu showing '63' and a range indicator '4 - 4095'. 3. 'IP address configuration' with two checkboxes: 'IPV4 address configuration' (checked) and 'IPV6 address configuration' (unchecked). Below these is an 'IP Pool' field showing 'Selected IP Pool Pod2IP-Pool' with a dropdown arrow. At the bottom, there is an 'Out-Of-Band Configuration' section with a toggle switch set to 'Enabled'. At the bottom of the wizard, there are three buttons: '<', 'Cancel', and 'Back | Create'.

CREATE A LOCAL USER POLICY

Step 25 Click on the **Create Policy** button and under the filter option, select the **UCS Server** option. Then ensure that the **Local User** policy radio button is selected and then click the **Start** button.

Create

Filters

Platform Type

- All
- UCS Server
- UCS Domain
- UCS Chassis
- HyperFlex Cluster
- Kubernetes Cluster

Search

- Adapter Configuration
- BIOS
- Boot Order
- Certificate Management
- Device Connector
- Ethernet Adapter
- Ethernet Network
- Ethernet Network Control
- Ethernet Network Group
- Ethernet QoS
- FC Zone
- Fibre Channel Adapter
- Fibre Channel Network
- Fibre Channel QoS
- IMC Access
- IPMI Over LAN
- ISCSI Adapter
- ISCSI Boot
- ISCSI Static Target
- LAN Connectivity
- LDAP
- Local User
- Network Connectivity
- NTP
- Persistent Memory
- Power
- SAN Connectivity
- SD Card
- Serial Over LAN
- SMTP
- SNMP
- SSH
- Storage
- Syslog
- Virtual KVM
- Virtual Media

Cancel Start

Step 26 Name the policy **PodXUSER-Policy**, where X is your pod number and click **Next**.

Create

1 General

2 Policy Details

General

Add a name, description and tag for the policy.

Organization *
default

Name *
Pod2USER-Policy

Set Tags

Description
<= 1024

Cancel Next

Step 27 Click the **Add New User** button at the bottom of the wizard. Then click on the + icon next to **New User**. Use the following credentials:

- Username: **PodXUser** (where X is your pod number)
- Password: **Cisco123!!** (You will also need to confirm the password.)

Step 28 Click **Create** to complete the policy creation wizard.

The screenshot shows the 'Create' policy wizard in the 'Policy Details' step. The 'Local Users' section is active, displaying a list of users. A user named 'Pod2User (readonly)' is listed with a role of 'readonly'. The 'Add New User' button is visible above the user list. The 'Enforce Strong Password' and 'Always Send User Password' options are checked. The 'Password History' is set to 5. The 'Create' button is visible at the bottom right.

Create

General

2 Policy Details

Enforce Strong Password

Enable Password Expiry

Password History: 5 (0 - 5)

Always Send User Password

Local Users

This policy will remove existing user accounts other than the ones configured with this policy. However, the default admin user account is not deleted from the endpoint device. You can only enable/disable or change account password for the admin account by creating a user with the user name and role as 'admin'. If there are no users in the policy, only the admin user account will be available on the endpoint device. By default, IPMI support is enabled for all users

[Add New User](#)

Pod2User (readonly) Enable

Username * Pod2User Role readonly

Password * Password Confirmation *

[Cancel](#) [Back](#) [Create](#)

CREATE A SERIAL OVER LAN POLICY

Step 29 Click on **Create Policy**. Under the filter option select **UCS Server** and then select the **Serial Over LAN** policy radio button and click **Start**.

The screenshot shows the 'Create' policy wizard interface. On the left, under 'Filters', the 'Platform Type' section has 'UCS Server' selected. The main area displays a grid of policy options. The 'Serial Over LAN' option is selected with a radio button. At the bottom, there are 'Cancel' and 'Start' buttons.

Step 30 Name the policy **PodXSerialLAN-Policy**, where X is your pod number and click **Next**.

The screenshot shows the 'Create' policy wizard in the 'General' tab. The 'Name' field contains 'Pod2SerialLAN-Policy'. The 'Organization' is set to 'default'. The 'Description' field is empty. At the bottom, there are 'Cancel' and 'Next' buttons.

Step 31 Review the available options but leave them at their default values and click on **Create** to complete the policy creation wizard.

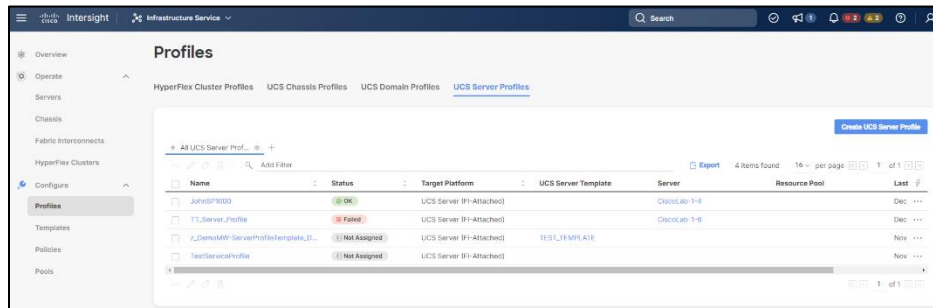
Task 9 has been completed!

Task 10 – Server Profile Deployment

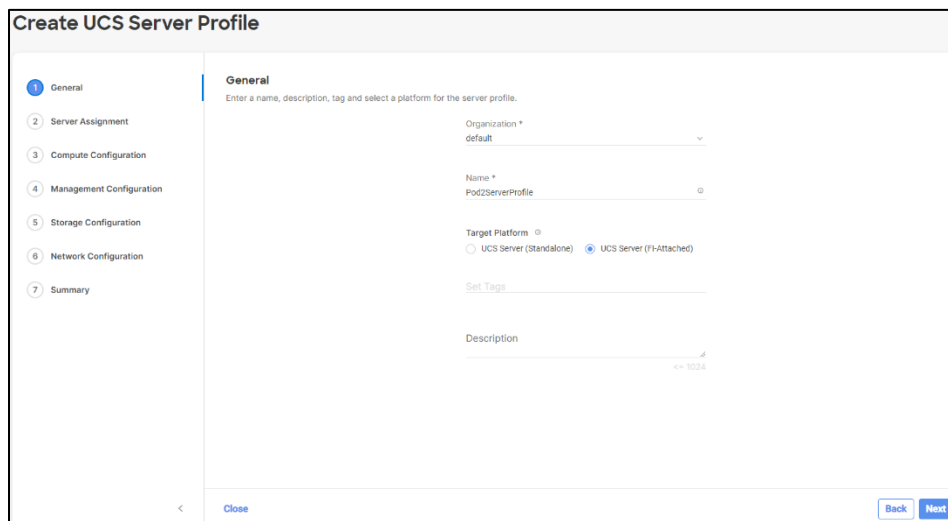
In this section, you will create and deploy a Server Profile to an available server using the policies and pools we have previously created.

Procedure

- Step 1** On the left-hand side of the screen, under **CONFIGURE**, select **Profiles**. Then click on the **UCS Server Profiles** tab.



- Step 2** Click on the Create UCS Server Profile button.
- Step 3** Name the Server Profile **PodXServerProfile**, where X is your pod number and ensure that the **UCS Server (FI-Attached)** radio button is highlighted. Then click **Next**.



Step 4 Select the server that corresponds to your Pod X and click **Next**.

The screenshot shows the 'Create UCS Server Profile' wizard at the 'Server Assignment' step. The left sidebar lists steps 1 through 7, with 'Server Assignment' selected. The main area has three buttons: 'Assign Now', 'Assign Server from a Resource Pool', and 'Assign Later'. A blue instruction box says: 'Click the appropriate button to assign a server now, from a resource pool, or later. If you choose to assign a server now, select the server, click Next, and select and attach policies to the server profile.' Below is a table with 4 items found, showing server details. The first item, 'CiscoLab-1-2', is selected.

Name	User Label	Health	Model	UCS Domain	Serial Nu...
<input type="radio"/> CiscoLab-1-1		Healthy	UCSX-210C-M6	CiscoLab	FCH243974WA
<input checked="" type="radio"/> CiscoLab-1-2		Healthy	UCSX-210C-M6	CiscoLab	FCH2446721K
<input type="radio"/> CiscoLab-1-3		Healthy	UCSX-210C-M6	CiscoLab	FCH250671MR
<input type="radio"/> CiscoLab-1-5		Healthy	UCSX-210C-M6	CiscoLab	FCH250671FA

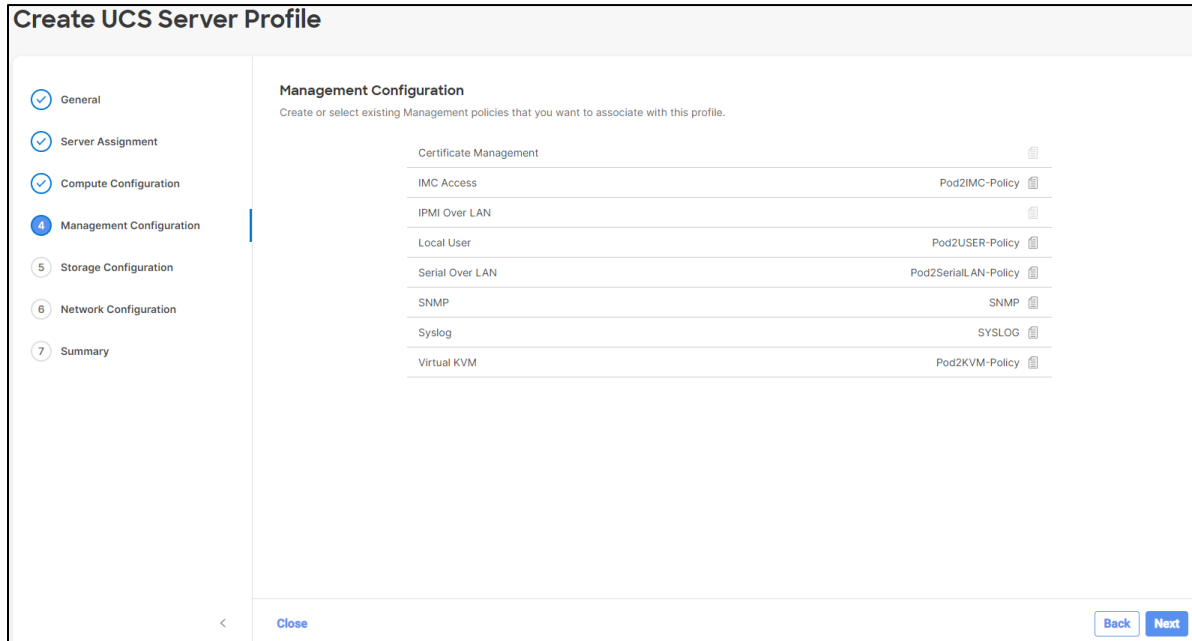
Step 5 Select the **UUID Pool** you created earlier and select the corresponding **BIOS**, **Boot Order**, **Power**, and **Virtual Media** policies that you previously created. Then click **Next**.

The screenshot shows the 'Create UCS Server Profile' wizard at the 'Compute Configuration' step. The left sidebar shows 'Compute Configuration' selected. The main area has a 'UID Assignment' section with 'Pool' and 'Static' buttons. Below, a table lists policies for UUID Pool, BIOS, Boot Order, Power, and Virtual Media, each with a link to edit.

UID Assignment	
Selected Pool	Pod2UUID-Pool
BIOS	Pod2BIOS-Policy
Boot Order	Pod2BFS-BOOT
Power	Pod2Power-Policy
Virtual Media	Pod2VMedia-Policy

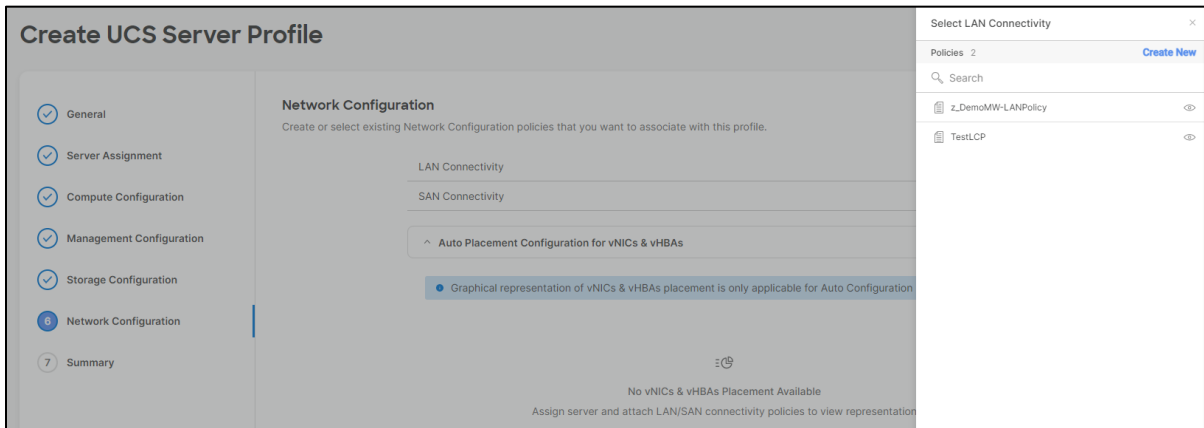
Step 6 Continue to select the corresponding policies that you previously created and then click **Next**.

NOTE: We are not going to be using the Certificate Management or IPMI policies.



Step 7 Skip the Storage Configuration by clicking **Next**.

Step 8 Click on **Select Policy** to the right of **LAN Connectivity** and then select **Create New**.



Step 9 Name the policy **PodXLAN-Policy**, where X is your pod number and click **Next**.

Step 10 Make sure you select the **Auto vNICs Placement** option and then click **Add vNIC**.

Policy Details
Add policy details

Enable Azure Stack Host QoS

IQN

None Pool Static

This option ensures the IQN name is not associated with the policy

vNIC Configuration

Manual vNICs Placement Auto vNICs Placement

For auto placement option the vNICs will be automatically distributed between adaptors during profile deployment. Learn more at [Help Center](#)

Add vNIC

0 items found 50 per page 0 of 0

Name	Switch ID	Failover	Pin Group	MAC Pool
NO ITEMS AVAILABLE				

Cancel Back Create

Step 11 Name the vNIC **PodX-vNIC0**, where X is your pod number. For the MAC address pool, select the pool you previously created.

General

Name *
Pod2-vNIC0 Pin Group Name

MAC

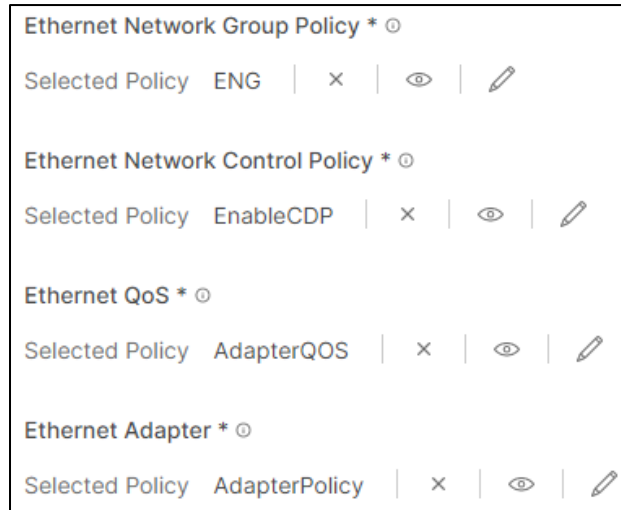
Pool Static

MAC Pool *
Selected Pool Pod2MAC-Pool

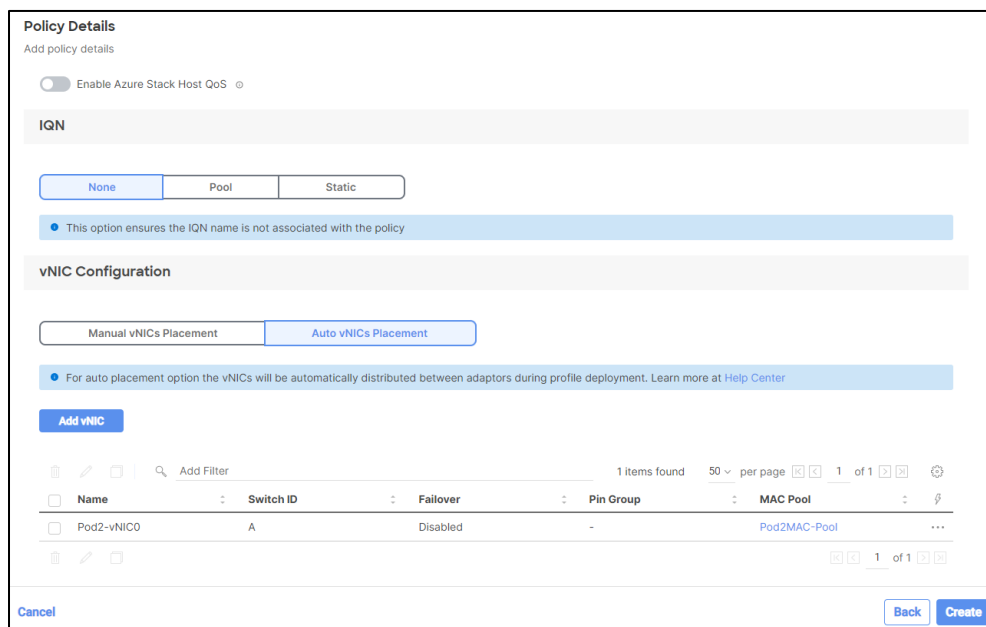
Step 12 Scroll down the page. For the required policies, select the following:

- Ethernet Network Group Policy: **ENG**
- Ethernet Network Control Policy: **EnableCDP**
- Ethernet QoS Policy: **AdapterQoS**
- Ethernet Adapter: **AdapterPolicy**

Step 13 Then click **Add**.

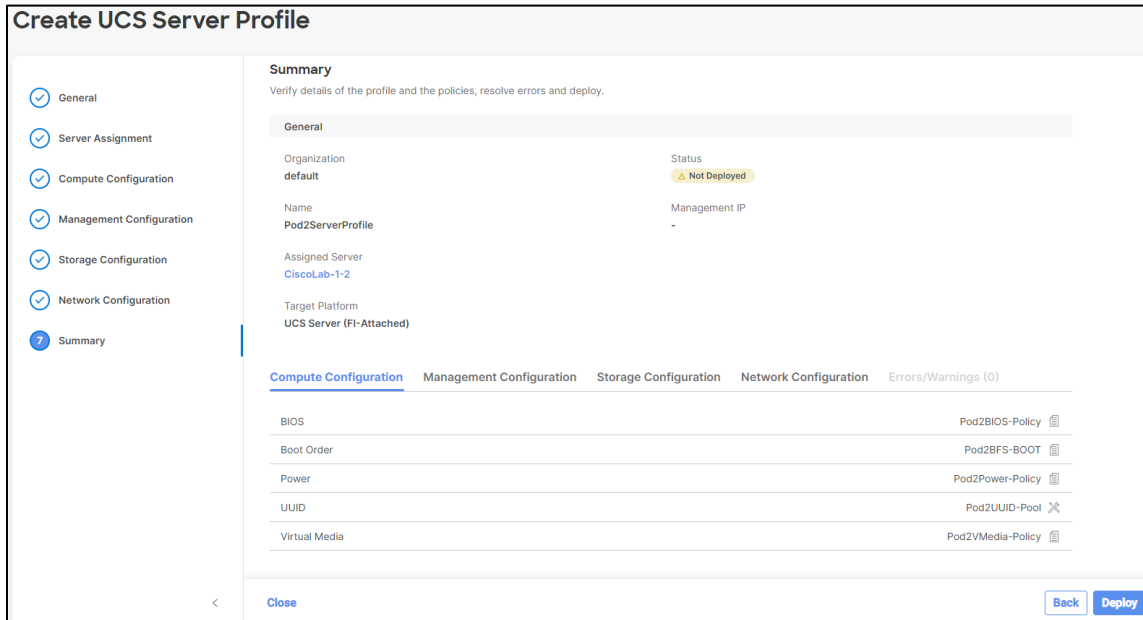


Step 14 On the next screen click **Create**. And on the following screen, click **Next**.





Step 15 Review your configuration. Click on the **Network Configuration** tab to see a graphical view of your vNIC configuration. When you are done reviewing, click **Deploy**. When asked to confirm, verify that you are deploying to the server for your pod, then click **Deploy** again.



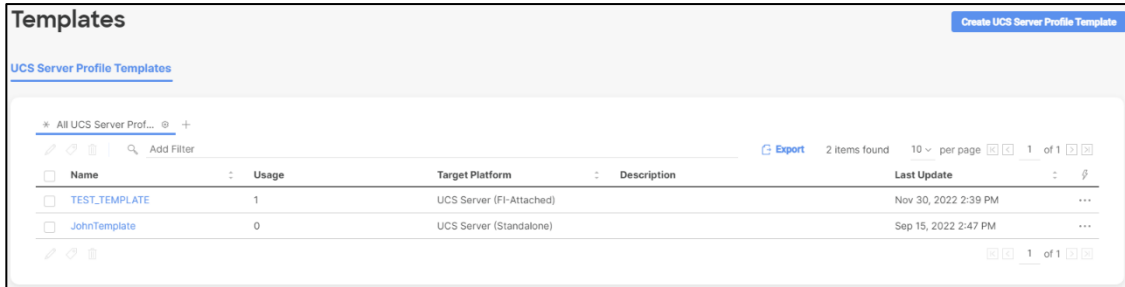
Task 10 has been completed!

Task 11 – Server Profile Template Deployment

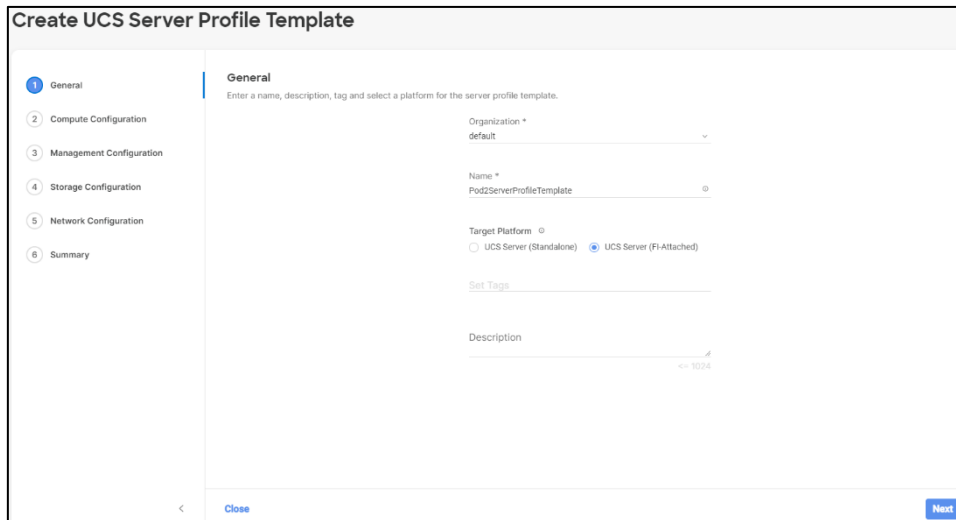
In this section, you will create and deploy a Server Profile Template to an available server using the policies and pools we have previously created.

Procedure

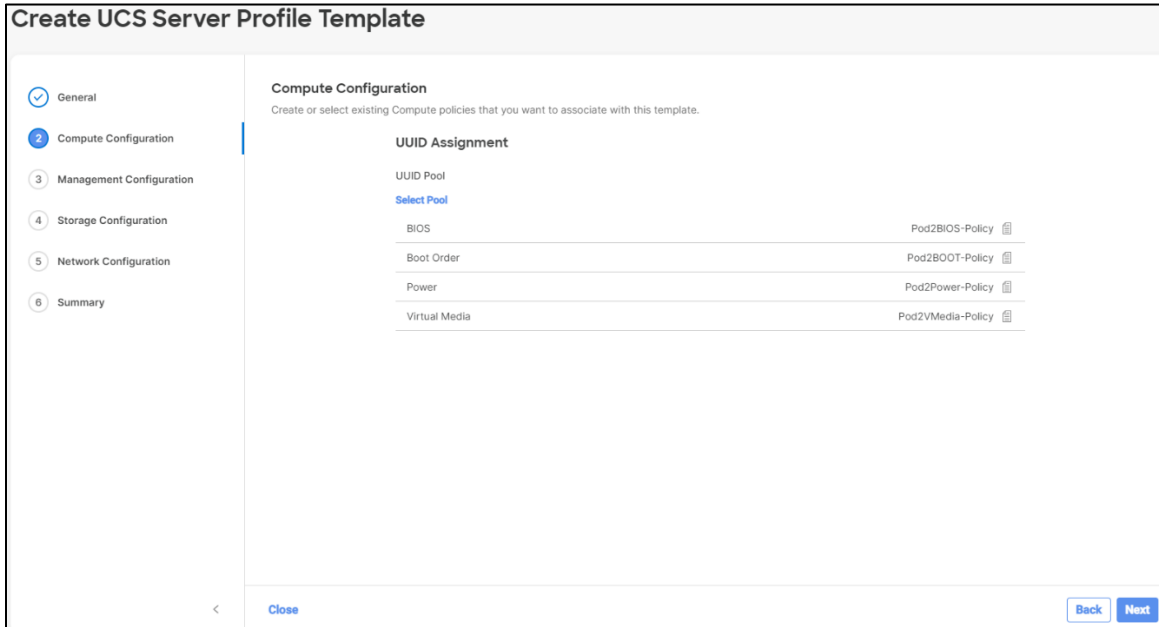
Step 1 In the menu, click on **Templates** and then select **Create UCS Server Profile Template**.



Step 2 Name the template **PodXServerProfileTemplate**, where X is your pod number. Also, ensure that the **UCS Server (FI-Attached)** radio button is selected and click **Next**.

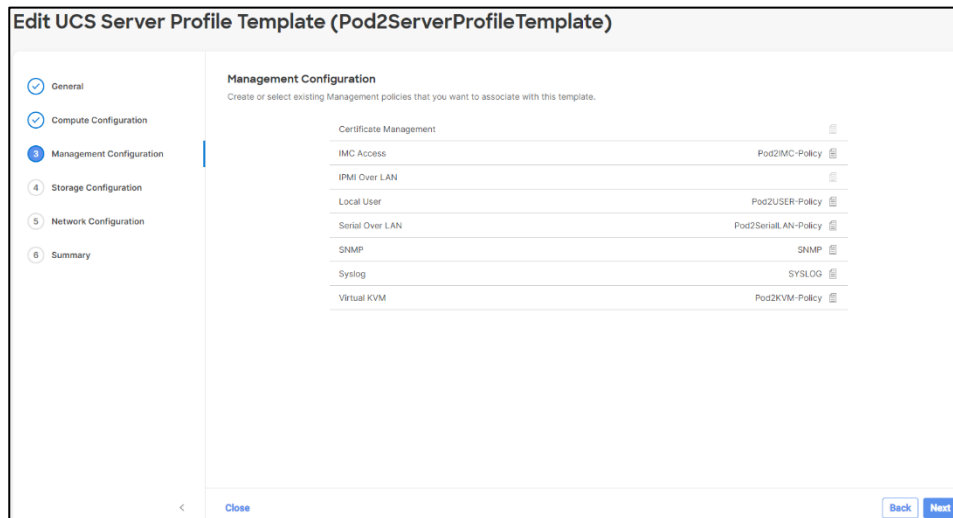


Step 3 On the **Compute Configuration** page, select the **UUID pool** for your pod and the corresponding policies you previously created for **BIOS**, **Boot Order**, **Power**, and **Virtual Media** and click **Next**.



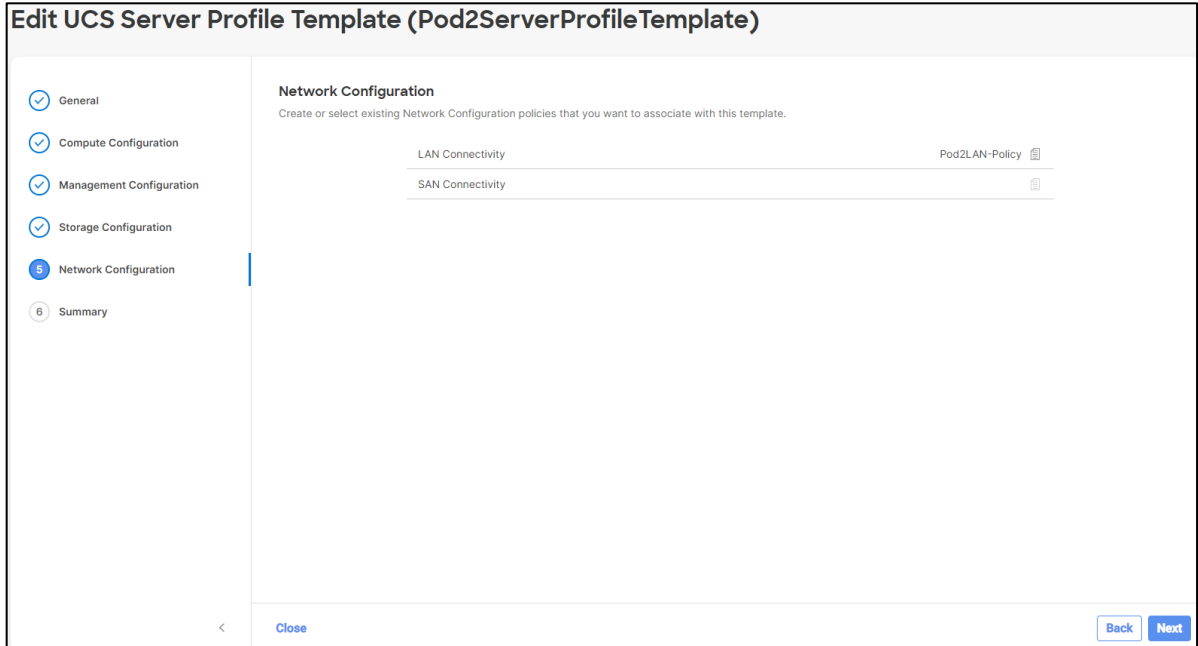
Step 4 Continue to select the corresponding policies that you previously created and then click **Next**.

NOTE: We are not going to be using the Certificate Management or IPMI policies.

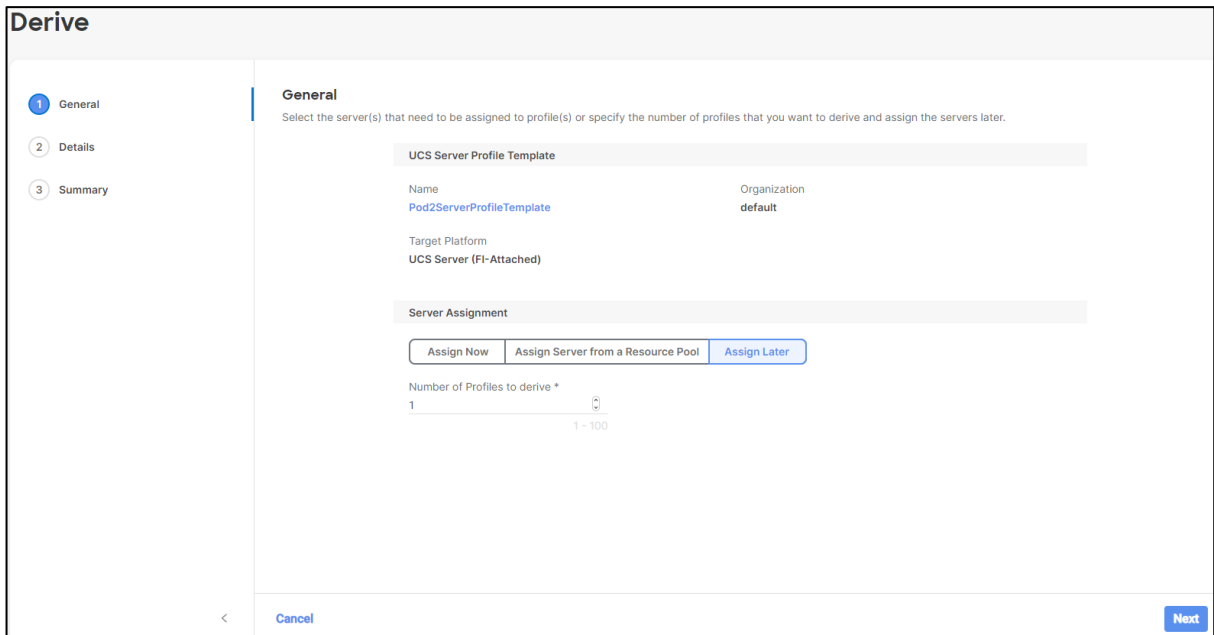


Step 5 Click **Next** on the Storage Configuration screen.

Step 6 On the **Network Configuration** screen, select the **LAN Connectivity** policy that you previously created and then click **Next**.



Step 7 Review your configuration and then click **Derive Profiles**. On the next screen, select **Assign Later** and click **Next**.



Step 8 Accept the defaults on the next screen and then click **Next**.

The screenshot shows the 'Derive' configuration interface with the 'Details' tab selected. On the left, a sidebar lists 'General', 'Details', and 'Summary'. The main area is titled 'Details' and contains a 'General' section with 'Organization *' set to 'default' and 'Target Platform' set to 'UCS Server (FI-Attached)'. Below this is a 'Description' field with a character count of '<= 1024' and a 'Set Tags' link. A 'Derive' section contains a table with one row: '1 Name *' with the value 'Pod2ServerProfileTemplate_DERIVED-1'. At the bottom right, there are 'Back' and 'Next' buttons.

Step 9 Review your configuration and then click **Derive**.

The screenshot shows the 'Derive' configuration interface with the 'Summary' tab selected. The sidebar now has 'General', 'Details', and 'Summary' all checked. The main area is titled 'Summary' and provides a 'Summary of the profiles that need to be derived from the profile template.' It includes a 'General' section with 'Template Name' as 'Pod2ServerProfileTemplate' and 'Organization' as 'default'. Below that, 'Target Platform' is 'UCS Server (FI-Attached)'. A table titled 'UCS Server Profiles' has two columns: 'Name' and 'Assigned Server', with one row showing 'Pod2ServerProfileTemplate_DERIVED-1' and a dash. At the bottom, there are tabs for 'Compute Configuration', 'Management Configuration', 'Storage Configuration', and 'Network Configuration', along with 'Errors/Warnings (0)'. The 'Compute Configuration' tab is active, showing a list of policies: BIOS (Pod2BIOS-Policy), Boot Order (Pod2BOOT-Policy), Power (Pod2Power-Policy), and Virtual Media (Pod2VMedia-Policy). At the bottom right, there are 'Back' and 'Derive' buttons.

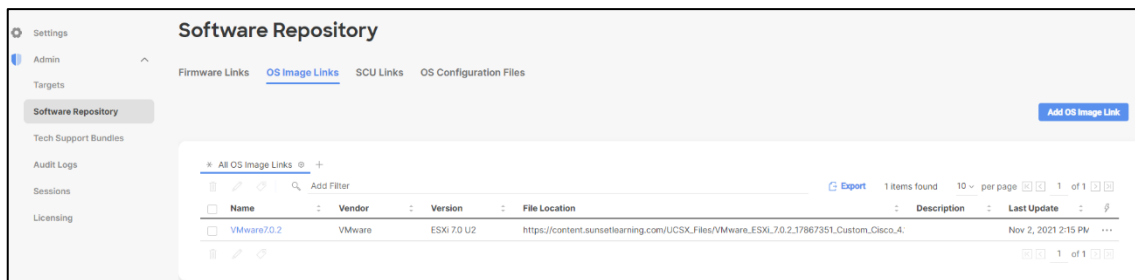
Task 11 has been completed!

Task 12 – Virtual Media Using OS Links

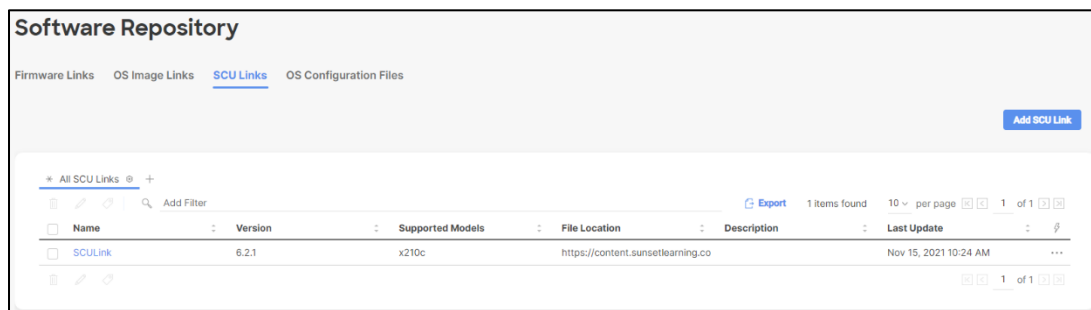
The purpose of this section is to introduce the learning to the concept of using OS links. OS links are used to enable to a remote repository to install an operating system from. We will guide the student to where the OS links are located and then how to use the OS links to do an installation of ESXi.

Procedure

- Step 1** On the left-hand side of the screen, click on **Software Repository** under the **ADMIN** menu. This brings you to the area of the dashboard that is used to map remote
- Step 2** On the top of the page, you will see links to different types of ISOs (Firmware, OS Image, SCU, OS Configuration) that can be used. Click on the **OS Image Links** tab. This will display the available OS ISOs available for mapping.



- Step 3** Click on the **SCU Links** tab to view the available Server Configuration Utility ISOs that are available. These files are used to download the drivers for the selected operating system.



- Step 4** To use these remote file links, click on the **Servers** menu under **OPERATE** on the left navigation pane.
- Step 5** Then click on the ... next to your server and you will see **Install Operating System** option. You will use this option in the next task.

Task 12 has been completed!

Task 13 – Installing VMware ESXi

In this section you will go through the steps of installing ESXi on one of the servers via Intersight.

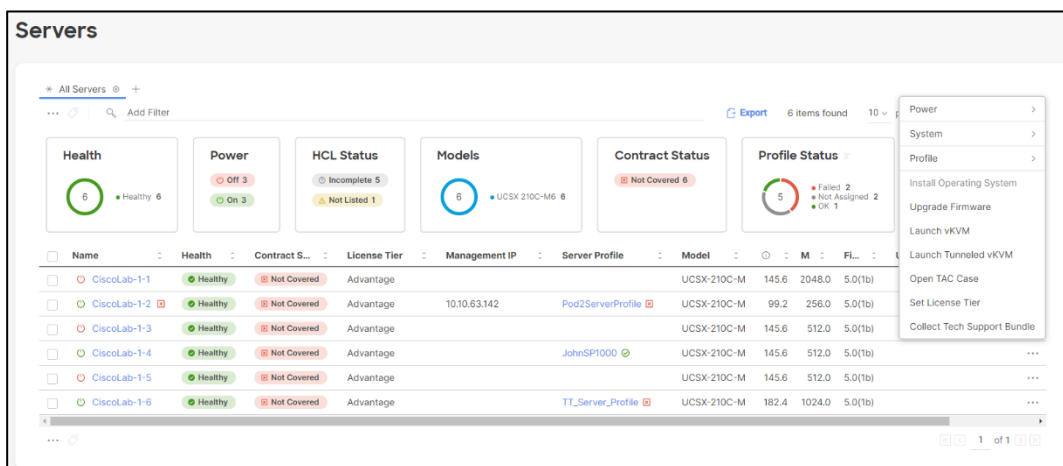
Note: There are two ways to install an operating system on a server:

1. Via Intersight (as shown in this task); and
2. Via the vKVM (as you will do in the next task)

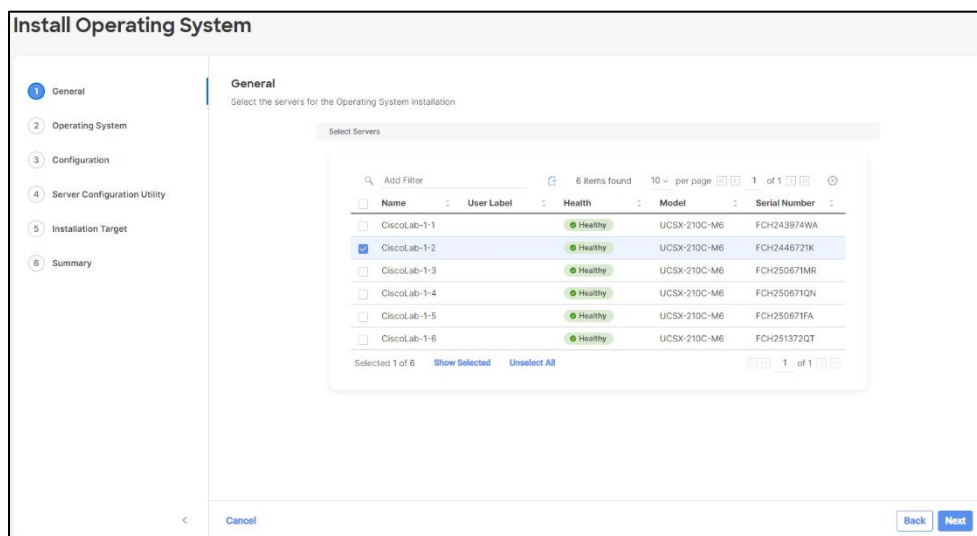
Caution In this task, you will go through the steps to install an OS via Intersight, but you will not perform the actual OS installation. In the next task, you will install the OS via the vKVM on the server.

Procedure

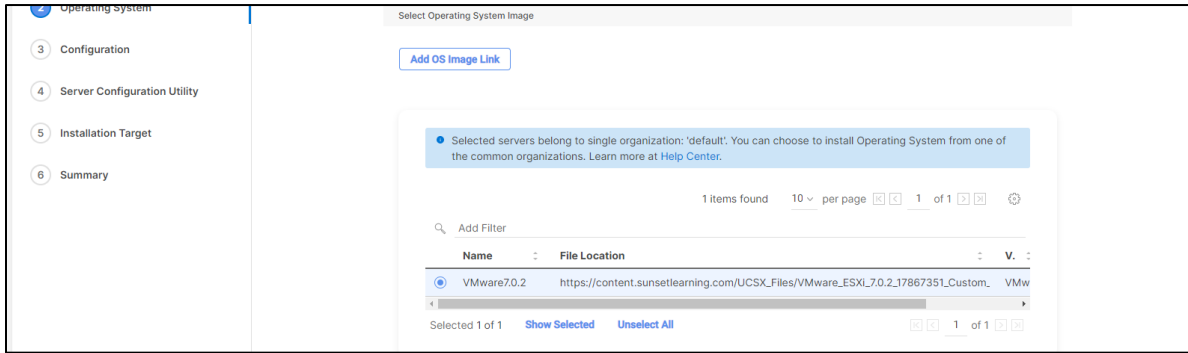
- Step 1** On the left-hand side of the screen, under **OPERATE**, click on **Servers**, and then select the **ellipsis (...)** next to your server. You will see in the drop-down that there is an **Install Operating System** option, select it.



- Step 2** On the **General** screen, ensure that only your server is selected and click **Next**.



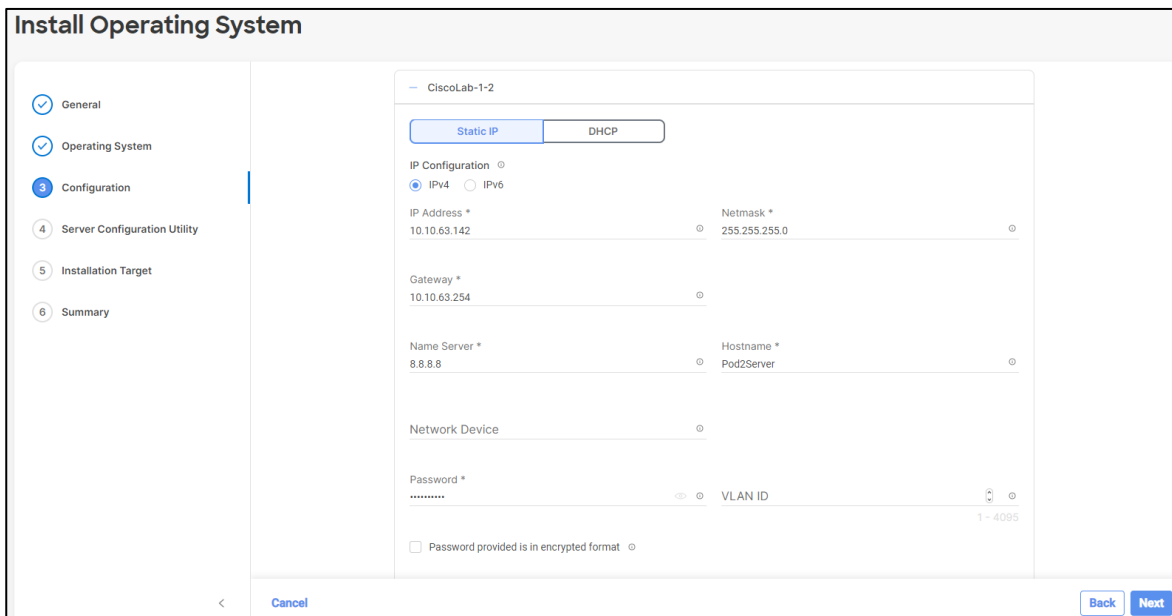
Step 3 Next, you will select the operating system that will be installed on the server. In the list of operating systems, select the **VMware7.0.2** radio button and then click **Next**.



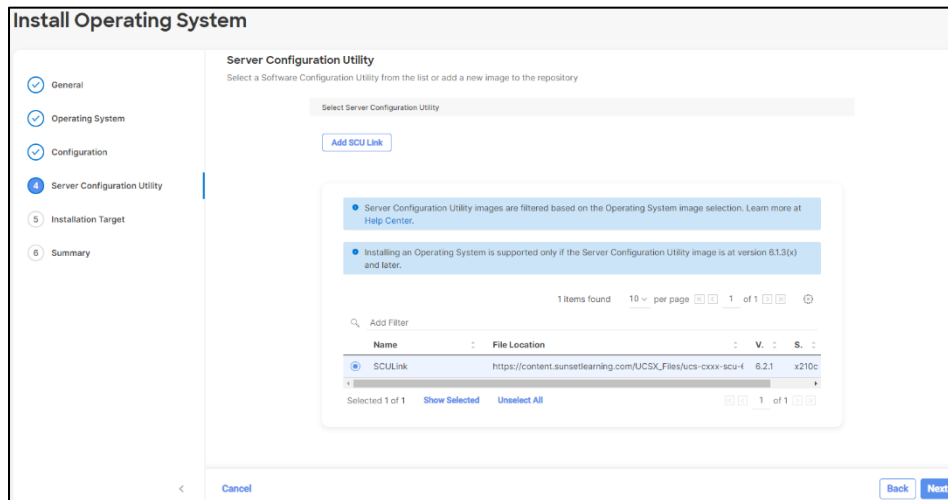
Step 4 Now, you will create the configuration for the server. Click on the + next to your server and fill in the following information:

- Keep **Static IP** selected
- Keep the **IPv4** radio button selected
- IP Address = **10.10.63.14X** (Where X is your Pod number)
- Netmask = **255.255.255.0**
- Gateway = **10.10.63.254**
- Name Server = **8.8.8.8**
- Hostname = **PodXServer** (Where X is your Pod number)
- Password = **Cisco123!!**

Step 5 Click **Next**.

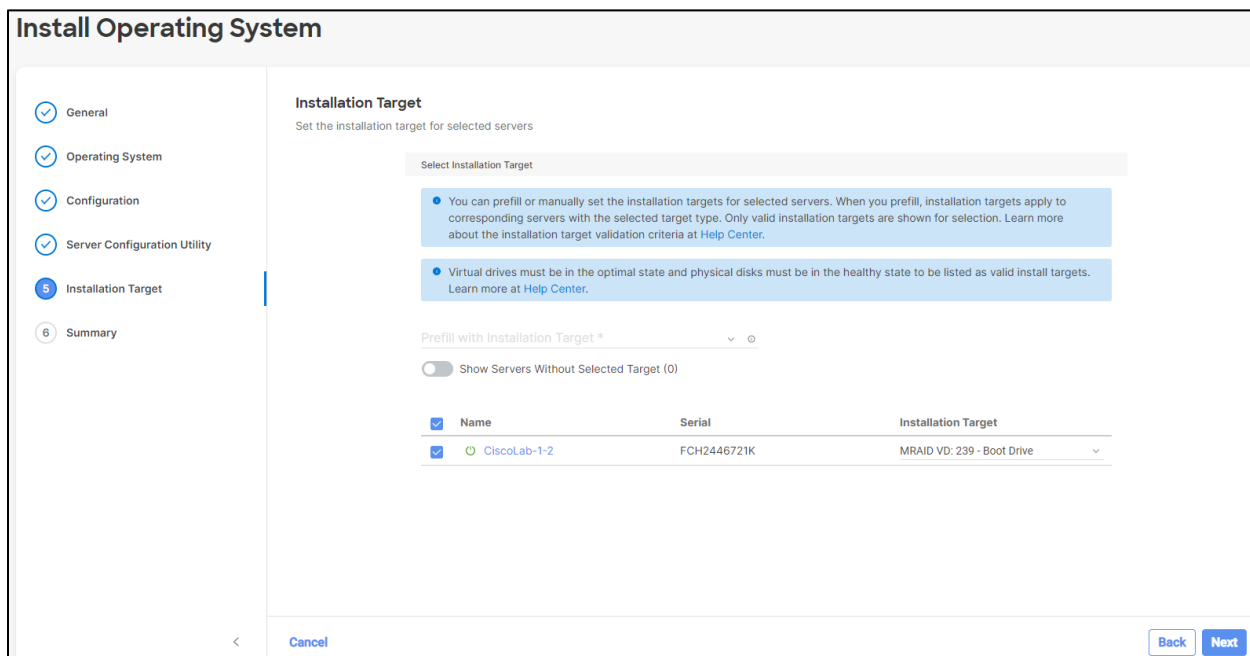


Step 6 On the next page, you will find the SCU link. This is the Server Configuration Utility that is used to download drivers for the operating system during the installation. Select **SCULink** and press **Next**.

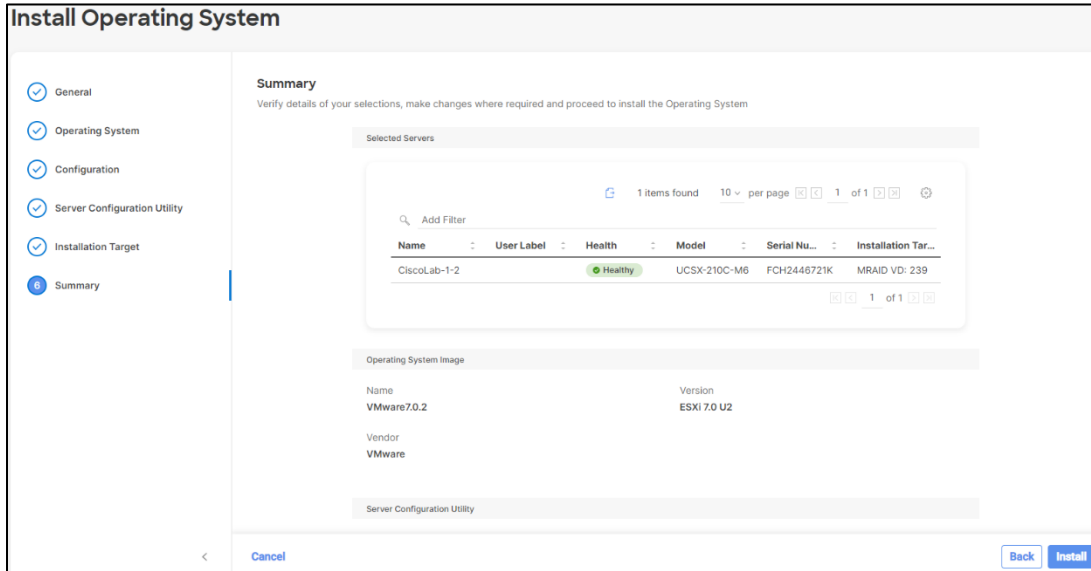


Step 7 On the **Installation Target** screen, you will see a drop-down under **Prefill with Installation Target***. Click the drop-down and select the **MRAID VD** option and then click **Next**.

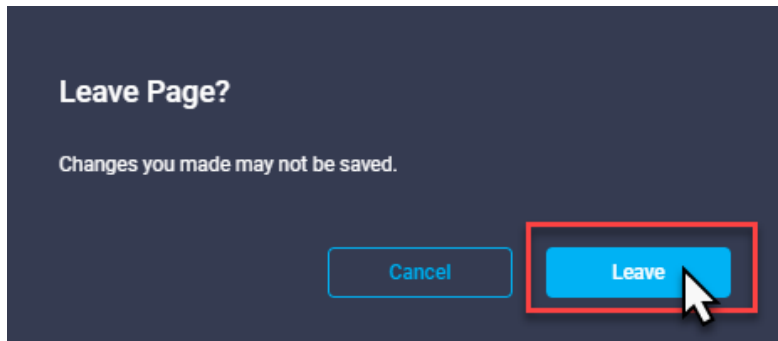
Note: The options shown in the drop-down list may be different from what is shown below. Select the option that includes MRAID VD as part of the name.



Step 8 On the **Summary** screen, review your configuration then click **Cancel** to cancel out of this OS installation.



Step 9 You will receive a pop up stating your changes will not be saved. Click the **Leave** button to leave the OS installation wizard.



Note If you had started the OS install process, you could review the progress of the installation by click on the Requests link at the top of the screen. You should see your installation In Progress and can click on the In Progress entry to get a more detailed view of the installation process.

Task 13 has been completed!

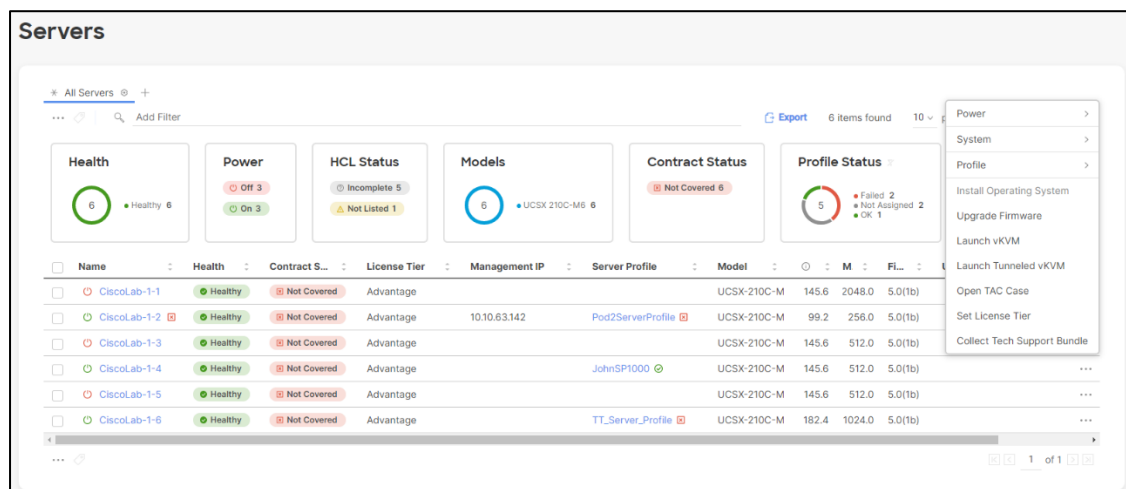
Task 14 – Accessing the KVM and Installing an Operating System (Do Not Attempt)

In this section you will be using the Virtual Media option in the KVM to install an Operating System.

Note: You will need to be connected to the SLI VPN before you can perform this task.

Procedure

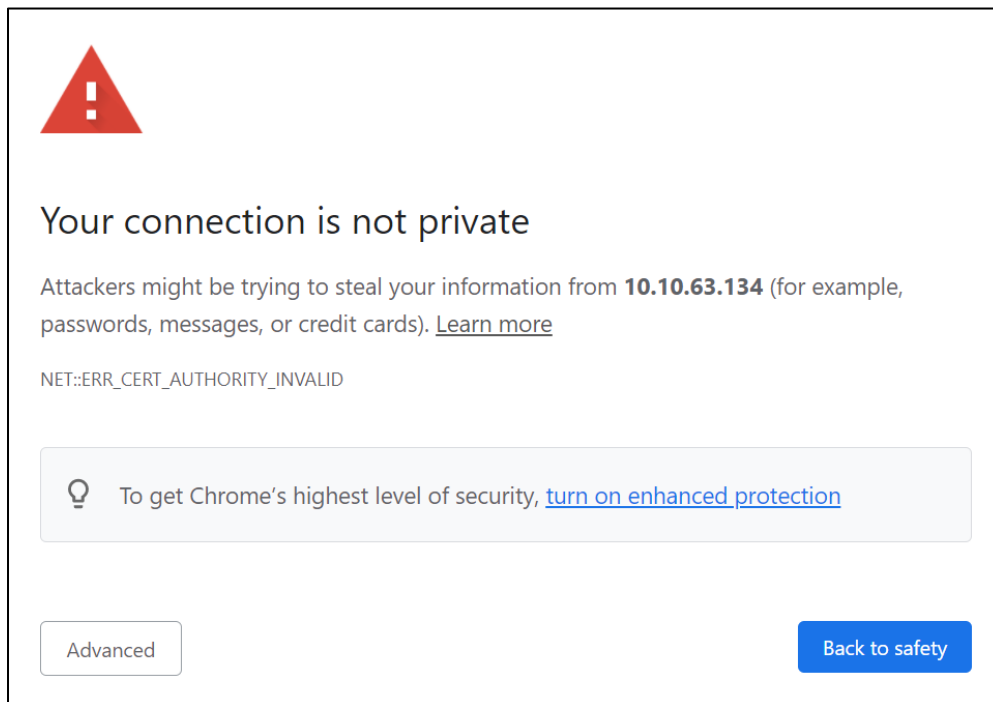
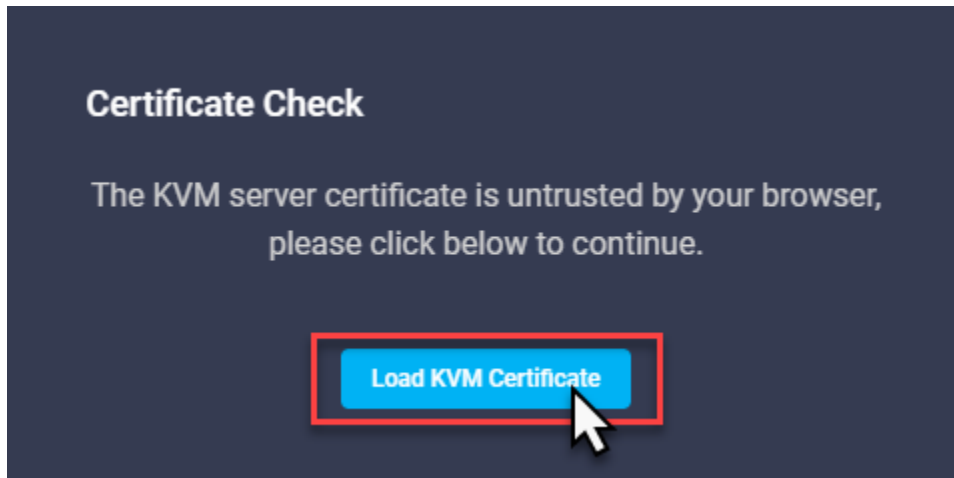
Step 1 On the left-hand side of the screen, under **OPERATE**, click on **Servers**, and then select the **ellipsis (...)** next to your server. You will see in the drop-down that there is a Launch **KVM** option, select it.



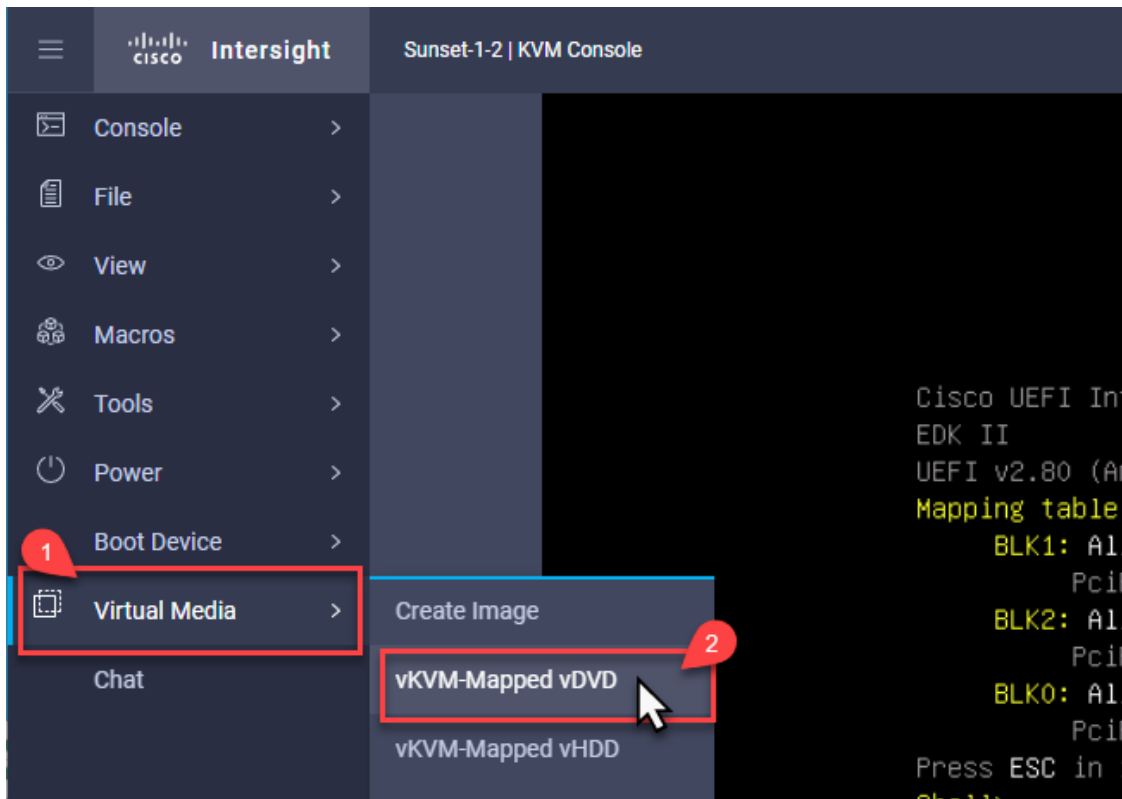
The screenshot displays the 'Servers' management page. At the top, there are summary cards for Health (6 Healthy), Power (3 Off, 3 On), HCL Status (5 Incomplete, 1 Not Listed), Models (6 UCSX 210C-M6), Contract Status (6 Not Covered), and Profile Status (5 total: 2 Failed, 2 Not Assigned, 1 OK). Below these is a table of servers with columns for Name, Health, Contract S..., License Tier, Management IP, Server Profile, Model, M, and FI... The table lists six servers, all with a 'Healthy' status and 'Advantage' license tier. A context menu is open over the first server, 'CiscoLab-1-1', showing options such as 'Power', 'System', 'Profile', 'Install Operating System', 'Upgrade Firmware', 'Launch vKVM', 'Launch Tunneled vKVM', 'Open TAC Case', 'Set License Tier', and 'Collect Tech Support Bundle'. The 'Launch vKVM' option is highlighted.

Name	Health	Contract S...	License Tier	Management IP	Server Profile	Model	M	FI...
CiscoLab-1-1	Healthy	Not Covered	Advantage			UCSX-210C-M	145.6	2048.0
CiscoLab-1-2	Healthy	Not Covered	Advantage	10.10.63.142	Pod2ServerProfile	UCSX-210C-M	99.2	256.0
CiscoLab-1-3	Healthy	Not Covered	Advantage			UCSX-210C-M	145.6	512.0
CiscoLab-1-4	Healthy	Not Covered	Advantage		JohnSP1000	UCSX-210C-M	145.6	512.0
CiscoLab-1-5	Healthy	Not Covered	Advantage			UCSX-210C-M	145.6	512.0
CiscoLab-1-6	Healthy	Not Covered	Advantage		TT_Server_Profile	UCSX-210C-M	182.4	1024.0

Step 2 A new window will pop up with a button that says **Load KVM Certificate**, click that button. You may get a security warning. Accept the security warning to display the KVM.

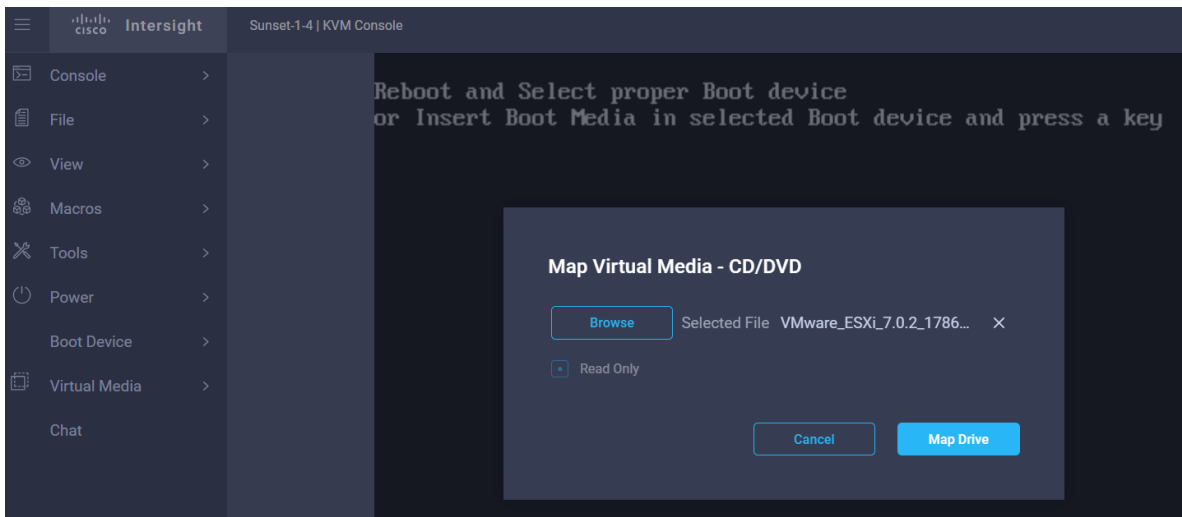


Step 3 When the KVM loads, click on the **Virtual Media** menu option, and select **vKVM-mapped vDVD** option. This will bring up the option to **browse** for the installation ISO file.

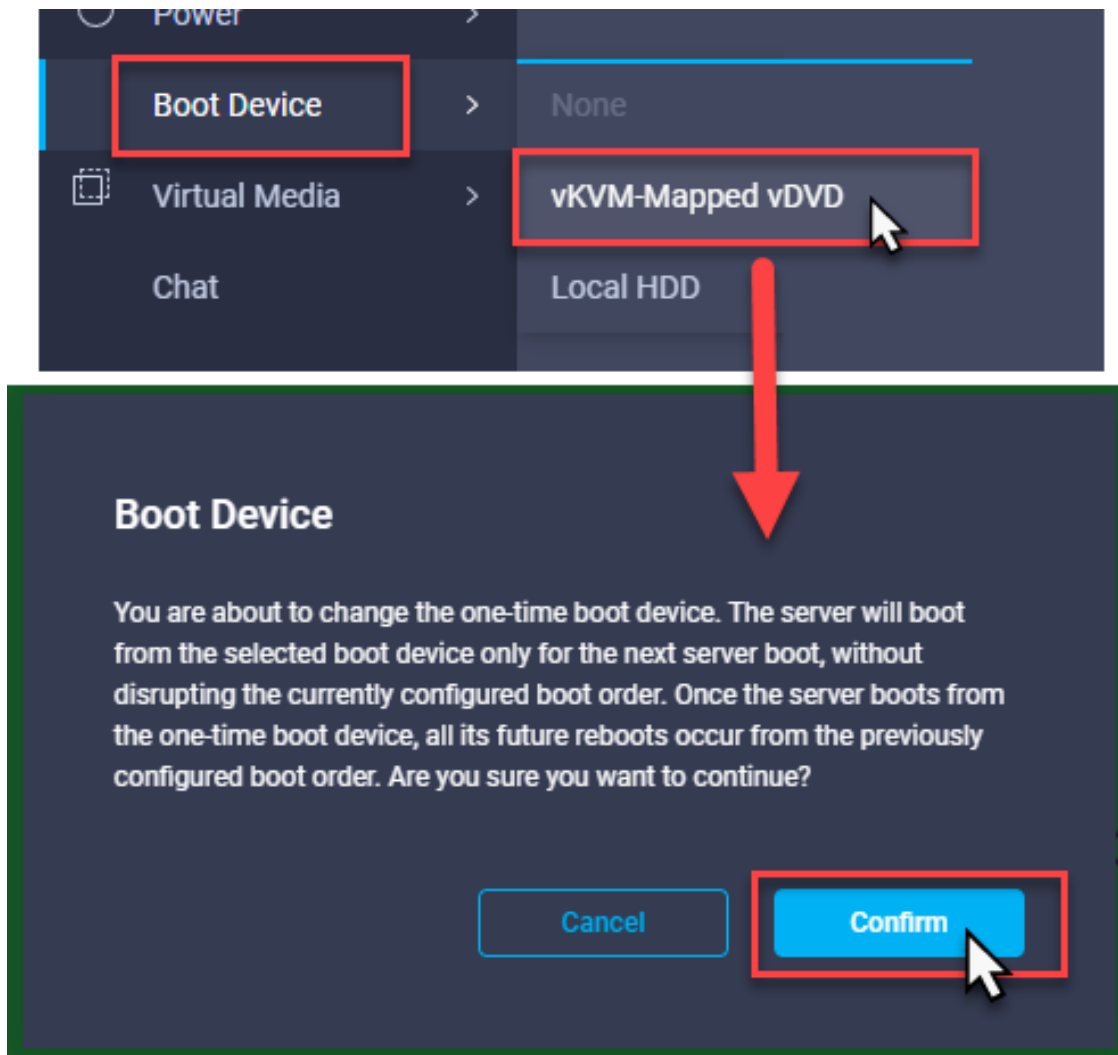


NOTE: If the instructor has not already provided the link, please ask them for it now.

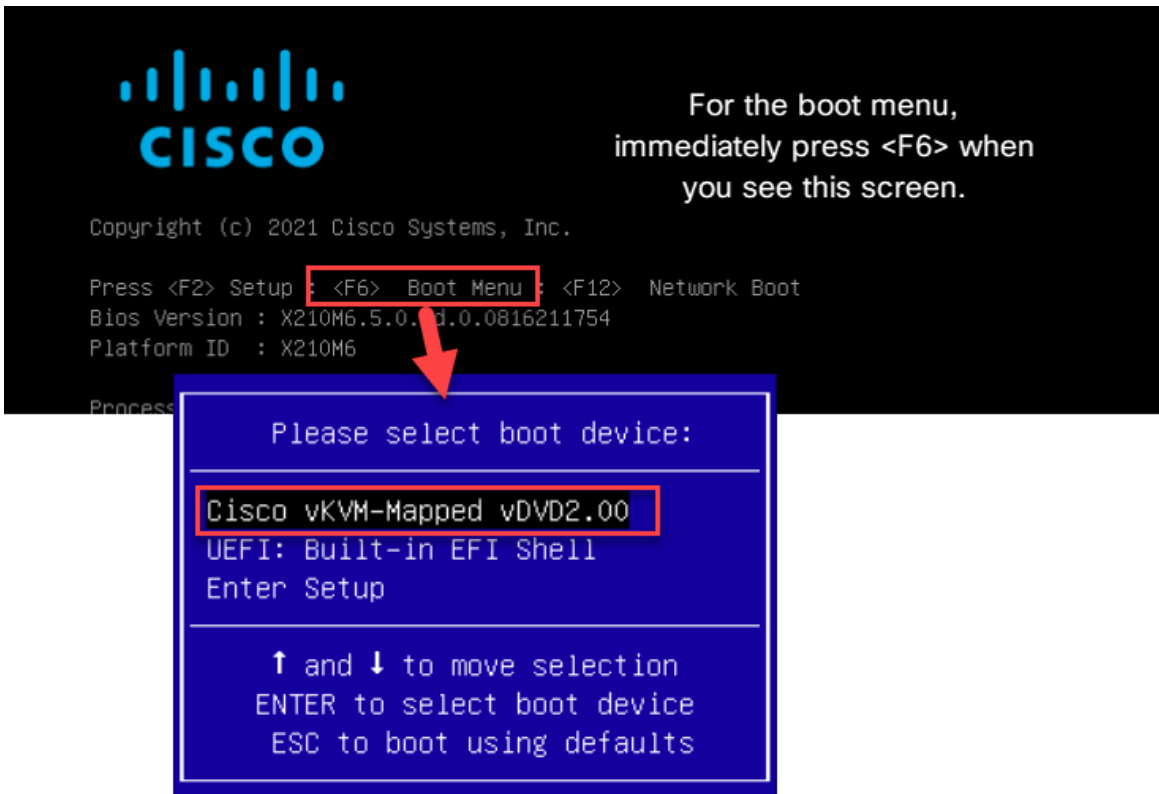
Step 4 Click **Browse** and select the VMware ISO file. Then click **Map Drive**.



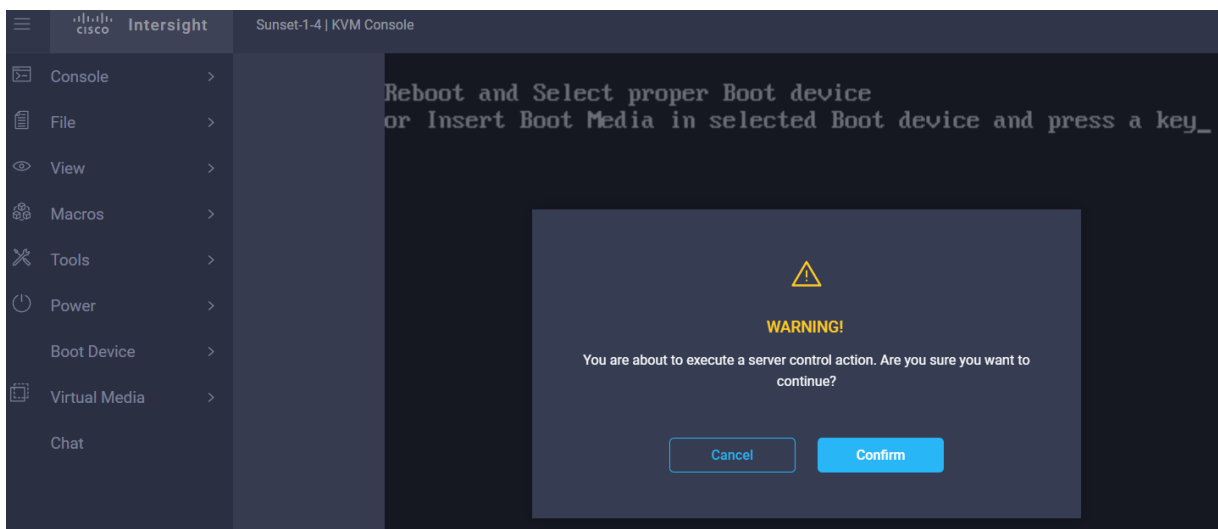
Step 5 Click on the **Boot Device** menu option. Select **vKVM-Mapped vDVD** from the select list. Then read the **Boot Device** message and click **Confirm** to confirm your choice.



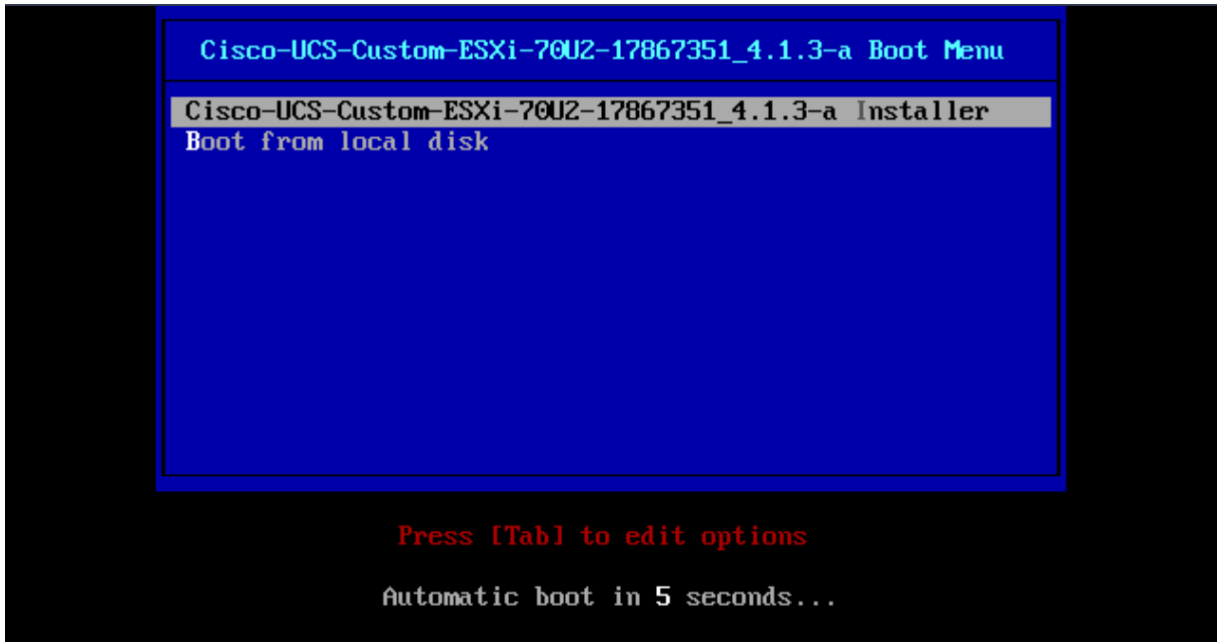
Step 6 Another way to boot from the virtual media is to reset the server, and after the RAID controller BIOS message completes, press <F6> for the Boot Menu. You can select **Cisco kVM-Mapped vDVD2.00** from there.

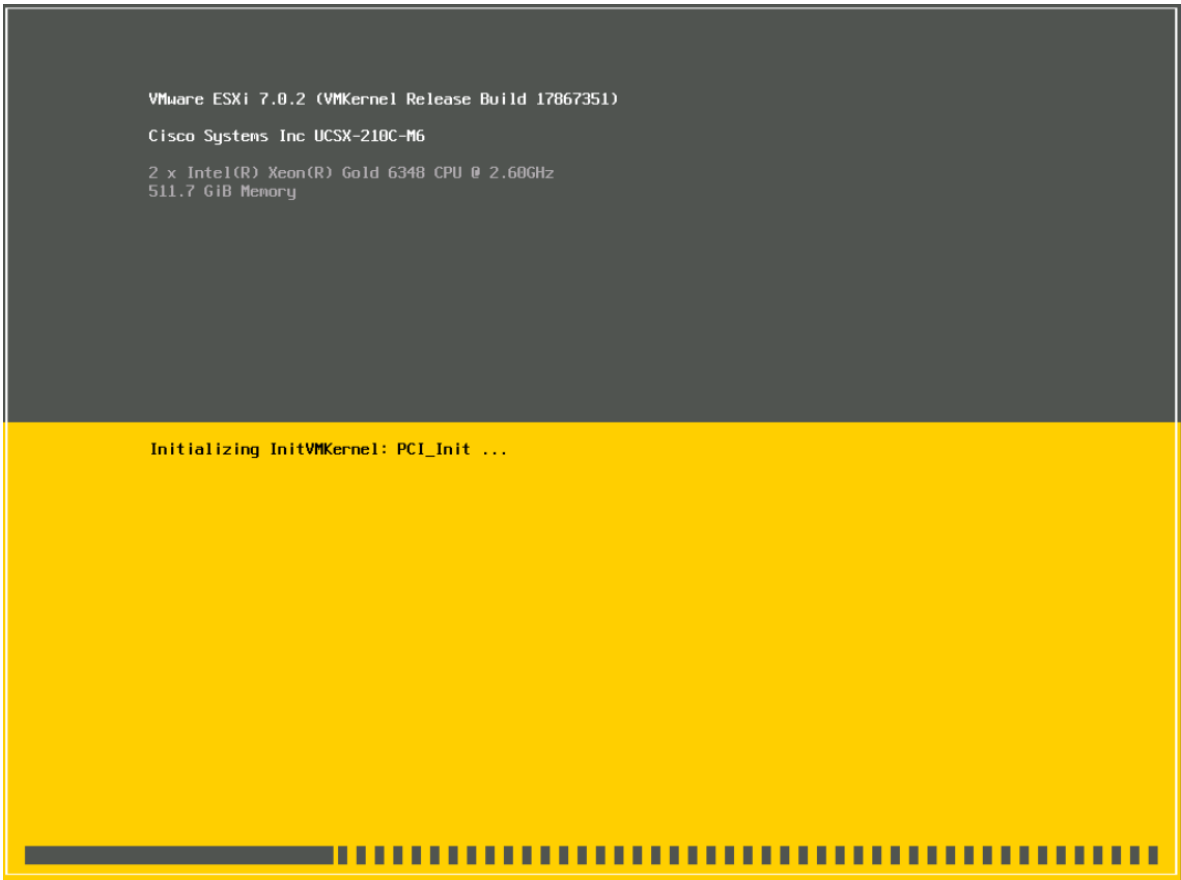


Step 7 To get the installation going, you will need to reset the server. Select the **Power** menu option and then click on **Reset System**. Confirm the warning message by clicking **Confirm**.



- Step 8** The server should automatically boot the installation ISO and begin the installation process.

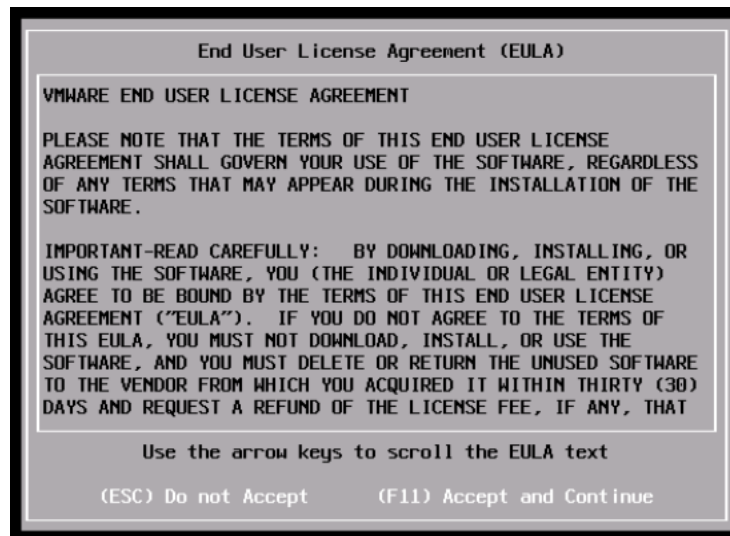




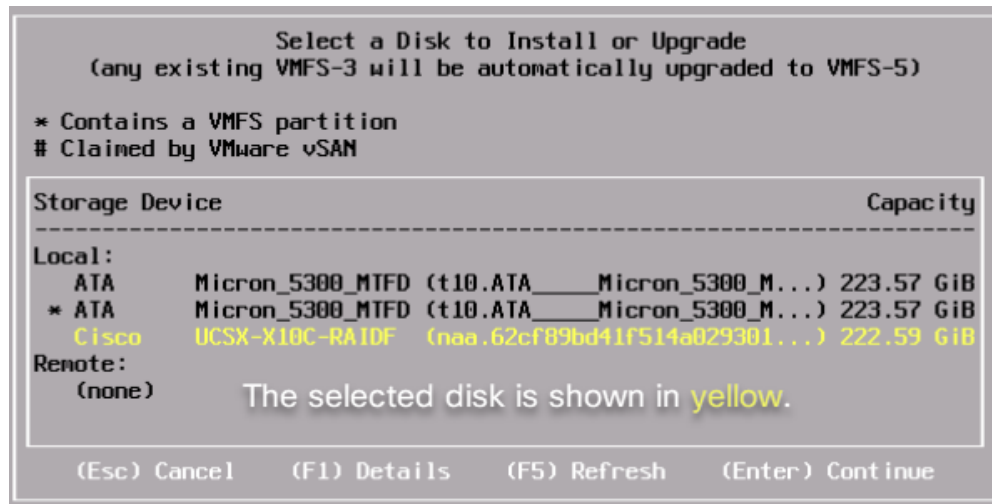
Step 9 Please wait several minutes for the installation ISO to load the installer. You will then be prompted to continue the installation; press **Enter** to continue.



Step 10 Accept the EULA by pressing **F11**.



Step 11 Next, you will be presented with the installation location. Ensure that the **RAIDF** option is selected, and then press **Enter**.



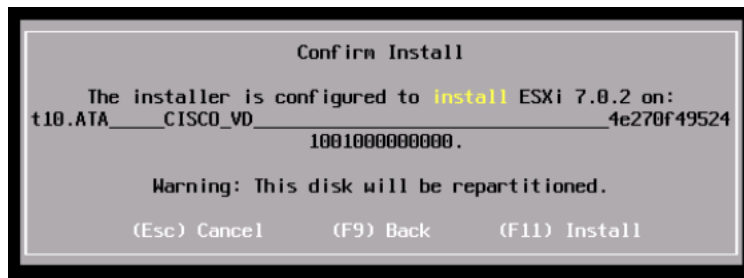
Step 12 You will then be asked to select the language. Select the **US Default** and press **Enter**.



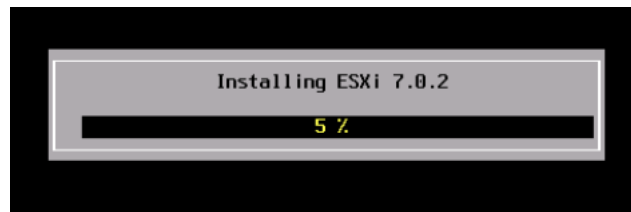
Step 13 Now you will create the password for root console access to the server. Use the password of **Cisco123!!** and confirm it before pressing **Enter** to continue.



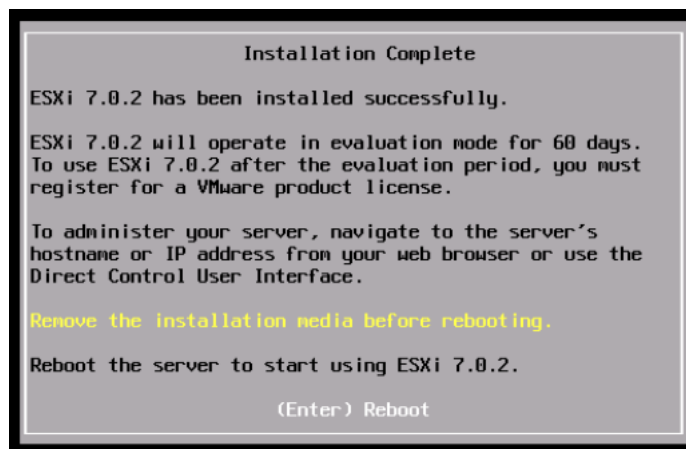
Step 14 The last step is to confirm the installation options and press **F11** to install.



Step 15 The installation should begin.



Step 16 The last step of the installation is to reboot the server. Press **Enter** to reboot the server.



Step 17 Observe the boot up process and ensure that the login screen is displayed before moving forward.

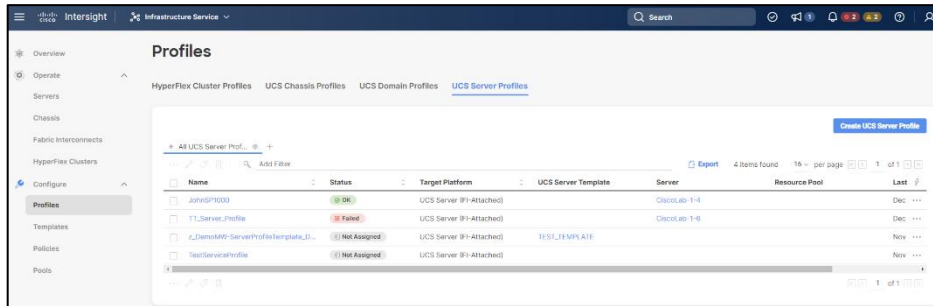
Task 14 has been completed!

Task 15 – Server Profile Deployment (Do Not Attempt)

In this section, you will create and deploy a Server Profile to an available server using the policies and pools we have previously created.

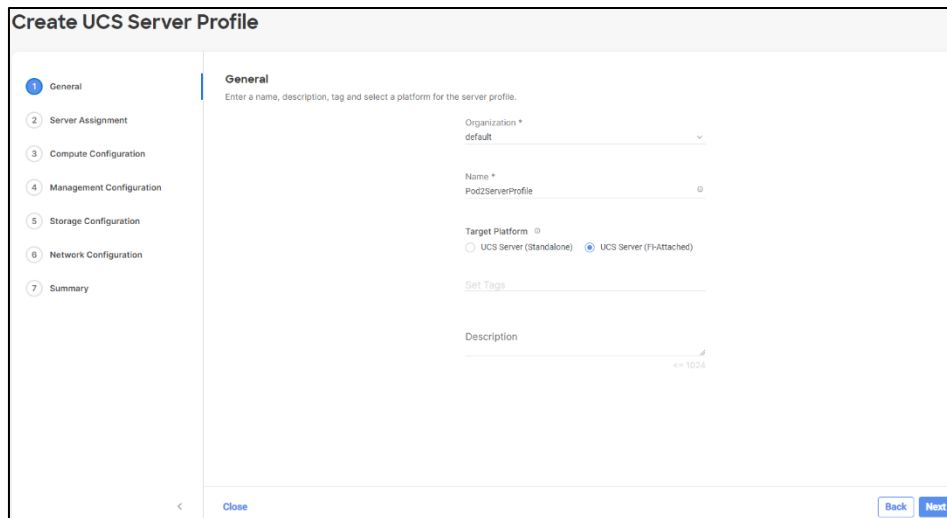
Procedure

Step 1 On the left-hand side of the screen, under **CONFIGURE**, select **Profiles**. Then click on the **UCS Server Profiles** tab.



Step 2 Click on the **Create UCS Server Profile** button.

Step 3 Name the Server Profile **PodXServerProfile**, where X is your pod number and ensure that the **UCS Server (FI-Attached)** radio button is highlighted. Then click **Next**.



Step 4 Select the server that corresponds to your Pod X and click **Next**.

Create UCS Server Profile

Server Assignment
Choose to assign a server now, from a resource pool, or later.

Click the appropriate button to assign a server now, from a resource pool, or later. If you choose to assign a server now, select the server, click Next, and select and attach policies to the server profile.

Name	User Label	Health	Model	UCS Domain	Serial Nu...
<input type="radio"/> CiscoLab-1-1		Healthy	UCSX-210C-M6	CiscoLab	FCH243974WA
<input checked="" type="radio"/> CiscoLab-1-2		Healthy	UCSX-210C-M6	CiscoLab	FCH2446721K
<input type="radio"/> CiscoLab-1-3		Healthy	UCSX-210C-M6	CiscoLab	FCH250671MR
<input type="radio"/> CiscoLab-1-5		Healthy	UCSX-210C-M6	CiscoLab	FCH250671FA

Selected 1 of 4

Step 5 Select the **UUID Pool** you created earlier and select the corresponding **BIOS**, **BOOT FROM SAN POLICY**, **Power**, and **Virtual Media** policies that you previously created. Then click **Next**.

Compute Configuration
Create or select existing Compute policies that you want to associate with this profile.

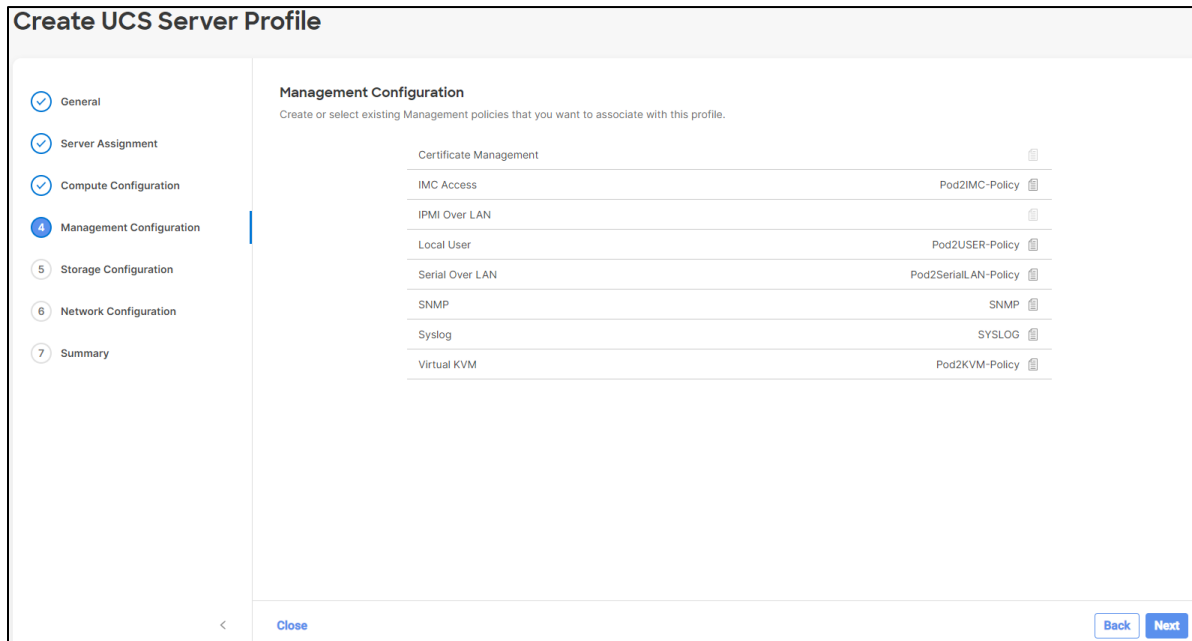
UUID Assignment

UUID Pool
Selected Pool Pod2UUID-Pool | × | eye | edit

BIOS	Pod2BIOS-Policy
Boot Order	Pod2BFS-BOOT
Power	Pod2Power-Policy
Virtual Media	Pod2VMedia-Policy

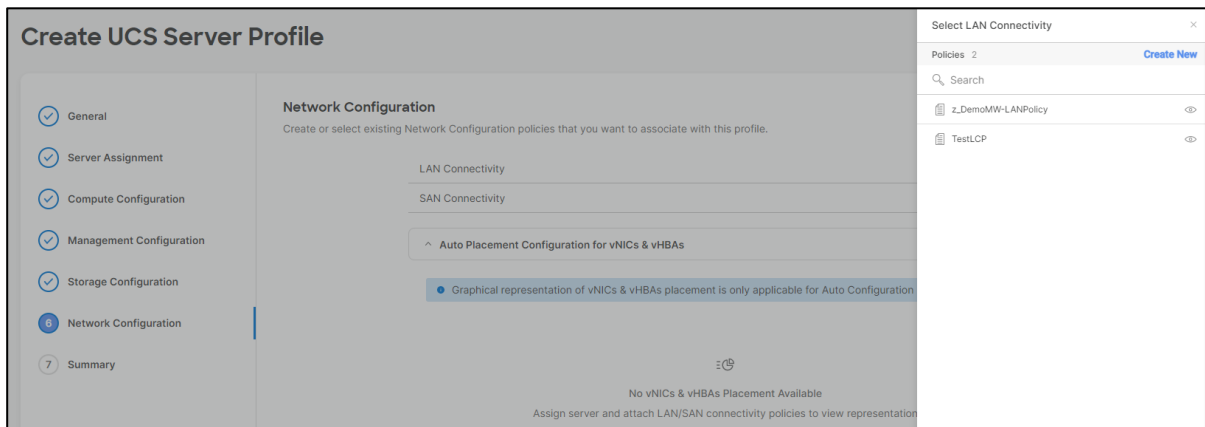
Step 6 Continue to select the corresponding policies that you previously created and then click **Next**.

NOTE: We are not going to be using the Certificate Management or IPMI policies.



Step 7 Skip the Storage Configuration by clicking **Next**.

Step 8 Click on **Select Policy** to the right of **LAN Connectivity** and then select **Create New**.



Step 9 Name the policy **PodXLAN-Policy**, where X is your pod number and click **Next**.

Step 10 Make sure you select the **Auto vNICs Placement** option and then click on **Add vNIC**.

Policy Details
Add policy details

Enable Azure Stack Host QoS

IQN

None Pool Static

This option ensures the IQN name is not associated with the policy

vNIC Configuration

Manual vNICs Placement Auto vNICs Placement

For auto placement option the vNICs will be automatically distributed between adaptors during profile deployment. Learn more at [Help Center](#)

Add vNIC

0 items found 50 per page 0 of 0

Name	Switch ID	Failover	Pin Group	MAC Pool
NO ITEMS AVAILABLE				

Cancel Back Create

Step 11 Name the vNIC **PodX-vNIC0**, where X is your pod number. For the MAC address pool, select the pool you previously created.

General

Name *
Pod2-vNIC0 Pin Group Name

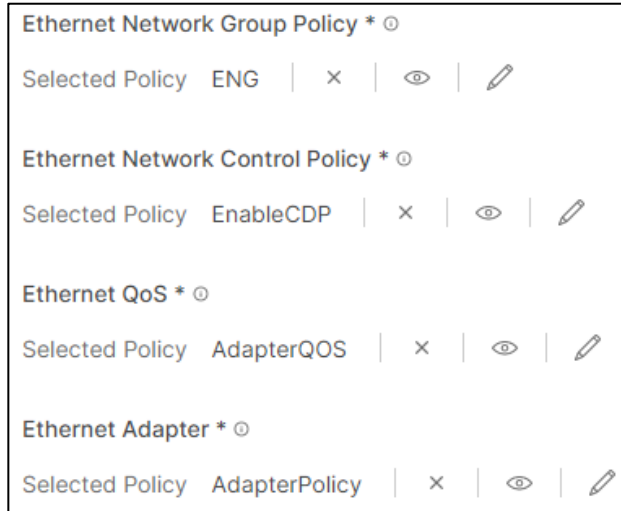
MAC

Pool Static

MAC Pool *
Selected Pool Pod2MAC-Pool

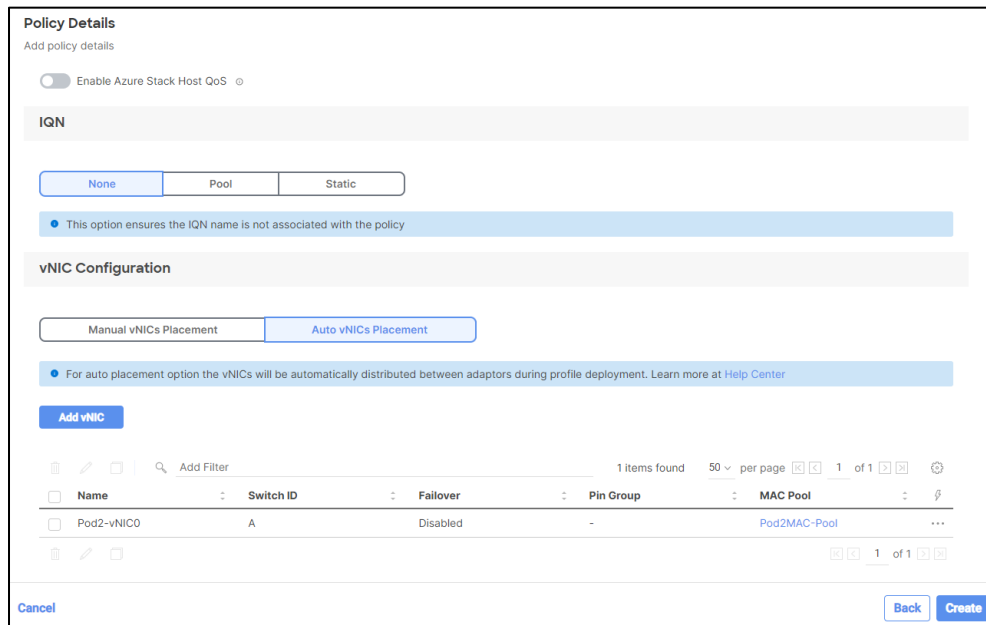
Step 12 Scroll down the page. For the required policies, select the following:

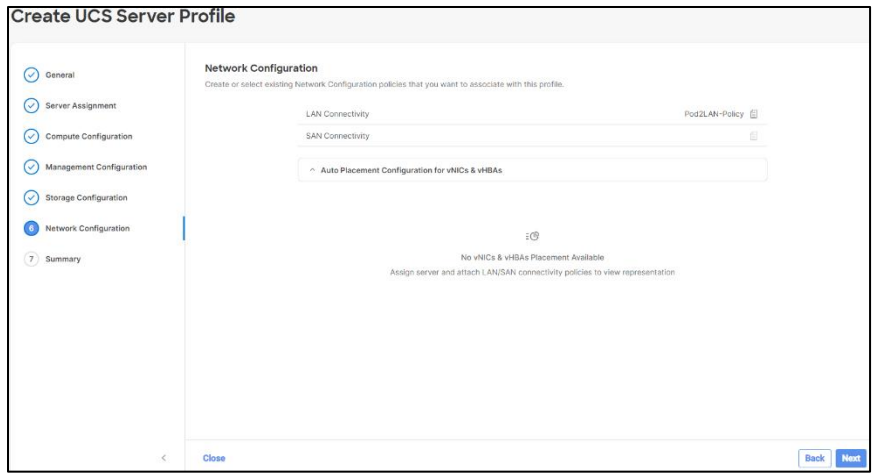
- Ethernet Network Group Policy: **ENG**
- Ethernet Network Control Policy: **EnableCDP**
- Ethernet QoS Policy: **AdapterQoS**
- Ethernet Adapter: **AdapterPolicy**



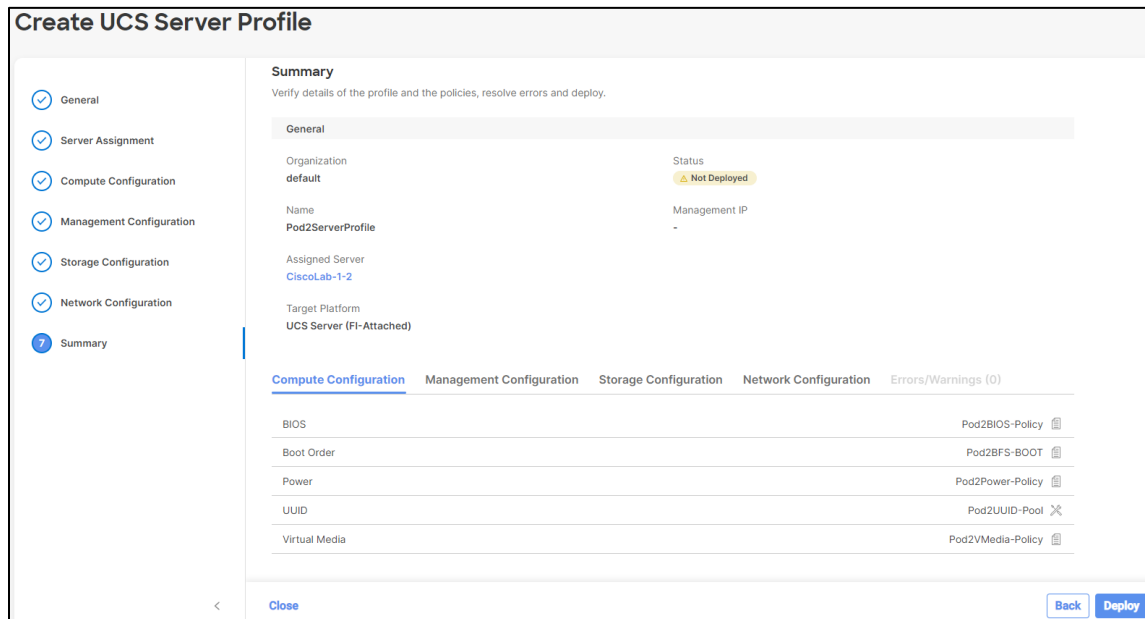
Step 13 Click **Add**.

Step 14 On the next screen click **Create**. And on the following screen, click **Next**.





Step 15 Review your configuration. Click on the **Network Configuration** tab to see a graphical view of your vNIC configuration. When you are done reviewing, click **Deploy**. When asked to confirm, verify that you are deploying to the server for your pod, then click **Deploy** again.



Step 16 Once the Server Profile deploys, the compute node will boot to a SAN device as an available option to install on. This is the FC NetApp Storage array. Please use that as the installation location for the ESXi OS.

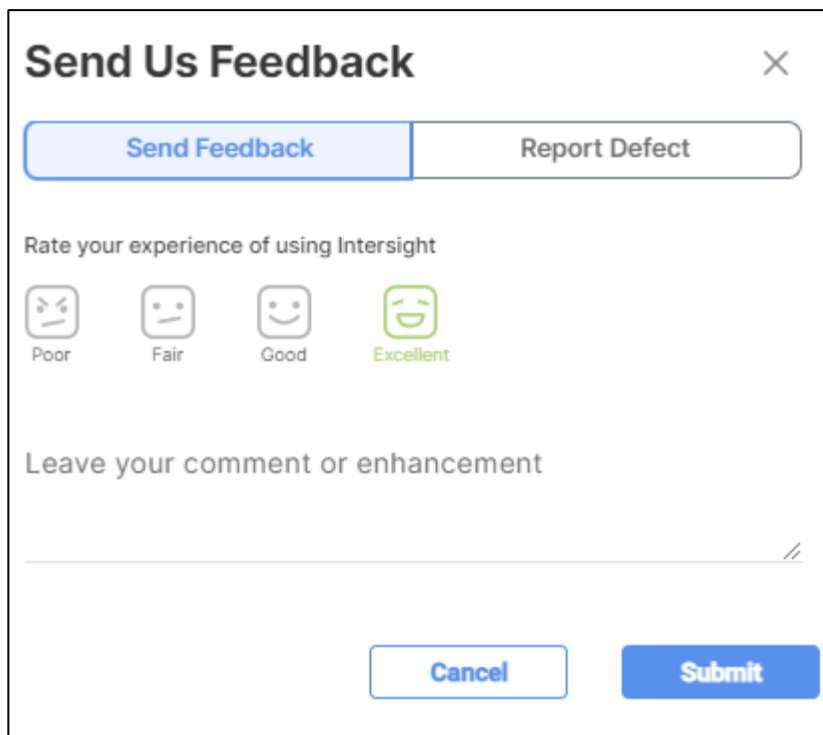
Task 10 has been completed!

Task 16 – Submitting Feedback and Further Information

The Feedback form is the Cisco Intersight user's primary means of communication with the Cisco engineering team. It is used to submit feedback, request feature enhancements, and report issues.

Procedure

- Step 1** In the top toolbar of the Cisco Intersight dashboard, click the **Help** icon and then, select **Send Us Feedback** from the resulting menu.
- Step 2** Briefly show the form then, explain its purpose and then, click **Cancel**.



The screenshot shows a modal dialog box titled "Send Us Feedback" with a close button (X) in the top right corner. At the top, there are two buttons: "Send Feedback" (highlighted in blue) and "Report Defect". Below these buttons, the text "Rate your experience of using Intersight" is displayed. Underneath, there are four smiley face icons representing different rating levels: "Poor" (frowning), "Fair" (neutral), "Good" (smiling), and "Excellent" (wide smiling, highlighted in green). Below the rating options is a text input field with the placeholder text "Leave your comment or enhancement". At the bottom of the dialog, there are two buttons: "Cancel" and "Submit".

What's Next

For More Information

For more information on Cisco UCS Cisco Intersight, visit the following websites:

[cisco.com/go/Cisco Intersight](https://cisco.com/go/Cisco%20Intersight)

[https://Cisco Intersight.com](https://Cisco%20Intersight.com)

communities.cisco.com/ucs

How to Find Support Information

The purpose of this section is to show where to locate the latest support information for Cisco Intersight. Click the links below:

[https://Cisco Intersight.com/help/](https://Cisco%20Intersight.com/help/) <https://Cisco>

[Intersight.com/help/supported_systems](https://Cisco%20Intersight.com/help/supported_systems)