Revised: July 7, 2025

Cisco Nexus Hyperfabric — Getting Started

Cisco Nexus Hyperfabric

The Cisco Nexus Hyperfabric is a fabric-as-a-service solution that allows you to design and build a physical network that is managed by a cloud-based service. Your network can start as small as a single switch and can grow to multiple locations, each with a fabric of many switches.

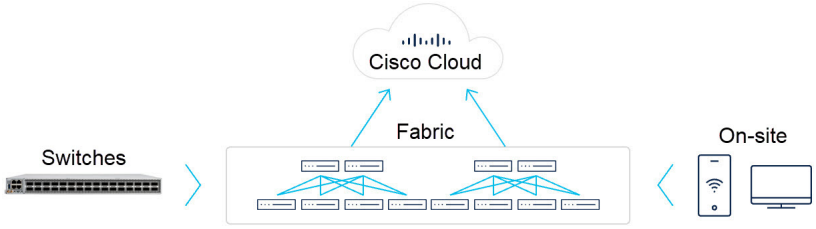
The design, deployment, and operation of the Cisco Nexus Hyperfabric is based on a shared responsibility model between you and Cisco. Cisco automation and operations staff own the proper functioning of the cloud-based service and the software upgrade process. Your staff maintains direct control of the timing of switch upgrades and of all interconnections to your applications, hosts, domestic network, and connectivity to the cloud-based service.

Components of a Cisco Nexus Hyperfabric deployment

These components comprise a Cisco Nexus Hyperfabric deployment:

- Cisco Nexus Hyperfabric service—A scalable, globally-distributed, multi-tenant cloud-based software-as-a-service (SaaS) network infrastructure management solution. The Cisco Nexus Hyperfabric service is hosted and operated by Cisco, and is the single point of provisioning and visibility for your fabrics.
- Cisco Nexus Hyperfabric switches—Cloud-managed Cisco 6000 switches on your premises or in a colocation environment. Bootstrapping and administration of the switches is handled by the cloud-based service.
- High-performance fabrics—Mesh or spine-leaf topologies that use EVPN VXLAN, Layer 2 VLANs, or IPv4/IPv6 routing.
- Graphical user interface (GUI) and the REST API—The interfaces that you can use to perform tasks in Cisco Nexus Hyperfabric.
- On-site page—Provides the network cabling technicians with step-by-step tasks to claim, bind, and cable the devices in your fabric. This page also provides real-time validation of the fabric topology.

Figure 1: Cisco Nexus Hyperfabric components



How Cisco Nexus Hyperfabric works

This is the overall process of how Cisco Nexus Hyperfabric works:

1. In collaboration with the Cisco Nexus Hyperfabric team, you design your fabric online using an automated design tool provided in the Cisco Nexus Hyperfabric GUI. The completed design is a blueprint for your new fabric.
2. When your fabric blueprint is complete, Cisco Nexus Hyperfabric generates these additional resources:
    - A detailed bill of materials (BoM) for purchasing the necessary fabric components, including switches and pluggables such as optics, Direct Attach Cables (DACs), and Active Optical Cables (AOCs)

- A complete cabling plan for your installer to wire the fabric

3. When you receive your components, your installer physically wires them according to the cabling plan.
4. Each new Nexus Hyperfabric switch contains an agent that allows it to contact Cisco Nexus Hyperfabric. You configure the management port of one switch and provide that port with an external Internet connection. That switch then contacts Cisco Nexus Hyperfabric. This Internet-connected switch is referred to as the "exit node".
5. The agent enables each switch to discover and authenticate its neighbors. As each switch discovers a path to an exit node in the fabric, the switch contacts the service through the exit node.
6. When your switches are connected and ready, you register ("claim") each switch online with Cisco, specifying the organization that owns the switch.

Note

In some cases, your switches might be received already claimed by your organization.

7. In Cisco Nexus Hyperfabric, you assign ("bind") each physical switch to its logical location ("node") in the fabric blueprint. When you bind a switch to a node in the blueprint, the switch can download its configuration from Cisco Nexus Hyperfabric.
8. After the fabric has been fully provisioned, you can connect your local hosts and servers to the fabric.

Switch telemetry

Cisco Nexus Hyperfabric provides nearly real-time telemetry for these switch stats:

- Switch—Port status, assertions, and traffic stats
- Interface—Port counters, link status, and network configuration
- Environmental—Per switch sensor readings for fans, PSUs, and other components
- Optics and pluggables—Digital optical monitoring (DOM) statistics

Nexus Hyperfabric use cases

Typical use cases for Cisco Nexus Hyperfabric include small to medium branch offices or remote colocation sites where you do not want on-premises management. The Cisco Nexus Hyperfabric is ideal for meeting needs such as

- deploying or extending new data center fabrics or easily building new data center fabrics
- deploying reliably and rapidly with basic network requirements and compute connectivity
- designing new data center networks easily and evolving them over time
- deploying small, spineless fabrics of one or two switches
- deploying seamlessly and extending distributed data centers to edge or co-locations, and
- starting small and expanding fabrics seamlessly without confined architectures.

Supported topologies

Cisco Nexus Hyperfabric supports these network topologies:

- A single switch or a redundant switch pair
- A small mesh network
- A spine and leaf fabric

A growing site could change the topology as needed by revisiting the design tool in Cisco Nexus Hyperfabric and creating an updated blueprint.

Single leaf switch or redundant pair

In a site with fewer than 50 hosts, a single leaf switch may be sufficient. For high availability, you can deploy a second switch in a redundant configuration.

Figure 2: Single leaf switch

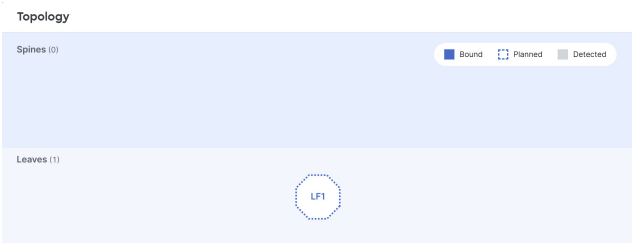


Figure 3: Redundant pair

Small mesh fabric

A small mesh fabric has two to five interconnected leaf switches.

Figure 4: Small mesh fabric

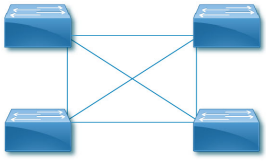


Figure 5: Small mesh fabric with 4 leaf switches

Spine and leaf fabric

A spine and leaf fabric has one to four spine switches and one to 32 leaf switches.

Figure 6: Spine and leaf fabric

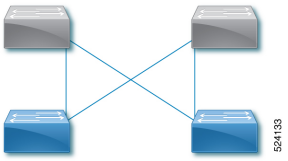
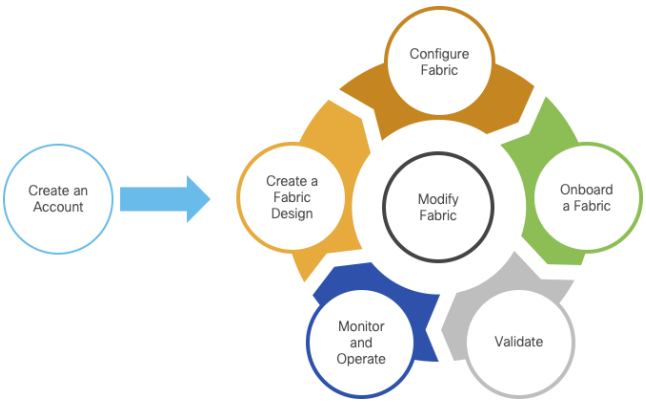


Figure 7: Spine and leaf fabric with 2 spine switches and 2 leaf switches

The Cisco Nexus Hyperfabric lifecycle

To design, deploy, and maintain a network based on the Cisco Nexus Hyperfabric, you will work together with Cisco to follow the process illustrated in the following lifecycle diagram.



1. Log in to Cisco Nexus Hyperfabric.

The first step in creating your cloud-managed network is logging in to the Cisco Nexus Hyperfabric portal and creating an organization in which you will design and operate your network fabric. See Log in to Cisco Nexus Hyperfabric, on page 5.

2. Create a fabric design.

   In Cisco Nexus Hyperfabric, you will design your fabric using the Blueprint Designer, selecting the switches and the topology to create a blueprint of your fabric. See Create a new fabric, on page 9.

3. Configure (or modify) the fabric.

   In the Blueprint Designer, configure the interconnections between the fabric switches. Configure the pluggables such as optics, Direct Attach Cables (DACs), and Active Optical Cables (AOCs), and configure the remaining ports for connection to servers and other network devices. See Connect the fabric, on page 11.

4. Onboard the fabric.

   When the Nexus Hyperfabric switches have been physically installed and wired according to the blueprint, they must be "claimed" by the organization and "bound" to their logical positions (nodes) in the blueprint. The switches will become cloud-managed through the Cisco Nexus Hyperfabric portal. See Onboard a fabric, on page 27.

5. Validate the design.

   After you bind the switches to the fabric blueprint, verify that traffic is being forwarded correctly.

6. Monitor and operate the fabric.

   See *Cisco Nexus Hyperfabric-Configure Fabrics*.

Accessing Cisco Nexus Hyperfabric

Log in to Cisco Nexus Hyperfabric

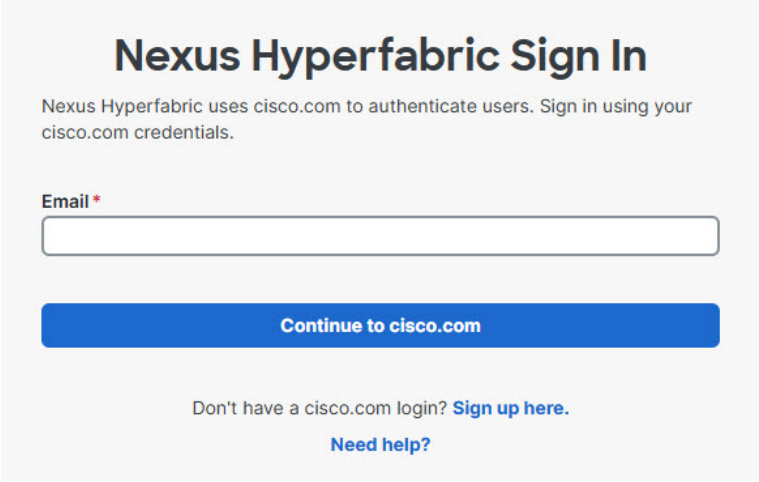
To get started in the design of your cloud-managed network, you must log in to the Cisco Nexus Hyperfabric. You must first have a cisco.com user account.

The other procedures in this document assume that you have logged in to the Cisco Nexus Hyperfabric.

Follow these steps to log in to Cisco Nexus Hyperfabric.

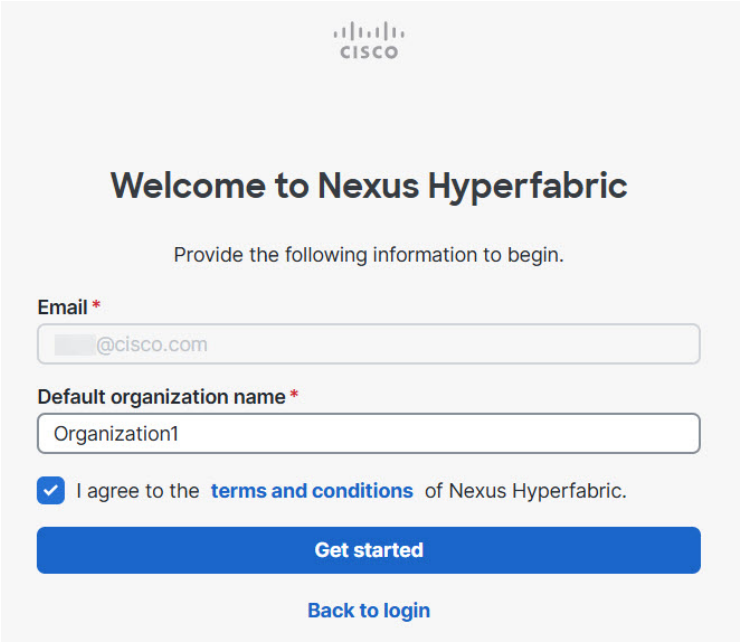
Step 1 Point your Web browser to https://hyperfabric.cisco.com/.

Step 2 If you already have an account, enter your cisco.com email address and click **Continue to cisco.com**. You will be authenticated by Cisco's Single Sign-On (SSO) service.



a) If you do not have an account, click **Sign up here** and fill out the requested information, then repeat this procedure.

Step 3 If you are not the admin for an existing organization, you can create an organization. Enter the name of your organization, check **I agree to the terms and conditions of Nexus Hyperfabric**, and click **Get started**.



The default organization name is your email address plus the word "scratch." "scratch" only indicates that this is your first organization and does not otherwise have any special significance. You can change the name, and the name can contain a limited selection of special characters. For a list of allowed special characters, see Guidelines for creating an organization, on page 7.

After you click **Get started**, Cisco Nexus Hyperfabric displays the main page for the organization.

Create an organization

Follow these steps to create an organization.

Step 1 Select **Organization** > **Create new organization**.

Step 2 Enter the name of the new organiziation, then click **Save**.

Guidelines for creating an organization

These guidelines apply for creating an organization:

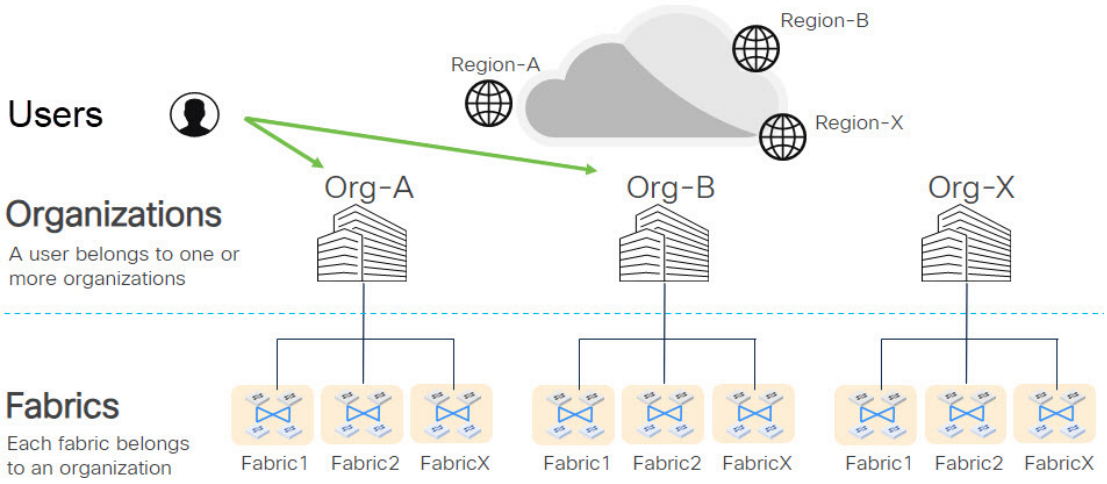
- You can include these special characters in an organization's name, as long as they are not the first nor last character in the name:
  - -
  - _
  - +
  - (space)
  - /
  - @
  - .
  - &

  You cannot include any other special characters.
- The name must be between 3 and 120 characters.
- You can create up to 10 organizations.
- You cannot delete an organization after you create it.
- You are by default an administrator of any organization that you create.

Add a new user

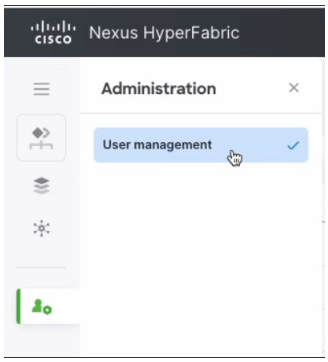
If you are an administrator for an organization, you can add a new user to that organization. A user can belong to multiple orgnizations. Figure 8: Users and organizations, on page 8 illustrates the association of users and organizations.

Figure 8: Users and organizations

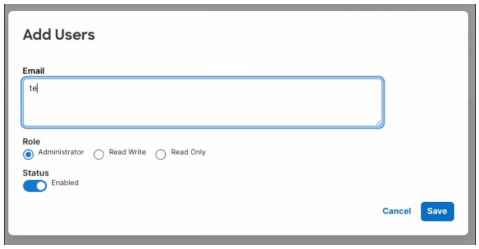


Follow these steps to add a new user.

Step 1 Select **Administration** > **User management**.



Step 2 Click **+ Add User**.



Step 3 Enter the email addresses of the new users.

You can enter a comma-separated list of email addresses. The role and status settings you select will apply to all users in this list.

Step 4 Select a role: **Administrator**, **Read Write**, or **Read Only**.

Step 5 Select the status of the users: **Enabled** or **Disabled**.

Step 6 Click **Save**.

Designing the fabric blueprint

Create a new fabric

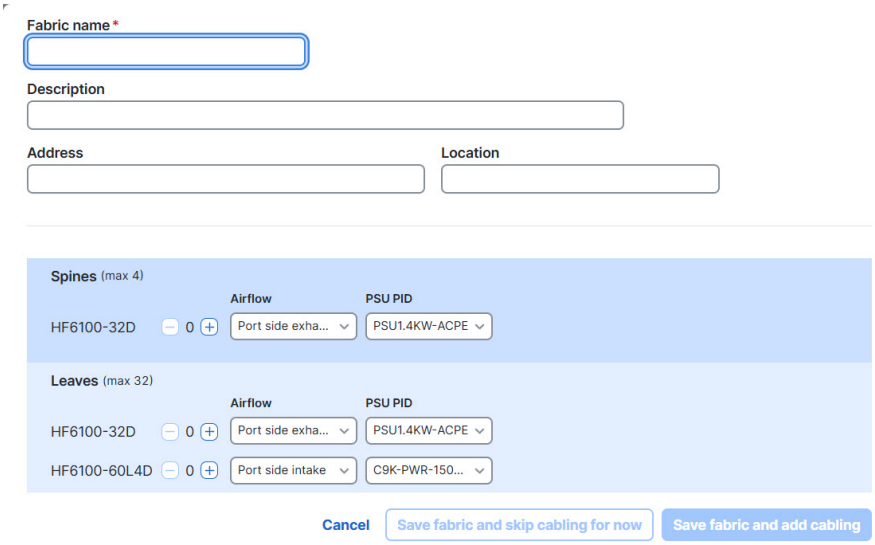
When you have created a new organization or need to add a fabric to an existing organization, you can use the Blueprint Designer in the Cisco Nexus Hyperfabric to create a blueprint for the new fabric.

For supported fabric topologies, see Nexus Hyperfabric use cases.

Follow these steps to create a new fabric.

Step 1 Select **Fabrics**.

Step 2 Click **+ Add new fabric**.



Step 3 Fill out the dialog box as necessary.

a) For **Fabric name**, enter a unique name from 3 to 120 characters. The name can contain a hyphen (-), but no other special characters.

b) For **Description**, enter a description of the fabric.

c) For **Address**, enter the physical address where the fabric is located.

d) For **Location**, enter additional location information about the fabric.

e) For **Spines**, select the quantity of switches, the airflow, and the PSU PID. Cisco Nexus Hyperfabric selects the fan PID automatically based on what you select for the airflow.

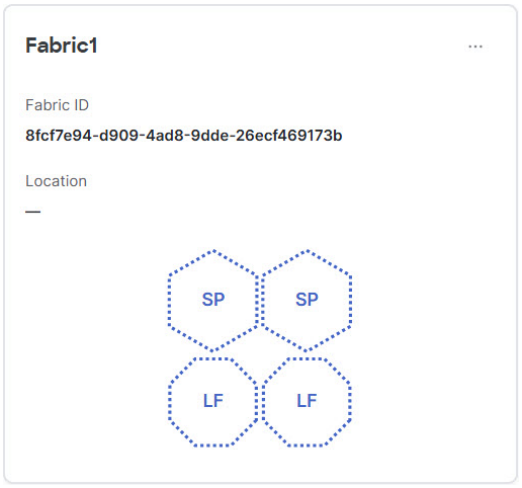
f) For **Leaves**, select the quantity of switches, the airflow, and the PSU PID. Cisco Nexus Hyperfabric selects the fan PID automatically based on what you select for the airflow.

To design a single-switch fabric or a mesh fabric, select only leaf switches. If you select one or more spine switches, select two or more switches to create a spine-and-leaf topology.

As you make your switch choices, Cisco Nexus Hyperfabric updates the topology.

Step 4 Click either **Save fabric and skip cabling for now** or **Save fabric and add cabling**.

If you do not want to add the cabling at this time, click **Save fabric and skip cabling for now**. Cisco Nexus Hyperfabric adds a tile for the new fabric. This example shows a spine-and-leaf fabric with two spine switches and two leaf switches:



If you want to add the cabling now, click **Save fabric and add cabling**, which opens the **Auto Cabling** dialog box. Follow these substeps.

a) For **Order**, enter the number of links that you want to have between each switch pair.

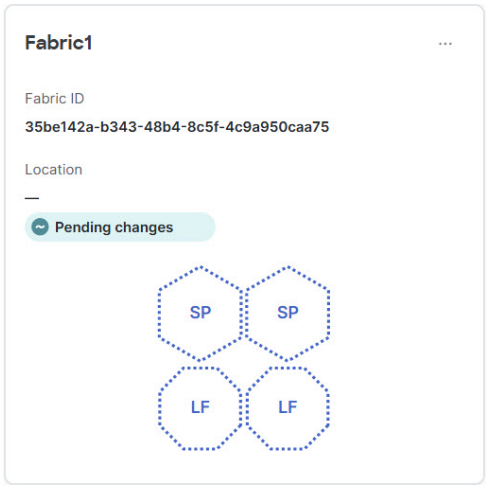
   In most cases, you can use the default of 1.

b) For **Pluggable**, enter the product ID of the optic. Optionally, select one of the optics from the table at the bottom of the dialog box to fill in the field based on what you chose. You can use the **Search** field and **Plug type**, **Speed**, and **Cable type** drop-down lists to filter the table.

c) Click **Save** at the bottom of the dialog box.

   The **Auto Cabling** dialog box closes and the **Fabric connects** table now shows how you should connect the switches.

Cisco Nexus Hyperfabric adds a tile for the new fabric. The tile shows "Pending changes" because you must review and push the cabling configuration change. For the procedure, see Finish and commit the design, on page 24. This example shows a spine-and-leaf fabric with two spine switches and two leaf switches:



Import a fabric blueprint

If you have a JSON file of a fabric blueprint, you can import that blueprint into your Cisco Nexus Hyperfabric organization to create a new fabric blueprint. Cisco Nexus Hyperfabric validates the blueprint when you attempt to import it. If Cisco Nexus Hyperfabric detects issues with the blueprint, it informs you of the issues and stops the import.

You can get example fabric blueprint JSON files from Cisco; contact your account team for more information.

Follow these steps to import a fabric blueprint.

Step 1 Select **Fabrics**.

Step 2 Click **Import new fabric**.

The **Import fabric configuration** dialog box appears.

a) Drag and drop the JSON file from your local system to the **Drag file here** area of the dialog box.

The **Drag file here** text changes to display the name of the JSON file.

b) Click **Import**.

While the Cisco Nexus Hyperfabric imports the blueprint, the text of the **Import** button changes to "Importing...". After Cisco Nexus Hyperfabric completes importing the blueprint, the fabric appears as part of your organization.

Limitations for importing a fabric blueprint

These limitations apply for importing a fabric blueprint:

- An imported fabric blueprint does not have any bound switches. You must bind switches after importing the JSON file.
- The JSON file of an exported fabric blueprint does not contain any password nor secrets. You must configure these manually after you import the JSON file.

Connect the fabric

After you have chosen the topology for your fabric, you must configure the physical ports and interconnections between the fabric switches. You must also configure ports for connection to servers and other network devices. You configure the fabric in Cisco Nexus Hyperfabric's Blueprint Designer using the workflow and procedures described in this document.

Note

In the Blueprint Designer, you can preconfigure ports and interconnections before your switches are physically installed and bound to the fabric, or you can wait until after the switches are onboarded and operational. The latter case has the advantage of status monitoring and testing as you configure. For example, any physical connection that does not match the blueprint generates an assertion, which can then be investigated and resolved.

The procedures for additional configuration, including port channels, logical networks, and routing tables, are described in other Cisco Nexus Hyperfabric articles.

Modifying fabrics

If you have administrator or read-write access to the organization, you can modify the design of an existing fabric on the **Fabrics** page. You can make changes to the fabric blueprint at any stage: from an undeployed fabric design to an installed and running fabric.

The **Fabrics** blueprint page operates in one of two modes:

- Edit mode—This is the default mode for a user with administrator or read-write access. All fabric edit options are exposed.
- Running mode—This is the default mode for a user with read-only access. Settings and status are displayed, but no edit options are exposed. You can switch to edit mode only if you have administrator or read-write access.

Note

All configuration procedures in this document assume that you are logged in with administrator or read-write access, and that the menus are in edit mode.

Modify a fabric

This procedure provides the typical workflow for making fabric configuration changes.

Follow these steps to modify a fabric.

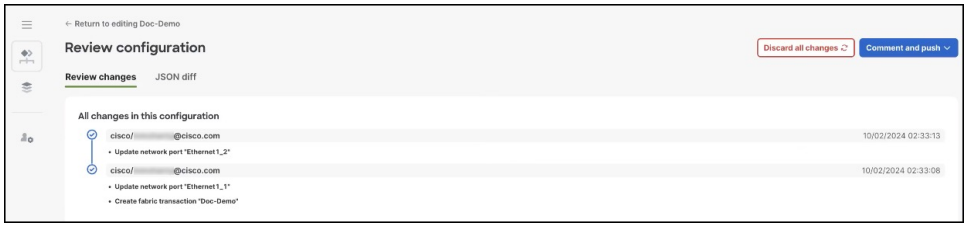
Step 1 Select **Fabrics**, then click the fabric that you want to configure.

Step 2 If the fabric is not in the edit mode, click **Switch to edit mode**.

Step 3 Make your changes.

Note Your changes are not applied to the fabric until you review, commit, and push them.

Step 4 When you're ready to apply your changes, click **Review configuration**.

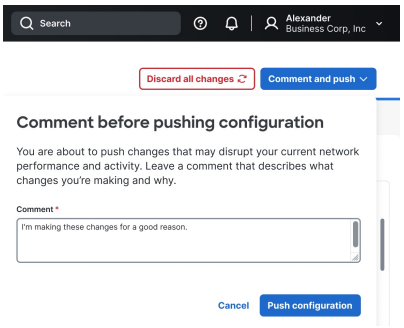


In the **Review configuration** page, you can view:

- a list of brief descriptions of the changes since the last push, including the author's ID and the date and time when the change was saved, and
- a 'diff' display of the fabric's JSON configuration file, showing the proposed changes in this commit.

Step 5 When you have reviewed the changes and are ready to apply them, click **Comment and push**.

Step 6 In the **Comment before pushing configuration** dialog box, enter the reason for the change.



Step 7 Click **Push configuration**.

Step 8 View the status of your changes.

On the **Fabrics** blueprint page, view the fabric card to see the status of the pushed changes. Your changes may take some time to apply or they might generate red assertions. For example, if you push changes to an installed and running fabric, and the changes conflict with the physical cabling of the fabric, an assertion is raised.

Deploying your fabric on site

The Cisco Nexus Hyperfabric greatly simplifies cabling operations of the switches in a fabric by providing features to guide tasks that you or a network cabling technician must perform on site. A network administrator uses Cisco Nexus Hyperfabric to create a blueprint that includes a cabling plan for the switches. You can view and follow tasks to set up the physical fabric topology or track the progress by going to a dedicated on-site page.

Alternatively, the network administrator can give a URL for a mobile-friendly web page of the blueprint to the network cabling technicians. The technicians then open the URL on a mobile device to view the blueprint and follow that to set up the physical fabric topology or to view the status of the fabric.

The URL is in the format of "https://hyperfabric.cisco.com/fabric/*fabric_ID*/on-site". You can get the fabric ID from the **Fabrics** page or the page for the specific fabric. This is an example URL:

```
https://hyperfabric.cisco.com/fabric/abc1d234-567e-8901-fghi-23j4k56l78mn/on-site
```

For more information about deploying your fabric on site, see *Cisco Nexus Hyperfabric — Deploying Your Fabric on Site*.

Auto-cabling

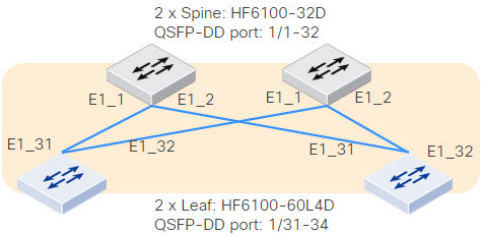
For a fabric blueprint for which you have not yet performed the cabling, auto-cabling can generate a switch-to-switch fabric connectivity plan based on the selected switch models and the number of switches. You can edit the plan as necessary.

As an example, assume you have this fabric blueprint:

- 2 HF6100-32D spine switches
- 2 HF6100-60L4D leaf switches
- 1 link for each switch pair

Auto-cabling will generate the connectivity plan as shown in the figure.

Figure 9: Auto-cabling example



This table specifies how the plan connects the switches:

Table 1: Auto-cabling example

From	To
Spine1 E1_1	Leaf1 E1_31
Spine1 E1_2	Leaf2 E1_31
Spine2 E1_1	Leaf1 E1_32
Spine2 E1_2	Leaf2 E1_32

If you have already cabled the switches, auto-cabling can detect the existing connectivity between the Hyperfabric switches to create a switch-to-switch fabric connectivity plan. This capability is useful if you change the blueprint, such as increasing the number of links for each switch pair or adding a new switch. You can use auto-cabling to generate a new connectivity plan that takes into account the changes in the blueprint.

Configure fabric connections using auto-cabling

You can use the auto-cabling feature to configure the fabric connections quickly and easily. This feature simplifies the process and in most cases creates a desirable cabling plan.

Follow these steps to configure fabric connections using auto-cabling.

Note

Auto-cabling uses only QSFP-DD ports. If you want to use an SFP56 port (10G, 25G, or 50G) for a switch-to-switch connection, you must configure the connections manually. For the procedure, see Configure fabric connections manually, on page 15.

For your switch fabric ports, if you want to use a non-default speed such as 40G, 100G, or 200G instead of the default of 400G, you must select the appropriate speed when you configure the ports. For the procedure, see Configure a port at the switch level, on page 16.

Step 1 Select **Fabrics**, then click the fabric for which you want to use auto-cabling.

Step 2 If the fabric is not in the edit mode, click **Switch to edit mode**.

Step 3 In the **Physical topology** area, click **Fabric connects**.

The **Fabric connects** table lists all configured connections, if any.

Step 4 Click **Auto Cabling**.

The **Auto Cabling** dialog box opens.

a) For **Order**, enter the number of links that you want to have between each switch pair.

   In most cases, you can use the default of 1.

b) For **Pluggable**, enter the product ID of the optic. Optionally, select one of the optics from the table at the bottom of the dialog box to fill in the field based on what you chose. You can use the **Search** field and **Plug type**, **Speed**, and **Cable type** drop-down lists to filter the table.

c) Click **Save** at the bottom of the dialog box.

   The **Auto Cabling** dialog box closes and the **Fabric connects** table now shows how you should connect the switches.

Configure fabric connections manually

You can use the auto-cabling feature to configure the fabric connections quickly and easily. However, you can also configure the fabric connections manually for precise control over the device connections.

Follow these steps to configure fabric connections manually.

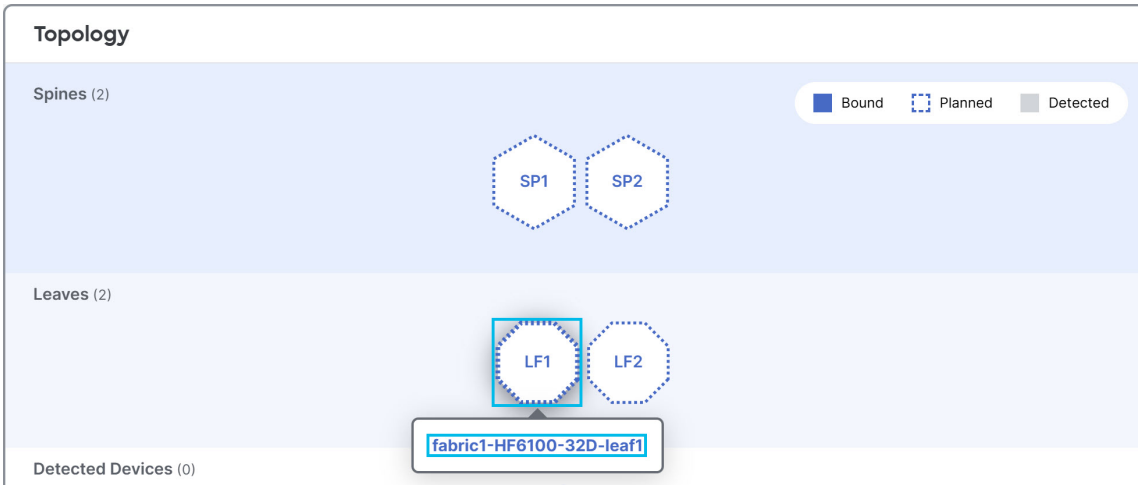
Note

For your switch fabric ports, if you want to use a non-default speed, you must select the appropriate speed when you configure the ports. For example, for QSFP-DD ports, you can use 40G, 100G, or 200G instead of the default of 400G. For the procedure, see Configure a port at the switch level, on page 16.

Step 1 Select **Fabrics**, then click the fabric that contains the switches that you want to connect.

Step 2 If the fabric is not in the edit mode, click **Switch to edit mode**.

Step 3 In the **Topology** area, click the switch position that you want to configure, then click the switch name.



Step 4 In the **Configure** area, click **Fabric connects**.

The **Fabric connects** table lists all configured connections.

Step 5 Click **+ Add port connection**.

A dialog box opens for configuring a new connection.

a) For **Port interface**, select an interface.
b) For **Pluggable**, enter the product ID of the optic. Optionally, select one of the optics from the table at the bottom of the dialog box to fill in the field based on what you chose. You can use the **Search** field and drop-down lists to filter the table.
c) For **To switch**, select the destination switch.
d) For **Port interface** under **To switch**, select the destination switch's port.
e) Click **Save** at the bottom of the dialog box.

Configure a port

Configure a port at the switch level

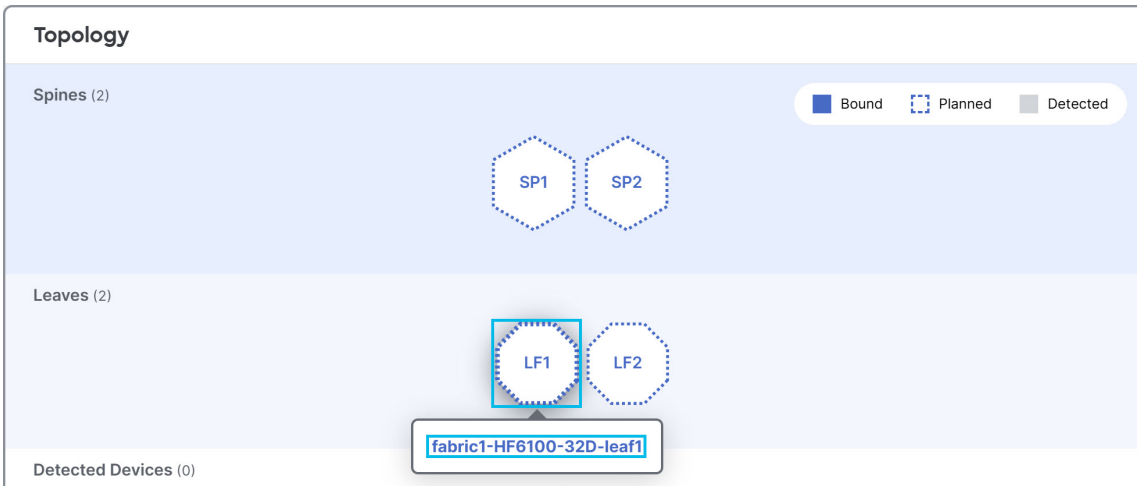
You can configure various properties of a switch's port, such as the role and speed, and if it is broken out. The port role specifies the type of connection provided by a port.

Follow these steps to configure a port at the switch level.

Step 1 Select **Fabrics**, then click the fabric that contains the switch.

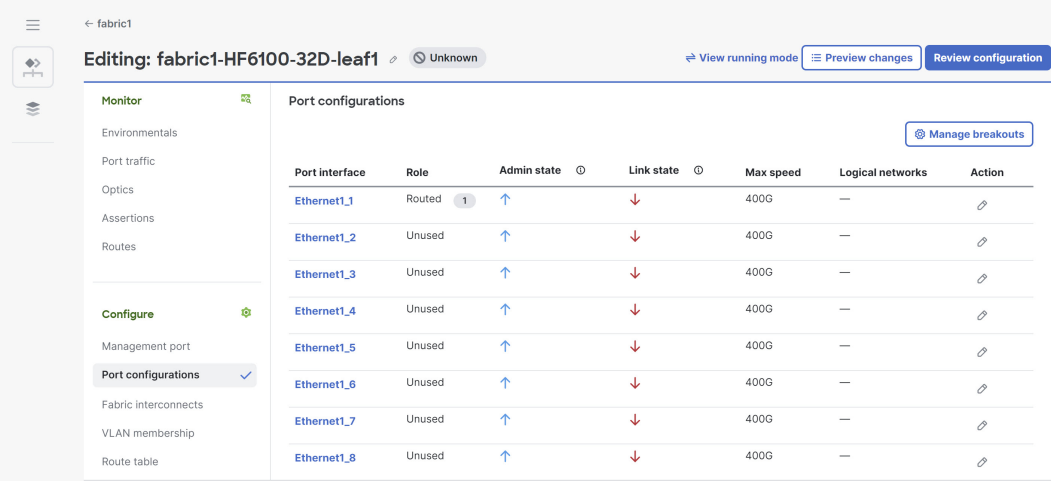
Step 2 If the fabric is not in the edit mode, click **Switch to edit mode**.

Step 3 In the **Topology** area, click the switch position that you want to configure, then click the switch name.



Step 4 In the **Configure** area, click **Port configurations**.

The **Port configurations** table lists all ports of the switch.



Step 5 (Optional) If you want to enable or disable breakout for any of the ports, click **Manage breakouts**.

a) For **Breakout option**, select **Disable** to disable breakout. Otherwise, select the desired option to enable breakout.

The value in parenthesis indicates the number of lanes per port and the speed of each lane. For example, the value "2x200G (4x50G)" indicates 2 ports of 200G speed each and each port uses four 50G lanes for a total of 400G speed and 8 lanes.

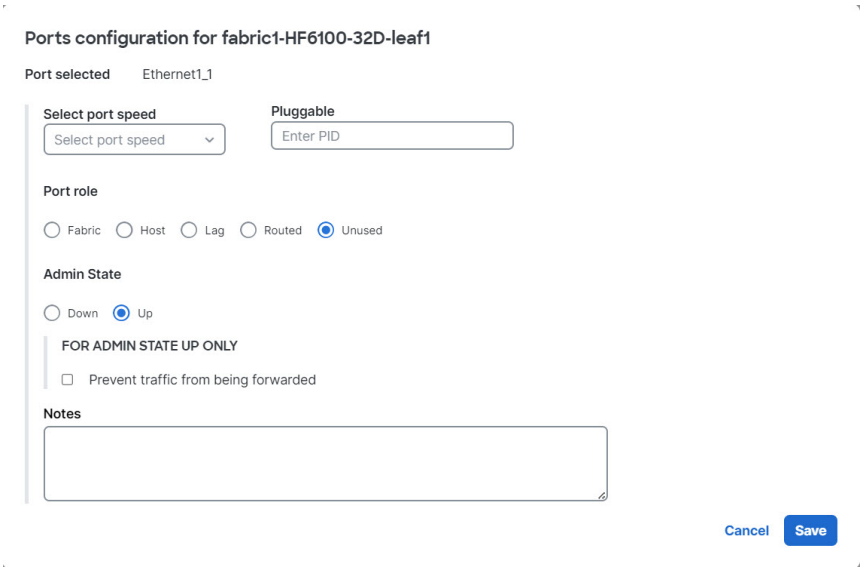
You must select an option that corresponds to the speed of pluggables on the connected switch.

b) (Optional) If you enabled breakout, select the cable type and optic type.

c) Click **Save**.

Step 6 In the **Port configurations** table, under the **Action** column, click the edit button (✎) for the port that you want to configure.

A dialog box opens for configuring the port.



a) For **Select port speed**, select the speed of the port.

The value in parenthesis indicates the number of lanes and the speed of each lane. For example, the value "200G (4x50G)" indicates that the port has a total speed of 200G and uses four 50G lanes.

By default, a port transmits and receives data at its highest speed. You can change the speed to something slower, if desired. You cannot change the speed of a broken out port.

For your switch fabric ports, if you want to use a non-default speed, you must select the appropriate speed. For example, for QSFP-DD ports, you can use 40G, 100G, or 200G instead of the default of 400G.

b) For **Pluggable**, enter the product ID (PID) of the optic for the port.

Forwarding error correction (FEC) is automatically set based on the specified pluggable. You cannot configure FEC manually.

c) For **Port role**, select **Fabric** for a port that connects to another leaf or spine switch in the fabric.

For other port types, select the role according to the purpose of the port.

- **Fabric**—Provides connectivity between fabric switches and allows for automatic discovery by peer switches. Select this for a port that connects to another leaf or spine switch in the fabric.
- **Host**—Provides a Layer 2 connection to a server or other general network device.
- **Port channel**—The port is a member of a port channel, also known as a link aggregation group (LAG). When you configure a port to be a member of a port channel, its role is automatically changed from **Unused** to **Port channel**. The **Port channel** role cannot be changed in this menu unless the port is first removed from the port channel.
- **Routed**—Provides a Layer 3 connection to a router or other network device.

  When you configure a routed port on a switch, you can select to enable VLAN tagging, which requires you to configure 802.1Q VLAN sub-interfaces on a Layer 3 interface to forward IPv4 and IPv6 packets to another device using static or dynamic routing protocols. You can use Layer 3 interfaces for IP routing. Alternatively, if you leave VLAN tagging disabled, you instead only select a route table (VRF) and specify IPv4 addresses or IPv6 addresses for the routes. See the succeeding substeps for the additional routed port configuration steps.
- **Unused**—The port does not forward or receive traffic.

d) If you chose **Routed** for the port role and you want to use VLAN tagging, toggle on **Enable VLAN tagging** and follow these additional steps.

1. Click **Add a sub interface**.
2. In **VLAN tag**, enter the tag.

   Do not assign the same VLAN tag to multiple sub-interfaces on the same physical interface.
3. For **Select VRF**, select a VRF instance.
4. For the **IP address** fields, enter an IPv4 address and mask, an IPv6 address, or both.

e) If you chose **Routed** for the port role and you do not want to use VLAN tagging, leave **Enable VLAN tagging** as toggled off and perform these additional steps.

1. For **Select route table**, select the desired route table (VRF).
2. For the **IP addresses** fields, enter one or more IPv4 or IPv6 addresses and masks.

   If you enter multiple addresses, separate each one with a comma.

f) For **Admin state**, select **Up** to enable the port.

- **Up**—The port will receive and forward traffic. This is the default state.

To set the port to be Up but not forwarding traffic, check **Prevent traffic from being forwarded**.

- **Down**—The port will not receive nor forward traffic.

g) Click **Save**.

Step 7 Repeat the previous step for every port on this switch that will connect to another leaf or spine switch or host in the fabric.

Step 8 Repeat this procedure for every leaf or spine switch in the fabric.

Configure multiple ports at the switch level

You can configure various properties of multiple ports of a switch simultaneously, such as the role and speed. The port role specifies the type of connection provided by a port.

Some properties choices expose additional properties that you cannot set using this procedure; you can set the additional properties only by configuring the ports individually. The descriptions in the steps specify which properties have this limitation.

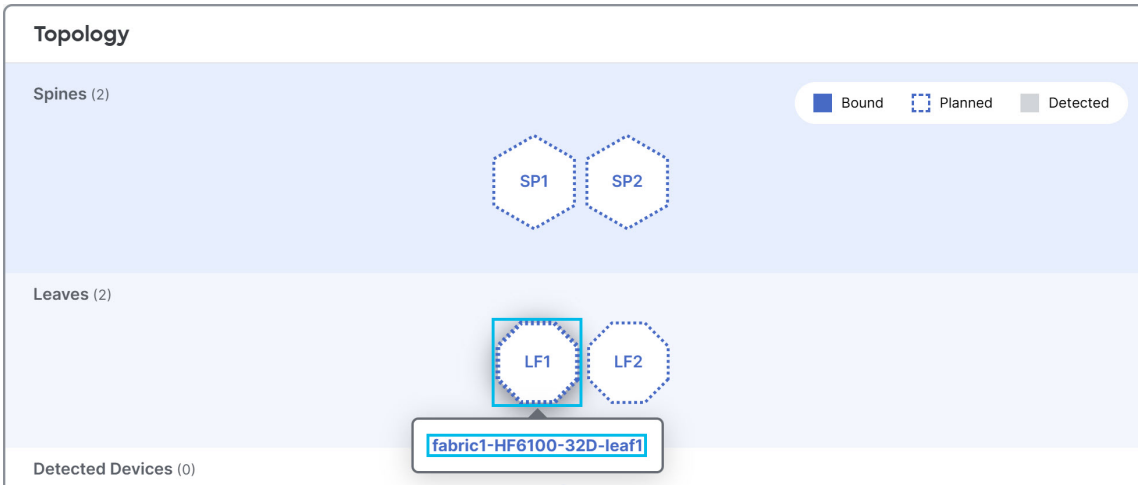
Follow these steps to configure multiple ports at the switch level.

Step 1 Select **Fabrics**, then click the fabric that contains the switch.

Step 2 If the fabric is not in the edit mode, click **Switch to edit mode**.

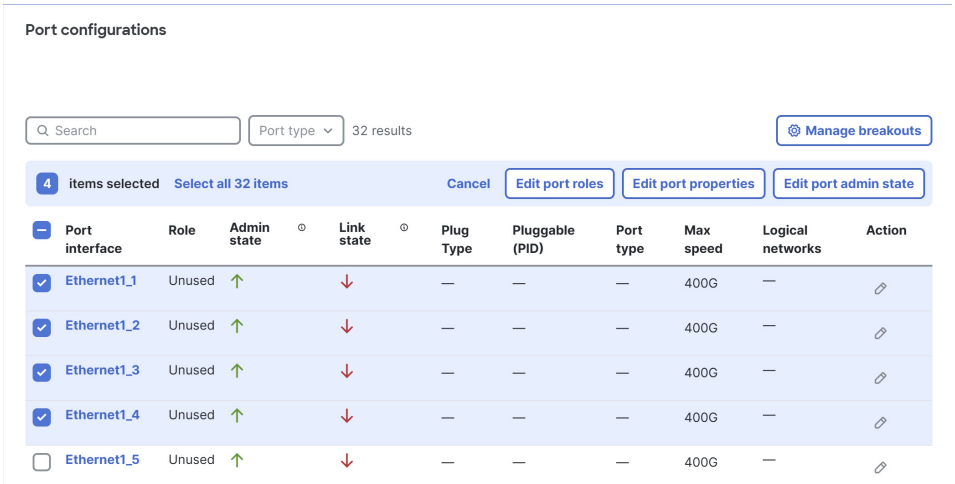
Step 3 In the **Topology** area, click the switch position that you want to configure, then click the switch name.

Figure 10: Clicking a switch position and switch name



Step 4 In the **Configure** area, click **Port configurations**, then select the ports that you want to configure by putting a check in the box next to each port ID.

Figure 11: Multiple ports selected



Step 5 If you want to change the role of the ports, click **Edit port roles**.

a) For **Port role**, select the desired role.

- **Fabric**—Provides connectivity between fabric switches and allows for automatic discovery by peer switches. Select this for a port that connects to another leaf or spine switch in the fabric.
- **Host**—Provides a Layer 2 connection to a server or other general network device. If you enabled global spanning tree, you cannot select the STP blocking modes using this procedure.
- **Port channel**—The port is a member of a port channel, also known as a link aggregation group (LAG). When you configure a port to be a member of a port channel, its role is automatically changed from **Unused** to **Port channel**. The **Port channel** role cannot be changed in this menu unless the port is first removed from the port channel.
- **Routed**—Provides a Layer 3 connection to a router or other network device. You cannot enable nor disable VLAN, add sub interfaces, select a route table, nor specify IP addresses using this procedure.
- **Unused**—The port does not forward nor receive traffic. If you intend to configure the port to be a port channel member, the role must initially be **Unused**.

b) Click **Save**.

Step 6 If you want to change the port properties, click **Edit port properties**. The properties include the port speed and pluggable.

a) For **Configure port speed**, select the speed of the port.

The value in parenthesis indicates the number of lanes and the speed of each lane. For example, the value "200G (4x50G)" indicates that the port has a total speed of 200G and uses four 50G lanes.

By default, a port transmits and receives data at its highest speed. You can change the speed to something slower, if desired. You cannot change the speed of a broken out port.

For your switch fabric ports, if you want to use a non-default speed, you must select the appropriate speed. For example, for QSFP-DD ports, you can use 40G, 100G, or 200G instead of the default of 400G.

b) For **Pluggable**, enter the product ID (PID) of the optic for the port or select the pluggable from the table.

c) Click **Save**.

Step 7 If you want to change the admininistrative state, click **Edit port admin state**.

a) For **Admin state**, select the desired state.

- **Up**—The port will receive and forward traffic. This is the default state.

  To set the port to be Up but not forwarding traffic, check **Prevent traffic from being forwarded**.

- **Down**—The port will not receive nor forward traffic.

b) Click **Save**.

Configure a port at the fabric level

You can configure any port of any switch in a fabric by going to the **Physical topology** area of that fabric. This page makes it easy to configure the ports of different switches.

Follow these steps to configure a port at the fabric level.

Step 1 Select **Fabrics**, then click the fabric that contains the switch for which you want to configure its ports.

Step 2 If the fabric is not in the edit mode, click **Switch to edit mode**.

Step 3 In the **Physical topology** area, click **Port configurations**.

The **Port configurations** table lists all ports of all switches in the fabric.

Step 4 Above the **Port configurations** table, you can use the various fields and drop-down lists to filter the table.

- **Search**—The table displays only the ports whose IDs contain the string that you enter.
- **From**—The table displays only the ports whose port number is equal to or greater than the integer that you enter.
- **To**—The table displays only the ports whose port number is equal to or less than the integer that you enter.
- **Port type**—The table displays only the ports with the type that you select.
- **Model**—The table displays only the ports with the model that you select.

Step 5 In the **Action** column, click the edit button (✎) for the port that you want to configure.

a) For **Select port speed**, select the speed of the port.

The value in parenthesis indicates the number of lanes and the speed of each lane. For example, the value "200G (4x50G)" indicates that the port has a total speed of 200G and uses four 50G lanes.

By default, a port transmits and receives data at its highest speed. You can change the speed to something slower, if desired. You cannot change the speed of a broken out port.

For your switch fabric ports, if you want to use a non-default speed, you must select the appropriate speed. For example, for QSFP-DD ports, you can use 40G, 100G, or 200G instead of the default of 400G.

b) For **Pluggable**, enter the product ID (PID) of the optic for the port.

Forwarding error correction (FEC) is automatically set based on the specified pluggable. You cannot configure FEC manually.

c) For **Port role**, select **Fabric** for a port that connects to another leaf or spine switch in the fabric.

For other port types, select the role according to the purpose of the port.

- **Fabric**—Provides connectivity between fabric switches and allows for automatic discovery by peer switches. Select this for a port that connects to another leaf or spine switch in the fabric.

- **Host**—Provides a Layer 2 connection to a server or other general network device.
- **Port channel**—The port is a member of a port channel, also known as a link aggregation group (LAG). When you configure a port to be a member of a port channel, its role is automatically changed from **Unused** to **Port channel**. The **Port channel** role cannot be changed in this menu unless the port is first removed from the port channel.
- **Routed**—Provides a Layer 3 connection to a router or other network device.

  When you configure a routed port on a switch, you can select to enable VLAN tagging, which requires you to configure 802.1Q VLAN sub-interfaces on a Layer 3 interface to forward IPv4 and IPv6 packets to another device using static or dynamic routing protocols. You can use Layer 3 interfaces for IP routing. Alternatively, if you leave VLAN tagging disabled, you instead only select a route table (VRF) and specify IPv4 addresses or IPv6 addresses for the routes. See the succeeding substeps for the additional routed port configuration steps.
- **Unused**—The port does not forward or receive traffic.

d) If you chose **Routed** for the port role and you want to use VLAN tagging, toggle on **Enable VLAN tagging** and follow these additional steps.

1. Click **Add a sub interface**.
2. In **VLAN tag**, enter the tag.

   Do not assign the same VLAN tag to multiple sub-interfaces on the same physical interface.
3. For **Select VRF**, select a VRF instance.
4. For the **IP address** fields, enter an IPv4 address and mask, an IPv6 address, or both.

e) If you chose **Routed** for the port role and you do not want to use VLAN tagging, leave **Enable VLAN tagging** as toggled off and perform these additional steps.

1. For **Select route table**, select the desired route table (VRF).
2. For the **IP addresses** fields, enter one or more IPv4 or IPv6 addresses and masks.

   If you enter multiple addresses, separate each one with a comma.

f) For **Admin state**, select **Up** to enable the port.

- **Up**—The port will receive and forward traffic. This is the default state.

  To set the port to be Up but not forwarding traffic, check **Prevent traffic from being forwarded**.
- **Down**—The port will not receive nor forward traffic.

g) Click **Save**.

Configure multiple ports at the fabric level

You can configure any port of any switch in a fabric by going to the **Physical topology** area of that fabric. This page makes it easy to configure the ports of multiple switches simultaneously.

Some properties choices expose additional properties that you cannot set using this procedure; you can set the additional properties only by configuring the ports individually. The descriptions in the steps specify which properties have this limitation.

Follow these steps to configure multiple ports at the fabric level.

Step 1 Select **Fabrics**, then click the fabric that contains the switches for which you want to configure their ports.

Step 2 If the fabric is not in the edit mode, click **Switch to edit mode**.

Step 3 In the **Physical topology** area, click **Port configurations**.

The **Port configurations** table lists all ports of all switches in the fabric.

Step 4 Above the **Port configurations** table, you can use the various fields and drop-down lists to filter the table.

- **Search**—The table displays only the ports whose IDs contain the string that you enter.
- **From**—The table displays only the ports whose port number is equal to or greater than the integer that you enter.
- **To**—The table displays only the ports whose port number is equal to or less than the integer that you enter.
- **Port type**—The table displays only the ports with the type that you select.
- **Model**—The table displays only the ports with the model that you select.

Step 5 Select the ports that you want to configure by putting a check in the box next to each port ID. The ports can belong to different switches.

Step 6 If you want to change the role of the ports, click **Edit port roles**.

a) For **Port role**, select the desired role.

- **Fabric**—Provides connectivity between fabric switches and allows for automatic discovery by peer switches. Select this for a port that connects to another leaf or spine switch in the fabric.
- **Host**—Provides a Layer 2 connection to a server or other general network device. If you enabled global spanning tree, you cannot select the STP blocking modes using this procedure.
- **Port channel**—The port is a member of a port channel, also known as a link aggregation group (LAG). When you configure a port to be a member of a port channel, its role is automatically changed from **Unused** to **Port channel**. The **Port channel** role cannot be changed in this menu unless the port is first removed from the port channel.
- **Routed**—Provides a Layer 3 connection to a router or other network device. You cannot enable nor disable VLAN, add sub interfaces, select a route table, nor specify IP addresses using this procedure.
- **Unused**—The port does not forward nor receive traffic. If you intend to configure the port to be a port channel member, the role must initially be **Unused**.

b) Click **Save**.

Step 7 If you want to change the port properties, click **Edit port properties**. The properties include the port speed and pluggable.

a) For **Configure port speed**, select the speed of the port.

The value in parenthesis indicates the number of lanes and the speed of each lane. For example, the value "200G (4x50G)" indicates that the port has a total speed of 200G and uses four 50G lanes.

By default, a port transmits and receives data at its highest speed. You can change the speed to something slower, if desired. You cannot change the speed of a broken out port.

For your switch fabric ports, if you want to use a non-default speed, you must select the appropriate speed. For example, for QSFP-DD ports, you can use 40G, 100G, or 200G instead of the default of 400G.

b) For **Pluggable**, enter the product ID (PID) of the optic for the port or select the pluggable from the table.

c) Click **Save**.

Step 8 If you want to change the admininistrative state, click **Edit port admin state**.

a) For **Admin state**, select the desired state.

- **Up**—The port will receive and forward traffic. This is the default state.

  To set the port to be Up but not forwarding traffic, check **Prevent traffic from being forwarded**.

- **Down**—The port will not receive nor forward traffic.

b) Click **Save**.

Guidelines for configuring ports

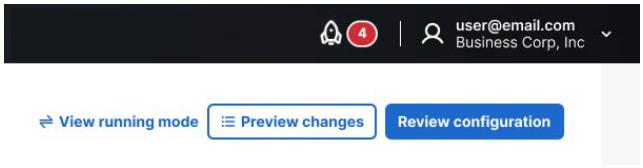
With the Cisco HF6100-60L4D switch, when you configure the speed of one of the SFP56 ports in a port group, the speed of the other port gets configured with the same speed.

Finish and commit the design

Your changes are not applied to the fabric until you review, commit, and push them.

Follow these steps to finish and commit the design.

Step 1 Click **Review configuration**.



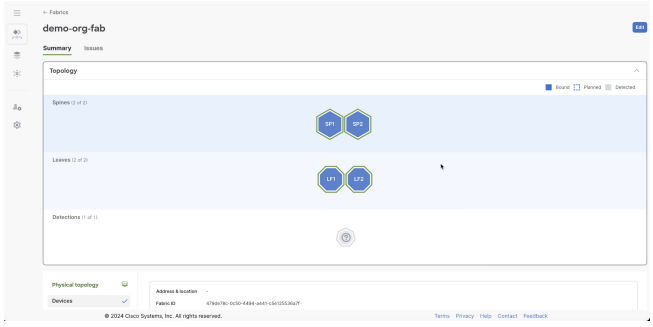
Step 2 Verify your changes in the review list.

Step 3 Click **Comment and push**.

Step 4 In the **Comment before pushing configuration** dialog box, enter the reason for the change.

Step 5 Click **Push configuration**.

If you bound any switches as part of this push, all switch icons should have a green outline.



A red outline indicates a red assertion and you should investigate the issue.

Bill of materials and ordering

Deployment

Deployment provides information about the assembly list and bill of materials (BOM) calculations and specifies if you need any parts for your fabric. You can export a CSV file of the assembly list and BOM for reference outside of Cisco Nexus Hyperfabric.

View or export deployment information

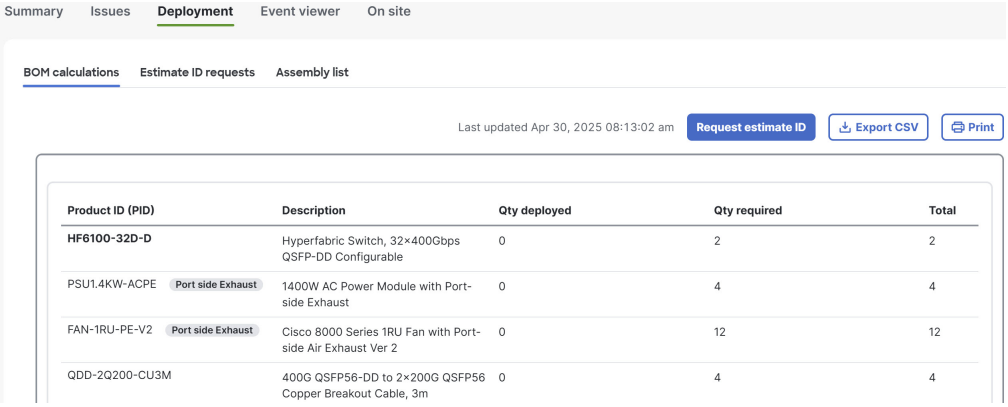
You can view deployment information or also export the deployment information to a CSV file to use as reference. You can view or export this information:

- A bill of materials for ordering products to build the fabric according to the blueprint design
- An assembly list to check the fulfillment of the necessary accessories, such as fans, power supplies, and optics required for each switch

Follow these steps to view or export deployment information.

Step 1 Select **Fabrics**, then click the desired fabric.

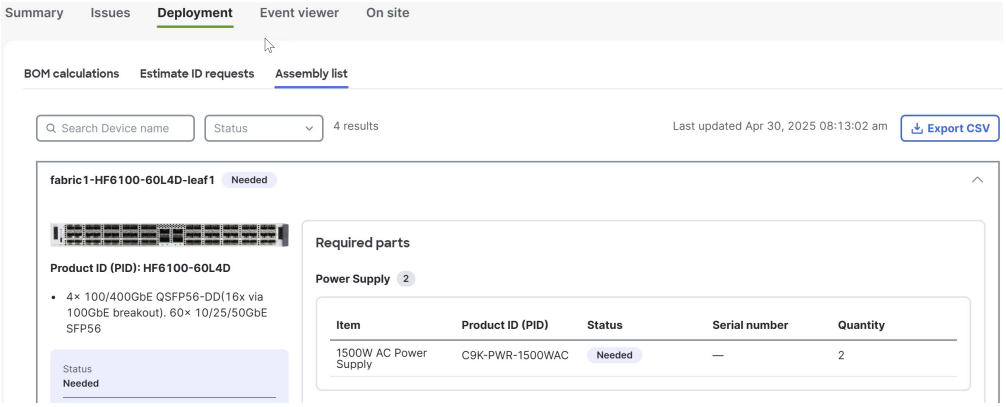
Step 2 Select **Deployment** > **BOM calculations**.



This page displays a bill of materials (BOM) of product IDs (PIDs), which specify the switches and accessories needed for this fabric design, as well as the optics based on the port connection configuration. The table shows how many of each PID are required and how many have been received and deployed.

Step 3 (Optional) To export the BOM as a comma-separated value (CSV) spreadsheet, click **Export CSV**.

Step 4 Click the **Assembly list**.



This page displays a list of accessories, such as fans, power supplies, and optics required for each switch. The table indicates whether the parts have been deployed and, if available, the serial numbers of the deployed parts.

Step 5 (Optional) To export the assembly list as a comma-separated value (CSV) spreadsheet, click **Export CSV**.

Request an estimate ID for a bill of materials

When you request an estimate ID for a bill of materials (BOM), Cisco Nexus Hyperfabric communicates with the Cisco Commerce Workspace (CCW) to create the estimate and sends you an email with the estimate ID. You can then work with your partner or sales team contacts to discuss the estimate and order the parts.

Cisco Nexus Hyperfabric retains estimate IDs for 90 days. From the **Estimate ID requests** page, you can download any of the BOMs to save for a longer amount of time. If an estimate ID expires, you can request a new estimate ID.

Follow these steps to request an estimate ID for a bill of materials.

Step 1 Select **Fabrics**.

Step 2 Click the fabric that has the BOM for which you want the estimate ID.

Step 3 Select **Deployment** > **BOM calculations**.

Step 4 Click **Request estimate ID** and perform these substeps.

a) In the **Request estimate ID** dialog box, click **Submit request**.

The dialog box closes and Cisco Nexus Hyperfabric sends you an email from "Cisco Hyperfabric <noreply@hyperfabric.cisco.com>". The body of the email contains the estimate ID and the estimate name.

b) (Optional) If you want to see information about this estimate ID and any past estimate IDs, select **Deployment** > **Estimate ID requests**.

From this page, you can download a BOM in the format of a CSV file by clicking the download button in the **Action** column.

Step 5 Provide your Cisco partner or sales team contacts with the estimate ID.

The estimate created by Cisco Nexus Hyperfabric is read-only. Your contacts must create a clone of the estimate, which will have a new estimate ID. Your contacts will then assist you with the cost estimate and complete your order using the new ID.

Onboarding the fabric

Onboard a fabric

This procedure provides a high-level overview of the tasks you must perform to onboard a fabric.

Before you can onboard a fabric, you must physically install your fabric and wire the fabric to match the Cisco Nexus Hyperfabric blueprint.

Follow these steps to onboard a fabric.

Step 1 Allow the switches to contact the Cisco Nexus Hyperfabric cloud service.

Step 2 Claim the switches to your organization.

Step 3 Bind each switch to its position in your fabric blueprint, allowing it to receive its specific configuration from the Cisco Nexus Hyperfabric.

Prerequisites for onboarding

Before you can onboard your installed fabric, you must have the following:

- A working Internet connection to which a switch can connect for HTTPS (port 443) traffic
- An available DNS server
- A configured proxy server, if needed to reach the cloud
- At least one management IPv4 or IPv6 address for a switch in your fabric

Note

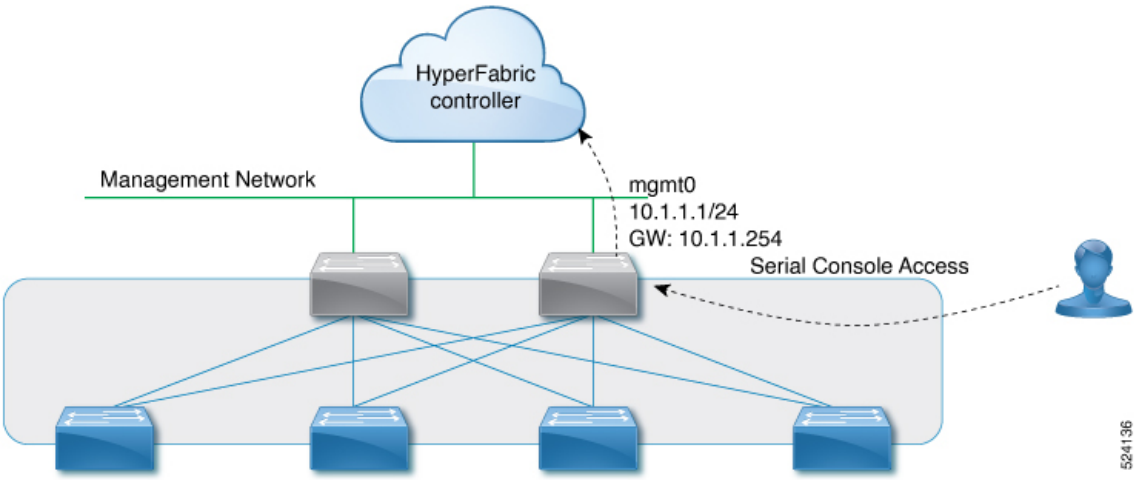
We recommend that you connect all switches in your fabric to a management network.

Connect the first switch to the Cisco Nexus Hyperfabric cloud service

Upon delivery, a new Nexus Hyperfabric switch contains an agent that allows it to discover its neighbors and to contact Cisco Nexus Hyperfabric.

The following diagram shows an example of configuring the first switch for out-of-band (OOB) management node connection to the Cisco Nexus Hyperfabric. The management node configuration can be achieved through DHCP, if available, or by serial port configuration if you need a static IP address.

Figure 12: Configuring the first switch for out-of-band management node connection to Cisco Nexus Hyperfabric



Typically, you will need to connect physically only one switch to the cloud. This switch automatically contacts Cisco Nexus Hyperfabric. When discovered by its neighbor switches in the fabric, this switch reports its availability as the "exit node" switch. Neighboring switches that lack OOB management connectivity can connect to Cisco Nexus Hyperfabric through the exit node switch.

Follow these steps to connect the first switch to the Cisco Nexus Hyperfabric cloud service.

Step 1 At the physical site, select a switch that will have the initial Internet connection. This cloud-connected switch will become the exit node.

Step 2 Connect the switch's OOB management interface to an Internet connection.

Step 3 If a DHCP server is present, you can skip the remaining steps in this procedure.

The switch will receive its DHCP configuration and will then contact Cisco Nexus Hyperfabric through the Internet connection.

Step 4 If you must configure a static IP address or if you must configure a proxy, connect a terminal to the serial console port of the switch using these connection parameters:

- 115200 baud
- no parity
- 8 data bits
- 1 stop bit

Step 5 Log in to the serial console using "ttg-admin" as the username and "hfabric2025" as the password.

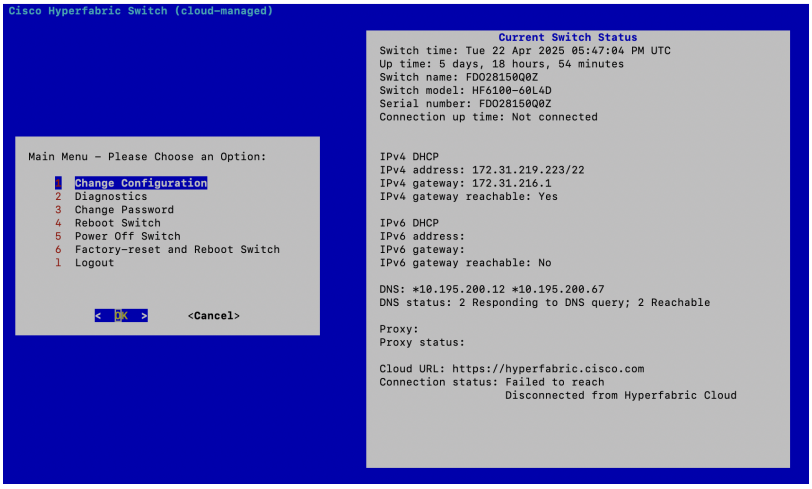
You are asked whether you want to change the default password, which we recommend that you do.

a) In the **Change default password** dialog, select **Yes**.
b) Enter the current password ("hfabric2025"), then enter your new password twice.

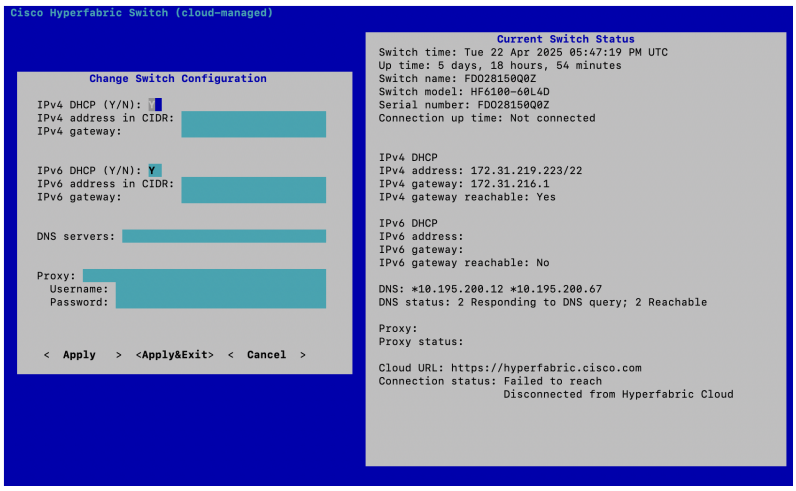
```
Changing password for ttg-admin.
Current password:
New password:
Retype new password:
passwd: password updated successfully
Press any key to continue
```

c) In the **Default password is changed successfully** dialog, select **OK**.

Step 6 In the console menu, select **Change Configuration**.



Step 7 Configure at least one management IPv4 or IPv6 address, or you can select DHCP if a DHCP server is present.



Step 8 (Optional) Configure one or more DNS addresses.

If you chose DHCP, keep these things in mind:

- You might not need any DNS addresses, although you can still configure DNS addresses if desired.
- You cannot have both a static DNS server configuration and a dynamic DNS server configuration. Cisco Nexus Hyperfabric overwrites the static configuration with the dynamic configuration.

Step 9 Configure a proxy setting, if needed.

Step 10 Click **Apply**.

a) Using the console, ensure that the **Connection status** shows that the switch is connected to the Cisco Nexus Hyperfabric cloud.

Neighboring switches can also now discover and access the Cisco Nexus Hyperfabric connection through this switch.

If the switch is not connected, you must troubleshoot the issue before you can proceed.

Tip In the console, you can check the reachability of the gateway, the DNS server, and Cisco Nexus Hyperfabric.

Claiming devices

Upon delivery, a new device is not associated with any owner or organization. Before deploying the device, you must claim it through Cisco Nexus Hyperfabric and add it to the organization that owns the fabric in which the device will be deployed.

Note

In some cases, your devices might already be claimed for your organization before delivery. If so, you can skip this procedure.

To claim the device, you must have physical and administrative access to the device.

Limitations for claiming devices

These limitations apply for claiming devices:

- You must claim the first device of your fabric using a claim code.
- When claiming devices without using claim codes, you can claim only switches that Cisco Nexus Hyperfabric has discovered. The discovery process is limited to switches that are directly connected to an already-claimed Nexus Hyperfabric switch. Only these directly connected devices will appear in the discovered list and be available for claiming.

Claim a device using a claim code

You must claim the first device of your fabric using a claim code. You can also claim subsequent devices using claim codes or you can claim discovered devices without using the claim codes. For information about claiming a device without using a claim code, see Claim a discovered device without using a claim code, on page 31.

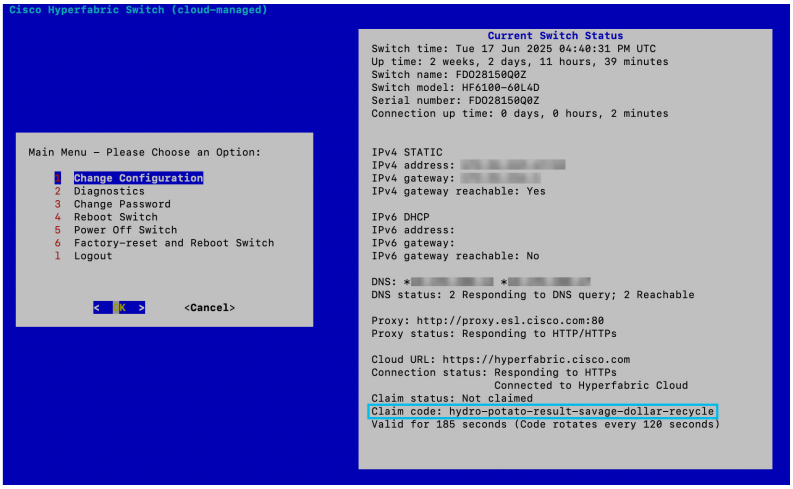
Follow these steps to claim a device using a claim code.

Step 1 Use the serial console to log in to the device and get the claim code that is shown in the serial console menu.

If you want to claim multiple devices, then get the code from every device that you want to claim.

The claim code that displays in the console changes every two minutes, although a code is valid for four minutes.

Figure 13: Example of a claim code



Step 2 In the Cisco Nexus Hyperfabric GUI, select **Inventory** > **Device Inventory**.

Step 3 Click **Claim devices**.

Step 4 Enter the claim code, then click **Claim**.

If you want to claim multiple devices, enter the codes separated by commas or new lines.

The device then becomes registered to the current organization as claimed. As the other fabric devices are installed and connected, unclaimed devices connected to the first device will be discovered.

Claim a discovered device without using a claim code

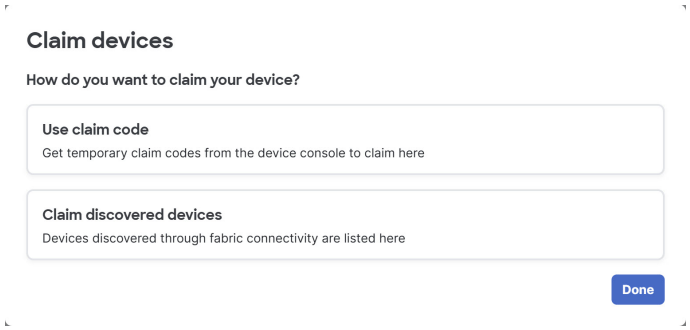
You must claim the first device of your fabric using a claim code, which means you cannot use this procedure for the first device. However, you can claim additional discovered devices without using the claim codes. For information about claiming the first device or a subsequent device using a claim code, see Claim a device using a claim code, on page 30.

Follow these steps to claim a discovered device without using a claim code.

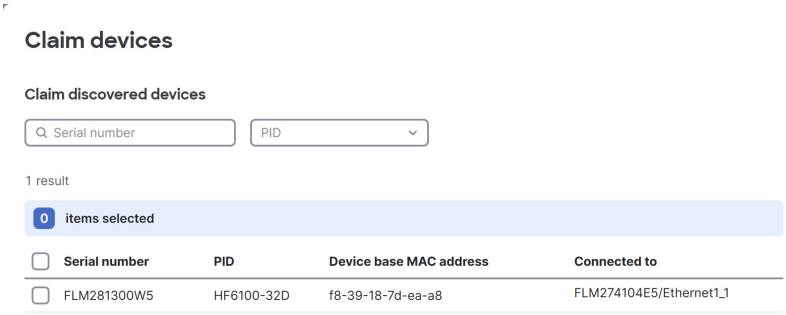
Step 1 Select **Inventory** > **Device Inventory**.

Step 2 Click **Claim devices**.

Step 3 Click **Claim discovered devices**.



Step 4 Select one or more switches, then click **Claim**.



The devices then become registered to the current organization as claimed.

Optionally, you can find the device with a specific serial number using the **Serial number** field and filter for switches with the product ID that you select from the **PID** drop-down.

Bind the switches

In Cisco Nexus Hyperfabric, you must assign each physical switch ("bind") to its logical position (node) in the fabric blueprint. When a switch has been bound to a node in the blueprint, it can download its configuration from Cisco Nexus Hyperfabric.

A switch that has been claimed but not yet bound to an organization's fabric is considered to be bound to the parking lot—a "null" fabric—until it is bound to an actual fabric.

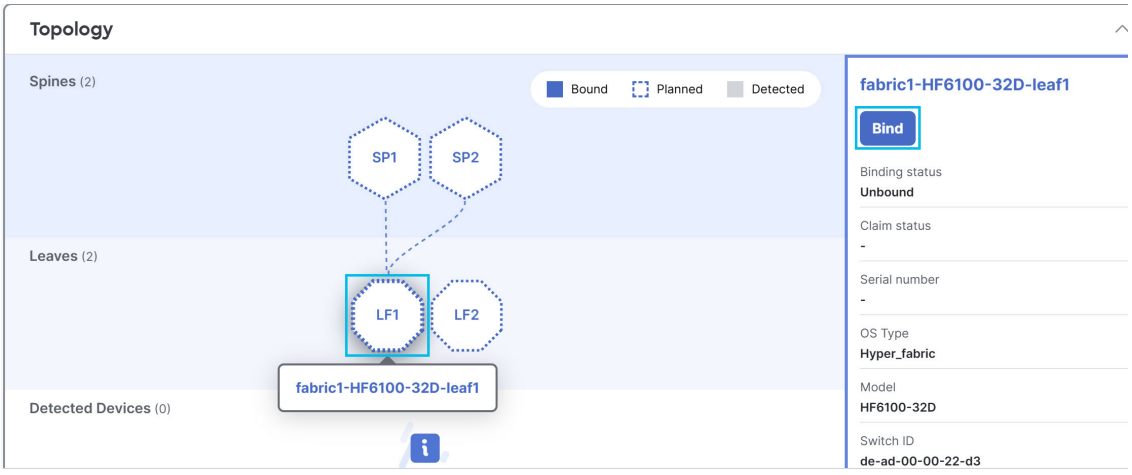
Follow these steps to bind the switches.

Step 1 Select **Fabrics**.

Step 2 Click the fabric that contains the switches.

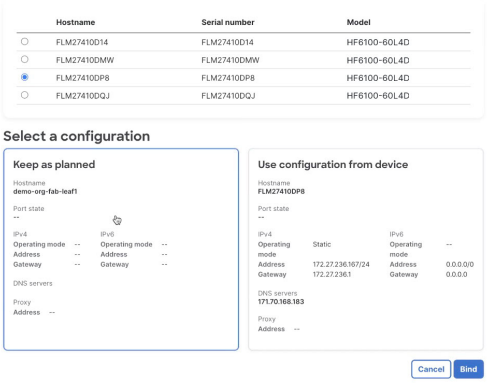
Step 3 If the fabric is not in the edit mode, click **Switch to edit mode**.

Step 4 In the **Topology** area, click the position of the switch that you want to bind, then click **Bind** in the switch information pane.



Step 5 Select the physical switch to assign to this position in the topology.

The window expands to show two options for the switch configuration.



Step 6 Select the configuration.

- **Keep as planned**—Uses the configuration that is defined in the blueprint. If you select this, ensure that your switch can still connect to the cloud with the configuration defined in the blueprint. See the "Configure the management interface" procedure in the *Cisco Nexus Hyperfabric — Configure Switches* document.
- **Use configuration from device**—Uses the current device settings that were configured through the serial port. Cisco Nexus Hyperfabric updates the blueprint with the device's settings.

Step 7 To bind the switch to this logical location in the fabric blueprint, click **Bind**.

When the binding operation for a switch has completed successfully, the switch icon in the topology view is blue.

Step 8 Repeat these steps to bind the remaining switches.

Step 9 Verify the cloud connectivity status of the switches.

a) Go back to the fabric page by clicking the name of the fabric near the top left of the page.

b) In the **Physical Topology** area, click **Cloud connectivity**.

On this page, these are some properties to observe:

- **Source IP:Port**—The source IP address and port.
- **Destination IP:Port**—The destination IP address and port.
- **Connection path**—The path through which the switch is connected to the cloud. These are the possible values:
  - **Management port**—The path is through the management port of the switch.
  - ***switch_name***—The path is through the specified switch, which is an exit node, on page 35.
  - ***port_ID***—The path is through the in-band management port of the switch. The port's ID is shown.
- **Certificate chain**—Specifies whether the switch's transport layer security (TLS) certificate is valid or invalid. If the certificate is invalid, click **Invalid** to see information about the issue.

View switch details by scanning the QR code

The Cisco 6000 series switches have stickers that have a unique QR code. The QR code provides a launch URL that contains the serial number of the switch. You can use a mobile device to scan the code, then open the URL to go to the switch details page in the Cisco Nexus Hyperfabric GUI.

For more information about the QR code, see the Cisco Nexus Hyperfabric Series – QR Code document.

Follow these steps to view switch details by scanning the QR code.

Step 1 Use a mobile device to scan the QR code.

Step 2 Go to the URL that the code provides.

One of these results occurs:

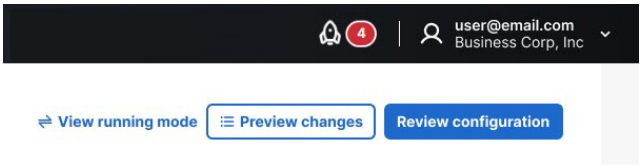
- If you are not logged into the Cisco Nexus Hyperfabric GUI, you are redirected to the login page. After you log in, the process continues as if you scanned the QR code while you were already logged in. See the other possible results.
- If you are logged into the Cisco Nexus Hyperfabric GUI and the switch is claimed by the organization that you are logged into, you see the GUI page that shows the details of the switch.
- If you are logged into the Cisco Nexus Hyperfabric GUI but the switch is unclaimed or the switch is claimed by an organization that you are not logged into, you cannot see the switch details.

Finish and commit the design

Your changes are not applied to the fabric until you review, commit, and push them.

Follow these steps to finish and commit the design.

Step 1 Click **Review configuration**.



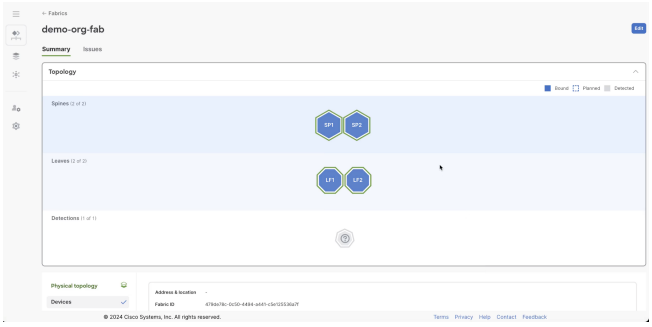
Step 2 Verify your changes in the review list.

Step 3 Click **Comment and push**.

Step 4 In the **Comment before pushing configuration** dialog box, enter the reason for the change.

Step 5 Click **Push configuration**.

If you bound any switches as part of this push, all switch icons should have a green outline.



A red outline indicates a red assertion and you should investigate the issue.

Terminology

Terminology

assertion

A statement used to test assumptions made by the system. If an assumed condition is true, the system is functioning as intended, which is a green assertion. If the condition evaluates to false, this is a red assertion that triggers an error or exception, alerting the operator to a potential failure or unexpected behavior. Assertions help ensure that the system is functioning as intended.

Assertions can be latched or unlatched, which affects whether an assertion becomes red when the assertion's condition evaluates to false. Generally, an assertion automatically becomes latched after 90 seconds. You can manually unlatch a latched assertion.

Example: Green and red, latched and unlatched assertion

When you bring up your fabric, the default port role is "Unused." Assume that there is no connection on Leaf1 Ethernet1_10. This results in the "Port link down" green assertion because the port role is "Unused." Even if you configure the port role to "Host" or "Routed," the "Port link unexpectedly down" red assertion is not raised because the port has never come up so far and the assertion is unlatched.

If Leaf1 Ethernet1_10 is set to "Routed" and it is UP, you will have the "Port link up" green assertion because the port role is "Host" and the port UP. If you then configure the port role to "Unused," the "Port link unexpectedly up" red assertion is raised because the assertion is latched, the port is UP, and the port's role is "Unused."

Example: Auto-latch assertion

Assume that you configured a BGP neighbor using the leaf switch Ethernet1_6 as the source port. Ethernet1_6 is set to "Routed" and it is UP. Initially, the "External BGP neighbor is up" assertion is unlatched. The assertion automatically becomes latched after 5 minutes. This results in the "External BGP neighbor is up" green assertion being raised if the BGP neighbor is established.

Example: Assertion suppression based on priority

Assume that Spine1 Ethernet1_1 (Fabric port) is UP and has the "Port not connected to expected neighbor" red assertion because of mis-cabling. Then, Spine1 Ethernet1_1 is set to Admin down, which raises the "Port link unexpectedly down" red assertion because the port that is set to "Fabric" is down. The "Port Connected to expected neighbor" assertion becomes "Unknown" because you must first fix the "Port link unexpectedly down" red assertion.

bind a switch

The process by which an organization's administrator maps a physical switch to a logical position in the fabric's blueprint. When a switch is bound, Cisco Nexus Hyperfabric pushes the blueprint-specified configuration to the switch.

blueprint

A conceptual design of a network fabric that fully specifies the topology, switch models, port types, connection types, interconnections, and network configuration of each switch. From the blueprint, a bill of materials and a cabling plan are generated.

claim a switch

The process by which an organization's administrator proves possession of and registers a physical switch to the organization.

exit node

During bring-up of the fabric, the fabric switch that has a working Internet connection to Cisco Nexus Hyperfabric. Other switches in the fabric can contact Cisco Nexus Hyperfabric through this switch.

fabric

A collection of switches specific to one organization, and each switch is specific to a single fabric. A fabric is the configuration and monitoring domain; users configure fabrics, not individual switches. A fabric is also a blueprint to which physical devices are bound and interconnected.

link aggregation control protocol

The link aggregation control protocol (LACP) is defined in the IEEE 802.3ad standard and enables devices to manage Ethernet channels between devices that conform to the standard. LACP facilitates the automatic creation of EtherChannels by exchanging LACP packets between Ethernet ports.

link layer discovery protocol

The link layer discovery protocol (LLDP) is a neighbor discovery protocol that is used for network devices to advertise information about themselves to other devices on the network. This protocol runs over the data-link layer, which allows two systems running different network layer protocols to learn about each other.

non-exit node

A node that does not have a direct connection to the Internet. A non-exit node uses the exit node as a proxy for its connection to the Internet.

organization

The basic unit of administration that may include one or more fabrics.

parking lot

A set of switches that are claimed to the organization but not yet bound to a fabric position. During a binding operation, these switches appear as a list of claimed switches that are available to be bound to a fabric position.

port channel

The port channel is a Layer 2 networking technology used to combine multiple physical Ethernet links into a single logical link. A basic port channel aggregates links from a single switch, while a multi-chassis port channel aggregates multiple physical links across a pair of switches, creating a single logical link.

port group

A port group is a collection of ports on a switch, and these ports have the same speed.

The numbers in the illustration indicate the port groups, and each group contains two ports. The remaining ports are not part of any port group and you can set their speed independently.

port role

The type of connection provided by a port. These are the supported port roles:

- **Fabric**—Provides connectivity between fabric switches and allows for automatic discovery by peer switches.

- **Host**—Provides a Layer 2 connection to a server or other general network device.
- **Port channel**—Specifies that the port is a member of a port channel.
- **Routed**—Provides a Layer 3 connection to a router or other network device.
- **Unused**—Specifies that the port does not forward nor receive traffic.

switch state

The operational status of a switch from delivery to being fully operational in the fabric of an organization. These are the states:

- **unclaimed**—The switch is not registered as being associated with any owner nor organization.
- **claimed**—An organization has proven that it has physical and administrative access to the switch.
- **unbound**—The switch has not been mapped to a logical position in a fabric blueprint.
- **bound**—The switch is mapped to a logical position in a fabric blueprint.

user

A person who has access, either read-only, read-write, or administrator, to an organization and its fabrics. A user may belong to one or more organizations. A user can create an organization only if the user is not a member of any existing organization.