



# Provision Fabric Networks

---

- [About Fabric Networks, on page 1](#)
- [New Automation for SD-Access, on page 3](#)
- [Add a Fabric Site, on page 4](#)
- [Configure Devices for a Fabric Site, on page 5](#)
- [Add a Device to a Fabric, on page 6](#)
- [Add a Device as a Border Node, on page 7](#)
- [Configure LISP Pub/Sub, on page 9](#)
- [Create an IP Transit Network, on page 9](#)
- [Create an SD-Access Transit Network, on page 10](#)
- [Select an Authentication Template, on page 11](#)
- [Configure Ports Within the Fabric Site, on page 12](#)
- [Configure Wireless SSIDs for Fabric Networks, on page 13](#)
- [Virtual Networks, on page 13](#)
- [Configure a Fabric Zone, on page 17](#)
- [Configure an Extended Node Device, on page 21](#)
- [Configure Supplicant-Based Extended Nodes, on page 28](#)
- [Configure a Port Channel, on page 35](#)
- [Multicast, on page 36](#)

## About Fabric Networks

A fabric network is a logical group of devices that is managed as a single entity in one or multiple locations. Having a fabric network in place enables several capabilities, such as the creation of virtual networks and user and device groups, and advanced reporting. Other capabilities include intelligent services for application recognition, traffic analytics, traffic prioritization, and steering for optimum performance and operational effectiveness.

Cisco DNA Center allows you to add devices to a fabric network. These devices can be configured to act as control plane, border, or edge devices within the fabric network.

## Fabric Sites

A fabric site is an independent fabric area with a unique set of network devices: control plane, border, edge, wireless controller, ISE PSN. Different levels of redundancy and scale can be designed per site by including local resources: DHCP, AAA, DNS, Internet, and so on.

A fabric site can cover a single physical location, multiple locations, or only a subset of a location:

- Single location: branch, campus, or metro campus
- Multiple locations: metro campus + multiple branches
- Subset of a location: building or area within a campus

A Software-Defined Access fabric network may comprise multiple sites. Each site has the benefits of scale, resiliency, survivability, and mobility. The overall aggregation of fabric sites accommodates a large number of endpoints and scales modularly or horizontally. Multiple fabric sites are interconnected using a transit site.

## Transit Sites

A transit site is a site that interconnects two or more fabric sites or connects the fabric site with external networks (Internet, data center, and so on). There are two types of transit networks:

- IP transit: Uses a regular IP network to connect to an external network or to connect two or more fabric sites. It leverages a traditional IP-based (VRF-LITE, MPLS) network, which requires remapping of VRFs and SGTs between sites.
- SD-Access transit: Uses LISP/VxLAN encapsulation to connect two fabric sites. The SD-Access transit area may be defined as a portion of the fabric that has its own control plane nodes, but does not have edge or border nodes. However, it can work with a fabric that has an external border. With an SD-Access transit, an end-to-end policy plane is maintained using SGT group tags.

## Fabric Readiness and Compliance Checks

### Fabric Readiness Checks

Fabric readiness checks are a set of preprovisioning checks done on a device to ensure that the device is ready to be added to the fabric. Fabric readiness checks are now done automatically when the device is provisioned. Interface VLAN and Multi VRF configuration checks are not done as part of fabric readiness checks.

Fabric readiness checks include the following:

- Connectivity checks: Checks for the necessary connectivity between devices; for example, connectivity from the edge node to map server, from edge node to border, and so on.
- Existing configuration check: Checks for any configuration on the device that conflicts with the configuration that is pushed through SD-Access and can result in a failure later.
- Hardware version: Checks if the hardware version of the device is supported.
- Image type: Checks if the device is running with a supported image type (IOS-XE, IOS, NXOS, Cisco Controller).
- Loopback interface: Checks for the loopback interface configuration on the device. A device must have a loopback interface numbered 0 with an IP address configured on it to work with the SDA application.

Lack of a loopback interface numbered 0 may cause fabric provisioning errors because Loopback0 is used as the routing locator (RLOC) by default.

- Software license: Checks if the device is running with an appropriate software license.
- Software version: Checks if the device is running with an appropriate software image.

For more information on the software versions supported, see the [Cisco SD-Access Hardware and Software Compatibility Matrix](#).

If an error is detected during any of the fabric readiness checks, an error notification is displayed on the topology area. You can correct the problem and continue with the provisioning workflow for the device.

### Fabric Compliance Checks

Fabric compliance is a state of a device to operate according to the user intent configured during the fabric provisioning. Fabric compliance checks are triggered based on the following:

- Every 24 hours for wired devices and every six hours for wireless devices.
- When there is a configuration change on the wired device.

A configuration change on the wired device triggers an SNMP trap, which in turn triggers the compliance check. Ensure that you have configured the Cisco DNA Center server as an SNMP server.

The following compliance checks are done to ensure that the device is fabric compliant:

- Virtual Network: Checks whether the necessary VRFs are configured on the device to comply with the current state of user intent for the VN on Cisco DNA Center.
- Fabric Role: Checks whether the configuration on the device is compliant with the user intent for a fabric role on Cisco DNA Center.
- Segment: Checks the VLAN and SVI configuration for segments.
- Port Assignment: Checks the interface configuration for VLAN and Authentication profile.

## New Automation for SD-Access

The enhanced Cisco SD-Access user interface (UX) integrates simplicity, flexibility, and a rich, intuitive context. The Beta version of the Cisco SD-Access UX augments the user experience and provides the following capabilities:

- Greater clarity in the association between the fabric elements like virtual networks and fabric site
- Enhanced workflows
- Succinct view of the fabric elements and their attributes

The enhanced Cisco SD-Access UX consists of the following:

- A summary page, each for virtual networks, fabric sites, and transit networks
- The **Virtual Networks** Summary view has four sections:

- The first section displays a count of tasks at different stages, a count of Layer 3 virtual networks and anycast gateways, a count of anycast gateways, Layer 2 virtual networks and their VLANs.
  - The second section shows a graphical representation of the virtual network tasks.
  - The third section displays a list of the saved tips.
  - The final section displays a card-based view of the different workflows offered.
- The **Fabric Sites** page provides three views: Summary view, Map view, and Table view.  
The Summary view shows tips and insights, and workflows that are in progress. It also provides a summary of the number of fabric sites, fabric zones, fabric devices, control planes, and border nodes.
  - The **Transits** page displays a summary of the number of SD-Access transits, SDWAN transits, and IP-based transits. This page also gives you the option to create a transit network.

Use the **Preview New SD-Access** toggle button on the Cisco DNA Center menu bar to switch between the old and enhanced Cisco SD-Access UX.




---

**Note** All the tasks described in this chapter pertain to the enhanced Cisco SD-Access UX.

---

## Add a Fabric Site

### Before you begin

You can create a fabric site only if IP Device Tracking (IPDT) is already configured for the site.

---

**Step 1** Click the menu icon (☰) and choose **Provision > Fabric Sites**.

**Step 2** Under **SUMMARY**, click the number that indicates the count of fabric sites.

**Step 3** Click **Create Fabric Sites and Fabric Zones**.

Alternatively, instead of the first three steps, click the menu icon (☰) and choose **Workflow > Create Fabric Site**.

**Step 4** In the **Create a Fabric site and Fabric Zones** window, click **Let's Do it** to go directly to the workflow.

**Step 5** In the **Fabric Site Location** window, choose an area, building, or floor to add as a fabric site.

**Step 6** In the **Wired Endpoint Data Collection** window, ensure that the **Monitor wired clients** check box is checked.

**Step 7** In the **Authentication Template** window, do the following:

a) Choose an authentication template for the fabric site:

- **Closed Authentication:** Any traffic before authentication is dropped, including DHCP, DNS, and ARP.
- **Open Authentication:** A host is allowed network access without having to go through 802.1X authentication.
- **Low Impact:** Security is added by applying an ACL to the switch port, to allow very limited network access before authentication. After a host has been successfully authenticated, additional network access is granted.
- **None**

- b) (Optional) If you choose **Closed Authentication**, **Open Authentication**, or **Low Impact**, click **Edit** to edit the authentication settings:
- **First Authentication Method**: Choose **802.1x** or **MAC Authentication Bypass (MAB)**
  - **802.1x Timeout (in seconds)**: Use the slider to specify the 802.1x timeout, in seconds.
  - **Wake on LAN**: Choose **Yes** or **No**.
  - **Number of Hosts**: Choose **Unlimited** or **Single**.
  - **BPDU Guard**: Use this check box to enable or disable the Bridge Protocol Data Unit (BPDU) guard on all the **Closed Authentication** ports.
  - **Pre-Authentication Access Control List**: Enable the toggle button to configure preauthentication control for **Low Impact** authentication. From the **Implicit Action** drop-down list, choose an implicit action. Enter a description for the rule. To add an access contract, click **Add Contract Action**, choose the rules, and click **Apply Table**.

**Step 8**

In the **Fabric Zones** window, choose one of the following options:

- To designate fabric zones and create scoped subnets, click **Setup Fabric Zones Now** and choose a fabric site from the network hierarchy displayed.
- To designate fabric zones later, click **Setup Fabric Zones Later**.

**Step 9**

In the **Summary** window, review the fabric site settings.

You can edit any of the fabric site or zone settings here.

**Step 10**

Click **Deploy**.

It takes a few seconds for the site and zones to be provisioned. Upon successful creation of the site, a **Success! Your fabric site is created** message is displayed.

---

## Configure Devices for a Fabric Site

You can configure the devices for a fabric site using the following tabs:

- **Fabric Infrastructure** tab: Assign devices to fabric roles.
- **Authentication Template** tab: Select an authentication template for the fabric. An authentication template is a predefined set of configurations that are retrieved from Cisco ISE.
- **Wireless SSIDs** tab: Specify wireless SSIDs within the network that hosts can access. You can select the guest or enterprise SSIDs and assign address pools, and click **Save**.
- **Port Assignment** tab: Apply specific configurations to each port, depending on the type of device that connects to the fabric site. To do this, select the ports that need a specific assignment, click **Assign**, and choose the port type from the drop-down list.

Note the following constraints:

- Cisco SD-Access deployments support only APs, extended nodes, user devices (such as a single computer or a single computer plus phone), and devices that need trunk ports like single servers.
- Servers with internal switches or virtual switches aren't supported.
- Other networking equipment (such as hubs, routers, or switches) isn't supported.

## Add a Device to a Fabric

After you have created a fabric site, you can add devices to the fabric site. You can also specify whether the device should act as a control plane node, an edge node, or a border node.

You can add a new device to the fabric site only if IP Device Tracking (IPDT) is configured for the fabric site.

A device which is assigned the Access role and has been provisioned before enabling IPDT on the site can't be added to the fabric. Reprovision such devices before adding them to the fabric site. Check the Provision workflow to confirm the status of **Deployment of IPDT** on the device.



### Note

- It's optional to designate the devices in a fabric site as control plane nodes or border nodes. You might have devices that don't occupy these roles. However, every fabric site must have at least one control plane node device and one border node device. In the current release for wired fabric, you can add up to six control plane nodes for redundancy.
- Currently, the Cisco Wireless Controller communicates only with two control plane nodes.

### Before you begin

Provision the device if you haven't already provisioned it:

- The **Provision > Network Devices > Inventory** window displays the discovered devices.
- The topology view shows a device in gray color if it has passed the fabric readiness checks and is ready to be provisioned.
- If an error is detected during any of the fabric readiness checks, an error notification is displayed on the topology area. Click **See more details** to check the problem area listed in the resulting window. Correct the problem and click **Re-check** to ensure that the problem is resolved.
- If you update the device configuration as part of problem resolution, ensure that you resynchronize the device information by performing an **Inventory > Resync** for the device.



### Note

You can continue to provision a device that has failed the fabric readiness checks.

**Step 1** Click the menu icon (☰) and choose **Provision > Fabric Sites**.

**Step 2** Under **SUMMARY**, click the number that indicates the count of fabric sites.

**Step 3** Select the fabric site to add a device.

The resulting topology view displays all devices in the network that have been inventoried. In the topology view, any device that is added to the fabric is shown in blue.

**Step 4** From the **List** view under the **Fabric Infrastructure** tab, click a device. A slide-in pane displays the following **Fabric** options:

Option	Description
Edge Node	Toggle the button next to this option to enable the selected device as an edge node.
Border Node	Toggle the button next to this option to enable the selected device as a border node.
Control Plane Node	Toggle the button next to this option to enable the selected device as a control plane node.

To configure a device as a fabric-in-a-box, select the **Control Plane Node**, **Border Node**, and **Edge Node** options.

To configure the device as a control plane and a border node, select both **Control Plane Node** and **Border Node**.

**Step 5** Click **Add**.

#### What to do next

After a device is added to the fabric, fabric compliance checks are automatically performed to ensure that the device is fabric-compliant. The topology displays a device that has failed the fabric compliance check in blue color with a cross-mark beside it. Click **See more details** on the error notification to identify the problem area and correct it.

## Add a Device as a Border Node

When you are adding a device to a fabric, you can add it in various combinations to act as a control plane, border node, or edge node as explained in [Add a Device to a Fabric, on page 6](#).

To add a device as a border node:

**Step 1** Click the menu icon (☰) and choose **Provision > Fabric Sites**.

**Step 2** In the **Fabric Sites** tab, under **SUMMARY**, click the number that indicates the count of fabric sites.

**Step 3** Select the fabric site to configure a border node.

The resulting topology view displays all devices in the network that have been inventoried. In the topology view, any device that is added to the fabric is shown in blue.

**Step 4** In the **List** view under the **Fabric Infrastructure** tab, click a device.

**Step 5** In the slide-in pane, enable the **Border Node** toggle button.

**Step 6** In the resulting slide-in pane, click the **Layer 3 Handoff** tab.

**Step 7** Check the **Enable Layer-3 Handoff** check box.

**Step 8** Enter the **Local Autonomous Number** for the device.

If the Local Autonomous Number is already configured on the device, this field displays the configured number and is disabled. You cannot change the Local Autonomous Number if it is already configured on the device.

- Step 9** To set a priority for the border node, check the **Modify Border Priority** check box and enter a priority value.
- The priority value ranges from 1 to 10. Lower the value, higher is the border priority. (1 indicates highest priority. 10 indicates lowest priority.) By default, the border priority is set to a value of 10.
- If two or more borders are configured in a network, traffic is routed through the border that has a higher priority. If no priority is set, the traffic is load balanced across the border nodes.
- Step 10** By default, a border is designated as an external border, wherein it acts as a gateway to all unknown traffic, without importing any external routes. A border can be configured to be an internal border, wherein it acts as a gateway to known traffic and imports specific external routes. A border can also have a combined role of internal and external borders.
- Check both **Default to all virtual networks** and **Do not import external routes** check boxes to designate the border as an external border, providing connectivity to unknown networks.
  - Do not check both **Default to all virtual networks** and **Do not import external routes** check boxes to designate the border as an internal border, operating as a gateway for specific network addresses.
  - Check the **Default to all virtual networks** check box to designate this border node as an internal and external border. It acts as a gateway to all known and unknown traffic that is sent from the edge nodes. (Do not check the **Do not import external routes** check box.)
- Step 11** Hover your cursor over **Add Transit Site** and select a transit network that is to be enabled on the border device.
- a) For an **IP:BGP IP TRANSIT**, configure the IP interface:
- Click **Add External Interface**.
  - Do the following steps in the resulting window:
    1. Choose an **External Interface**.
    2. The **Remote AS Number** is automatically derived from the selected Transit or Peer network.
    3. Enter the **Interface Description**.
    4. (Optional) Hover your cursor over the **Actions** drop-down list, and choose **Enable All** or **Disable All**.
    5. Toggle the **Enable Layer-3 Handoff** button for the intended virtual network. This virtual network is advertised by the border to the remote peer. You can select one, multiple, or all virtual networks.
    6. Enter a VLAN ID for the selected virtual network.
    7. Click **Save**.
  - Choose an IP pool from **Select IP Pool** drop-down list. The selected Pool is used to automate IP routing between the border node and the IP peer.
- Step 12** (Optional) Perform this step only if you are connecting a nonfabric network to the fabric network or you are migrating from a traditional network to an SDA network. Click the **Layer 2 Handoff** tab.
- A list of virtual networks and the count of IP pools in each virtual network is displayed.
- a) Click a virtual network that is to be handed off.
- A list of IP address pools that are present in the virtual network and a list of interfaces through which you can connect nonfabric devices are displayed.



- b) Select an **External Interface**.
- c) Enter the **Interface Description**.
- d) Enter the **External VLAN** number into which the fabric must be extended.

In releases earlier than Cisco DNA Center 2.1.2.6, a virtual network can only be handed off on a single interface. The same virtual network cannot be handed off through multiple interfaces.

In Cisco DNA Center Release 2.1.2.6 and later releases, a virtual network can be handed off on a single interface or on multiple interfaces. Layer 2 handoff for a segment can also be done on two different devices. In both cases, ensure that there are no loops that are formed in the network.

- e) Click **Save**.

**Step 13** Click **Add**.

---

## Configure LISP Pub/Sub

You can configure LISP Pub/Sub on a fabric site only when you add the first control plane to your fabric.

### Before you begin

Ensure that the fabric devices operate on Cisco IOS XE 17.6.1 or later releases.

---

**Step 1** Click the menu icon (☰) and choose **Provision > Fabric Sites**.

**Step 2** Under **SUMMARY**, click the number that indicates the count of fabric sites.

**Step 3** Select the fabric site to add a device.

The resulting topology view displays all devices in the network that have been inventoried. In the topology view, any device that is added to the fabric is shown in blue.

**Step 4** From the **List** view under the **Fabric Infrastructure** tab, click a device that is to be configured as a control plane.

**Step 5** In the slide-in pane, enable the **Control Plane Node** toggle button to configure this plane.

**Step 6** In the **Configure Control Plane** slide-in pane, choose **LISP PubSub** route distribution protocol and click **Add**.

**Step 7** Click **Add**.

**Step 8** Click **Deploy**.

**Step 9** In the **Modify Fabric** window, schedule the operation and click **Apply**.

To verify the configuration of LISP Pub/Sub in the fabric site, see the LISP Pub/Sub status on the **SITE SUMMARY** window.

---

## Create an IP Transit Network



**Step 1** Click the menu icon (☰) and choose **Provision > Transits**.

- Step 2** Click **Create Transit**.
- Step 3** In the **Transit** slide-in pane, enter a name for the transit network.
- Step 4** Choose **IP-Based**.  
The routing protocol is set to BGP by default.
- Step 5** Enter the Autonomous System Number (ASN) for the transit network.
- Step 6** Click **Save**.
- 

## Create an SD-Access Transit Network

To add an SD-Access transit network:

---

- Step 1** Click the menu icon () and choose **Provision > Transits**.
- Step 2** Click **Create Transit**.
- Step 3** In the **Transit** slide-in pane, enter a name for the transit network.
- Step 4** Choose an SD-Access **Transit Type**.  
To configure a transit for fabric sites that don't have a LISP Pub/Sub control plane, choose **SD-Access (LISP/BGP)**.  
To configure a transit for fabric sites that have a LISP Pub/Sub control plane, choose **SD-Access (LISP PubSub)**.  
To share the **SD-Access (LISP PubSub)** transit with other Cisco DNA Center clusters, choose **Yes, Share**. Otherwise, choose **No, keep it local**.
- Note** The **Yes, Share** option is visible only if the **Multiple Cisco DNA Center** package is installed on all the Cisco DNA Center clusters.
- Step 5** Choose a **Transit Control Plane Node Site** from the drop-down list. Choose at least one transit map server.
- Step 6** Choose a **Transit Control Plane Node** for the transit network from the drop-down list.
- Step 7** (Optional) To configure additional map server, click the plus icon () and repeat [Step 5, on page 10](#) and [Step 6, on page 10](#).
- Step 8** Click **Save**.

After creating the transit network, the **Transits** window displays the newly created transit and its attributes.

**Note** You can't add an **SD-Access (LISP PubSub)** transit to a fabric site that uses LISP/BGP control plane. You can't add **SD-Access (LISP/BGP)** transit to a fabric site that uses LISP Pub/Sub control plane.

---

### What to do next

To interconnect the fabric sites with an SD-Access Transit, add the transit to the border node.

# Select an Authentication Template

You can configure an authentication template that applies to all devices in the fabric site.

- 
- Step 1** Click the menu icon (☰) and choose **Provision > Fabric Sites**.
- Step 2** Under **SUMMARY**, click the number that indicates the count of fabric sites.
- Step 3** Click a fabric site.
- Step 4** Click the **Authentication Template** tab.
- Step 5** Under **Select Authentication Template**, choose an authentication template for the site:
- **Open Authentication:** A host is allowed network access without having to go through 802.1X authentication.
  - **Closed Authentication:** Any traffic prior to authentication is dropped, including DHCP, DNS, and ARP.
  - **Low Impact:** Security is added by applying an ACL to the switch port, to allow limited network access prior to authentication. After a host has been successfully authenticated, additional network access is granted.
  - **None**

You can edit the settings of the selected authentication template to address site-specific authentication requirements.

Before you change the site-level authentication, you must resynchronize any fabric device whose Access Points were onboarded through macros or autoconf and haven't yet undergone the periodic resync.

- Step 6** (Optional) To edit the settings of the chosen authentication method, click **Edit**.
- a) In the slide-in pane, complete the following:
- **First Authentication Method:** Choose **802.1x** or **MAC Authentication Bypass (MAB)**
  - **802.1x Timeout (in seconds):** Use the slider to specify the 802.1x timeout, in seconds.
  - **Wake on LAN:** Choose **Yes** or **No**.
- Wake on LAN (WoL) is supported only in the following scenarios:
- The source (WoL initiator) and destination (sleeping host) are both in the same subnet and Layer 2 Flooding is enabled.
  - The source is outside the SD-Access fabric but located in the network that is connected to the fabric through Layer 3 handoff and the destination is in an SD-Access subnet with IP-Directed Broadcast enabled.
- Note** The following topologies do not support Wake on LAN:
- The WoL initiator and the sleeping host are on different subnets within the same Layer 3 Virtual Network.
  - The WoL initiator routes to the sleeping host over an SD-Access Transit.
- **Number of Hosts:** Choose **Unlimited** or **Single**.
- Note** **Number of Hosts** specifies the number of data hosts that can be connected to a port. With **Single**, you can have only one data client on the port. With **Unlimited**, you can have multiple data clients and one voice client on the port.

- **Pre-Authentication Access Control List:** Enable the toggle button to configure preauthentication control for **Low Impact** authentication. From the **Implicit Action** drop-down list, choose an implicit action. Enter a description for the rule. To add an access contract, click **Add Contract Action**, choose the rules, and click **Apply Table**.

b) Click **Save**.

The saved modifications apply only to the site for which the authentication template is edited.

**Step 7** Click **Deploy**.

The Hitless Authentication Change feature lets you switch from one authentication method to another without removing the devices from the fabric.

## Configure Ports Within the Fabric Site

The **Port Assignment** tab lets you configure each access device in the fabric site. You can specify network behavior settings for each port on a device.

**Step 1** Click the menu icon (☰) and choose **Provision > Fabric Sites**.

**Step 2** Under **SUMMARY**, click the number that indicates the count of fabric sites.

**Step 3** Select a fabric site.

**Step 4** Click the **Port Assignment** tab.

**Step 5** From the list of fabric devices, expand the drop-down for the device that you want to configure. The ports that are available on the device are displayed.

**Step 6** Check the check box for the ports of the device.

**Step 7** Hover your cursor over **Configure** and choose **Assign Ports**.

**Step 8** In the slide-in pane, choose the **Connected Device Type** from the following options in the drop-down list:

Option	Description
User Devices (ip-phone, computer, laptop)	Configures the port to connect to a host device.
Access Point (AP)	Configures the port to connect to an access point.
Trunk	Configure the port as a trunk port.
Supplicant-Based Extended Node	Configures the port to receive a supplicant-based extended node.

- To connect host devices, choose **User Devices (ip-phone, computer, laptop)** and do the following:
  - Choose the VLAN name for data from the **VLAN Name (Data)** drop-down list.
  - Choose a security group from the **Security Group** drop-down list.
 

Security groups are supported only with the **None** authentication template.
  - Choose the VLAN name for voice from the **VLAN Name (Voice)** drop-down list.
  - Choose the authentication type from the **Authentication Template** drop-down list.

- e. Enter a **Description** for the connected device.
- To connect an access point, choose **Access Point (AP)** and do the following:
  - a. Choose the VLAN name from the **VLAN Name (Data)** drop-down list.
  - b. Choose the authentication type from the **Authentication Template** drop-down list.
  - c. Enter a **Description** for the connected device.
- To connect a supplicant-based extended node device, choose **Supplicant-Based Extended Node**.
- To connect a trunk port, choose **Trunk** and enter a **Description** for the port.

**Step 9** Click **Update**.

---

## Configure Wireless SSIDs for Fabric Networks

### Before you begin

Ensure to add the wireless device to the fabric site.

---

- Step 1** Click the menu icon (☰) and choose **Provision > Fabric Sites**.
  - Step 2** Under **SUMMARY**, click the number that indicates the count of fabric sites.
  - Step 3** Select a fabric site.
  - Step 4** Click the **Wireless SSIDs** tab and specify the wireless SSIDs within the network that the hosts can access.
  - Step 5** Click **Choose Pool** and select an IP pool reserve for the SSID.
  - Step 6** From the **Assign SGT** drop-down list, choose a security group for the SSID.
  - Step 7** Check the **Enable Wireless Multicast** check box to enable wireless multicast on the SSIDs.
- 

## Virtual Networks

Virtual networks are overlays that are used to segment traffic within a common physical network infrastructure; this is also known as macro-segmentation. Layer 2 Virtual Networks segment switched traffic and Layer 3 Virtual Networks segment routed traffic. Each endpoint that is connected to a Cisco SD-Access fabric is assigned to a specific virtual network based on the static edge port configurations or the dynamic policy from Identity Service Engine. Within a virtual network, endpoints can communicate with each other unless explicitly blocked by micro-segmentation policy. Endpoints across different virtual networks cannot communicate with each other by default. Inter-virtual network traffic requires connectivity policy to be implemented outside of the Cisco SD-Access fabric, such as on a fusion device.

A typical use case for virtual networks is an office building containing both corporate endpoints and building management systems. The corporate endpoints need to be segmented from building systems, such as lighting, heating, ventilation, and air conditioning. In this case a network administrator could macro-segment the

corporate endpoints and the building systems using two or more virtual networks to block unauthorized access between the building systems and corporate endpoints.

A Layer 3 virtual network may span multiple fabric sites and across network domains (wireless LAN, campus LAN, and WAN). A Layer 2 virtual network resides within a single fabric site.

## Create a Layer 3 Virtual Network

---

- Step 1** Click the menu icon (☰) and choose **Workflows > Create Layer 3 Virtual Networks**. Alternatively, you can navigate to the **Layer 3** tab under **Provision > Virtual Networks** and click **Create Layer 3 Virtual Networks**.
- Step 2** If the task overview window opens, click **Let's Do it** to go directly to the workflow.
- Step 3** In the **Choose your creation process** window, enter the number of Layer 3 virtual networks that you want to create.
- Step 4** In the **Create your Layer 3 virtual networks** window, enter the name of the Layer 3 virtual networks.
- Step 5** In the **Select your Fabric Sites** window, click one of the following:
- **By Layer 3 Virtual Network** tab: To associate the Layer 3 virtual networks to multiple fabric sites, choose the Layer 3 virtual network and fabric sites from the corresponding drop-down lists. You can assign a virtual network to multiple fabric sites. Repeat this association for all the Layer 3 virtual networks that you created.
  - **By Fabric Site** tab: To assign multiple Layer 3 virtual networks to a fabric site, choose the fabric site and choose Layer 3 virtual networks from the corresponding drop-down lists. You can assign multiple Layer 3 virtual networks to a fabric site. Repeat this association for all the required fabric sites.
- Step 6** In the **Configuring traffic exit behavior** window, configure the exit behavior of the traffic when this virtual network is associated with multiple fabric sites.
- By default, **Local Exit** is selected. This option allows the traffic to exit through the local border of each associated fabric site.
  - To anchor a virtual network and enable the traffic to exit at a designated border, choose **Anchor (Multisite Remote Border)**.
- From the list of associated fabric sites, choose a site whose border serves as an exit for all traffic in this virtual network. The other associated fabric sites inherit the virtual network.
- Step 7** Review the Layer 3 virtual network settings on the **Summary** window.
- Step 8** In the **Let's begin deploying your Layer 3 virtual network** window, click **Create** to create the context of the virtual network.
- Step 9** To assign the virtual network to the selected sites, click **Deploy**.
- Step 10** To verify the virtual network creation, click **View All Virtual Networks**.
- The **Virtual Networks** window displays the details of all the Layer 3 virtual networks in a fabric.
-

## Create a Layer 2 Virtual Network

---

- Step 1** Click the menu icon (☰) and choose **Workflows > Create Layer 2 Virtual Networks**.  
Alternatively, you can navigate to the **Layer 2** tab under **Provision > Virtual Networks** and click **Create Layer 2 Virtual Networks**.
- Step 2** If the task overview window opens, click **Let's Do it** to go directly to the workflow.
- Step 3** In the **Configure VLANs** window, to enter the number of VLANs that you want to connect to the fabric, do the following:
- Enter a **VLAN Name** and optional **VLAN ID** for each of the VLANs.
  - In the **Traffic Type** drop-down list, choose **Data** or **Voice**.  
Flooding is enabled by default for a Layer 2 virtual network.
  - (Optional) Toggle the **Wireless** button to enable wireless.
- Step 4** In the **Select a fabric site for each Layer 2 virtual network** window, choose a fabric site for the Layer 2 virtual network.  
Optionally, you can choose a Layer 3 virtual network to associate with this Layer 2 virtual network.
- Note** You can create a pure Layer 2 virtual network by not choosing a Layer 3 Virtual Network in the **L3VN Name** drop-down.
- Step 5** In the **Summary** window, review your Layer 2 virtual network settings and click **Create**.
- Step 6** To confirm the provisioning of the Layer 2 virtual network, click **Submit**.  
After the Layer 2 virtual network is provisioned, a success message is displayed.
- Step 7** To verify the creation of the Layer 2 virtual network, click **Virtual Network overview**. In the **Virtual Networks** window, the **Layer 2** tab displays the details of all the Layer 2 virtual networks in the fabric.
- 

## Associate a Layer 3 Virtual Network to a Fabric Site

---

- Step 1** Click the menu icon (☰) and choose **Provision > Virtual Networks**.
- Step 2** Under **NETWORK OBJECTS**, click the number that indicates the count of **Layer 3 Virtual Networks**.  
The resulting window displays all the Layer 3 virtual networks that are created at the global level.
- Step 3** In the **Layer 3** tab, under the **Actions** column for a desired Layer 3 virtual network, hover your cursor over the ellipsis icon (⋮) and choose **Add to Fabric Site**.
- Step 4** In the **Select Fabric Site** slide-in pane, choose a site and click **Select**.
- 

## Create Anycast Gateways

### Before you begin

Ensure that you have created a Layer 3 virtual network.

- Step 1** Click the menu icon (☰) and choose **Provision > Virtual Networks**.
- Step 2** Under **LAYER 2**, click the number that indicates the count of **Anycast Gateways**.
- Step 3** In the **Anycast Gateway** tab, click **Create Anycast Gateway**.

Alternatively, in the **Layer 3** tab, hover your cursor over the ellipsis icon (⋮) under the **Actions** column for a Layer 3 virtual network, choose **Create Anycast Gateways** and skip to [Step 6, on page 16](#).

- Step 4** Click **Let's Do it**.
- Step 5** In the **Select Layer 3 Virtual Networks to configure** window, select one or more virtual networks to add a gateway.
- Step 6** In the left pane of the **Add IP Pools and VLANs** window, choose the Layer 3 virtual network for which you want to create the gateway and do the following:
- Choose an **IP Pool** from the drop-down list.
  - For an **INFRA\_VN**, do the following:
    - Choose **AP** or **Extended Node** from the **Pool Type** drop-down list.
    - Enter a valid **VLAN Name** or check the **Auto generate VLAN name** check box.
    - Enter a custom **VLAN ID** for the virtual network.
    - To onboard a supplicant-based extended node, check the **Supplicant-Based Extended Node Onboarding** check box.

**Note** This check box is displayed only when you choose the **Extended Node** pool type.
  - To enable the IP-Directed Broadcast feature, click the **Directed Broadcast** toggle button on.
 

**Note**

    - Enable Layer 2 flooding before enabling Directed Broadcast.
    - Routers and Nexus 7000 Series Switches don't support Directed Broadcast.
    - Before enabling Directed Broadcast, ensure that you have enabled underlay multicast.
  - Enter a valid **VLAN Name** or check the **Auto generate VLAN name** check box.
  - Enter a custom **VLAN ID** for the virtual network.
 

**Note**

    - VLAN IDs 1, 1002-1005, 2046, and 4095 are reserved and can't be used.
    - If you don't provide a custom VLAN ID, Cisco DNA Center generates a VLAN ID in the range of 1021–2020.
  - Choose **Data** or **Voice** from the **Traffic Type** drop-down list.
  - Choose a **Security Group** from the drop-down list.
  - To include this IP pool in the critical IP address pool, click the **Critical VLAN** toggle button on.
 


A critical pool is used for closed authentication profile when an authentication server isn't available. A critical VLAN is assigned to the critical pool and all unauthenticated hosts are placed in the critical VLAN in the absence of an authentication server.
  - To enable Layer 2 virtual network, click the **Enable** toggle button.
  - To enable Layer 2 flooding, click the **Flooding** toggle button.



**Note** Layer 2 flooding requires underlay multicast, which is configured during LAN automation. If you don't provision the underlay through LAN automation, configure underlay multicast manually.

- k) To enable this IP pool as a wireless IP address pool, click the **Wireless** toggle button.
- l) To enable onboarding of bridge-mode virtual machines that are connected to the fabric-enabled wireless network, click the **Bridge Mode VM** toggle button.

**Note** **Bridge Mode VM** toggle button is displayed only when you enable the Wireless toggle button.

- m) To associate more IP pools, click the  icon and repeat the steps.

**Step 7** Review the endpoint connectivity settings in the **Summary** window.

**Step 8** In the **Let's begin creating your Gateways** window, click **Create**.

**Step 9** To verify the gateway creation after you see a success message, click **View All Virtual Networks**.

---

## Configure a Fabric Zone

A fabric site (parent site) can be divided into fabric zones with smaller subnets to help you manage the network easily. A fabric zone can have its own edge nodes and extended nodes, but it connects to the parent site for a control plane and border. If you migrated from an earlier Cisco DNA Center release to the current release, you can create a fabric zone on the existing fabric site. This fabric zone inherits all the properties of its parent site.

### Before you begin

- Ensure that you have created a network hierarchy under the Global site.
- Select a parent site that is not at the lowest level in the hierarchy.

The following is the broad workflow to configure a fabric zone.

1. Create a fabric zone in one of the following ways:
  - Create a fabric site and its zones using the **Create Fabric Site** workflow. For more information, see [Create a Fabric Site and Its Fabric Zones, on page 18](#).
  - Edit an existing fabric site to add fabric zones to it. For more information, see [Create a Fabric Zone Within a Fabric Site, on page 19](#).
2. Add edge nodes and extended nodes to the fabric zone. For more information, see [Add a Device to a Fabric, on page 6](#).
3. Assign Layer 3 virtual networks and segments to the fabric zone. For more information, see [Add Layer 3 Virtual Networks to a Fabric Zone, on page 19](#).



---

**Note** Only the virtual networks and segments of the parent site are available to the fabric zone.


---



- 
- Note** After a segment is added to a fabric zone, it can't be updated in the parent site.  
You can't edit edge nodes and extended nodes of a fabric zone in its parent site.  
You can configure the edge node of a fabric zone as a control plane or a border of the parent site.
- 

## Create a Fabric Site and Its Fabric Zones

---

- Step 1** Click the menu icon () and choose **Provision > Fabric Sites**.
- Step 2** Click **Create Fabric Site**.  
Alternatively, click the menu icon and choose **Workflows > Create Fabric Site**.
- Step 3** If a task overview window appears, click **Let's Do It** to go directly to the workflow.
- Step 4** In the **Fabric Site Location** window, choose an area, building, or floor to add as a fabric site.
- Step 5** In the **Wired Endpoint Data Collection** window, ensure that the **Monitor wired clients** check box is checked.
- Step 6** In the **Authentication Template** window, do the following:
- a) Choose an authentication template for the fabric site:
    - **Closed Authentication:** Any traffic before authentication is dropped, including DHCP, DNS, and ARP.
    - **Open Authentication:** A host is allowed network access without having to go through 802.1X authentication.
    - **Low Impact:** Security is added by applying an ACL to the switch port, to allow limited network access before authentication. After a host has been successfully authenticated, additional network access is granted.
    - **None**
  - b) (Optional) If you choose **Closed Authentication**, **Open Authentication**, or **Low Impact**, click **Edit** to edit the authentication settings:
    - **First Authentication Method:** Choose **802.1x** or **MAC Authentication Bypass (MAB)**
    - **802.1x Timeout (in seconds):** Use the slider to specify the 802.1x timeout, in seconds.
    - **Wake on LAN:** Choose **Yes** or **No**.
    - **Number of Hosts:** Choose **Unlimited** or **Single**.
    - **BPDU Guard:** Use this check box to enable or disable the Bridge Protocol Data Unit (BPDU) guard on all the **Closed Authentication** ports.
    - **Pre-Authentication Access Control List:** Enable the toggle button to configure preauthentication control for **Low Impact** authentication. From the **Implicit Action** drop-down list, choose an implicit action. Enter a description for the rule. To add an access contract, click **Add Contract Action**, choose the rules, and click **Apply Table**.
- Step 7** In the **Fabric Zones** window, to designate fabric zones and create scoped subnets, click **Setup Fabric Zones Now**.  
To enable a fabric zone, choose a fabric site in the network hierarchy.

- Step 8** In the **Summary** window, review the fabric site settings.  
You can edit any of the fabric site or zone settings here.
- Step 9** Click **Deploy**.  
It takes a few seconds for the site and zones to be provisioned. Upon successful creation of the site, a **Success! Your fabric site is created** message is displayed.  
The newly created fabric zone is tagged with an “FZ” in the site hierarchy pane.
- 

## Create a Fabric Zone Within a Fabric Site

---

- Step 1** Click the menu icon (☰) and choose **Provision > Fabric Sites**.
- Step 2** Under **SUMMARY**, click the number that indicates the count of fabric sites.
- Step 3** For the fabric site where you want to designate fabric zone, under the **Actions** column, hover your cursor over the ellipsis icon (⋮) and choose **Edit Fabric Zone**.
- Step 4** In the **Fabric Zones** window, choose an area, building, or floor.
- Step 5** Click **Next**.
- Step 6** Review the fabric site settings that are displayed in the **Summary** window.  
You can edit any of the fabric site or zone settings here.
- Step 7** Click **Deploy**.  
It takes several seconds for the site and zones to be provisioned. A **Success! Your fabric site is created** message is displayed.  
The newly created fabric zone is tagged with an “FZ” in the site hierarchy pane.
- 

### What to do next

- Add only edge node and extended node devices to the newly created fabric zone.  
Devices assigned to a fabric zone can't be assigned to the parent site. However, an edge node device assigned to a fabric zone can still be configured as a control plane or a border node for the parent site.
- Assign IP pools and virtual networks to the fabric zone.

## Add Layer 3 Virtual Networks to a Fabric Zone

### Before you begin


Ensure that you have created the fabric zone.




---

**Note** You can add only the Layer 3 virtual networks of a parent site to a fabric zone.

---

- 
- Step 1** Click the menu icon () and choose **Provision > Virtual Networks**.
  - Step 2** Under **NETWORK OBJECTS**, click the number that indicates the count of **Layer 3 Virtual Networks**.  
The resulting window displays all the Layer 3 virtual networks at a global level.
  - Step 3** Click Fabric Site: **Global**.
  - Step 4** In the **Select Fabric Site** slide-in pane, choose a fabric zone and click **Select**.
  - Step 5** In the **Layer 3** tab, click **Add Layer 3 VN**.
  - Step 6** In the **Add Virtual Network** slide-in pane, choose the virtual networks to add to the fabric zone. Click **Update**.
- 

## Add Layer 2 Virtual Networks to a Fabric Zone


### Before you begin




---

**Note** After you add the gateways to a fabric zone, you can't remove them at the parent site.

---

- 
- Step 1** Click the menu icon () and choose **Provision > Virtual Networks**.
  - Step 2** Under **LAYER 2**, click the number that indicates the count of **Layer 2 Virtual Networks**.  
The resulting window displays all the Layer 2 virtual networks at a global level.
  - Step 3** Click Fabric Site: **Global**.
  - Step 4** In the **Select Fabric Site** slide-in pane, choose a fabric zone and click **Select**.
  - Step 5** In the **Layer 2** tab, click **Add Layer 2 Virtual Network**.
  - Step 6** In the **Select L2VNs** slide-in pane, choose the Layer 2 virtual networks.
  - Step 7** Click **Add**.
- 

## Add Anycast Gateways to a Fabric Zone

### Before you begin

Ensure that you have created the fabric zone.



---

**Note** You can add only the anycast gateways of a parent site to a fabric zone.

---

After you add an anycast gateway to a fabric zone, you can't update it at the parent site.

- 
- Step 1** Click the menu icon (☰) and choose **Provision > Virtual Networks**.
- Step 2** Under **LAYER 2**, click the number that indicates the count of **Anycast Gateways**.  
The resulting window displays all the anycast gateways at a global level.
- Step 3** Click Fabric Site: **Global**.
- Step 4** In the **Select Fabric Site** slide-in pane, choose a fabric zone and click **Select**.
- Step 5** In the **Anycast Gateway** tab, click **Add Anycast Gateway**.
- Step 6** In the **Select Anycast Gateway(s)** slide-in pane, choose the Layer 3 virtual networks and click **Next**.
- Step 7** Choose the anycast gateways that you want to add.
- Step 8** Click **Add**.
- 

## Configure an Extended Node Device

An extended node is configured by automated workflow. After configuration, the extended node device is displayed in the fabric topology view. You can assign ports for the extended nodes using the **Port Assignment** tab.



---

**Note** You can't onboard the extended nodes through the GUI-based provisioning workflows. An Extended node is onboarded only through the SD-Access automated workflow after resetting the device configuration to the factory default and powering on the device.

---

A device is onboarded according to the Cisco DNA license of its Extended Node neighbor and its own Cisco DNA license:

- If the neighbor is operating with a Cisco DNA Essentials license, the device is onboarded as a standard Extended Node, regardless of its Cisco DNA license.
- If the neighbor is operating with a Cisco DNA Advantage license, the device is onboarded as a standard Extended Node if it has a Cisco DNA Essentials license.
- If the neighbor is operating with a Cisco DNA Advantage license, the device is onboarded as a Policy Extended Node if it has a Cisco DNA Advantage license.
- If the device has more than one neighbor, and those neighbors have different Cisco DNA license levels, the device is onboarded as a standard Extended Node, regardless of its Cisco DNA license.

Extended node devices support multicast traffic.

Policy Extended Nodes are extended nodes that support security policy within the virtual network. You can select a **Group** during port assignment for a Policy Extended Node.

Policy Extended Node devices include Cisco Catalyst Industrial Ethernet (IE) 3400, IE 3400 Heavy Duty series switches, and Cisco Catalyst 9000 series switches that run Cisco IOS XE Release 17.1.1s or later.

Cisco Digital Building series switches, Cisco Catalyst 3560-CX switches, and Cisco Industrial Ethernet 4000, 4010, and 5000 series switches can't be configured as Policy Extended Nodes.

## Steps to Configure an Extended Node

When configured as a fabric edge, Cisco Catalyst 9300, Cisco Catalyst 9400, and Cisco Catalyst 9500 series switches support extended nodes.



**Note** Cisco Catalyst 9200 series switches that are configured as fabric edge nodes don't support extended node devices.

The following are the minimum supported software versions on the extended nodes:

- Cisco Industrial Ethernet 4000, 4010, 5000 series switches: 15.2(7)E0s with LAN base license enabled.  
If you have an IP services license, you must change the Switch Database Management (SDM) template to `dual-ipv4-and-ipv6 default` manually.
- Cisco Catalyst IE 3400, 3400 Heavy Duty (X-coded and D-coded) series switches: Cisco IOS XE Release 17.1.1s.
- Cisco Catalyst IE 3300 series switches: Cisco IOS XE Release 16.12.1s.
- Cisco Digital Building series switches, Cisco Catalyst 3560-CX switches: Release 15.2(7)E0s.

The minimum software version that is required on a policy extended node device and on the edge node device supporting the policy extended node is Cisco IOS XE Release 17.1.1s.

The following configuration steps are applicable to both a standard Extended Node and Policy Extended Node.

### Before you begin

To configure a device as a Policy Extended Node, both the device and the edge node supporting it must have the Network Advantage and DNA Advantage license levels enabled.

- 
- Step 1** Configure a network range for the extended node. See [Configure IP Address Pools](#). This step comprises adding an IP address pool and reserving the IP pool at the site level. Ensure that the CLI and SNMP credentials are configured.
- Step 2** Assign the extended IP address pool to INFRA\_VN. See [Create Anycast Gateways, on page 15](#). Choose **Extended Node** as the **Pool Type**.
- Cisco DNA Center configures the extended IP address pool and VLAN on the supported fabric edge device. This enables the onboarding of extended nodes.
- Step 3** Configure the DHCP server with the extended IP address pool and Option 43. Ensure that the extended IP address pool is reachable from Cisco DNA Center.

**Note** For a detailed description of Option 43, see [DHCP Controller Discovery](#).

**Step 4** Connect the extended node device to the fabric edge device. You can have multiple links from the extended node device to the fabric edge.

**Step 5** Create a port channel on the fabric edge node that is connected to the extended node. For a subsequent extended node in a ring or daisy chain, create the port channel on the previous extended node it connects to.

**Note** Complete this step only if the global authentication mode for the fabric is **Open Authentication**, **Low Impact**, or **Closed Authentication**. If the fabric site is set to **None** authentication mode, the port channel is automatically created during the onboarding of the extended nodes using Plug and Play provisioning.

To create a port channel, complete the following steps:

- a) Click the menu icon (☰) and choose **Provision > Fabric Sites**.
- b) In the **Fabric Sites** tab, click the number that indicates the count of fabric sites.
- c) Select a fabric site.
- d) In the **Fabric Infrastructure** tab, choose a fabric edge node (or an extended node, depending on the connection).
- e) In the slide-in pane, under the **Port Channel** tab, click **Create Port Channel**.
- f) Complete the following:

- Choose an **Extended Node** in the **Connected Device Type** drop-down list.
- Enter a description.
- Choose **Port Aggregation Protocol (PAgP Desirable)**.  
Starting with Cisco IOS XE Release 17.1.1s, IE 3300 and IE 3400 devices support PAgP.
- Select **On** for IE 3300 and IE 3400 devices if they are running versions earlier than Cisco IOS XE Release 17.1.1s.

**Note** Link Aggregation Control Protocol (LACP) doesn't work for extended node onboarding.

- Choose the ports to be bundled as a port channel.

- g) Click **Done**.

This creates a port channel on the fabric edge node (or the extended node) to onboard an extended device.

**Step 6** Power up the extended node device if it has no previous configuration. If the extended node device has configurations, write-erase the previous configurations and reload the extended node device.

Cisco DNA Center adds the extended node device to the Inventory and assigns the same site as the fabric edge. The extended node device is then added to the fabric. Now the extended node device is onboarded and ready to be managed.

After the configuration is complete, the extended node appears in the fabric topology with a tag (X) to indicate that it is an extended node.

---

## Upgrade an Extended Node to a Policy Extended Node

Cisco SD-Access automation onboards a policy extended node-capable device with a Cisco DNA Essentials license as an extended node. You can convert this extended node device to a policy extended node by upgrading its license to Cisco DNA Advantage.

In a daisy chain, you cannot upgrade an extended node to a policy extended node if its upstream device is an extended node.

In a ring, you cannot upgrade an extended node to a policy extended node if both its neighbors are extended nodes.

After you upgrade the node to policy extended node, you cannot reconfigure it as an extended node.

To convert an extended node to a policy extended node, do the following:

### Before you begin

- Ensure that the extended node is already onboarded.
- Update the Smart Licensing credentials on Cisco DNA Center.

---

**Step 1** Change the license level on the device from Cisco DNA Essentials to Cisco DNA Advantage, using the Cisco DNA Center License Manager:

- Click the menu icon (☰) and choose **Tools > License Manager**.
- In the **Devices** tab, select the device.
- Choose **Actions > Change License > Change DNA License**.
- In the **Change DNA License Level** window, click **Advantage**.
- Click **Confirm**.
- In the **Success** message window, click **OK**.

The device reloads.

**Step 2** Wait for the node to become **Reachable** and get to the **Managed** state.

The **Provision > Network Devices > Inventory** window displays the reachability status of all the devices.

**Step 3** If you see a "Netconf Connection Refused" error, resynchronize the device. Repeat the resynchronization process until the error goes away.

- In the **Provision > Network Devices > Inventory** window, select the device.
- Choose **Actions > Inventory > Resync Device**.

**Step 4** Upgrade to policy extended node.

- In the **Provision > Fabric Sites** window, select the site in which the device is onboarded.
  - In the **Fabric Infrastructure** tab, click a device to edit its attributes.
  - In the **Fabric** tab, toggle the **Policy** button under **Extended Node Attributes**.
  - In the **Policy Extended Node Upgrade** window that comes up, click **Upgrade**.
- 


## Delete an Extended Node

This task describes the steps to delete an extended node, policy extended node, and authenticated extended node.

---

**Step 1** Remove the extended node device from the fabric.



- a) Click the menu icon () and choose **Provision > Fabric Sites**.
- b) In the **Fabric Sites** tab, click the number that indicates the count of fabric sites.
- c) Select the fabric site that contains the extended node device.
- d) In the **Fabric Infrastructure** tab, click the extended node device.
- e) In the slide-in pane, click **Remove From Fabric**.
- f) Click **Add**.

**Step 2** Delete the device from **Inventory**.

For steps to delete the device from inventory, see [Delete a Network Device](#).

**Step 3** For a supplicant-based extended node device, delete the port assignment configuration in the fabric edge node or the FIAB.

---

## Configure a REP Ring Topology for Extended Nodes and Policy Extended Nodes

To enable redundancy with a recovery time of less than 50 ms for network failures with extended nodes, configure a Resilient Ethernet Protocol (REP) ring for the fabric site.

Unless explicitly stated, the term *extended node* also represents a policy extended node.

The following devices can be configured in a REP ring:

- **Extended Node:**
  - Cisco Industrial Ethernet (IE) 4000, 4010, 5000 series switches that operate Cisco IOS 15.2(7)E3 and later releases.
  - Cisco Catalyst IE3300 series switches that operate Cisco IOS XE 17.3.3 and later releases.
- **Policy Extended Node:**
  - Cisco Catalyst IE3400, IE3400H series switches that operate Cisco IOS XE 17.3.3 and later releases.

### Limitations of a REP Ring

- To add an extended node into an existing REP ring, first delete the REP ring. Deleting the REP ring enables the Per VLAN Spanning Tree Protocol (PVSTP), which avoids Layer 2 loops. Then, add the new extended node to the fabric and recreate the REP ring to include the new extended node.
- Multiple rings within a given REP ring and a ring of rings aren't supported.
- A node in a REP ring can have other nodes connected to it in a daisy chain manner. However, a node in a daisy chain can't have a ring of nodes connected to it.
- A REP ring or a daisy chain can't be a mix of extended nodes and policy extended nodes. A REP ring or a daisy chain must consist entirely of either extended nodes or policy extended nodes.
- By default, a maximum of 18 devices can be onboarded in a single REP ring. To onboard more than 18 devices, increase the BPDU timer using **spanning-tree vlan *infra VN* VLAN **max-age 40**** command. Use the Cisco DNA Center templates to configure the command.

Note that in some rare instances, when the last two nodes of the ring try to onboard simultaneously, a port channel might not be created between these nodes. A port channel is established between the last two nodes of the ring when a REP ring is created.

Unless otherwise stated, the following steps are applicable to both extended node and policy extended node.

### Before you begin

Ensure that you have onboarded the fabric edge nodes and extended nodes.

Identify the fabric edge node and its interfaces that terminate the REP ring.




---

**Note** The REP ring configuration procedure may disrupt the network traffic for a brief period.

---

- 
- Step 1** Click the menu icon (☰) and choose **Workflows > Configure REP Ring**.  
Alternatively, you can navigate to the Fabric Site topology view, select the Fabric Edge node or the FIAB node on which you want to create the REP ring and click **Create REP Ring** under the **REP Rings** tab.
- Step 2** If a task overview window appears, click **Let's Do It** to go directly to the workflow.
- Step 3** In the **Select a fabric site** window, select a site that has both edge node and extended nodes.
- Step 4** In the **Select a fabric edge node** window, choose a fabric edge node.
- Step 5** In the **Select Extended Nodes connected to Fabric Edge** window, choose the extended nodes that connect to the fabric edge node.  
You can choose two extended nodes to connect to the fabric edge node.
- Step 6** Review and edit (if necessary) your fabric site, edge node, and extended node selections.
- Step 7** To initiate the REP ring configuration, click **Provision**.  
You can see a detailed status of the configuration progress on the **REP Ring Configuration Status** window.
- Step 8** The **REP Ring Summary** window displays the details of the REP ring that is created along with the discovered devices.
- Step 9** After the creation of the REP ring, a success message is displayed.  
To verify the creation of the REP ring, go to the fabric site window and click the fabric edge node.  
In the slide-in window, under the **REP Ring** tab, you can see the list of all REP rings that exist on that edge node.  
Click a REP ring name in the list to view its details, such as the devices present in the ring, ports of each device that connect to the ring, and so on.
- 

## View REP Ring Status

To view the status of the devices in a REP ring, do the following:

- 
- Step 1** In the Cisco DNA Center GUI, click the menu icon (☰) and choose **Provision > Fabric Sites**.
- Step 2** In the **Fabric Sites** tab, click the number that indicates the count of fabric sites.
- Step 3** Select a fabric site from the list that displays all the fabric sites.
- Step 4** In the **Fabric Infrastructure** tab, click the fabric edge node or the FIAB.

A slide-in window displays the details of the fabric edge node or the FIAB that is selected.

**Step 5** In the **REP Rings** tab, click **View** to see the **REP Ring Topology Status**.

The **REP Topology Status** section displays the current state of all the devices in the REP Ring. The state, as displayed in the **Role** column, can be **Open**, **Fail**, or **Alt**.

**Open** indicates that the device link is up and it forwards traffic.

**Fail** indicates that the device link is down.

**Alt** indicates that the device link is up but the port cannot forward traffic.

---

## Delete a REP Ring

**Step 1** Click the menu icon (☰) and choose **Provision > Fabric Sites**.

**Step 2** In the **Fabric Infrastructure** tab, click the fabric edge node that terminates the REP Ring.

A slide-in window displays the details of the fabric edge node selected.

**Step 3** In the **REP Rings** tab, for the desired REP Ring, click **Actions (...)** > **Delete**.

This deletes the REP Ring.

---

## Delete a Node from a REP Ring

This task describes the steps to delete one extended node or multiple extended nodes from a REP ring.



**Note** After the extended nodes are removed, the downsized REP ring should use the existing interfaces to create a link to the neighboring devices.

---

### Before you begin

Ensure that the REP ring to which the node belongs is not incomplete.

**Step 1** Manually remove the extended node devices from the network.

Alternatively, if a device in a REP ring goes down, the **Fabric Infrastructure** window displays a notification.

**Step 2** Click the menu icon (☰) and choose **Provision > Fabric Sites**.

**Step 3** In the **Fabric Infrastructure** tab, click the fabric edge node that terminates the REP ring.

A slide-in pane displays the details of the selected fabric edge node.

**Step 4** In the **REP Rings** tab, for the desired REP ring, choose **Actions (...)** > **Rediscover**.

The extended node device is deleted from the REP ring and the REP ring display is updated.

## Configure Supplicant-Based Extended Nodes

Supplicant-based extended nodes, also called Authenticated Extended Nodes (AENs), are extended node devices that receive an IEEE 802.1x (Dot1x) supplicant configuration and are onboarded into the SD-Access network only after a complete authentication and authorization. To onboard a supplicant-based extended node device, the authenticator port on the fabric edge must be configured with a Closed Authentication Template.

The following platforms support supplicant-based extended node onboarding:

### Fabric Edge or FIAB:

Cisco Catalyst 9000 Series – C9300, C9400, C9500, and C9500H switches that operate Cisco IOS XE 17.7.1 or later.

### Supplicant-based Extended Node:

Cisco Catalyst 9000 Series – C9200, C9300, C9400, C9500, and C9500H switches that operate Cisco IOS XE 17.7.1 or later.

## Steps to Configure a Supplicant-Based Extended Node

### Before you begin

- Configure Cisco ISE and ensure that it operates Release 3.1 or later. See [Configure Cisco Identity Services Engine to Onboard Supplicant-Based Extended Node, on page 30](#).
- Add the fabric edge node or FIAB device to the fabric and ensure that it operates Cisco IOS XE 17.7.1 or later.
- Set the Path MTU appropriately for the path between the fabric edge node and Cisco ISE. We recommend a value of 9100. Note that the Path MTU is set for all the devices in the fabric during LAN automation or when the underlay is configured.

**Step 1** Configure AAA server settings in Cisco DNA Center.

- Define Cisco ISE as the AAA server for device authentication in the **System > Settings > External Services > Authentication and Policy Servers** window.

For the complete procedure, see "Configure Authentication and Policy Servers" in the [Cisco DNA Center Administrator Guide](#).

- Add the Cisco ISE server to the global site. For information, see [Add Cisco ISE or Other AAA Servers](#).

**Step 2** (Optional) Configure Cisco DNA Center to authorize the device before onboarding.

- Click the menu icon (☰) and choose **System > Settings > Device Settings > PnP Device Authorization**.
- Check the **Device Authorization** check box to enable authorization on the device.
- Click **Save**.

**Step 3** Configure the Cisco DNA Center appliance to manage your PKI certificates.

- a) Click the menu icon (☰) and choose **System > Settings > Trust & Privacy > PKI Certificates**.
- b) In the **PKI Certificates** window, click **Use Cisco DNA Center**.
- c) In the **CA Management** tab, click **Download CA Certificate**.
- d) Add the certificate to the Cisco ISE Trusted Certificate Store. For more information, see the [Cisco Identity Services Engine Administrator Guide](#).

If you use an external certificate, add that certificate to the Cisco ISE Trusted Certificate Store.

**Step 4** Configure the DHCP server with the extended IP address pool and Option 43. Ensure that the extended IP address pool is reachable from Cisco DNA Center.

For a detailed description of Option 43, see [DHCP Controller Discovery](#).

**Step 5** Enable **Closed Authentication** and disable Bridge Protocol Data Unit (BPDU) Guard on the fabric Site.

By default, selecting Closed Authentication pushes the BPDU Guard configuration on all the downlink access ports. When a remote switch like an extended node is connected, BPDU Guard pushes the port to error disabled mode. To disable BPDU Guard, uncheck the **Enable BPDU Guard** check box during the Closed Authentication configuration.

For more information, see [Select an Authentication Template](#).

**Step 6** Assign an extended IP address pool to INFRA\_VN, as described in [Create Anycast Gateways, on page 15](#).

In the **Create Anycast Gateways** workflow, choose **Extended Node** as the **Pool Type** and check the **Supplicant-Based Extended Node Onboarding** check box.

Cisco DNA Center configures the extended IP address pool and VLAN on the supported fabric edge device. This enables the onboarding of extended nodes.

**Note** Extended IP address pool is successfully assigned only if the fabric edge devices operate Cisco IOS XE 17.7.1 or later. If you upgraded from an earlier release of Cisco DNA Center, the supplicant-based extended node migration must be complete before configuring the extended IP address pool.

**Step 7** Connect the extended node device to the fabric edge node or the FIAB.

After powering on, the extended node device is in **Pending Authorization** state if you chose to authorize the device before onboarding (Step 2). You can check the status of the device in the **Provision > Plug and Play** window.

**Step 8** (Optional) Authorize the device.

Perform this step only if the device is in **Pending Authorization** state.

- a) Click the menu icon (☰) and choose **Provision > Plug and Play**.
- b) In the **Plug and Play** window, select the supplicant-based extended node device and choose **Actions > Authorize**.

The authorization process provisions the supplicant-based extended node device for completing a certificate-based EAP-TLS authentication with Cisco ISE. After authentication, Cisco ISE authorizes the supplicant-based extended node device for complete access. The supplicant-based extended node device is then fully onboarded into the SD-Access fabric.

---

After a supplicant-based extended node device is onboarded into the fabric, access to the fabric edge-supplicant port is only based on authentication status. If the device or the port goes down, the authentication session is cleared, and traffic is not allowed on the port. When the port comes up again, it goes through the IEEE 802.1x (Dot1x) authentication process to regain access to the SD-Access network.

## Replace a Faulty Port

If the link between the authenticator (fabric edge or FIAB) port and the supplicant port goes down, you can replace the faulty port and configure a new port through the **Port Assignment** menu.

- 
- Step 1** To replace the supplicant port, follow these steps:
- Clear the configuration on the new supplicant port.
  - Copy the existing configuration from the current supplicant port to the new supplicant port to allow 802.1X authentication.
- Step 2** To replace the authenticator port, follow these steps:
- Assign the supplicant port to the new interface of the authenticator. For information on Port Assignment, see [Configure Ports within the Fabric Site](#). Choose **Supplicant-Based Extended Node** as the **Connected Device Type**.
  - Clear the existing port assignment on the old interface of the authenticator.
- Step 3** Disconnect the physical connection between the old ports of the authenticator and the supplicant. Connect a cable between the new ports of the authenticator and the supplicant. Bring this link up.
- Step 4** After the link between the new ports of the authenticator and supplicant is up, do the following steps:
- Resynchronize the device information in Cisco DNA Center by performing an **Inventory > Resync Device** for both the authenticator and the supplicant. See [Resynchronize Device Information](#).
  - Assign the new supplicant port to the authenticator. For information on Port Assignment, see [Configure Ports within the Fabric Site](#). Choose **Authenticator Switch** as the **Connected Device Type**.
  - Clear the port assignment on the old supplicant port.
- 

## Configure Cisco Identity Services Engine to Onboard Supplicant-Based Extended Node

This task describes how to profile an Supplicant-Based Extended Node (SBEN) device in Cisco Identity Services Engine (ISE). The steps listed below are part of the Cisco ISE configuration procedure. For more information, refer the [Cisco Identity Services Engine Administrator Guide](#).

### Before you begin

Download the CA certificate from Cisco DNA Center.

- 
- Step 1** Import the CA certificate into Cisco ISE:
- From the Cisco ISE home page, choose **Administration > System > Certificates > System Certificates > Import**. In the **Import** window, ensure that you select the **Trust for client authentication and Syslog** check box. For more information, see the "Import the Root Certificates to the Trusted Certificate Store" section in the [Cisco Identity Services Engine Administrator Guide](#).
- Step 2** Configure the following authorization profiles with their RADIUS attributes:
- From the Cisco ISE main menu, choose **Policy > Policy Elements > Results > Authorization > Authorization Profiles**. Configure the following profiles:

```
SBEN-DHCP:
Access Type = ACCESS_ACCEPT
Filter-ID = SBEN_DHCP_ACL.in

SBEN_LIMITED_ACCESS_AUTHZ:
Access Type = ACCESS_ACCEPT
Filter-ID = SBEN_MAB_ACL.in
cisco-av-pair = interface-template-name=SWITCH_SBEN_MAB_TEMPLATE

SBEN_FULL_ACCESS_AUTHZ :
Access Type = ACCESS_ACCEPT
cisco-av-pair = interface-template-name=SWITCH_SBEN_FULL_ACCESS_TEMPLATE
```

**Step 3**

Define the device profiling policy in the **Profiling Policies** window.

- a) From the Cisco ISE main menu, choose **Policy > Profiling > Profiling Policies**.
- b) In the **Profiling Policies** window, add a new **DHCP-v-i-vendor-class** condition for the **Cisco-Device: Cisco-Switch** policy.

## Configure Cisco Identity Services Engine to Onboard Supplicant-Based Extended Node

\* Name  Description

Policy Enabled

\* Minimum Certainty Factor  (Valid Range 1 to 65535 )

\* Exception Action

\* Network Scan (NMAP) Action

Create an Identity Group for the policy  Yes, create matching Identity Group  
 No, use existing Identity Group hierarchy

Parent Policy

\* Associated CoA Type

System Type

Rules

If	Condition	Then	Value
	Cisco-IOS-NMAPOSCheck	Certainty Factor Increases	10
	CDP_cdpCachePlatform_CONTAINS_9200...	Certainty Factor Increases	20
	DHCP_v-i-vendor-class_CONTAINS_9200...	Certainty Factor Increases	20

Condition Name	Expression	Operator	Value
	DHCP:v-i-ven...	CONTAIN	9200
	DHCP:v-i-ven...	CONTAIN	9300
	DHCP:v-i-ven...	CONTAIN	9500

- c) Create a new child policy for the supplicant device, under **Cisco-Switch** and apply the **CdpCachePlatform** and **V-I-Vendor-Class** conditions.

Ensure that the **Minimum Certainty Factor** value for the child policy is higher than that of the parent policy.

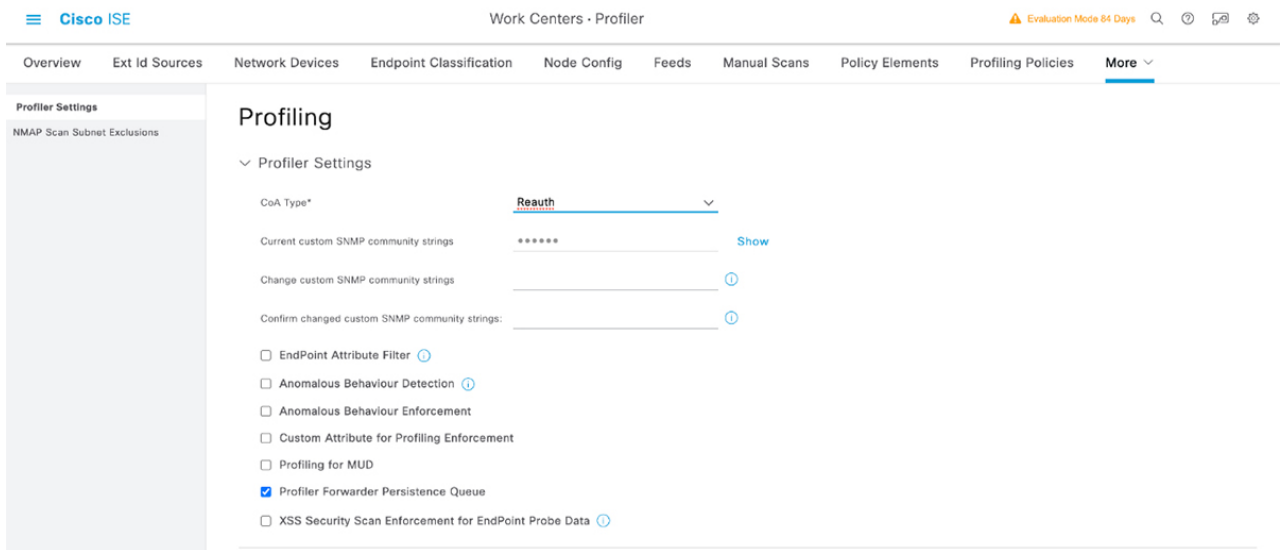


* Name	CAT9K_EN	Description	<input type="text"/>
Policy Enabled	<input checked="" type="checkbox"/>		
* Minimum Certainty Factor	30	(Valid Range 1 to 65535 )	
* Exception Action	NONE	▼	
* Network Scan (NMAP) Action	NONE	▼	
Create an Identity Group for the policy	<input checked="" type="radio"/> Yes, create matching Identity Group <input type="radio"/> No, use existing Identity Group hierarchy		
* Parent Policy	Cisco-Switch	▼	
* Associated CoA Type	Global Settings	▼	
System Type	Administrator Created		
Rules			
If	Condition	CDP_odpCachePlatform_CONTAINS_C92...	▼
Then	Certainty Factor Increases	▼	30
If	Condition	DHCP_v-i-vendor-class_CONTAINS_C920...	▼
Then	Certainty Factor Increases	▼	30

**Step 4** Set the global Change of Authorization (CoA) type to **Reauth**.

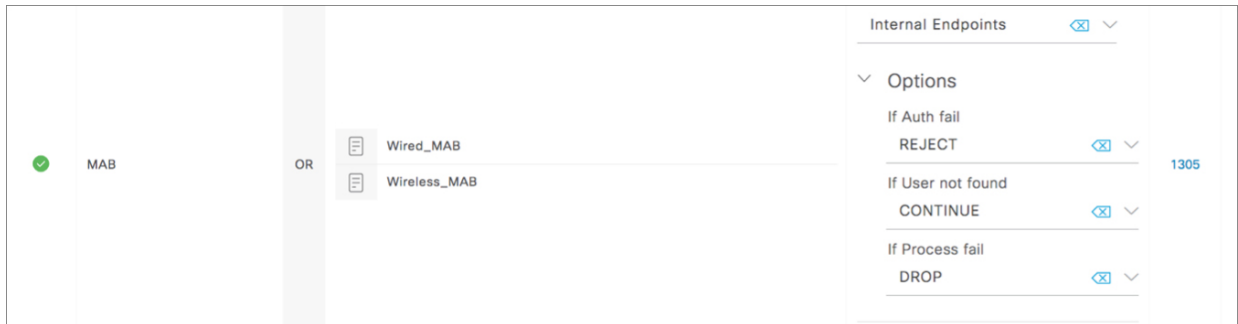
To configure the **CoA Type**, from the Cisco ISE home page, navigate to **Work Centers > Profiler > Settings**.

Choose **Reauth** from the **CoA Type** drop-down list.

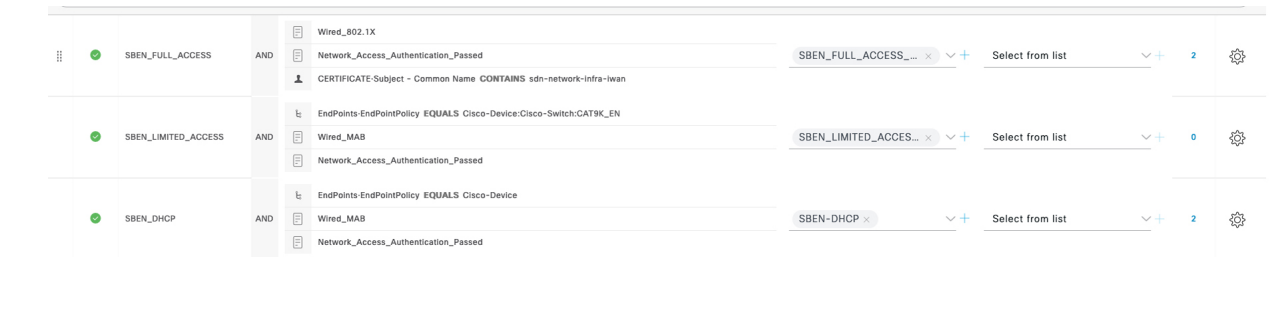


**Step 5** Define the authorization policy in the **Authorization Policy** window.

- a) From the Cisco ISE home page, choose **Policy > Policy Sets > Default > Authorization Policy**.
- b) Ensure that the default MAB policy is set to **CONTINUE** option for the **If User not found** field.



c) In the **Authorization Policy** window, configure the authorization policies for the supplicant device and associate the policies with the authorization profiles that were created earlier (SBEN-DHCP, SBEN\_LIMITED\_ACCESS\_AUTHZ, SBEN\_FULL\_ACCESS\_AUTHZ).



# Configure a Port Channel

A group of ports bundled together to act as a single entity is called a port channel. Port channels between a fabric edge and its remotely connected devices like extended nodes or servers increase the connection resiliency and bandwidth.

## Create a Port Channel

Complete the following steps only when the authentication is **Closed Authentication**.



---

**Note** The following steps are automated for other authentication modes.

---

- 
- Step 1** Click the menu icon (☰) and choose **Provision > Fabric Sites**.
- Step 2** Under **SUMMARY**, click the number that indicates the count of fabric sites.
- Step 3** Select a fabric site.
- Step 4** In the **Fabric Infrastructure** tab, click a fabric edge node.
- Step 5** In the **Port Channel** tab of the slide-in pane, click **Create Port Channel**.
- Step 6** From the **Connected Device Type** drop-down, choose the type of connected device.
- To create a port channel between a fabric edge node and an extended node or between two extended nodes, choose **Extended Node**.
  - To create a port channel with a fabric edge node or extended node on one side and a third party device or a server port on the other side, choose **Trunk**.
- Step 7** Enter a **Description** for the new port channel.
- Step 8** Choose a protocol:
- For the extended nodes that run Cisco IOS XE Release 16.12.1s and earlier releases, select **On** as the protocol.
  - For the extended nodes that run Cisco IOS XE Release 17.1.1s and later releases, select **Port Aggregation Protocol (PAgP)** as the protocol.
  - Don't select **Link Aggregation Control Protocol (LACP)** as the protocol for extended nodes. You can only connect the trunk ports or the server ports in the LACP mode.
- Step 9** From the list of ports displayed, choose the ports to be bundled.
- Note** You cannot have more than 16 members in a port channel that is connected in the LACP mode.  
You cannot have a more than eight members in a port channel that is connected in the PAgP mode.
- Step 10** Click **Done**.
-

## Update a Port Channel

### Before you begin

Ensure that at least one member interface exists before you update a port channel.

---

- Step 1** Click the menu icon (☰) and choose **Provision > Fabric Sites**.
- Step 2** Under **SUMMARY**, click the number that indicates the count of fabric sites.
- Step 3** Select a fabric site.
- Step 4** In the **Fabric Infrastructure** tab, click a fabric edge node.
- Step 5** In the slide-in pane, click the **Port Channel** tab.
- Step 6** From the list of port channels displayed, click the port channel to be updated.  
The resulting window displays all the interfaces and the status of the selected port channel.
- Step 7** Update the port channel.  
You can either add interfaces to the port channel or delete existing interfaces on the port channel.
- Step 8** Click **Done**.
- 

## Delete a Port Channel

- Step 1** Click the menu icon (☰) and choose **Provision > Fabric Sites**.
- Step 2** Under **SUMMARY**, click the number that indicates the count of fabric sites.
- Step 3** Select a fabric site.
- Step 4** In the **Fabric Infrastructure** tab, click a fabric edge node.
- Step 5** In the slide-in pane, click the **Port Channel** tab.  
The **Port Channel** view lists all the existing port channels.
- Step 6** Check the check box for the port channel and click **Delete**.
- Step 7** At the prompt, click **Yes**.
- 

## Multicast

Multicast traffic is forwarded in different ways:

- Through shared trees by using a rendezvous point. PIM SM is used in this case.
- Through shortest path trees (SPT). PIM source-specific multicast (SSM) uses only SPT. PIM SM switches to SPT after the source is known on the edge router that the receiver is connected to.

See [IP Multicast Technology Overview](#).

## Configure Multicast

Cisco DNA Center provides a workflow to enable group communication or multicast traffic in virtual networks. The workflow also allows you to choose multicast implementation in the network: native multicast or headend replication.



---

**Note** You can enable multicast on a virtual network whose border serves as a multisite remote border. Configuring multicast on such a virtual network configures multicast on the devices in the inherited virtual network too, provided the inherited virtual network already contains a segment. If the inherited virtual network doesn't have a segment, multicast is deployed only after the first segment is created. Ensure that a virtual network and its inherited networks deploy the same type of multicast implementation. The edge node devices of an inherited virtual network cannot be configured as a rendezvous point (RP).

---

- 
- Step 1** Click the menu icon (☰) and choose **Workflows > Configure Multicast**.
- Step 2** If a task overview window appears, click **Let's Do It** to go directly to the workflow.
- Step 3** In **Select a site to enable multicast** window, select a **Site** from the drop-down list.
- Step 4** In the **Enabling Multicast** window, choose the method of multicast implementation for the network from the following:
- **Native Multicast**
  - **Head-end replication**
- Step 5** In the **Virtual Networks** window, select the virtual network on which you want to set up multicast.
- Note** You can't select an inherited virtual network to set up multicast.
- Step 6** In the **Multicast pool mapping** window, select an IP address pool from the **IP Pools** drop-down list. The selected IP address pool is associated with the chosen virtual network.
- Step 7** In the **Select multicast type** window, choose the type of multicast to implement:
- **SSM** (Source Specific Multicast)
  - **ASM** (Any Specific Multicast)
- Step 8** Do the following:
- a) On selecting **SSM**, configure the SSM list by adding an IP group range for each virtual network. You can add multiple IP group ranges for a virtual network.
    1. Choose an IP group range from 225.0.0.0 to 239.255.255.255.
    2. Enter the **Wildcard Mask** for the IP group.
  - b) On selecting **ASM**, choose the type of RP (internal or external).
- Step 9** To configure a rendezvous point, do the following:
- If you choose to configure an internal rendezvous point:

- a) Select the devices that you need configured as internal rendezvous points. The second rendezvous point that you select is the redundant rendezvous point. Click **Next**.
- b) Assign internal rendezvous points to each of the listed virtual networks.

If you choose to configure an external rendezvous point:

- a) In the **Setup your External RP** window, enter the IPv4 or IPv6 address of the external rendezvous point.  
(Optional) Enter a second set of IPv4 or IPv6 addresses.
- b) In the **Select which RP IP Address(es) to utilize** window, select an IP address for each virtual network.

**Step 10**

Review the multicast settings that are displayed in the **Summary** window and modify, if necessary, before submitting the configuration.

Click **Finish** to complete the multicast configuration.

---