



Provision Fabric Networks

- [About Fabric Networks, on page 1](#)
- [Configure a Fabric Domain, on page 4](#)

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 and Fabric Domains

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 fabric domain can consist of one or more fabric sites and transit site. Multiple fabric sites are connected to each other using a transit site.

There are two types of transit sites:

- SD-Access transit: Enables a native SD-Access (LISP, VXLAN, CTS) fabric, with a domain-wide control plane node for intersite communication.
- IP-based transit: Leverages a traditional IP-based (VRF-LITE, MPLS) network, which requires remapping of VRFs and SGTs between sites.

Multi-Site Fabric Domain

A multi-site fabric domain is a collection of fabric sites interconnected via a transit site. A fabric site is a portion of the fabric that has its own set of control plane nodes, border nodes, and edge nodes. A given fabric site can also include fabric WLC and APs, and a related site-specific ISE PSN. Multiple fabric sites in a single fabric domain are interconnected using a transit site.

A Software-Defined Access (SDA) fabric may comprise multiple sites. Each site has the benefits of scale, resiliency, survivability, and mobility. The overall aggregation of sites (that is, the fabric domain) must also be able to accommodate a very large number of endpoints and scale modularly or horizontally by aggregating sites contained within each site.

Transit Sites

A transit site is a site that connects two or more fabric sites with each other 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.
- **SDA transit:** Uses LISP/VxLAN encapsulation to connect two fabric sites. The SDA 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. Using SDA transit, an end-to-end policy plane is maintained using SGT group tags.

Create an IP Transit Network

To add a new IP transit network:

-
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision > Fabric**.
 - Step 2** Hover the mouse pointer over **Add Fabric or Transit/Peer Network**.
 - Step 3** From the drop-down list, click **Transit/Peer Network**.
 - Step 4** Enter a transit name for the network.
 - Step 5** Choose **IP-Based** as the transit type.
The routing protocol is set to BGP by default.
 - Step 6** Enter the Autonomous System Number (ASN) for the transit network.
 - Step 7** Click **Save**.
-

Create an SDA Transit Network

To add a new SDA transit network:

-
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision > Fabric**.
 - Step 2** Hover the mouse pointer over **Add Fabric or Transit/Peer Network**.
 - Step 3** From the drop-down menu, click **Transit/Peer Network**.
 - Step 4** Enter a transit name for the network.

- Step 5** Choose **SD-Access** as the transit type.
- Step 6** Enter the **Site for the Transit Control Plane** for the transit network. Choose at least one transit map server.
- Step 7** Enter the **Transit Control Plane** for the transit network.
- Step 8** Repeat Step 7 and Step 8 to add a second map server.
- Step 9** Click **Save**.
-

What to do next

After you create an SDA transit, go to the fabric site and connect the sites to which you want to connect the SDA transit. Go to **Provision > Fabric > Fabric Site**. Choose the fabric site that you created. Click **Fabric Site > Border > Edit Border > Transit**. From the drop-down list, point to your SDA transit site and click **Add**.

Create a Fabric Domain

Cisco DNA Center creates a default fabric domain called *Default LAN Fabric*.

Before you begin

Ensure that your network has been designed, the policies have been retrieved from the Cisco Integrated Services Engine (ISE) or created in the Cisco DNA Center, and the devices have been inventoried and added to the sites.

-
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision > Fabric**.
- Step 2** Hover the mouse pointer over **Add Fabric or Transit/Peer Network**.
- Step 3** Click **Add Fabric** from the pop-up.
- Step 4** Enter a fabric name.
- Step 5** Choose one fabric site.
- Step 6** Click **Add**.
-

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 (brownfield 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 configured on it to work with the SDA application.
- 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.

Configure a Fabric Domain

You can add devices to sites and assign roles to these devices—border, control plane, or edge. You can also configure IP address pools to enable communication between hosts.

Add a Fabric Site

Before you begin

You can create a new fabric site only if IP Device Tracking (IPDT) is already configured for the site. This means that you should have enabled **Monitor wired clients** while configuring Telemetry settings for the site.

-
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision > Fabric**.
- Step 2** Hover the mouse pointer over **Add Fabric or Transit/Peer Network**.
- Step 3** From the drop-down list, click **Fabric**.
- Step 4** In the **Add Fabric Site** pane that slides in, choose a **Site** from the list of Sites that appears.
- Step 5** Click **Next**.
- Step 6** Select the virtual networks that are to be added to the fabric site.
- Step 7** Click **Finish**.

If IPDT is not already enabled for the site (if **Monitor wired clients** is not selected during the Network Telemetry Settings), the fabric site is not added.

Add a Device to a Fabric

After you have created a fabric domain, you can add fabric sites, and then add devices to the fabric site. You can also specify whether the devices 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 cannot 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 is optional to designate the devices in a fabric domain as control plane nodes or border nodes. You might have devices that do not occupy these roles. However, every fabric domain 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 have not already provisioned it:

1. In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision > Devices > Inventory**.
2. The **Inventory** window displays the discovered devices.
3. The topology view shows a device in gray color if it has passed the fabric readiness checks and is ready to be provisioned.
4. 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.
5. 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 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision > Fabric**.
The window displays all the provisioned fabric domains.

Step 2 From the list of fabric domains, choose a fabric.
The resulting screen displays all the sites in that fabric domain.

Step 3 Choose a site.

All devices in the network that have been inventoried are displayed in the topology view. Any device that is added to the fabric is shown in blue.

Step 4 In the List view, click a device. The device details window slides in with the following **Fabric** options:

Option	Description
Edge	Click the toggle button next to this option to enable the selected device as an edge node.
Border	Click the toggle button next to this option to enable the selected device as a border node.
Control Plane	Click the toggle 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**, **Border**, and **Edge** options.

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

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 5](#).

To add a device as a border node:

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision > Fabric**.
A list of all provisioned fabric domains is shown.

Step 2 From the list of fabric domains, choose a fabric.
A list of all fabric sites is shown.

- Step 3** From the list of fabric sites, choose a site. 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** Click a device.
- Step 5** In the slide-in window that appears, click the **Border** toggle button.
- Step 6** In the resulting window, 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** From the **Select IP Pool** drop-down list, choose an IP address pool.
- Select an IP pool only if you want to add an IP transit network.
- Step 10** Choose a transit network that is enabled on the border device:
- To enable SDA transit on the border, choose a user-created SDA transit domain from the **Select Transit/Peer Network** drop-down list.
Click **Add**.
 - To enable IP transit on the border, choose a user-created IP transit domain from the **Select Transit/Peer Network** drop-down list.
Click **Add**.
- Do the following steps in the resulting window:
- Choose an IP pool from Design Hierarchy. The selected pool is used to automate IP routing between the border node and the IP peer.
 - Click **Add Interface** to enter interface details on the next screen.
 - Choose **External Interface** from the drop-down list.
 - Enter a custom description for the interface at **Interface Description**.
 - Enter the **Remote AS Number**.
 - Check the **Virtual Network** from the list. This virtual network is advertised by the border to the remote peer. You can select one, multiple, or all virtual networks.
 - Click **Save**.
- Step 11** 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 sent from the edge nodes. (Do not check the **Do not Import External Routes** check box.)

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.

After you select a virtual network, a list of IP address pools that are present in the virtual network appears. A list of interfaces through which you can connect nonfabric devices is also displayed.

- b) Select an **External Interface**.

In Cisco DNA Center Release 2.1.2.6, you can select more than one interface on which you can do a Layer 2 handoff.

- 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 formed in the network.

- e) Click **Save**.

Step 13 Click **Add**.

Configure Host Onboarding

The **Host Onboarding** tab lets you configure settings for the various kinds of devices or hosts that can access the fabric domain.

The **Host Onboarding** tab has the following subtabs:

- **Authentication** tab: Select an authentication template for the fabric. An Authentication template is a predefined set of configurations that are retrieved from Cisco ISE. After selecting the authentication template, click **Save**.
- **Virtual Networks** tab: Associate IP address pools to virtual networks (default, guest, or user defined), and click **Update**. The IP address pools displayed are site-specific pools only.
- **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 domain. 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 equipments (such as hubs, routers, or switches) aren't supported.

Select the Authentication Template

You can select the authentication template that applies to all devices in the fabric domain.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision > Fabric**.

Step 2 In the resulting window, click a fabric.

Step 3 From the **Fabric Sites** pane, choose a site.

Step 4 Click the **Host Onboarding** tab.

Step 5 In the **Authentication** tab, choose an authentication template for the site:

- **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 very limited network access prior to authentication. After a host has been successfully authenticated, additional network access is granted.
- **No Authentication**
- **Open Authentication:** A host is allowed network access without having to go through 802.1X authentication.

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 devices where APs were onboarded through macros or autoconf and haven't yet undergone the periodic resynch.

Step 6 (Optional) To edit the settings of the chosen authentication method, click **Edit**.

A window slides in, displaying the parameters of the selected authentication method: **First Authentication Order**, **802.1x to MAB Fallback**, **Wake on LAN**, and **Number of hosts**.

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.

Make the required changes and click **Save**.

The edit window closes. 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.

Associate Virtual Networks to the Fabric Domain

IP address pools enable host devices to communicate within the fabric domain.

When an IP address pool is configured, Cisco DNA Center immediately connects to each node to create the appropriate switch virtual interface (SVI) to allow the hosts to communicate.

You cannot add an IP address pool, but you can configure a pool from the ones that are listed. The IP address pools listed are created when the network is designed.

You can configure the following features of a virtual network using this procedure:


- Common IP address pool
- Wireless IP address pool
- Critical IP address pool
- IP Directed Broadcast
- Custom VLAN ID
- Layer 2 Flooding
- Anchored virtual network

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision > Fabric**.

Step 2 In the resulting window, click a fabric.

Step 3 In the **Fabric Sites** pane, select a site.

Step 4 In the **Host Onboarding** tab, click **Virtual Networks**.

Step 5 To associate one or more virtual network(s) to the selected fabric site, click the  icon (**Add Virtual Network**).

a) In the **Add Virtual Network** slide-in pane, select the virtual networks to be added to the fabric site.

b) Click **Update**.

Step 6 To edit a virtual network, in the **Virtual Networks** tab, click a virtual network.

Step 7 Review the following fields in the **Edit Virtual Network** slide-in pane:

Field	Description
IP Pool Name	IP address pools that are associated with the virtual network.
VLAN	ID of the VLAN that is associated with the virtual network.
VLAN Name	Name of the VLAN associated with the virtual network.
Traffic Type	Type of traffic enabled on the virtual network.
Scalable Group	Group that the IP pool belongs to.
Common Pool	Selected IP pool is shared across multiple sites in a fabric. To enable or disable the common pool, choose Actions > Enable/Disable Common Pool .
Wireless Pool	Selected IP pool is enabled as a Wireless Pool . To enable or disable the selected IP pool as a wireless pool, choose Actions > Enable/Disable Wireless Pool .

Field	Description
	If enabled, you can choose from only the defined wireless pool while configuring wireless SSID for the fabric.
Layer-2 Only	Selected IP pool is used exclusively as a Layer 2 segment.
IP Directed Broadcast	IP Directed Broadcast setting for the selected IP pool. To enable this setting, check the check box. To disable it, uncheck the check box.
Layer-2 Flooding	Layer 2 flooding setting for the selected IP pool. To enable this setting, check the check box. To disable it, uncheck the check box. Layer 2 flooding is disabled by default.

Step 8

To associate one or more IP address pool(s) to the selected virtual network, click **Add**.

In the **Edit Virtual Network** slide-in pane, do the following:

- a) Choose the **IP Address Pool** from the drop-down list.
- b) Enter a valid **VLAN Name**.
- c) Enter a custom **VLAN** number for the virtual network.

Note the following:

- VLAN IDs 1, 1002-1005, 2046, and 4095 are reserved and cannot be used.
- If you do not provide a custom VLAN ID, Cisco DNA Center generates a VLAN ID in the range of 1021 to 2020.

- d) Choose a **Scalable Group** from the drop-down list.
- e) Choose the **Traffic** type from the drop-down list.

You can choose to send voice or data traffic through the virtual network.

- f) To enable Layer 2 flooding, check the **Layer-2 Flooding** check box.

Note Layer 2 flooding requires underlay multicast, which is configured during LAN Automation. If you do not provision the underlay through LAN Automation, configure underlay multicast manually.

- g) To include this IP pool in the critical IP address pool, check the **Critical Pool** check box.

A critical pool is used for closed authentication profile when an authentication server is not 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.

- h) To enable this IP pool to be shared across multiple sites in a fabric, check the **Common Pool** check box.

The **Intersite Layer 2 Handoff** feature supports sharing an IP pool among multiple sites in a fabric.

- i) To enable this IP pool as a wireless IP address pool, check the **Wireless Pool** check box.
- j) To enable the IP Directed Broadcast feature, check the **IP Directed Broadcast** check box.

Note

- Enable Layer-2 flooding before enabling IP Directed Broadcast.
- You cannot enable the IP Directed Broadcast feature on a segment that has Intersite Layer 2 Handoff enabled on it.
- Routers and Nexus 7000 Series Switches do not support the IP Directed Broadcast feature.

k) Click **Add** to save the settings.

The settings you specify here are deployed to all devices in the virtual network.

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

Step 9

To anchor this virtual network and enable its border to be a common border for all traffic through this virtual network, check the **Use Border/CP for this site to be common for the Virtual Network** check box.

An anchored virtual network can be added to other fabric sites to enable multisite guest access to a common border.

An anchored virtual network is displayed with an anchor tag next to it.

Note

- You cannot anchor a virtual network if it contains segments.
- Before anchoring a virtual network, ensure that all control plane and border devices are provisioned.
- If you enable multicast on the anchored virtual network, multicast is configured on the edge devices of the inherited virtual network, provided the inherited virtual network has segments configured. If the inherited virtual network does not have a segment, multicast is deployed only after the first segment is created.

Step 10

After associating IP pools to all virtual networks, click **Save**.

Configure Wireless SSIDs for the Fabric Domain

Step 1

From the **Wireless SSID** section, specify the wireless SSIDs within the network that the hosts can access.

Step 2

Click **Choose Pool** and select an IP pool reserve for the SSID.

Step 3

From the **Assign SGT** drop-down list, choose a scalable group for the SSID.

Step 4

Check the **Enable Wireless Multicast** check box to enable wireless multicast on the SSIDs.

Configure Ports Within the Fabric Site

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



Note

The settings you make here for the ports override the general settings you made for the device in the **Virtual Networks** section.

Step 1

In the Cisco DNA Center GUI, click the **Menu** icon () and choose **Provision > Fabric**.

Step 2

In the resulting window, click a fabric.

Step 3

From the **Fabric Sites** pane, select a site.

Step 4

From the **Host Onboarding** tab, click **Port Assignment** tab.

Step 5 From the list of fabric devices displayed in the left pane, choose the device that you want to configure. The ports available on the device are displayed in the right pane.

Step 6 From the right pane, select the ports of the device and click **Assign**.

Step 7 In the **Port Assignment** pane that slides in, select the **Connected Device Type** from the following options in the drop-down list:

Option	Description
Trunk	Configure the port as trunk port.
Access Point(AP)	Configures the port to connect to an access point.
User Devices (ip-phone, computer, laptop)	Configures the port to connect to a host device.

- a) To connect a trunk port, select **Trunk** and provide a **Description** for this port.
- b) To connect an access point, select **Access Point(AP)** and do the following:
 1. Select the VLAN and IP address from the **VLAN Name / IP Address Pool (Data)** drop-down list.
 2. Select the **Authentication** type from the drop-down list.
 3. Provide a **Description** about the connected device.
- c) To connect host devices, select **User Devices (ip-phone, computer, laptop)** and do the following:
 1. Select the IP address pool for data from the **VLAN Name / IP Address Pool (Data)** drop-down list.
 2. Select the **Scalable Groups**, which are the groups you have provisioned.
Scalable groups are supported only with No Authentication profile.
 3. Select the IP address pool for voice from the **VLAN Name / IP Address Pool (Voice)** drop-down list.
 4. Select the authentication template from the **Authentication** drop-down list.
 5. Enter a **Description** for the connected device.
- d) Click **Update**.

Step 8 After completing all port assignments, click **Deploy**.

Configure an Extended Node Device

Extended nodes are those devices that run in Layer 2 switch mode and do not support fabric technology natively. An extended node is configured by an automated workflow. After configuration, the extended node device is displayed on the fabric topology view. **Port Assignment** on the extended nodes is done on the **Host Onboarding** window.



Note Extended Nodes cannot be onboarded through the User Interface-based provisioning workflows. Extended nodes are onboarded only through the SD-Access automated workflow after resetting the device configuration to factory default and powering on the device.

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 the policy extended node.

Cisco Catalyst Industrial Ethernet (IE) 3400, IE 3400 Heavy Duty series switches, and Cisco Catalyst 9000 series switches that run Cisco IOS XE 17.1.1s or later releases of the software are policy extended node devices.

Cisco Digital Building series switches, Cisco Catalyst 3560-CX switches, and Cisco Industrial Ethernet 4000, 4010, and 5000 series switches are not policy extended node devices. They do not support Cisco TrustSec and **Group** selection during port assignment.

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.

The minimum supported software version on the edge nodes that support policy extended nodes is Cisco IOS XE 17.1.1s.



Note Cisco Catalyst 9200 series switches that are configured as fabric edge nodes do not 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
- Cisco Catalyst IE 3400, 3400 Heavy Duty (X-coded and D-coded) series switches: IOS XE 17.1.1s
- Cisco Catalyst IE 3300 series switches: IOS XE 16.12.1s
- Cisco Digital Building series switches, Cisco Catalyst 3560-CX switches: 15.2(7)E0s

Ensure the following before configuring a policy extended node:

- The minimum software version required on a policy extended node device and on the edge device supporting the policy extended node is Cisco IOS XE 17.1.1s.
- Both the policy extended node 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 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 under the **Fabric > Host Onboarding** tab. 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 connected to the extended node.

Complete this step only if the global authentication mode for the fabric is not **No Authentication**. Authentication modes can be **Open, Low Impact**, or **Closed**.

To create a port channel, complete the following steps:

- a) Go to **Provision > Fabric > Fabric Infrastructure** and select the fabric edge node. A window with the device name as the title slides in.
- b) In the **Port Channel** tab, click **Create Port Channel**.
- c) Fill in all the fields in the pane:
 - Select **Extended Node** from the **Connected Device Type** drop down.
 - Select **Port Aggregation Protocol (PAgP)**.
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 17.1.1s.
 - Note that Link Aggregation Control Protocol (LACP) does not work for extended node onboarding.
 - Select the ports to be bundled as a port channel.
- d) Click **Done**.

This creates a port channel on the fabric edge 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.

If there are errors in the workflow while configuring an extended node, an error notification is displayed as a banner on the topology window.

Default LAN Fabric EQ Find by device IP, type, role, family & MAC

✔ Fabric Infrastructure ✔ Host Onboarding Show Task Status

✘ One (1) Critical Alert and One (1) Information Alert on this page. [Collapse to hide.](#)

✘ One (1) Critical Alert
Failure on one or more extended device workflows [See more detail.](#)

i One (1) Information Alert
For each site assign at least 1 Control Plane and 1 Edge node. If the site needs external connectivity, assign at least 1 Border, Select Device(s) to assign the roles.

Click **See more details** to see the error.

A Task Monitor window slides in, displaying the status of the extended node configuration task.

Click **See Details** to see the cause of error and possible solution.

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

Do the following steps only when authentication is Closed Authentication. Note that the following steps are automated for other authentication modes.

-
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision > Fabric**.
- Step 2** In the resulting window, click a fabric.
- Step 3** From the **Fabric Sites** pane, select a site.
- Step 4** When you click the **Fabric Infrastructure** tab, all fabric devices are displayed.
- Step 5** Click a fabric edge node.
A window with the device name as the title slides in.
- Step 6** In the **Port Channel** tab, click **Create Port Channel**.
- Step 7** From the **Connected Device Type** drop-down, select 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 8** Enter a suitable **Description** for the new port channel.
- Step 9** Select an appropriate 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.
 - Do not 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 10** 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 11** Click **Done**.
A new port channel that is created is displayed in the window.
-

Update a Port Channel

Before you begin

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

- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision > Fabric**.
- Step 2** In the resulting window, click a fabric.
- Step 3** From the **Fabric Sites** pane, select a site.
- Step 4** When you click the **Fabric Infrastructure** tab, all fabric devices are displayed.
- Step 5** Click a fabric edge node.
A window with the device name as the title slides in.
- Step 6** Select the **Port Channel** tab.
- Step 7** From the list of port channels displayed, select the port channel to be updated.
The resulting window displays all the interfaces and the status of the selected port channel.
- Step 8** Do the desired update on the port channel.
You can either add interfaces to the port channel or delete existing interfaces on the port channel.
- Step 9** Click **Done**.
-

Delete a Port Channel

- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision > Fabric > Fabric Infrastructure**.
- Step 2** Click the device whose port channel you want to delete.
A window with the device name slides in.
- Step 3** Click the **Port Channel** tab.
The resulting **Port Channel** view lists all the existing port channels.
- Step 4** Select the port channel and click **Delete**.
- Step 5** At the prompt, click **Yes**.
-

Multicast Overview

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 that helps enable group communication or multicast traffic in the virtual networks. The workflow also allows you to choose multicast implementation in the network: native multicast or headend replication.



Note In Cisco DNA Center Release 2.2.2.4 and later, 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 does not 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 devices of an inherited virtual network cannot be configured as rendezvous point (RP).

-
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision**.
The window displays all provisioned fabric domains.
- Step 2** From the list of fabric domains, choose a fabric. You can view all the sites configured for the fabric. Select the site for which you want to configure multicast.
- Step 3** On the **Fabric Sites** pane, click the gear icon next to the selected site.
- Step 4** Choose **Configure Multicast** from the drop-down list.
The resulting window starts a workflow for multicast configuration.
- Step 5** In the **Enabling Multicast** window, choose the method of multicast implementation for the network, **Native Multicast** or **Head-end replication**, and click **Next**.
- Step 6** In the **Virtual Networks** window, select the virtual network on which you want to set up multicast. Click **Next**.
Note You cannot select an inherited virtual network to set up multicast.
- Step 7** 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. Click **Next**.
- Step 8** From the **Select multicast type** window, choose the type of multicast to implement, and click **Next**:
- **SSM** (Source Specific Multicast)
 - **ASM** (Any Specific Multicast)
- Step 9** 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.
 3. Click **Next**.

b) On selecting **ASM**, choose the type of rendezvous point (RP):

- **Internal RP**
- **External RP**

Click **Next**.

Step 10 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 will be the redundant rendezvous point. Click **Next**.
- b) Assign internal rendezvous points to each of the listed virtual networks. Click **Next**.

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) You can enter a second set of IPv4 or IPv6 addresses.
Click **Next**.
- b) In the **Select which RP IP Address(es) to utilize** window, select an IP address for each Virtual Network.
Click **Next**.

Step 11 Review the multicast settings displayed in the **Summary** window and modify, if required, before submitting the configuration.

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

Intersite Layer 2 Handoff

The intersite Layer 2 handoff feature lets you extend an IP subnet across multiple sites in a fabric. The same IP subnet coexists across sites in a fabric.

Note the following restrictions:

- A device that is configured as fabric-in-a-box or as a border and an edge cannot be used for intersite Layer 2 handoff.
- Intersite Layer 2 handoff and SDA transit together are not supported.
- Wake on LAN feature is not supported on those segments where Intersite Layer 2 handoff is enabled.

Before you begin

- Ensure that all the devices are discovered and provisioned and that IP pools are reserved on the site from which the IP pools will be shared.
- Ensure that the sites that share an IP pool are underlay connected. Without this connection between the borders, DHCP might not work on the hosts that try to get IP addresses on the common subnet.
- Ensure that underlay multicast is configured, which is required for Layer 2 flooding to work. Underlay multicast gets configured during the LAN automation workflow.

Step 1 [Associate Virtual Networks to the Fabric Domain](#). Ensure that you check the **Layer-2 Flooding** and **Common Pool** check boxes.

With **Layer-2 Flooding** and **Common Pool** enabled, the IP pool becomes eligible to be extended to other sites.

Step 2 Configure Layer 2 handoff on the border.

- a) From the **Provision > Fabric > Fabric Infrastructure** tab, select the border device on which the intersite Layer 2 handoff is to be configured.
- b) From the **L2 Handoff** section, select the virtual network to which the common IP pool is associated.
- c) Configure the external interface of the border that connects it to other borders across sites.
- d) Check the **Extend the subnet to other site** check box and assign an external VLAN number to the common IP pool.

Step 3 Repeat the preceding steps for the other sites that share the IP pool.

Ensure that you specify the same external VLAN number on all the interconnected borders.
