# Setting Up Fabric Interconnects



## Initial Fabric Interconnect Configuration

The initial configuration for a Fabric Interconnect can be done by using the serial console when the Fabric Interconnect boots for the first time. This can happen either during factory install, or after the existing configuration is cleared. The configuration wizard enables you to select the management mode and other parameters such as the administrative subnet, gateway, and DNS IP addresses for each Fabric Interconnect. For the management mode, you can choose whether you want to manage the Fabric Interconnect through Cisco UCS Manager or Cisco Intersight.

You can change the management mode for the Fabric Interconnects between Cisco Intersight and Cisco UCS Manager. However, this is a disruptive process because it will cause all endpoint configurations to be reset, and will result in the loss of the current configuration.

**Note** All the discovered servers, chassis, and Fabric Extenders (FEX) must be decommissioned before changing the management mode.

The erase configuration option, which is available in both management modes, allows you to clear the existing configuration and reboot the Fabric Interconnects. After the Fabric Interconnects are rebooted, the initial configuration screen appears, and you can configure the Fabric Interconnects with the appropriate management mode.

This configuration process is valid for Cisco UCS 6400 Series Fabric Interconnects and Cisco UCS 6500 Series Fabric Interconnects in a cluster setup.

**Note** Cisco UCS 6500 Series Fabric Interconnects support UCSM Managed Mode (UMM) from firmware version 4.2(3b) onwards.

To configure the Fabric Interconnects in a cluster:

1. Configuring Fabric Interconnect-A Using the Console
2. Configuring Fabric Interconnect-B Using the Console

After completing the initial configuration of the Fabric Interconnects, you must claim them for use with the Cisco Intersight platform. For more information about claiming devices in Cisco Intersight, see Target Claim in Intersight Managed Mode.

After you claim the Fabric Interconnects, they appear in the list of available devices. The device type for Fabric Interconnects managed through Cisco Intersight is **Intersight Managed Domain**. The **Device IP** field shows the IP addresses of both the Fabric Interconnects, and the **Device ID** field shows the serial numbers of both the Fabric Interconnects. The Fabric Interconnects now appear in the **Fabric Interconnects** table view.

After you claim the Fabric Interconnects, you must configure the ports on the Fabric Interconnect to discover the connected chassis and servers. For each Fabric Interconnect, you can view the properties, and an inventory of its components, including ports, fan modules, and power supply units (PSUs).

# Configuring Fabric Interconnect-A Using the Console

**Step 1** Connect to the console port.

**Step 2** Power on the Fabric Interconnect.
You will see the power-on self-test messages as the Fabric Interconnect boots.

**Step 3** When the unconfigured system boots, it prompts you for the setup method to be used. Enter **console** to continue the initial setup using the console CLI.

**Step 4** Enter the management mode for the Fabric Interconnect:

- **intersight** to manage the Fabric Interconnect through Cisco Intersight
- **ucsm** to manage the Fabric Interconnect through Cisco UCS Manager

**NOTE:**

- Standalone option is not supported in the Intersight Managed Mode.
- If the Fabric Interconnect is an Intersight Managed Mode only Fabric Interconnect, which is the default mode, then you can select No and choose the required one.

**Step 5** Enter **y** to confirm that you want to continue the initial setup.

**Step 6** To use a strong password, enter **y**

**Step 7** Enter the password for the admin account. For more details, see Fabric Interconnect Password Guidelines.

**Step 8** To confirm, re-enter the password for the admin account.

**Step 9** Enter **yes** to continue the initial setup for a cluster configuration.

**Step 10** Enter the Fabric Interconnect fabric (either **A** or **B** ).

**Step 11** Enter the system name.

**Step 12** Enter the IPv4 or IPv6 address for the management port of the Fabric Interconnect.

If you enter an IPv4 address, you will be prompted to enter an IPv4 subnet mask. If you enter an IPv6 address, you will be prompted to enter an IPv6 network prefix.

**Step 13** Enter the respective IPv4 subnet mask or IPv6 network prefix, then press **Enter**.

You are prompted for an IPv4 or IPv6 address for the default gateway, depending on the address type you entered for the management port of the Fabric Interconnect.

**Step 14** Enter either of the following:

- IPv4 address of the default gateway
- IPv6 address of the default gateway

**Step 15** Enter the IPv4 or IPv6 address for the DNS server.

The address type must be the same as the address type of the management port of the Fabric Interconnect.

**Step 16** Enter **yes** if you want to specify the default Domain name, or **no** if you do not.

**Step 17** (Optional) Enter the default Domain name.

**Step 18** Review the setup summary and enter **yes** to save and apply the settings, or enter **no** to go through the setup again to change some of the settings.

If you choose to go through the setup again, it provides the values that you previously entered, and the values appear in brackets. To accept previously entered values, press **Enter**.

---

### Example

Here is an example of how to configure Fabric Interconnect-A in Cisco Intersight management mode for a cluster configuration using the console and management addresses:

```
Enter the configuration method (console/gui)?  console
Enter the management mode [ucsm/intersight]? intersight
You have chosen to setup a new Fabric Interconnect in “intersight” managed mode. Continue?
 (y/n): y
Enforce strong password? (y/n) [y]:n

Enter the password for "admin":
Confirm the password for "admin":
```

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

Enter the system name: UCS

Physical Switch Mgmt0 IP address : 15.XX.XX.XX

Physical Switch Mgmt0 IPv4 netmask : 255.255.255.X

IPv4 address of the default gateway : 15.XX.XX.XX

DNS IP address : 15.XX.XX.XX

Configure the default domain name? (yes/no) [n]:

Following configurations will be applied:

Management Mode=intersight
Switch Fabric=A
System Name=UCS-A
Enforced Strong Password=no
Physical Switch Mgmt0 IP Address=15.XX.XX.XX
Physical Switch Mgmt0 IP Netmask=255.255.255.X
Default Gateway=15.XX.XX.XX
Ipv6 value=0
DNS Server=15.XX.XX.XX

Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
Applying configuration. Please wait.

Configuration file - Ok
```

### What to do next

Configure the Fabric Interconnect-B using the console.

# Configuring Fabric Interconnect-B Using the Console

This procedure describes setting up Fabric Interconnect-B using IPv4 or IPv6 addresses for the management port.

**Step 1** Connect to the console port.

**Step 2** Power up the Fabric Interconnect.
You will see the power-on self-test messages as the Fabric Interconnect boots.

**Step 3** When the unconfigured system boots, it prompts you for the setup method to be used. Enter **console** to continue the initial setup using the console CLI.

**Note** Fabric Interconnect-A should detect Fabric Interconnect-B in the cluster. If it does not, check the physical connections between the L1 and L2 ports, and verify that Fabric Interconnect-B has been enabled for a cluster configuration.

**Step 4** Enter **y** to add Fabric Interconnect-B to the cluster.

**Step 5** Enter the admin password of the peer Fabric Interconnect.

**Step 6** Enter the IP address for the management port on Fabric Interconnect-B.

**Step 7** Review the setup summary and enter **yes** to save and apply the settings, or enter **no** to go through the setup again to change some of the settings.

If you choose to go through the setup again, it provides the values you previously entered, and the values appear in brackets. To accept previously entered values, press **Enter**.

### Example

Here is an example of how to configure Fabric Interconnect-B in Cisco Intersight management mode for a cluster configuration using the console and management addresses:

```
Enter the configuration method. (console/gui) ? console

Installer has detected the presence of a peer Fabric interconnect. This Fabric interconnect
 will be added to the cluster. Continue (y/n) ? y


Enter the admin password of the peer Fabric interconnect:
Connecting to peer Fabric interconnect... done
Retrieving config from peer Fabric interconnect... done
Peer Fabric interconnect management mode : intersight
Peer Fabric interconnect Mgmt0 IPv4 Address: 15.XX.XX.XX
Peer Fabric interconnect Mgmt0 IPv4 Netmask: 255.255.255.0

Peer FI is IPv4 Cluster enabled. Please Provide Local Fabric Interconnect Mgmt0 IPv4 Address


Physical Switch Mgmt0 IP address : 15.XX.XX.XX

Local fabric interconnect model(UCS-FI-6454)
Peer fabric interconnect is compatible with the local fabric interconnect. Continuing with
 the installer...

Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
Applying configuration. Please wait.

Configuration file - Ok
```

### What to do next

Claim the Intersight Managed Domain through Cisco Intersight. For more information, see Target Claim in Intersight Managed Mode.

# Configuring Fabric Interconnect-A Using the GUI

*Configuring Fabric Interconnect-A Using GUI*

This procedure describes setting up Fabric Interconnect-A using GUI.

For detailed information on how to configure Fabric Interconnect-A using GUI, see Initial System Setup for a Cluster Configuration.

1. Power on the Fabric Interconnect.

   You will see the power on self-test messages as the Fabric Interconnect boots.

2. If the system obtains a lease, go to step 6, otherwise, continue to the next step.
3. Connect to the console port.
4. At the installation method prompt, enter **`gui`**

   .
5. If the system cannot access a DHCP server, you are prompted to enter the following information:
   - IPv4 or IPv6 address for the management port on the Fabric Interconnect.
   - IPv4 subnet mask or IPv6 prefix for the management port on the Fabric Interconnect.
   - IPv4 or IPv6 address for the default gateway assigned to the Fabric Interconnect.

**Note** In a cluster configuration, both Fabric Interconnects must be assigned the same management interface address type during setup.

6. Copy the web link from the prompt into a web browser and go to the Cisco UCS Fabric Interconnect Setup GUI launch page.

**Note** You can choose between two modes: UCSM Managed and Intersight Managed Fabric Interconnects based on your preferences.

7. In the **Cisco UCS Fabric Interconnect Setup GUI** launch page, select **Express Setup**.
8. In the **Express Setup** page, enter the Fabric Interconnects configuration details.

**Note** From Cisco UCS Manager 4.2(2) onwards, you can choose GUI setup method to configure Fabric Interconnects. If the Fabric Interconnect defaults to Intersight managed mode, you can choose to change during confirmation and select required mode again in console setup method alone.

9. In the **Basic Settings** area:
   - For the **Fabric Setup** option, select **Fabric A**.
   - Select IPv4 or IPv6 address that Cisco Intersight Managed Mode will use.

   and click **Submit**.
10. In the **System Setup** area, complete the following fields:

| Field | Description |
|---|---|
| **Enforce Strong Password** | Choose Yes or No to enforce strong password. |

| Field | Description |
|---|---|
| **System Name** | The name assigned to the Cisco UCS domain.<br>In a standalone configuration, the system adds "-A" to the system name. In a cluster configuration, the system adds "-A" to the Fabric Interconnect assigned to fabric A, and "-B" to the Fabric Interconnect assigned to fabric B. |
| **Admin Password** | The password used for the Admin account on the Fabric Interconnect.<br>Choose a strong password that meets the guidelines for Cisco UCS Manager passwords. This password cannot be blank. |
| **Confirm Admin Password** | The password used for the Admin account on the Fabric Interconnect. |
| **Mgmt IP Address** | The static IPv4 or IPv6 address for the management port on the Fabric Interconnect. |
| **Mgmt IP Netmask** or **Mgmt IP Prefix** | The IPv4 subnet mask or IPv6 prefix for the management port on the Fabric Interconnect.<br>**Note** The system prompts for a **Mgmt IP Netmask** or a **Mgmt IP Prefix** based on what address type you entered in the **Mgmt IP Address**. |
| **Default Gateway** | The IPv4 or IPv6 address for the default gateway assigned to the management port on the Fabric Interconnect.<br>**Note** The system prompts for a **Default Gateway** address type based on what type you entered in the **Mgmt IP Address** field. |
| **DNS Server IP** | The IPv4 or IPv6 address for the DNS Server assigned to the Fabric Interconnect. |
| **Domain Name** | The name of the domain in which the Fabric Interconnect resides. |

**Note**

- For Intersight Managed Mode Fabric Interconnects, DNS is mandatory
- Standalone option is not supported in the Intersight Managed Mode.

11. Click **Submit**.

A page displays the results of your setup operation.

**What to do next**

Configure the Fabric Interconnect-B using the GUI.

# Configuring Fabric Interconnect-B Using the GUI

*Configuring Fabric Interconnect-B Using GUI*

This procedure describes setting up Fabric Interconnect-B using GUI.

You can either follow the procedure below for configuring the Fabric Interconnect-B or watch Cisco UCS Manager Initial Setup part 2.

**Note** When adding a new Fabric Interconnect to an existing High Availability cluster, for example, during a new install or when replacing a Fabric Interconnect, the new device will not be able to log into the cluster as long as the authentication method is set to remote. To successfully add a new Fabric Interconnect to the cluster, the authentication method must be temporarily set to local and the local admin credentials of the primary Fabric Interconnect must be used.

1. Power up the Fabric Interconnect.

   You will see the power-up self-test message as the Fabric Interconnect boots.
2. It the system obtains a lease, go to step 6, otherwise, continue to the next step.
3. Connect to the console port.
4. At the installation method prompt, enter **`gui`**.

   .
5. If the system cannot access a DHCP server, you are prompted to enter the following information:
   - IPv4 or IPv6 address for the management port on the Fabric Interconnect.
   - IPv4 subnet mask or IPv6 prefix for the management port on the Fabric Interconnect.
   - IPv4 or IPv6 address for the default gateway assigned to the Fabric Interconnect.

   **Note** In a cluster configuration, both Fabric Interconnects must be assigned the same management interface address type during setup.
6. Copy the web link from the prompt into a web browser and go to the Cisco UCS Fabric Interconnect Setup GUI launch page.

**Note** You can choose between two modes: UCSM Managed and Intersight Managed Fabric Interconnects based on your preferences.

7. In the **Cisco UCS Fabric Interconnect Setup GUI** launch page, select **Express Setup**.
8. In the **Express Setup** page, enter the Fabric Interconnects configuration details.

**Note** From Cisco UCS Manager 4.2(2) onwards, you can choose GUI setup method to configure Fabric Interconnects. If the Fabric Interconnect defaults to Intersight managed mode, you can choose to change during confirmation and select required mode again in console setup method alone.

9. In the **Basic Settings** area:
   - For the **Fabric Setup** option, make sure **Fabric B** is selected.
10. In the **System Setup** area, enter the password for the Admin account into the **Admin Password of Master** field.

    The **Manager Initial Setup** area is displayed.
11. In the **Manager Initial Setup** area, the field that is displayed depends on whether you configured the first Fabric Interconnect with an IPv4 or IPv6 management address. Complete the field that is appropriate for your configuration, as follows:

| Field | Description |
|---|---|
| **Peer FI is IPv4 Cluster enabled. Please Provide Local Fabric Interconnect Mgmt0 IPv4 Address** | Enter an IPv4 address for the Mgmt0 interface on the local Fabric Interconnect. |
| **Peer FI is IPv6 Cluster Enabled. Please Provide Local Fabric Interconnect Mgmt0 IPv6 Address** | Enter an IPv6 for the Mgmt0 interface on the local Fabric Interconnect. |

12. Click **Submit**.

    A page displays the results of your setup operation.

### What to do next

Claim the Intersight Managed Domain through Cisco Intersight. For more information, go to Target Claim in Intersight Managed Mode.

# Fabric Interconnect Password Guidelines

Cisco recommends using a strong password; otherwise, the password strength check for the admin user of the Fabric Interconnect, Cisco Intersight rejects any password that does not meet the following requirements:

- Must contain a minimum of eight characters and a maximum of 80 characters.

- Must contain at least three of the following:
  - Lower case letters
  - Upper case letters
  - Digits
  - Special characters
- Must not contain a character that is repeated more than three times consecutively, such as aaabbb.
- Must not be identical to the username or the reverse of the username.
- Must pass a password dictionary check. For example, the password must not be based on a standard dictionary word.
- Must not contain the following symbols: $ (dollar sign), ? (question mark), and = (equals sign).
- Should not be blank.

# Migrating to Cisco UCS 6500 Series Fabric Interconnects

### Replacing Cisco UCS 6400 Series Fabric Interconnect-B with Cisco UCS 6500 Series Fabric Interconnect-B

This section describes the process of migrating from Cisco UCS 6400 Series Fabric Interconnects to Cisco UCS 6500 Series Fabric Interconnects.

**Procedure:**

1. To have minimal traffic loss during migration, ensure that there are redundant paths from the chassis over fabrics A and B, and vNIC should either be redundant or that the fabric failover is enabled. Since inflight packet loss is expected during the IFM migration, best to perform the next set of operations only during a maintenance window.
2. Power down the Cisco UCS 6400 Series Fabric Interconnect by unplugging it from the power source.

   If you are monitoring the migration using a KVM session, you may need to reconnect the KVM session when you power down the Fabric Interconnect.
3. Disconnect all connections such as the network management port, L1/L2 ports, rack server, Chassis IOM/IFM ports, fabric extenders, uplink ports, and fibre connections from the Cisco UCS 6400 Fabric Interconnect-B.
4. Replace Cisco UCS 6400 Series Fabric Interconnect-B with Cisco UCS 6500 Series Fabric Interconnect.
5. Connect all connections such as the network management port, L1/L2 ports, rack server, Chassis IOM/IFM ports, fabric extenders, uplink ports, and fibre connections onto the new Cisco UCS 6500 Series Fabric Interconnects.

   Proper cables should be used to connect to the UCS 6500 Series Fabric Interconnect. For more information, refer to the Cisco UCS 6500 Series Fabric Interconnect Hardware Installation Guide and Cisco UCS 6500 Series Fabric Interconnect Data Sheet.

**Note** You can choose to migrate IFM to UCSX-I-9108-100G on UCSX-9508 Chassis.

UCS-IOM-2204/2208XP are not supported with Cisco UCS 6500 Series Fabric Interconnect. You can migrate to UCS-IOM-2408 on the Cisco UCS 5100 series Chassis.

6. Connect the power to the new Cisco UCS 6500 Series Fabric Interconnect, it will automatically boot and run POST tests.

   **Important** Directly connect the console port to a terminal and observe the boot sequence. You should at some point see the Basic System Configuration Dialog, where you will configure the switch as a peer interconnect. If the Cisco UCS 6500 Series Fabric Interconnect have been previously configured or been part of a cluster, it will need to have all configuration information wiped before it can be added to a cluster. Immediately disconnect the L1 and L2 connections and login to the Fabric Interconnect and run the erase configuration to clear out existing configuration.

7. Create new Port policies for Cisco UCS 6500 Series Fabric Interconnect-B to reflect connectivity with the Fabric Interconnect.
   - Configure Ethernet/FC breakout ports as required.
   - Configure Port roles/ Port channels as required.

8. Edit the domain profile for the cluster and change the Fabric Interconnect-B Port policy to refer to the new Cisco UCS 6500 Series Fabric Interconnect-B Port policy.

**Note** **Deploy domain profile** will be part of the replacement workflow. Therefore, no need to deploy the profile after modifying the port policy. Domain profile deployment will fail as the Fabric Interconnect model has not been updated.

9. Go to **Operate** > **Fabric Interconnects** to view the new Cisco UCS 6500 Series Fabric Interconnect and the old Cisco UCS 6400 Series Fabric Interconnect.

10. Click **Replace Fabric Interconnect** option for Cisco UCS 6400 Series Fabric Interconnect to start the Replacement workflow.

11. Verify that
    - The disconnected Fabric Interconnect cluster is removed from inventory.
    - The domain profile is reassigned to the new Fabric Interconnect cluster and deployed.
    - The servers, chassis, and FEX are inventoried and discovered under the new Fabric Interconnect cluster.
    - The server and chassis profiles are redeployed with Fabric Interconnect related policies.

**Note**

- If there is a mix of different IFM models, the chassis profile will not be pushed until both the IFM are the same.

  For example, if you migrate the IFM to UCSX-I-9108-100G from UCSX-I-9108-25G, and have chassis profile deployed prior to the migration, the chassis profile will not be deployed when the chassis has a mix of different IFM models. The chassis profile will be automatically deployed after both the IFM in the chassis have been migrated to UCSX-I-9108-100G.

**Replacing Cisco UCS 6400 Series Fabric Interconnect-A with Cisco UCS 6500 Series Fabric Interconnect-A**

Repeat the above-mentioned procedure for Fabric Interconnect-A and complete the UCS 6400 Series Fabric Interconnect to UCS 6500 Series Fabric Interconnect migration.

# Migrating from UCSX-I-9108-25G to UCSX-I-9108-100G IFM on an existing domain with Cisco UCS 6500 Series Fabric Interconnect and UCSX-9508 Chassis

Follow the below procedure to move to 100G IFM from UCSX-I-9108-25G IFM with Cisco UCS 6500 Series Fabric Interconnect and UCSX-9508 chassis.

**Procedure:**

1. To have minimal traffic loss during migration, ensure that there are redundant paths from the chassis over fabrics A and B, and vNIC should either be redundant or that the fabric failover is enabled. Since inflight packet loss is expected during the IFM migration, best to perform the next set of operations only during a maintenance window.
2. Proceed with replacing one IFM at a time.

   Start from Fabric Interconnect-B Port policy, unconfigure the server ports toward the migrating UCSX-I-9108-25G IFM. Once the server ports are unconfigured, the peer fabric interconnect will take over traffic-forwarding for these migrating UCS chassis.
3. Deploy the domain profile.
4. Disconnect the cables connecting the peer Cisco UCS 6500 Series Fabric Interconnect-B and the corresponding UCSX-I-9108-25G IFM from each migrating chassis.
5. Remove and replace the migrating UCSX-I-9108-25G IFM with UCSX-I-9108-100G IFM. Connect the UCSX-I-9108-100G IFM to the peer Cisco UCS 6500 Series Fabric Interconnect-B with proper cables. For more information, refer to the Cisco UCS 6500 Series Fabric Interconnect Data Sheet.

   At this point, the migrating UCS chassis will have a mix of UCSX-I-9108-25G and UCSX-I-9108-100G IFM.
6. Configure the Fabric Interconnect-B Port policy, then deploy the domain profile. Verify that the 100GbE links come up between the IFMs and the fabric interconnects.

- UCSX-I-9108-100G IFM will be auto-upgraded if the firmware is not the same with the Fabric Interconnect.
- Once IFM comes online, it will be discovered and inventoried automatically. Blades in the chassis will get discovered, Server profile will get deployed automatically. Server will not be rebooted or have any disruption.
- The Chassis profile will be automatically deployed after both the IFM in the chassis have been migrated to UCSX-I-9108-100G.

7. After completing IFM migration towards Cisco UCS 6500 Series Fabric Interconnect-B, repeat steps 3 through 7 for replacing the other UCSX-I-9108-25G connected to the Cisco UCS 6500 Series Fabric Interconnect-A and complete the UCSX-I-9108-100G IFM migration for the UCS domain.

# Fabric Interconnect Views

# Fabric Interconnects Table View

From the **Service Selector** drop-down list, select **Infrastructure Service**. Navigate to **Operate > Fabric Interconnects**, to launch the Fabric Interconnects Table view. Click the **Settings** icon (the gear icon representation), and select the columns that you want in the Table view. You can add the specific columns, or sort the columns by tags.

You can view the following details in the Fabric Interconnects Table view:

- **Name**—Displays the name of the Fabric Interconnect.
- **Health**—Status of the health of the Fabric Interconnect corresponds to the alarms on the servers. For more details, see Alarms.
- **Contract Status**—Displays the status of service contract for the Fabric Interconnect based on the current validity of their associated contracts. You can identify the SmartNet Contract ID details of the server, and cross launch the Cisco Commerce Software Subscriptions and Service Portal.
- **Management IP**—Displays the IP address of the management interface on the Fabric Interconnect.
- **Model**—Displays the Server Model of the Cisco Fabric Interconnect.
- **Expansion Modules**—Displays the total number of expansion modules in the Fabric Interconnect available to expand Ethernet, FCoE, or Fibre Channel ports.
- **Bundle Version**—The firmware bundle version to which the Fabric Interconnect was upgraded.

**Note** For newly claimed Fabric Interconnects, bundle version will be available only on the subsequent firmware upgrade.

- **NX-OS Version**—The firmware version running on the Fabric Interconnect.
- **User Label**—Displays the assigned user label that helps in identification of the Fabric Interconnect.

- **UCS Domain Profile**—UCS Domain Profile to which the Fabric Interconnect belongs. For standalone servers, this column is not applicable.
- **Ports**—Displays the **Total** ports, **Used** number of ports, and the **Available** ports.
- **Serial**—Displays the host ID of the Fabric Interconnect.
- **Organizations**—Lists the organizations to which the Fabric Interconnect is assigned.
- **Admin Evacuation Mode**—Displays the status of the evacuation mode in Enabled or Disabled state.

**Fabric Interconnects Table Summary Dashboard**

The following widgets are available in the Fabric Interconnects table view:

- **Health**—The pie chart provides a visual representation of the health of the Fabric Interconnects.
- **Connection**—The badge displays the connection status of the Fabric Interconnects.
- **Bundle Version**—The pie chart displays the firmware bundle version to which the Fabric Interconnect was upgraded.
- **NX-OS Version**—The pie chart displays the firmware version running on the Fabric Interconnect.
- **Models**—The pie chart displays the total number of Fabric Interconnects distributed by the model of the Fabric Interconnect.
- **Contract Status**—The badges display the status of the service contract of the Fabric Interconnects based on the current validity of their associated contracts.

# Fabric Interconnects Details View

When you select a Fabric Interconnect in the **Fabric Interconnects** table view, a Details page with information specific to the Fabric Interconnect is displayed. If a Fabric Interconnect is in **Not Connected** status, you can view the device details to resolve the issue. To view further recommendations for troubleshooting, see Troubleshooting.

In addition to the Fabric Interconnect **Health** status, you can view the following information in the Fabric Interconnects Details page:

- **Name**—Displays the name of the Fabric Interconnect.
- **Peer Switch**—Name of the Primary or Subordinate Fabric Interconnect, depending on the device you choose to view. Click **Peer FI** to view the details of the other Fabric Interconnect.
- **User Label**—The assigned user label for the Fabric Interconnect.
- **Model**—The model number of the Fabric Interconnect.
- **Organizations**—Displays the organization to which the Fabric Interconnect is assigned.
- **Expansion Modules**—The number of expansion modules in the Fabric Interconnect.
- **Serial**—The serial number of the Fabric Interconnect.
- **Management IP**—The IP address of the management interface on the Fabric Interconnect.

- **Switch Profile**—The name of the switch profile created for the UCS Domain that belongs to the Fabric Interconnect.
- **Switch Profile Status**—The current status of the switch profile associated with the Fabric Interconnect.
- **Bundle Version**—The firmware bundle version to which the Fabric Interconnect was upgraded.
- **NX-OS Version**—The firmware version running on the Fabric Interconnect.
- **Ports**—The total number of the ports.
- **Used**—The number of used ports
- **Available**—The number of ports available for use.
- **Tags**—The existing tags for the Fabric Interconnects. You can add new tags, or modify the existing ones from **Manage** tags.

The **Properties** area displays a graphical view of the Fabric Interconnect. The **Health Overlay** function enables you to monitor the health of the ports on the Fabric Interconnect. Additionally, this area provides the following information:

- **Mode**—Fabric Interconnects operate in two main switching modes: Ethernet or Fibre Channel. These modes are independent of each other. They determine how the Fabric Interconnect behaves as a device between the server and network/server and storage device.
  - **Ethernet Mode**—The Ethernet switching mode determines how the Fabric Interconnect behaves as a switching device between the servers and the network. The Fabric Interconnect operates in either of the following Ethernet switching modes:
    - **End-Host Mode**—Allows the Fabric Interconnect to act as an end host to the network, representing all servers (hosts) connected to it through virtual Network Interface Cards (vNICs).
    - **Switch Mode**—Allows the Fabric Interconnect to run STP to avoid loops. Broadcast and multicast packets are handled in the traditional way.
  - **FC Mode**—The Fibre Channel switching mode determines how the Fabric Interconnect behaves as a switching device between the servers and storage devices. The Fabric Interconnect operates in either of the following Fibre Channel switching modes:
    - **End-Host Mode**—Allows the Fabric Interconnect to act as an end host to the connected fibre channel networks, representing all servers (hosts) connected to it through virtual Host Bus Adapters (vHBAs).
    - **Switch Mode**—Allows the Fabric Interconnect to connect directly to a storage device.
  - **Admin Evac State**—Specifies the evacuation state of Fabric Interconnect traffic. This can be one of the following options:
    - **Disabled**—Restarts traffic on the Fabric Interconnect.
    - **Enabled**—Stops traffic on the Fabric Interconnect.
  - **Oper Evac State**—Specifies the operational evacuation state of Fabric Interconnect traffic.
- **FC Zone Count**
  - **FC Zone Limit**—The maximum number of Fibre Channel zones allowed on this Fabric Interconnect.

- **FC User Zone Limit**—The maximum number of user-created Fibre Channel zones allowed on this Fabric Interconnect.
- **FC Zone Count**—The number of Fibre Channel zones defined on this Fabric Interconnect.
- **FC User Zone Count**—The number of user-created Fibre Channel zones defined on this Fabric Interconnect.

- **Access**
  - **IP Address**—The IP address to use when communicating with the Fabric Interconnect.
  - **Subnet Mask**—The subnet mask associated with the IP address.
  - **Default Gateway**—The gateway associated with the IP address.
  - **MAC**—The MAC address.
- **VLAN Details**
  - **VLAN Port Limit**—The maximum number of VLAN ports allowed on this Fabric Interconnect.
  - **Access VLAN Port Count**—The number of available VLAN access ports.
  - **Border VLAN Port Count**—The number of available VLAN border ports.
  - **Compressed Optimization Sets**—The number of VP optimization groups.
  - **Compressed VLAN Port Count**—The number of compressed VLAN ports.
  - **Uncompressed VLAN Port Count**—The number of uncompressed VLAN ports.
  - **Reserved VLAN Range**—The range of VLAN IDs reserved for system use.
- **Fabric Interconnect License**

  Cisco UCS 6454 and 64108 Fabric Interconnects require port-based licensing. To activate unlicensed ports, a product activation key must be installed for each respective port. Beginning with UCS software release version 4.2(3), Cisco UCS 6536 Fabric Interconnect supports a perpetual software license, which activates all ports and software features of the Fabric Interconnect.

**Note** This section appears only for Cisco UCS 6536 Fabric Interconnect and displays the message: "Perpetual software license is installed. All ports in this Fabric Interconnect are licensed."

### Supported Fabric Interconnects Models

The Fabric Interconnects models supported in Intersight Managed Mode are:

UCS-FI-6454

UCS-FI-64108

UCS-FI-6536

The Fabric Interconnects models supported in UCSM Managed Mode are:

UCS-FI-6248UP, UCS-FI-6296UP

UCS-FI-6332, UCS-FI-6332-16UP

UCS-FI-M-6324

UCS-FI-6454

UCS-FI-64108

UCS-FI-6536

### Alarms

Intersight provides fault monitoring capabilities to track and set up alarms for all managed UCS and HyperFlex systems. An alarm alerts you about a failure in the setup (a fault) or a threshold that has been raised. An alarm in Intersight includes information about the operational state of the affected object at the time the fault was raised. Click on a specific alarm to view the fault code, the source type and name, component on which the fault occurred, and a description of the fault.

**Note** Intersight managed devices must be running with firmware version of 4.1(3) or later releases to generate alarms.

Click on any of the categories to view more details about the alarms.

- **All(Info)**—Displays the total number of faults both Critical and Warning.
- **Critical**—Displays the total number of Critical faults. Raised when a service-affecting condition requires an immediate corrective action. For example, the severity could indicate that the managed object is out of service and its capability must be restored immediately.
- **Warning**—Displays the total number of Warning faults. Raised when a potential or impending service-affecting fault occurs.

  This fault could have no significant or immediate effects on the system. A warning status indicates that you must take the appropriate action to diagnose the fault and correct the problem to prevent it from becoming a more serious service-affecting fault.

# Fabric Interconnects Inventory View

When you select a Fabric Interconnect in the **Fabric Interconnects** table view, you can view the inventory of its components on the **Inventory** tab.

For the selected Fabric Interconnect, you can view details of each of the following components:

- **Ports & Port Channels**—You can see a summary of the Ethernet ports, FC ports, Ethernet Port Channels, and FC Port Channels on the Fabric Interconnect. When you click a specific port, you can view the properties and graphical view of that port.

  You can **Enable** or **Disable** a port or a port channel from this view. Disabling a port may lead to traffic disruption. The device connected to a disabled port will also go offline. Disabling a port channel will lead to the member ports also getting disabled.

**Reset** option from the Fabric Interconnects inventory view allows you to reset a port or an Ethernet port which has server role configuration. The **Reset** action is also available for Backplane Ports on the FEX under the FEX inventory view.

**Note** This action should be attempted only when the port is not converged due to incorrect configurations. Resetting a port will lead to traffic disruption.

- **Fan Modules**—You can see a summary of the fan modules on the Fabric Interconnect. When you click a specific fan module, you can view the list of fans on the fan module, and the properties and graphical view of that fan module.
- **PSUs**—You can see a summary of the Power Supply Units (PSUs) on the Fabric Interconnect. When you click a specific PSU, you can view the properties and graphical view of that PSU.
- **Local Storage**—You can see a summary of the partitions on the Fabric Interconnect, including details such as their size and current usage.

# Fabric Interconnects Connections View

The Connections view provides a list of all the components that are directly or indirectly connected to your Fabric Interconnect, such as servers, chassis, and Fabric Extenders (FEX).

Depending on the information available for the selected Fabric Interconnect, the following is displayed:

- **Compute**
  - **Servers**—The details of all the servers that are connected to the Fabric Interconnect. These details are Name, Health, User Label, Slot Id, Management IP, Model, and Serial.
  - **Chassis**—The details of all the chassis that are connected to the Fabric Interconnect. These details are Name, Health, Model, and Serial.
- **Network**
  - **Fabric Extenders**—The details of the Fabric Extenders that are connected to the Fabric Interconnect. These details are Name, Health, Model, Vendor, and Serial.
- **Decommissioned**
  - **Devices**—The details of decommissioned devices. These details are Type, Model, Serial, Decommissioned Date.

# Fabric Interconnects UCS Domain Profile View

The **UCS Domain Profile** view displays a graphic representation of the port configuration, VLAN and VSAN configuration, and the UCS Domain Configuration. Additionally, the following information is displayed:

- **Details**

- **Status**—Status of the UCS Domain profile deployment to the assigned Fabric Interconnect pair
- **Name**
- **Fabric Interconnect A**—Name of Fabric Interconnect A
- **Fabric Interconnect B**—Name of Fabric Interconnect B
- **Last Update**—Date and time that the UCS Domain profile was last updated
- **Description**—Optional description of the UCS Domain profile

- **Tags**—The existing tags for the Domain. You can add new tags, or modify the existing ones from **Manage** tags.
- **Policies**

  View the **Policies** that are attached to the UCS Domain profile. The **Policies** pane displays details of the **Port**, **VLAN and VSAN**, and **UCS Domain Configuration**. A graphical representation of the ports configuration on the Fabric Interconnects, including port roles and port channels and a list of associated policies is displayed. The VLAN, VSAN, and UCS Domain Configuration lists the Domain policies associated with the selected Domain profile.

# Fabric Interconnect Topology View

For more information, see Topology.

# Fabric Interconnect Metrics View

For more information, see Fabric Interconnects Metrics.

# Fabric Interconnect Actions

The Fabric Interconnect Actions allows you to perform specific management operations on that Fabric Interconnect. In Cisco Intersight, when you click a Fabric Interconnect, the Fabric Interconnects Table view is displayed. In this page, click the Ellipsis (…) icon to perform Fabric Interconnect actions.

**Fabric Interconnect Actions**: You can perform the following operations to manage a Fabric Interconnect:

- **Enable/Disable Evacuation Mode**—Fabric Evacuation refers to the ability that allows you to stop all active traffic flowing through the selected Fabric Interconnect. You can use the **Enable Evacuation Mode** to evacuate all the Ethernet and Fibre Channel traffic flowing through the selected Fabric Interconnect, from all blades and rack servers. This Evacuation Mode option provides more control so that you can perform maintenance operations on the Fabric Interconnect with Evacuation Mode enabled, and also test the traffic high availability behavior during the setup.

  Use the **Disable Evacuation Mode** to restore the traffic to flow through both the Fabric Interconnects paths.

  An alarm is raised on the Fabric Interconnect when the Evacuation Mode is enabled. You can monitor the progress of the traffic evacuation in the Requests view. The evacuation state of the Fabric Interconnect

is displayed in the **Fabric Interconnects Table View** and the **Fabric Interconnects Details View** > **Inventory** tab. The alarm gets cleared when the Evacuation Mode is disabled. For more information, see Cisco Intersight Alarms Reference Guide.

- If Traffic Evacuation Mode is **Enabled**, the IOM or FEX backplane ports or ports towards the servers are set to **admin-down**. In case of directly attached rack servers, the server ports on the Fabric Interconnect connected to these rack servers are set to **admin-down**.
- During Fabric Evacuation for the Intersight Managed Mode domains with direct attached rack servers, the server ports are shut down. In case of Intersight Managed Mode domains with IOM or IFM and rack servers behind the FEX, the HIF ports are shut down.
- You must explicitly configure Traffic Evacuation Mode as **Disabled** to move the backplane ports or server ports on Fabric Interconnect connected to the rack servers back to the **Up** state and resume the traffic flow.

**Note**

- If traffic evacuation mode is enabled on a Fabric Interconnect within a pair, it will be disabled on its peer Fabric Interconnect. By default, Traffic Evacuation Mode is disabled.
- You can toggle the **Force Evacuation** option when one or more of the peer Fabric Interconnect IOMs/FEX are not operable or disconnected.

Traffic evacuation for a Fabric Interconnect is not allowed if it can cause a traffic outage for servers in the domain. For example, if a chassis has connectivity to only one Fabric Interconnect, and you evacuate this Fabric Interconnect, servers on this chassis loses the connectivity to the rest of the data center. Select **Force Evacuation** if you want to override this restriction and proceed.

**Note** You cannot perform evacuation on Fabric Interconnect when:

- The Peer Fabric Interconnect is disconnected.
- The Fabric Interconnect firmware upgrade is in progress.
- The domain profile deployment is in progress.

Traffic evacuation on a Fabric Interconnect can take 7 to 10 minutes to complete, depending on the system scale. During this time, traffic evacuation to the other Fabric Interconnect can take 1 to 2 seconds for an individual vNIC or vHBA. Ensure to configure redundancy for vNIC or vHBA to minimize traffic disruption.

- **Launch UCS Manager**— Launch Cisco UCS Management interface from Cisco Intersight.
- **Launch CLI**—Launch command line interface from Cisco Intersight.

**Note** Launch Cisco UCS Manager and Launch CLI options are available only for UCSM Managed Mode Fabric Interconnects.

- **Open TAC Case**—Open a case to report an issue with the server.
- **Upgrade Firmware**—Perform a firmware upgrade. For more information, see the Firmware Upgrade.
- **Set User Label**—Allows you to set, update, or delete user labels for each Fabric Interconnect. It must be between 1 and 64 alphanumeric characters, containing only the following special characters: ! # $ % & * + , ( ) [ ] { } | / . ? @ _ : ; ~
- **Replace Fabric Interconnect**—Remove the old Fabric Interconnect and connect the new Fabric Interconnect.
- **Replace UCS Domain**—Remove the old Fabric Interconnect cluster and connect the new Fabric Interconnect cluster.

**Note**

- Replace Fabric Interconnect and Replace UCS Domain options are available only for Intersight Managed Mode Fabric Interconnects.
- To perform Replace UCS Domain action, you must ensure that the Domain Profile is in associated state with the Fabric Interconnect.

- **Collect Tech Support Bundle**—Collect the tech support bundle. An Account Administrator or a user with Support Services role can select the device and collect the tech support bundle file for the selected device. The downloaded file can be accessed by navigating to **Admin** > **Tech Support Bundles** section. This file can be shared with the TAC team for troubleshooting any issue.