



Provision Fabric Networks

- [Cisco SD-Access Zero-Trust Security Solution](#), on page 1
- [About Fabric Networks](#), on page 8
- [New Automation for SD-Access](#), on page 10
- [Add a Fabric Site](#), on page 11
- [Configure Devices for a Fabric Site](#), on page 12
- [Add a Device to a Fabric](#), on page 13
- [Add a Device as a Border Node](#), on page 14
- [Configure LISP Pub/Sub](#), on page 17
- [Create an IP Transit](#), on page 18
- [Create an SD-Access Transit](#), on page 18
- [Select an Authentication Template](#), on page 19
- [Configure Ports Within the Fabric Site](#), on page 20
- [Configure Wireless SSIDs for Fabric Networks](#), on page 21
- [Virtual Networks](#), on page 22
- [Configure a Fabric Zone](#), on page 29
- [Configure an Extended Node Device](#), on page 34
- [Configure Supplicant-Based Extended Nodes](#), on page 41
- [Configure a Port Channel](#), on page 48
- [Multicast](#), on page 49

Cisco SD-Access Zero-Trust Security Solution

Networks need protection against external and internal threats. Cisco SD-Access provides a zero-trust security solution for your workplace. The Cisco SD-Access zero-trust security solution provides secure access to users and devices from all locations across the network.

The Cisco SD-Access zero-trust security solution includes the following capabilities:

- **Identify and verify all endpoints:** SD-Access establishes an initial level of trust with each connecting endpoint.
- **Establish policy and segmentation:** SD-Access ensures least-privilege access based on the endpoint and user type.
- **Continuously monitor endpoints:** SD-Access continuously monitors the endpoints to ensure compliance.

- Threat mitigation: SD-Access allows you to quarantine the endpoints that are noncompliant or exhibit malicious behavior.

The Cisco SD-Access zero-trust security solution provides the flexibility to adopt a path to a zero-trust workplace based on your network settings and services. You can configure how users connect to the network using dynamic rules and automated segmentation.

The Cisco SD-Access zero-trust security solution provides the capability to automate network access policies using the following features:

- Endpoint visibility: You can identify and group endpoints. You can map their interactions through traffic flow analysis and define access policies.
- Trust monitoring: You can continuously monitor the endpoint behavior, scan for vulnerabilities, verify trustworthiness for continued access, and isolate rogue or compromised endpoints.
- Network Segmentation: You can enforce group-based access policies and secure network through multilevel segmentation.

The Cisco SD-Access zero-trust security solution enables you to explore various paths to zero-trust workplace based on your network settings and services. You can discover your optimal path based on your current network status, and explore the benefits of each added step on the zero-trust journey.

Zero-Trust Overview Dashboard

The SD-Access **Zero-Trust Overview** dashboard provides an overview of your zero-trust workplace journey. Click the menu icon (☰) and choose **Provision > Zero-Trust Overview** to view this dashboard.

The zero-trust workplace journey has the following phases:

- Day 0: For starting your zero-trust workplace journey. For more information, see [Day 0 View of Zero-Trust Overview Dashboard, on page 2](#).
- Day *n*: For ongoing monitoring and configuration changes of your zero-trust workplace journey. For more information, see [Day n View of Zero-Trust Overview Dashboard, on page 5](#).

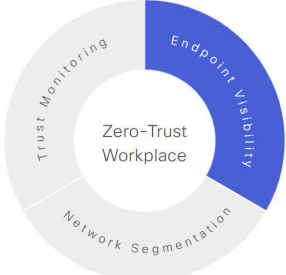
Day 0 View of Zero-Trust Overview Dashboard

Before you start your SD-Access zero-trust workplace journey, the day 0 view of the **Zero-Trust Overview** dashboard consists of the following sections:

Cisco DNA Center Provision / SD-Access / Zero-Trust Overview


Welcome to Cisco SD-Access! [Take a Tour](#)

SD-Access offers a turnkey, zero-trust security solution to automate network access policies. Security is deeply embedded within the network, and a software-defined approach allows rapid iteration and innovation.



Endpoint Visibility

Identify and group endpoints. Map their interactions through traffic flow analysis and define access policies.



Explore and start your journey to SD-Access Zero-Trust Workplace

Explore different paths to Zero-Trust Workplace based on your network settings and services. Flexible adoption pathways to reach complete SD-Access mean there is no one-user-fits-all approach. Discover your optimal path based on where your network is currently, and explore the benefits of each added step on on your Zero-Trust journey.

NETWORK CONNECTIVITY

[With Wireless](#) [With CAT9K](#) [With Traffic Telemetry Appliance](#)

SERVICES

[With ISE](#) [With Talos](#) [With CBAR Enabled](#)




I'm Done Exploring and Ready to Start My Journey

Once you are done exploring your options and have selected your preferred path settings above, click on Start My Journey to start your Cisco SD-Access to Zero-Trust Workplace.

Start my journey with creation of network fabric

I already have connectivity and want to start with Endpoint Visibility

[Start My Journey](#)



- **Welcome to Cisco SD-Access!:** This section consists of an overview video that provides a short overview of the multiple paths towards a full SD-Access zero-trust workplace. It also consists of a circle containing sections for each pillar of the SD-Access zero-trust workplace:
 - **Endpoint Visibility**
 - **Trust Monitoring**
 - **Network Segmentation**

Hover your cursor over each section to view more information.

- **Explore and start your journey to SD-Access Zero-Trust Workplace:** This section allows you to explore the different paths to a zero-trust workplace based on your network settings and services, and discover the optimal path for your network. This section consists of the **Network Connectivity** and **Services** options, and a circular journey map with details about the paths. Based on the options that you choose for network connectivity and services, the journey map displays the available paths to your zero-trust workplace journey.

To view details about each recommended step in the journey map, hover your cursor over the corresponding step around the journey map.

- **I'm Done Exploring and Ready to Start My Journey:** After exploring the paths and selecting your preferred settings, use this section to start your journey to a zero-trust workplace.

Get Started with SD-Access Zero-Trust Workplace Journey

Step 1 Click the menu icon (☰) and choose **Provision > Zero-Trust Overview**.

Step 2 Under **Explore and start your journey to SD-Access Zero-Trust Workplace**, do the following:

a) For **Network Connectivity** settings, choose the required options:

- Enable **With Wireless** to use wireless devices in your zero-trust workplace journey.
- Enable **With CAT9K** to use Cisco Catalyst 9000 Series devices or enable **With Traffic Telemetry Appliance** to use the Cisco DNA Traffic Telemetry Appliance in your zero-trust workplace journey.

b) For **Services** settings, choose the required options:

- Enable **With ISE** to use Cisco Identity Services Engine in your zero-trust workplace journey.
- Enable **With Talos** to use Talos Intelligence in your zero-trust workplace journey.
- Enable **With CBAR Enabled** to use Controller-Based Application Recognition (CBAR) in your zero-trust workplace journey.

c) (Optional) To view details about each recommended step in the journey map, hover your cursor over the corresponding step around the journey map.

Step 3 Under **I'm Done Exploring and Ready to Start My Journey**, choose one of the following options:

- To create a fabric network and start your journey towards a zero-trust workplace, click **Start my journey with creation of network fabric**.

- If you already have fabric network connectivity and want to start your journey towards zero-trust workplace with endpoint visibility, click **I already have connectivity and want to start with Endpoint Visibility**.

Step 4 Click **Start My Journey**.

Step 5 In the **Modify Journey Map** dialog box, do the following:

a) Review your journey map settings.

Note

- Cisco DNA Center displays a message if it doesn't discover the selected services for your network.
- Cisco DNA Center displays a message if it discovers additional services that were not selected in the journey.

b) (Optional) To remove a selected service from your journey map settings, uncheck the corresponding check box.

c) Click **Confirm**.

Day *n* View of Zero-Trust Overview Dashboard

After starting your SD-Access zero-trust workplace journey, the day *n* view of the **Zero-Trust Overview** dashboard consists of the following sections:

Cisco DNA Center Provision / SD-Access / Zero-Trust Overview

Your Journey to SD-Access Zero-Trust Workplace

Take a Tour

Zero Trust Workplace

Your journey to Zero-Trust Workplace

50%

Recommended Steps 1 of 3 ● Current Step

L2 Switched Access

SD-Access can be deployed alongside existing Layer 2 switched access networks, without prior conversion to Layer 3 routed access.

Tip

ROI Report 1 Month

---	---
TIME SAVED	COST SAVED

Your Journey Map

Modify My Journey Hide Map

⚠ Three (3) Warning Alerts on this page. [Expand](#) to see detail.

▼ Your Services and Network Settings SUGGESTED STEPS

- 📶 Wireless
- 🟢 CAT9K
- 📶 Talos
- 📶 CBAR

Your SD-Access Overview

Virtual Networks

16

Virtual Networks

[Go to Page](#)

Fabric Sites

Network Segmentation

A portion of the fabric with its own control plane nodes, border nodes, and edge nodes.

[Go to Page](#)



Endpoint Analytics

Endpoint Visibility



Identify, verify, and build detailed endpoint profiles, and group similar endpoints by applying AI/ML techniques to better identify who/what is in the network.


[Go to Page](#)

- **Your Journey to SD-Access Zero-Trust Workplace:** This section consists of the following dashlets:
 - The **Zero Trust Workplace** dashlet displays the percentage progress of your zero-trust workplace journey.

- The **Recommended Steps** dashlet displays the next recommended steps for your zero-trust workplace journey. Use the arrow buttons ( and ) to scroll through all the steps. This dashlet also displays the tips for some steps. If available, click **Tip** to view the tips for the corresponding step.
- The **ROI Report** dashlet displays the time and cost savings based on the implemented steps as you progress through your zero-trust workplace journey. Use the drop-down in this dashlet to choose the time period for the report. Click **ROI Report** to view the report.
- **Your Journey Map:** This section displays the details of network connectivity and service settings for your zero-trust workplace journey. Click **Modify My Journey** to modify your zero-trust workplace journey. Click **Hide Map** to hide the journey map.

This section displays the warning alerts for your journey, if available. Click **Expand** to view the details of the alerts. If a selected service is currently unavailable in your network and you want to remove it from your journey, click the corresponding **Remove From Journey** option. If you want to get a selected service that is currently unavailable in your network, click the corresponding hyperlink to get the service.




Expand the **Your Services and Network Settings** drop-down to view the list of selected services for your journey. The  icon next to a service indicates that the service is currently available in your network. The  icon next to a service indicates that the service is currently unavailable in your network.

Hover your cursor over the corresponding  icon to view the **Update Needed** dialog box with details about the unavailable service. In the **Update Needed** dialog box, do the following:

- To remove the service from your journey, click **Remove From Journey**.
- To get the unavailable service in your network, click the corresponding hyperlink.


Enable the **Suggested Steps** toggle button to view the suggested order of steps around your journey map.

To view details about each step in the journey map, hover your cursor over the corresponding step around the journey map.

The  icon next to a step indicates that the corresponding configurations are incomplete. A number next to a step (for example, ) indicates the suggested order of the recommended steps for your journey map. The  icon next to a step indicates that the corresponding configurations are complete.

- **Your SD-Access Overview:** This section consists of dashlets for each functional area of your zero-trust workplace journey. Click the corresponding **Go to Page** option to open the relevant window. Each dashlet indicates its corresponding pillar of the zero-trust workplace journey in its upper-right corner.

Modify SD-Access Zero-Trust Workplace Journey

Step 1 Click the menu icon () and choose **Provision > Zero-Trust Overview**.

Step 2 Under **Your Journey Map**, click **Modify My Journey**.

Step 3 Under **Explore and start your journey to SD-Access Zero-Trust Workplace**, do the following:

a) For **Network Connectivity** settings, choose the required options:

- Enable **With Wireless** to use wireless devices in your zero-trust workplace journey.

- Enable **With CAT9K** to use Cisco Catalyst 9000 Series devices or enable **With Traffic Telemetry Appliance** to use the Cisco DNA Traffic Telemetry Appliance in your zero-trust workplace journey.
- b) For **Services** settings, choose the required options:
- Enable **With ISE** to use Cisco Identity Services Engine in your zero-trust workplace journey.
 - Enable **With Talos** to use Talos Intelligence in your zero-trust workplace journey.
 - Enable **With CBAR Enabled** to use Controller-Based Application Recognition (CBAR) in your zero-trust workplace journey.
- c) (Optional) To view details about each recommended step in the journey map, hover your cursor over the corresponding step around the journey map.

Step 4 Under **I'm Done Exploring and Ready to Start My Journey**, choose one of the following options:

- To create a fabric network and start your journey towards a zero-trust workplace, click **Start my journey with creation of network fabric**.
- If you already have fabric network connectivity and want to start your journey towards zero-trust workplace with endpoint visibility, click **I already have connectivity and want to start with Endpoint Visibility**.

Step 5 Click **Modify My Journey**.

Step 6 In the **Modify Journey Map** dialog box, do the following:

- a) Review your journey map settings.
- Note**
- Cisco DNA Center displays a message if it doesn't discover the selected services for your network.
 - Cisco DNA Center displays a message if it discovers additional services that were not selected in the journey.
- b) (Optional) To remove a selected service from your journey map settings, uncheck the corresponding check box.
- c) Click **Confirm**.
-

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.

Transits

A transit 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 the 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 Sites and Fabric Zones**.
- Step 4** In the **Create Fabric Sites 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 **Wired Endpoint Data Collection** check box is checked.
- Step 7** In the **Authentication Template** window, do the following:
- 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 and 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 later, click **Setup Fabric Zones Later**.
- To designate fabric zones and create scoped subnets, click **Setup Fabric Zones Now** and choose a fabric site from the network hierarchy displayed.

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 by using the following tabs:

- **Fabric Infrastructure**: Assign devices to fabric roles.
- **Authentication Template**: Select an authentication template for the fabric.
- **Wireless SSIDs**: Specify wireless SSIDs within the network that hosts can access. You can select the guest or enterprise SSIDs and assign address pools.
- **Port Assignment**: 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 such as 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 add a device to a fabric, you can add it in various combinations to act as a control plane node, border node, or edge node, as described in [Add a Device to a Fabric, on page 13](#).

This section describes how to add a device as a border node and configure the following:

- Border node type: Internal, External, or Internal and External ([Step 9, on page 15](#))
- Border node Priority ([Step 10, on page 15](#))
- Border node Affinity-ID ([Step 10, on page 15](#))
- Associated transit: SD-Access transit or IP-based transit ([Step 11, on page 16](#))
- IP address pool allocation for Layer 3 handoff ([Step 11, on page 16](#))

Before you begin

To use the Border Node Affinity-ID feature, ensure that you create an SD-Access LISP Pub/Sub transit. For more information, see [Create an SD-Access Transit, on page 18](#). When adding the first control plane node in the local fabric site, ensure that you select the LISP Pub/Sub control plane protocol. For more information, see [Configure LISP Pub/Sub, on page 17](#). The border node must be running Cisco IOS XE Release 17.8.1 or later.

-
- 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** In the **Fabric Sites** window, select the fabric site to configure a border node.
The resulting topology view displays all the devices in the network inventory. In the topology view, any device that is operating in a fabric role is shown in blue.
- Step 4** 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's already configured on the device.
- Step 9** Configure the type of border node. By default, a border node is designated as an external border node, wherein it acts as the default gateway to the fabric site, without importing any external routes.

A border node can be configured to be an internal border node, wherein it isn't the default gateway and only imports external routes. A border node can also have a combined role of internal and external borders.
- Check both the **Default to all virtual networks** and **Do not import external routes** check boxes to designate the border as an external border node.
 - Uncheck both the **Default to all virtual networks** and **Do not import external routes** check boxes to designate the border as an internal border node.
 - Check the **Default to all virtual networks** check box to designate the border node as an external and internal border. It acts as the fabric default gateway and also imports BGP-learned routes into the fabric site. (Don't check the **Do not import external routes** check box.)
- For information about border node types, see the [Cisco SD-Access Solution Design Guide](#).
- Step 10** To configure the border node priority, affinity-ID and native multicast across SD-Access transit, click **Advanced Attributes** and configure the following:
- a) To change the border node priority, check the **Modify Border Priority** check box and enter a new priority value.
 - Priority value ranges from 1 to 10.
 - 1 indicates the highest priority.
 - 10 indicates the lowest priority.
 - The default priority value is 10.

If two or more border nodes are configured in a fabric site, traffic is routed through the border node that has a higher priority. If the priority values are the same, traffic is load balanced across the border nodes.
 - b) (Optional) To configure the border node affinity-ID, check the **Modify Border Node Affinity-ID** check box and enter values for the following fields:
 - **Affinity-ID Prime**: A lower relative prime value indicates a higher preference.

- **Affinity-ID Decider:** When the prime value is the same for two border nodes, the decider value is used as a tie-breaker to determine the border node preference.

Affinity-ID is a relative value, considering the value of this border node among the received values from all the other available border nodes. The lower the relative value of affinity-ID, the higher the preference for a destination border node. By default, the affinity-ID value isn't provisioned.

When the received affinity-ID values are equal, priority is used to determine the border node preference.

Note For proper functionality of the Affinity-ID feature, ensure that you configure an affinity-ID on all border nodes connected to the same SD-Access transit.

- c) (Optional) To configure native multicast over multiple sites that are connected to an SD-Access transit, check the **Enable Multicast over SD-Access Transit** check box.

Note Ensure that you enable a similar check box for the SD-Access transit too.

You can view the border node priority and affinity-ID deployment logs in **Activities > Audit Logs**.

Step 11

Hover your cursor over **Add Transit Site** and select a transit that will be connected to this border node.

In an **IP:BGP IP TRANSIT**, you can choose to either automate the IP address allocation for a virtual network or manually assign the Local and Peer IP addresses for a virtual network. You cannot do both.

- a) (Optional) To enable Cisco DNA Center to allocate IP address for the connection between the border node and peer, choose an IP address pool from the **Select IP Address Pool** drop-down list.

Note **Select IP Address Pool** is disabled if you have manually assigned the Local and Peer IP addresses.

- b) To configure the handoff interface, click **Add External Interface**.

Do the following steps in the resulting window:

1. Select an interface from the **External Interface** drop-down.
2. The **Remote AS Number** is automatically derived from the selected Transit or Peer network.
3. (Optional) Enter the a description for the interface in the **Interface Description** field.
4. (Optional) From the **Actions** drop-down list, choose **Enable All** or **Disable All**.
5. Click the **Enable Layer 3 Handoff** toggle button for the virtual network. This virtual network is advertised by the border node to the peer through BGP. You can select one, multiple, or all virtual networks.
6. In the **VLAN ID** field, enter an ID for the selected virtual network.
7. (Optional) To manually assign the IPv4 and IPv6 **Local IP Address** and **Peer IP Address** for the selected virtual network, enter the IP addresses and subnet mask in the CIDR notation (IP address/prefix-length).

Note The **Local IP Address** and **Peer IP Address** fields are disabled if you have already selected an IP Pool.

8. Click **Save**.

- c) Click **Add**.

Step 12

(Optional) Perform this step only if you are connecting a traditional network to the fabric site or you are migrating from a traditional network to an SD-Access network. Click the **Layer 2 Handoff** tab.

A list of virtual networks and the count of IP address 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 to the traditional network are displayed.

- b) Select an interface from the **External Interface** drop down.
 c) (Optional) Enter a description for the interface in the **Interface Description** window.
 d) In the **External VLAN** field, enter the VLAN number into which the fabric must be extended.

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 no loops are formed in the network.

Because a border node is connected to the traditional network, it is subject to broadcast storms, Layer 2 loops, and spanning-tree problems that can occur in Layer 2 switched access networks. To prevent disruption of control plane node services or border node services connecting to other external networks, a border node should be dedicated to the Layer 2 handoff feature and not colocated with other fabric roles or services.

- 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 Release 17.6.1 or later.

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 Pub/Sub** 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


- 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

To add an SD-Access transit:

- 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.
- Step 4** Choose an SD-Access **Transit Type**.

To configure a transit for the fabric sites that don't have a LISP Pub/Sub control plane, choose **SD-Access (LISP/BGP)**.
To configure a transit for the fabric sites that have a LISP Pub/Sub control plane, choose **SD-Access (LISP Pub/Sub)**.
To share the **SD-Access (LISP Pub/Sub)** 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 an additional map server, click the plus icon () and repeat [Step 5, on page 18](#) and [Step 6, on page 18](#).
- Step 8** (Optional) To configure native multicast over the LISP Pub/Sub-based SD-Access transit, click **Advanced Attributes**.
In the **Advanced Attributes** slide-in pane, check the **Multicast Over SD-Access Transit** check box.
In the **Advanced Attributes** slide-in pane, click **Save**.

Note To complete the native multicast configuration over multiple sites that are connected to the SD-Access transit, ensure that you enable multicast over SD-Access transit on the border nodes.
- Step 9** Click **Save**.

After a transit is created, the **Transits** window displays the newly created transit and its attributes.

Note You can't add an **SD-Access (LISP Pub/Sub)** 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 corresponding to the device that you want to configure. The ports that are available on the device are displayed.

Step 6 Check the corresponding check box.

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

Step 8 In the slide-in pane, choose the **Connected Device Type**:

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.

Option	Description
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:
 - a. Choose the VLAN name for data from the **VLAN Name (Data)** drop-down list.
 - b. Choose a security group from the **Security Group** drop-down list.
Security groups are supported only with the **None** authentication template.
 - c. Choose the VLAN name for voice from the **VLAN Name (Voice)** drop-down list.
 - d. 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** From the **Choose Pool** drop-down list, choose an IP address pool reserved for the SSID.
The wireless IP address pools that are configured for Layer 3 and Layer 2 segments are available in this drop-down list.
- 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 macrosegmentation. 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 the Cisco Identity Service Engine. Within a virtual network, endpoints can communicate with each other unless explicitly blocked by microsegmentation policy. Endpoints across different virtual networks cannot communicate with each other by default. Intervirtual 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 must be segmented from building systems, such as lighting, heating, ventilation, and air conditioning. In such a scenario, a network administrator can use macrosegmentation to 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 in **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 **Layer 3 Virtual Networks** window, do the following:
- In the **Layer 3 Virtual Network name** field, enter a name for the Layer 3 virtual network.
 - (Optional) To create another Layer 3 virtual network, click the plus icon () and enter a name for the Layer 3 virtual network.
- Step 4** In the **Fabric Sites and Fabric Zones (Optional)** window, configure the following:
- Click **Select Fabric Sites** and choose the fabric sites.
You can assign a virtual network to multiple fabric sites. To choose the fabric sites, do one of the following:
 - Click the plus icon () next to the required fabric sites.
 - Click the fabric site name and click **Add Selected**.

Note To choose multiple fabric sites, press **Shift**, click the fabric site names, and click **Add Selected**.

 - To choose all the fabric sites, click **Add All**.
- Repeat this association for all the Layer 3 virtual networks that you created.
- Click **Assign**.
 - Click **Select Fabric Zones** and do one of the following:

- Click the plus icon () next to the required fabric zones.
- Click the fabric zone name and click **Add Selected**.
Note To choose multiple fabric zones, press **Shift**, click the fabric zone names, and click **Add Selected**.
- To choose all the fabric zones, click **Add All**.

d) Click **Assign**.

Step 5 Review the Layer 3 virtual network settings in the **Summary** window.

Step 6 In the **Created and Deploy (Step 1 of 2)** window, click **Create** to create the context of the virtual network.

Step 7 In the **Created and Deploy (Step 2 of 2)** window, click **Deploy** to assign the virtual network to the selected sites.

Step 8 To verify the virtual network creation, click **View Layer 3 Virtual Networks**.

In the **Virtual Networks** window, the **Layer 3** tab displays the details of all the Layer 3 virtual networks.

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 **Configuration Attributes** window, configure the following:


- a) In the **VLAN Name** field, enter the VLAN name.
- b) In the **VLAN ID** field, enter the VLAN ID. The valid range for VLAN ID is from 2 through 4093.

Note The VLAN IDs from 1002 through 1005 and 2046 are reserved VLAN IDs.

- c) From the **Traffic Type** area, choose **Data** or **Voice**.
- d) Check the **Fabric-Enabled Wireless** check box to enable wireless.
The **Layer 2 Flooding** check box is enabled by default for a Layer 2 virtual network.
- e) To add another Layer 2 virtual network, click the plus icon () and repeat [3.a, on page 23](#) to [3.d, on page 23](#).

Step 4 In the **Associated Fabric Sites and Fabric Zones** window, choose a fabric site for the Layer 2 virtual network from the **Fabric Sites** drop-down. Optionally, to choose the fabric zone to associate with this Layer 2 virtual network, do the following:

a) Click **Select Fabric Zones** and do one of the following:

- Click the plus icon () next to the required fabric zones.
- Click the fabric zone name and click **Add Selected**.
Note To choose multiple fabric zones, press **Shift**, click the fabric zone names, and click **Add Selected**.
- To choose all the fabric zones, click **Add All**.

b) Click **Assign**.

Repeat this association for all the Layer 2 virtual networks that you created.


Step 5 In the **Summary** window, review your Layer 2 virtual network settings and click **Create**.

Step 6 In the **Create** window, click **Deploy** to deploy the Layer 2 virtual network.

After the Layer 2 virtual network is provisioned, a success message is displayed.

Step 7 To verify the virtual network creation, click **View Layer 2 Virtual Networks**. In the **Virtual Networks** window, the **Layer 2** tab displays the details of all the Layer 2 virtual networks.

Associate Layer 3 Virtual Networks to Fabric Sites

Step 1 Click the menu icon () and choose **Provision > Virtual Networks**.

Step 2 Under **SUMMARY**, 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, check the check box next to the Layer 3 virtual networks for which you want to edit the fabric site association.


Note You can edit up to five Layer 3 virtual networks.

Step 4 Hover your cursor over **More actions**, and choose **Edit Fabric Site and Fabric Zone Associations**.

Step 5 In the **Fabric Sites and Fabric Zones (Optional)** window, configure the following:

a) Click **Select Fabric Sites** and choose the fabric sites.

You can assign a virtual network to multiple fabric sites. To choose the fabric sites, do one of the following:

- Click the plus icon () next to the required fabric sites.
- Click the fabric site name and click **Add Selected**.


Note To choose multiple fabric sites, press **Shift**, click the fabric site names, and click **Add Selected**.

- To choose all the fabric sites, click **Add All**.

Repeat this association for all the Layer 3 virtual networks.

b) Click **Assign**.

c) Click **Select Fabric Zones** and do one of the following:

- Click the plus icon () next to the required fabric zones.
- Click the fabric zone name and click **Add Selected**.

Note To choose multiple fabric zones, press **Shift**, click the fabric zone names, and click **Add Selected**.

- To choose all the fabric zones, click **Add All**.

d) Click **Assign**.

- Step 6** Review the Layer 3 virtual network sites on the **Summary** window.
- Step 7** In the **Created and Deploy (Step 1 of 2)** window, click **Update** to assign the Layer 3 virtual networks to the selected sites.
- Step 8** In the **Created and Deploy (Step 2 of 2)** window, click **Deploy** to deploy the Layer 3 virtual networks.
- Step 9** To verify the virtual networks, click **View Layer 3 Virtual Networks**.
In the **Virtual Networks** window, the **Layer 3** tab displays the details of all the Layer 3 virtual networks.

Create Anycast Gateways

Before you begin

Ensure that you have created a Layer 3 virtual network. For more information, see [Create a Layer 3 Virtual Network, on page 22](#).

-
- Step 1** Click the menu icon (☰) and choose **Provision > Virtual Networks**.
- Step 2** Under **SUMMARY**, click the number that indicates the count of **Anycast Gateways**.
- Step 3** In the **Anycast Gateway** tab, click **Create Anycast Gateways**.
Alternatively, click the menu icon and choose **Workflows > Create Anycast Gateways**.
- Step 4** If the task overview window opens, click **Let's Do it** to go directly to the workflow.
- Step 5** In the **Layer 3 Virtual Networks** window, select one or more virtual networks to add a gateway.
- Click the plus icon (+) next to the required fabric sites.
 - Click the fabric site name and click **Add Selected**.
- Note** To choose multiple fabric sites, press **Shift**, click the fabric site names, and click **Add Selected**.
- To choose all the fabric sites, click **Add All**.
- Step 6** In the left pane of the **Configuration Attributes** window, choose the Layer 3 virtual network for which you want to create the anycast gateway and do the following:
- a) From the **IP Address Pool** drop-down list, choose an IP address pool.
 - b) For **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 active only when you choose the **Extended Node** pool type.

- c) To enable the IP-Directed Broadcast feature, check the **IP-Directed Broadcast** check box.

Note

- When you enable Directed Broadcast, Cisco DNA Center automatically enables Layer 2 flooding.
- Routers and Cisco Nexus 7000 Series Switches don't support Directed Broadcast.
- Before enabling Directed Broadcast, ensure that you have enabled underlay multicast.

- d) To enable the intrasubnet routing, check the **Intra-Subnet Routing** check box.

Note When you enable intrasubnet routing, Cisco DNA Center automatically disables the **Fabric-Enabled Wireless** and **Layer 2 Flooding** check boxes.

- e) Enter a valid **VLAN Name** or check the **Auto generate VLAN name** check box.

- f) 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.

- g) Choose **Data** or **Voice** from the **Traffic Type** area.

- h) From the **Security Group** drop-down list, choose a security group.

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

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.

Note When you enable critical VLAN, Cisco DNA Center automatically generates the VLAN name.

- j) To enable this IP pool as a wireless IP address pool, check the **Fabric-Enabled Wireless** check box.

- k) 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 don't provision the underlay through LAN automation, configure the underlay multicast manually.

- l) To enable onboarding of bridge-mode virtual machines that are connected to the fabric-enabled wireless network, check both the **Fabric Enabled Wireless** and the **Multiple IP to MAC** check boxes.

- m) To enable a wired host to have multiple IPv4 addresses (IP aliasing), check only the **Multiple IP to MAC** check box.

You can have a maximum of 1000 IPv4 addresses for a single MAC address.

- n) To associate more IP pools, click the plus icon (+) and repeat the steps.

Step 7

In the **Fabric Zones (Optional)** window, do the following:

- a) Click **Select Fabric Zones** and do one of the following:

- Click the plus icon (+) next to the required fabric zones.
- Click the fabric zone name and click **Add Selected**.

Note To choose multiple fabric zones, press **Shift**, click the fabric zone names, and click **Add Selected**.

- To choose all the fabric zones, click **Add All**.

b) Click **Assign**.

Step 8 Review the anycast gateway settings in the **Summary** window.

Step 9 In the **Create** window, click **Deploy**.

Step 10 To verify the gateway creation after you see a success message, click **View Anycast Gateway**.

In the **Virtual Networks** window, the **Anycast Gateway** tab displays the details of all the anycast gateways.

Virtual Network Policy

Configure a virtual network (VN) policy to allow route leaks between Layer 3 VNs, without using a fusion device. Use a VN policy to provide the endpoints (hosts or users) with access to shared services like DHCP, DNS, Internet access, and so on, through Cisco DNA Center automation. The shared services connect to a Provider VN. The endpoints that use the shared services reside in a Subscriber VN. A VN policy establishes communication between the Provider VN and the Subscriber VNs.

You can create a VN policy, edit a VN policy, and delete a VN policy for the following deployments:

- Single site fabric with IP Transit
- Multi-site fabric with SDA Transit

Guidelines to Configure a Virtual Network Policy

Consider the following guidelines before you configure a virtual network policy:

- To configure a VN Policy, a device should operate Cisco IOS XE 17.9.1 or a later release.
- VN Policy is supported only on the fabric sites that have a LISP Pub/Sub control plane.
- To configure a VN policy on a multisite fabric with SD-Access transit, ensure that all the sites have the provider VN.
- If you configure multiple VN policies in your network, the same VN cannot be the Provider VN in more than one policy.
- VN Policy does not support overlapping IP pools.
- Provider VN in a policy cannot be configured as a Subscriber VN in another VN Policy and conversely.
- Add the Provider VN to all the fabric sites where a VN Policy is applicable.
- Ensure that the Provider VNs do not leak into each other outside the fabric. Else, it might result in route leaks between the Subscriber VNs.
- VN policy is not supported on router devices.
- Inter-VN multicast through a VN policy is not supported. You cannot route multicast between the Layer 3 virtual networks that are interconnected through a VN policy.

Create a Virtual Network Policy

To create a VN policy, follow these steps:

-
- Step 1** Click the menu icon (☰) and choose **Workflows > Create Virtual Network Policy**.
Alternatively, navigate to **Layer 3 Virtual Networks** tab under **Provision > Virtual Networks** and click **Policies**. In the **Policies** window, click **Create Virtual Network Policy**.
- Step 2** Follow the on-screen guidance to provide a name for the policy, to select a Provider VN and the Subscriber VNs.
You can assign this VN policy to one or more fabric sites.
In a multisite deployment where an SD-Access transit connects the fabric sites, ensure that you select all the fabric sites that are connected by the SD-Access transit.
- Step 3** On the **Summary** page, review the VN Policy configuration.
To make changes, click **Edit** next to the group of settings that you want to change.
- Step 4** Click **Create**.
-

Edit a Virtual Network Policy

You can edit a VN Policy to add or delete Subscriber VNs and to assign or remove the policy from a fabric site.

-
- Step 1** Click the menu icon (☰) and choose **Provision > Virtual Networks**.
- Step 2** Click the number that indicates the count of **Layer 3 Virtual Networks**.
- Step 3** In the **Policies** tab, select the policy to be edited, and click **More Actions > Edit Policy**.
- Step 4** Follow the on-screen guidance to edit the policy.
-

Delete a Virtual Network Policy

To delete a VN Policy, follow these steps:

-
- Step 1** Click the menu icon (☰) and choose **Provision > Virtual Networks**.
- Step 2** Click the number that indicates the count of **Layer 3 Virtual Networks**.
- Step 3** In the **Policies** tab, select the policy to be deleted, and click **More Actions > Delete Policy**.
- Step 4** In the **Delete Policy** slide-in pane, click **Apply**.
-

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 29](#).
 - 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 30](#).
2. Add edge nodes and extended nodes to the fabric zone. For more information, see [Add a Device to a Fabric, on page 13](#).
3. Assign Layer 3 virtual networks and segments to the fabric zone. For more information, see [Associate Layer 3 Virtual Networks to Fabric Zones, on page 31](#).



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 Sites and Fabric Zones**.
Alternatively, click the menu icon and choose **Workflows > Create Fabric Sites and Fabric Zones**.
- 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 **Wired Endpoint Data Collection** 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 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** Review the fabric site settings in the **Summary** window.
You can edit any of the fabric site or zone settings here.
- Step 6** Click **Deploy**.
It takes several seconds for the fabric site and fabric zones to be provisioned. After the provisioning, a success 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.

Associate Layer 3 Virtual Networks to Fabric Zones

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 **SUMMARY**, 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** In the **Layer 3** tab, check the check box next to the Layer 3 virtual networks for which you want to edit the fabric zone associations.
- Note** You can edit up to five Layer 3 virtual networks.
- Step 4** Hover your cursor over **More actions**, and choose **Edit Fabric Site and Fabric Zone Associations**.
- Step 5** In the **Fabric Sites and Fabric Zones (Optional)** window, configure the following:
- a) Click **Select Fabric Zones** and choose the fabric zones.
You can assign a virtual network to multiple fabric zones in a fabric site. To choose the fabric zones, do one of the following:

- Click the plus icon (+) next to the required fabric zones.
- Click the fabric zone name and click **Add Selected**.

Note To choose multiple fabric zones, press **Shift**, click the fabric zone names, and click **Add Selected**.

- To choose all the fabric zones, click **Add All**.

- Click **Assign**.
- Repeat this association for all the Layer 3 virtual networks.

Step 6 Review the Layer 3 virtual network zones on the **Summary** window.

Step 7 In the **Created and Deploy (Step 1 of 2)** window, click **Update**.

Step 8 In the **Created and Deploy (Step 2 of 2)** window, click **Deploy** to deploy the Layer 3 virtual networks.

Step 9 To verify the virtual networks, click **View Layer 3 Virtual Networks**.

In the **Virtual Networks** window, the **Layer 3** tab displays the details of all the Layer 3 virtual networks.

Associate Layer 2 Virtual Networks to Fabric Zones

Before you begin



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

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

Step 2 Under **SUMMARY**, 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 site and click **Select**.

Step 5 In the **Layer 2** tab, check the check box next to the Layer 2 virtual networks for which you want to edit the fabric zone associations.

Note You can edit up to five Layer 2 virtual networks.

Step 6 Hover your cursor over **More actions**, and choose **Edit Layer 2 Fabric Zone Associations**.

Step 7 In the **Associated Fabric Sites and Fabric Zones** window, configure the following:

- Click **Select Fabric Zones** and choose the fabric zones.

You can assign a virtual network to multiple fabric zones in a fabric site. To choose the fabric zones, do one of the following:

- Click the plus icon (+) next to the required fabric zones.

- Click the fabric zone name and click **Add Selected**.

Note To choose multiple fabric zones, press **Shift**, click the fabric zone names, and click **Add Selected**.

- To choose all the fabric zones, click **Add All**.

b) Click **Assign**.

c) Repeat this association for all the Layer 2 virtual networks.

Step 8 In the **Summary** window, review your Layer 2 virtual network settings and click **Create**.

Step 9 In the **Create** window, click **Deploy** to deploy the Layer 2 virtual network.

After the Layer 2 virtual network is provisioned, a success message is displayed.

Step 10 To verify the virtual network creation, click **View Layer 2 Virtual Networks**. In the **Virtual Networks** window, the **Layer 2** tab displays the details of all the Layer 2 virtual networks.

Associate Anycast Gateways to Fabric Zones

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 **SUMMARY**, 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 site and click **Select**.

Step 5 In the **Anycast Gateway** tab, check the check box next to the anycast gateways for which you want to edit the fabric zone associations.

Note You can edit up to five anycast gateways.

Step 6 Hover your cursor over **More actions**, and choose **Edit Fabric Zone Associations**.

Step 7 In the **Fabric Zones (Optional)** window, do the following:

a) Click **Select Fabric Zones** and do one of the following:

- Click the plus icon (**+**) next to the required fabric zones.
- Click the fabric zone name and click **Add Selected**.

Note To choose multiple fabric zones, press **Shift**, click the fabric zone names, and click **Add Selected**.

- To choose all the fabric zones, click **Add All**.

b) Click **Assign**.

Step 8 Review the anycast gateway settings in the **Summary** window.

Step 9 In the **Create** window, click **Deploy**.

Step 10 To verify the gateway creation after you see a success message, click **View Anycast Gateway**.

In the **Virtual Networks** window, the **Anycast Gateway** tab displays the details of all the anycast gateways.

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 25](#). 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, reset the device configuration to factory default and reload it.

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:

- a) Click the menu icon (☰) and choose **Tools > License Manager**.
- b) In the **Devices** tab, select the device.
- c) Choose **Actions > Change License > Change DNA License**.
- d) In the **Change DNA License Level** window, click **Advantage**.
- e) Click **Confirm**.
- f) 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 is no longer displayed.

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

Step 4 Upgrade to policy extended node.

- a) In the **Provision > Fabric Sites** window, select the site in which the device is onboarded.
- b) In the **Fabric Infrastructure** tab, click a device to edit its attributes.
- c) In the **Fabric** tab, click the **Policy** toggle button under **Extended Node Attributes**.
- d) In the **Policy Extended Node Upgrade** window that is displayed, 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 an 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 fabric in a box (FIAB).
A slide-in pane 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 that it is forwarding 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 43](#).
- 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.
- a) 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](#).
 - b) 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.
- a) Click the menu icon (☰) and choose **System > Settings > Device Settings > PnP Device Authorization**.
 - b) Check the **Device Authorization** check box to enable authorization on the device.
 - c) 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 25](#).

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, on page 20](#). 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, follow these 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, on page 20](#). 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.

* 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	<input type="text" value="Cisco-IOS-NMAPOSCheck"/>	Then	<input type="text" value="Certainty Factor Increases"/>	<input type="text" value="10"/>	
If	Condition	<input type="text" value="CDP_cdpCachePlatform_CONTAINS_9200..."/>	Then	<input type="text" value="Certainty Factor Increases"/>	<input type="text" value="20"/>	
If	Condition	<input type="text" value="DHCP_v-i-vendor-class_CONTAINS_9200..."/>	Then	<input type="text" value="Certainty Factor Increases"/>	<input type="text" value="20"/>	

Condition Name	Expression	OR
	<input type="text" value="DHCP:v-i-ven..."/> <input type="text" value="CONTAIN"/> <input type="text" value="9200"/>	OR
	<input type="text" value="DHCP:v-i-ven..."/> <input type="text" value="CONTAIN"/> <input type="text" value="9300"/>	
	<input type="text" value="DHCP:v-i-ven..."/> <input type="text" value="CONTAIN"/> <input type="text" value="9500"/>	

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

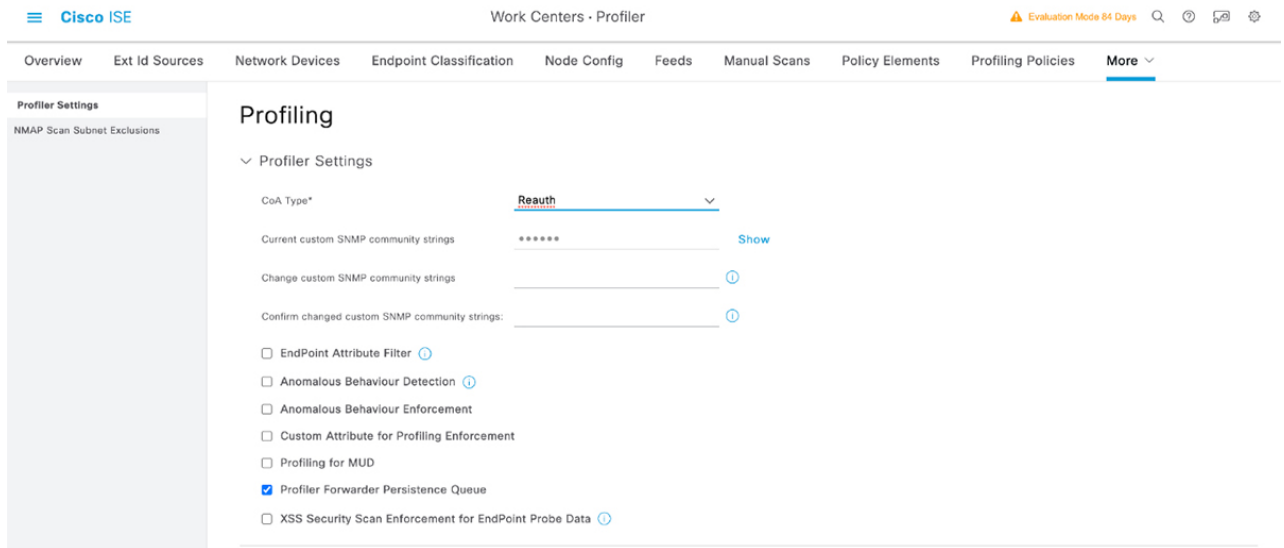
Ensure that the **Minimum Certainty Factor** value for the child policy is higher than that of the parent policy.

* 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_cdpCachePlatform_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**.

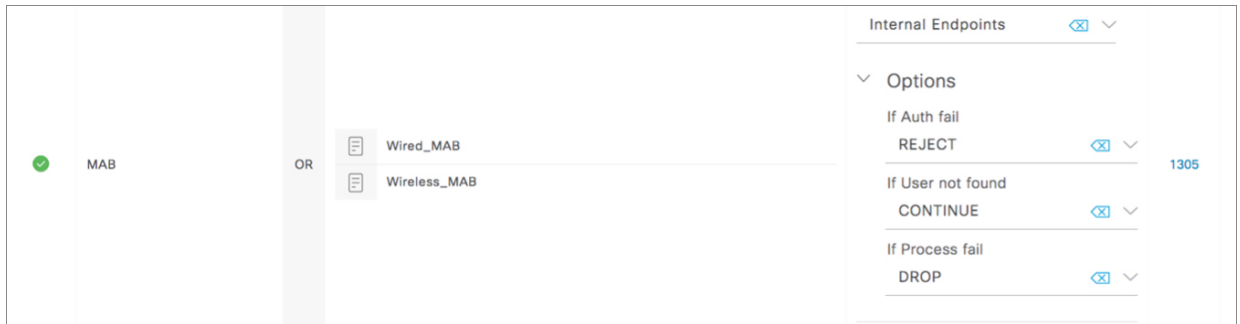
To configure the **CoA Type**, from the Cisco ISE home page, navigate to **Work Centers > Profiler > Settings**.

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

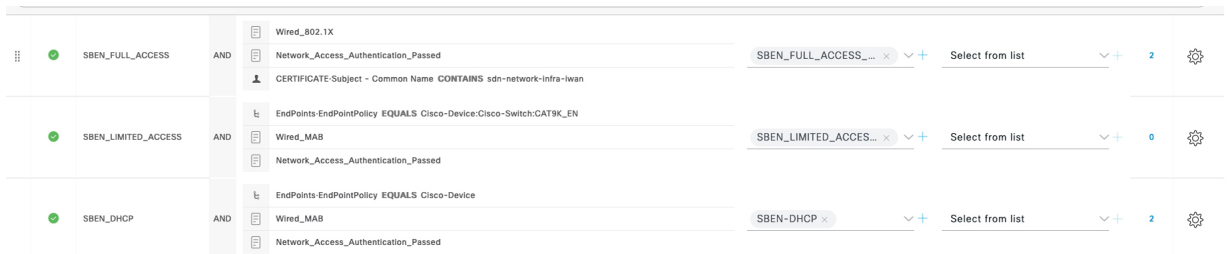


Step 5 Define the authorization policy in the **Authorization Policy** window.

- 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, such as extended nodes or servers, increase the connection resiliency and bandwidth.

Create a Port Channel

Before you begin

The authentication must be **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 list, 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, choose **On** as the protocol.
- For the extended nodes that run Cisco IOS XE Release 17.1.1s and later releases, choose **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 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 the **Fabric Site** window, select a site in the site hierarchy pane.
- Step 4** In the **Replication Mode** 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 for 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 **Multicast Mode** window, choose the type of multicast to implement:
- **SSM** (Source Specific Multicast)
 - **ASM** (Any Specific Multicast)
 - Select **SSM** and **ASM** to configure both together.
- 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. By default, 232.0.0.0/8 range of IPv4 address is selected. You can optionally modify the IPv4 address range. Choose an IP group range from 225.0.0.0 to 239.255.255.255.
 2. For IPv6 addresses, FF3x::/32 is reserved for SSM.

- b) On selecting **ASM**, in the **Multicast Group to Rendezvous Point Mapping** window, configure the rendezvous point for each virtual network:
1. Choose the type of rendezvous point: **External** or **Fabric**.
 2. Configure the rendezvous points in the respective tabs: **IPv4 RP** and **IPv6 RP**.
 3. You can define any number of external rendezvous points.
 4. Optionally, you can define a group-to-rendezvous point mapping. There could be one or multiple IPv4/IPv6 multicast groups that are associated with a rendezvous point.
 5. You can either have a rendezvous point with no mapping or with mapping. Both can't be configured together.
 6. The permitted multicast group ranges for IPv6 and IPv4 FF00:/8 and 225.0.0.0/8 - 239.0.0.0/8 respectively.

Step 9 In the **Summary** window, review the multicast settings. To modify any of the settings, click **Edit**.

Step 10 In the **Deploy Multicast** window, click **Now** or **Later** to indicate when you want to start the multicast configuration. Click **Deploy** to complete the configuration.
