Provision Your Network

- Provisioning, on page 1
- Add a Device to a Site, on page 1
- Tag Devices, on page 2
- Tag Devices Using Rules, on page 2
- Edit Device Tags, on page 3
- Provisioning Devices, on page 4
- Check the LAN Automation Status, on page 14
- Delete a Device After Provisioning, on page 15
- Fabric Sites and Fabric Domains, on page 15
- Multi-Site Fabric Domain, on page 16
- Transit Sites, on page 16
- Configuring Fabric Domains, on page 17

Provisioning

After you have configured the policies for your network in Cisco DNA Center, you can provision your devices. In this stage, you deploy the policies across your devices.

There are three aspects to provisioning devices:

- Assign devices to the inventory and deploy the required settings and policies.
- Add devices to sites.
- Create fabric domains and add devices to the fabric.

Add a Device to a Site

Procedure

**Step 1**
From the Cisco DNA Center home page, click **Provision**.
The Inventory page displays the device information gathered during the Discovery process.

**Step 2**
Check the check box next to the device or devices that you want to associate to a site.
Tag Devices

A device tag allows you to group devices based on an attribute or a rule. A single device can have multiple tags; similarly, a single tag can be applied to multiple devices.

You can add tags to or remove tags from devices in the Provision window.

Procedure

Step 1 From the Cisco DNA Center home page, click Provision. The Device Inventory page displays device information gathered during the discovery process.

Step 2 Check the check box next to the device(s) for which you want to apply a tag, then click Tag Device.

Step 3 Enter a tag name in the Tag Name field.

- If you are creating a new tag, click Create New Tag. You can also create a new tag with a rule. See Tag Devices Using Rules, on page 2 for more information.

- If you are using an existing tag, select the tag from the list, then click Apply.

A tag icon and the tag name(s) appear under the device name(s) for which you applied the tag(s).

Step 4 To remove a tag from a device, do one of the following:

- Click Create New Tag, unselect all tags, then click Apply.

- Hover your cursor over the tag icon or tag name, then click X to disassociate the tag from the device.

Tag Devices Using Rules

You can group devices based on tags in which you define a rule. When you define a rule, Cisco DNA Center automatically applies the tag to all devices that match the specified rule. Rules can be based on device name, device family, device series, IP address, location, or version.

Procedure

Step 1 From the Cisco DNA Center home page, click Provision. The Device Inventory page displays device information gathered during the discovery process.

Step 2 Check the check box next to the device(s) for which you want to apply a tag, then click Tag Device.
Step 3 Enter a tag name in the Tag Name field, then click Create New Tag with Rule.

The Create New Tag window appears.

The Manually Added field under Total Devices Tagged Count indicates the number of devices you selected in Step 2.

Step 4 Click Add Condition, then complete the required fields for the rule.

The Matching Devices number automatically changes to indicate how many devices match this condition.

You can have two options to create additional conditions:

- And conditions—Click the Add Condition link. And appears above the condition.

- Or conditions—Click the add icon (+) next to an existing condition. Or appears next to the condition.

You can add as many conditions as needed. As you make changes to the rule, the Matching Devices count changes to reflect how many devices in the inventory match the rule you specified. You can click on the device number to view the devices that match the rule.

Step 5 Click Save to save your tag with the defined rule.

A tag icon and the tag name(s) appear under the device name(s) for which you applied the tag(s).

As devices are added to the inventory, if they match the rules you defined, the tag is automatically applied to the devices.

---

**Edit Device Tags**

You can edit device tags that you previously created.

**Procedure**

Step 1 From the Cisco DNA Center home page, click Provision. The Device Inventory page displays device information gathered during the discovery process.

In the Device Name column, you can see any previously created device tags listed under the device names.

Step 2 Without selecting any devices, click Tag Device.

The previously created tags are listed.

Step 3 Hover your cursor over the tag you want to edit, then click the pencil icon next to the tag name.

Alternatively, you can select Tag Device > View All Tags, then click the pencil icon next to the tag you want to edit.

Step 4 Make changes to the tag, then click Save to save your changes.
Provisioning Devices

Provision a Cisco Wireless Controller

Before you begin

• Make sure that you have defined the following global network settings before provisioning a Cisco Wireless Controller:
  • Network servers, such as AAA, DHCP, and DNS. For more information, see Configure Global Network Servers.
  • Device credentials, such as CLI, SNMP, HTTP, and HTTPS. For more information, see Configure Global CLI Credentials, Configure Global SNMPv2c Credentials, Configure Global SNMPv3 Credentials, and Configure Global HTTPS Credentials.
  • IP address pools. For more information, see Configure IP Address Pools.
  • Wireless settings, such as SSIDs, wireless interfaces, and wireless radio frequency profiles. For more information, see Configure Global Wireless Settings.

• Make sure that you have a wireless controller in your inventory. If not, discover the device using the Discovery feature. For more information, see Discover Your Network.

• Make sure that the wireless controller is added to a site. For more information, see Add a Device to a Site, on page 1.

Procedure

Step 1  From the Cisco DNA Center home page, choose Provision > Devices.
       The Device Inventory window appears.

Step 2  Click the Device Inventory tab.
       All discovered wireless controllers are listed.

Step 3  Check the check box next to the controller device name that you want to provision.

Step 4  From the Action drop-down list, choose Provision.

Step 5  In the Assign Site window, assign a site for the controller.

Step 6  In the Find Site field, enter the name of the site to which you want to associate the controller. To assign multiple controllers to the same site, check the All Same Site check box.

Step 7  Click Next.
       The Configuration window appears.

Step 8  Choose a role for the wireless controller: Active Main WLC or Guest Anchor.

Step 9  In the Managed AP Locations field, enter the AP locations managed by the controller. Here you have the option to change, remove, or reassign the site.
Inheritance of managed AP locations lets you automatically choose a site along with the buildings and floors under that particular site. One site can be managed by only one wireless controller.

**Step 10** If you have selected the **WLC Role** as **Active Main WLC**, under **Interface and VLAN Configuration**, click on **Add** and configure the interface and the VLAN.

The **Configure Interface and VLAN** window appears.

**Step 11** From the **Interface Name** drop-down list, choose the interface name.

**Step 12** In the **VLAN ID** text box, enter a value for the VLAN ID.

**Step 13** In the **Interface IP Address** text box, enter the interface IP address.

**Step 14** In the **Interface Net Mask (in bits)** text box, enter the interface net mask details.

**Step 15** In the **Gateway IP Address** text box, enter the gateway IP address.

**Step 16** In the **LAG/Port Number**, enter the LAG or the port number.

**Step 17** Click **OK**.

**Step 18** For a guest anchor wireless controller, you can change the VLAN ID configuration by changing the **VLAN ID** under **Assign Guest SSIDs to DMZ site**.

**Step 19** Click **Next**.

**Step 20** The **Summary** window displays the following information:

- System Details
- Global Setting
- SSID
- Managed Sites
- Interfaces

**Step 21** Click **Deploy** to provision the controller.

The **Status** column in the **Device Inventory** window shows **SUCCESS** after a successful deployment.

**Note** After provisioning, if you want to make any changes, click **Design**, change the site profile, and provision the controller again.

---

**Onboard APs with Zero Touch Provisioning—Day 0 Provisioning**

Follow this workflow for zero-touch provisioning of APs.

**Before you begin**

- Design the network hierarchy, with sites, buildings, floors, and so on. For more information, see Create a Site in a Network Hierarchy, Add Buildings, and Add a Floor to a Building.

- Create a network profile. For more information, see Create a Wireless Sensor Device Profile.

- Provision a Cisco Wireless Controller. For more information, see Provision a Cisco Wireless Controller, on page 4.
• Configure the DHCP server with Option #43 or Option #60. These are the IP addresses of the Cisco DNA Center Plug and Play (PnP) server. This helps the AP to contact the Plug and Play server to download configurations. For more information, see About Global Network Settings.

• The APs should be in the factory reset state without any wireless controller configurations.

**Procedure**

**Step 1**  
The AP that is connected to a switch contacts the DHCP server and then connects to a Plug and Play server.

**Step 2**  
The DHCP server allocates IP address with Option #43, which is the IP address of the Cisco DNA Center Plug and Play server.

**Step 3**  
The AP starts the Plug and Play agent and contacts the Plug and Play server.

**Step 4**  
From the **Provision > Unclaimed Devices** tab, find the AP. The **Device Status** shows as **Unclaimed**.

**Step 5**  
Claim the device.

**Step 6**  
Check the check box next to the AP device name, and click **Claim Device**.

**Step 7**  
Enter a **Device Name**.

**Step 8**  
From the **Choose a site** drop-down list, choose a site for the AP.

**Step 9**  
By default, the customer RF profile that you marked as default under **Network Settings > Wireless > Wireless Radio Frequency Profile** is selected in the **Choose a RF Profile** drop-down list. You can change the default RF Profile value for an AP by selecting a value from the **Choose a RF Profile** drop-down list. The options are High, Typical, and Low. The AP group is created based on the RF profile selected.

**Step 10**  
Click **Apply**.

**Step 11**  
The AP gets the Plug and Play configurations with wireless controller details and joins the wireless controller successfully.

**Step 12**  
At this stage, the **Onboarding Status** on the **Provision > Unclaimed** of the AP is **ExecutedWorkflow** and the **Device Status** under **Provision > Unclaimed Device** page is **Onboarding**.

**Step 13**  
After the AP is provisioned, the **Provision Status** on the **Device Inventory > Inventory** page changes to **Success**.

**Step 14**  
The **Onboarding Status** on **Provision > Unclaimed** changes to **Executed Workflow**.

---

**Provision a Cisco AP—Day 1 AP Provisioning**

**Before you begin**

Make sure that you have the Cisco AP in your inventory. If not, discover APs using the Discovery feature. See **Discover Your Network**.

**Procedure**

**Step 1**  
From the Cisco DNA Center home page, choose **Provision > Devices**.
The Device Inventory window appears.

**Step 2**
Click the Device Inventory tab.

All discovered controllers are displayed.

**Step 3**
Check the check box next to the AP device name that you want to provision.

**Step 4**
From the Action drop-down list, choose Provision.

The Assign Site window appears.

**Step 5**
Assign an AP to the site.

**Step 6**
In the Find Site field, enter the name of the site to which you want to associate the AP. To assign multiple APs to the same site, check the All Same Site check box.

**Step 7**
Click Next.

The Configuration window appears.

**Step 8**
By default, the customer RF profile that you marked as default under Network Settings > Wireless > Wireless Radio Frequency Profile is chosen in the RF Profile drop-down list. You can change the default RF Profile value for an AP by selecting a value from the RF Profile drop-down list. The options are High, Typical, and Low. The AP group is created based on the RF profile selected.

**Step 9**
Click Deploy to provision the AP.

You are prompted with a message stating that creation or modification of an AP group in progress.

**Note**  
After completion, the devices are rebooted.

**Step 10**
Click OK.

The Status column in the Device Inventory window shows SUCCESS after a successful deployment.

---

**Provision a Brownfield Device**

**Before you begin**

With Cisco DNA Center, you can add and provision brownfield devices such as wireless controllers to the network. Brownfield refers to devices that belong to existing sites with pre-existing infrastructure.

- Start by running a Discovery job on the device. All your devices are displayed on the Inventory window. For more information, see Discover Your Network and About Inventory.

- The wireless controller should be reachable and in Managed state on the Inventory window. For more information, see About Inventory.

**Procedure**

**Step 1**
From the Cisco DNA Center home page, choose Provision > Devices.

The Device Inventory window appears.

**Step 2**
Click the Inventory tab.
All discovered wireless controllers are listed.

**Step 3**  
Click **Filter** and enter the appropriate values in the selected filter field. For example, for the **Device Name** filter, enter the name of the device.

The data that is displayed in the **Devices** table is automatically updated according to your filter selection.

**Step 4**  
Check the check box adjacent to the controller device name that you want to provision.

**Step 5**  
From the **Action** drop-down list, choose **Learn Device Config**.

The **Assign Site** window appears.

**Step 6**  
Assign a site for the controller.

**Step 7**  
From the **Choose a site** drop-down list, choose the site to which you want to associate the controller.

**Step 8**  
Click **Next**.

The **Learnt Configurations** window lists all the learned configurations.

**Step 9**  
Click **Network** in the left pane.

The right pane displays configurations that were learned as part of device configuration learning, and shows the following information:

- **AAA Server** details.
- **Systems Settings**, with details about the IP address and protocol of the AAA server.

**Step 10**  
Enter the **Shared Secret** for the AAA server.

**Step 11**  
Click **Wireless** in the left pane.

The right pane lists all the enterprise and guest SSIDs that are present on the device.

**Step 12**  
For an SSID with a preshared key (PSK), enter the **passphrase key**.

**Step 13**  
Click **Discarded Config** in the left pane.

The right pane lists the conflicting or the existing configurations on Cisco DNA Center. The discarded configuration entries are categorized as:

- Duplicate design entity
- Unknown device configuration for Radio Policy

**Step 14**  
Click **Next**.

The **Network Profile** window lists the network profile or site profile that is created based on the AP and WLAN combination.

**Step 15**  
Click **Save**.

A message saying "Brownfield Configuration is Successful" is displayed.

**Step 16**  
Choose **Design > Network Profiles** to assign a site to the network profile.

**Step 17**  
In the **Network Profiles** window, click **Assign Site** to add sites to the selected profile.

**Step 18**  
In the **Add Sites to Profile** window, choose a site from the drop-down list, and click **Save**.

**Step 19**  
Click the **Provision** tab.

**Step 20**  
Click **Filter** and enter the appropriate values in the selected filter field.
The data that is displayed in the Devices table is automatically updated according to your filter selection.

Step 21 Check the check box adjacent to the controller device name that you want to provision.

Step 22 From the Action drop-down list, choose Provision.

Step 23 Review the details in the Assign Site window, and click Next.

The Configurations window appears.

Step 24 Under Interface and VLAN Configuration, click +Add to configure interface and VLAN details.

Step 25 In the Configure Interface and VLAN window, configure the required fields, and click OK.

Step 26 Click Next.

Step 27 The Summary window displays the following information:

- Device Details
- Network Settings
- SSID
- Managed Sites
- Interfaces

Step 28 Click Deploy to provision the device. The Provision Status column in the Device Inventory window shows SUCCESS after a successful deployment.

---

Guest Anchor Configuration and Provisioning

Follow these steps to configure a guest anchor wireless controller.

Procedure

Step 1 Design a network hierarchy, with sites, buildings, floors, and so on. For more information, see Create a Site in a Network Hierarchy, Add Buildings, and Add a Floor to a Building.

Step 2 Configure network servers, such as AAA, DHCP, and DNS servers. For more information, see Configure Global Network Servers and Add Cisco ISE or Other AAA Servers.

Step 3 Create SSIDs for a guest wireless network with external web authentication and central web authentication with Cisco ISE. For more information, see Create SSIDs for a Guest Wireless Network.

Step 4 Discover the wireless controller using the Cisco Discovery Protocol (CDP) or an IP address range and ensure that the devices are in the Inventory window and in the Managed state. For more information, see About Discovery.

Step 5 Provision a foreign wireless controller as the active main wireless controller. See Provision a Cisco Wireless Controller, on page 4.

Step 6 Choose the role for the wireless controller as guest anchor and provision the guest anchor controllers. For more information, see Provision a Cisco Wireless Controller, on page 4.
Step 7: Configure device credentials, such as CLI, SNMP, HTTP, and HTTPS. See Configure Global CLI Credentials, Configure Global SNMPv2c Credentials, Configure Global SNMPv3 Credentials, and Configure Global HTTPS Credentials.

Provision a Sensor Device

Provisioning a sensor device applies to Cisco Aironet 1800s Active Sensors.

Before you begin

Provisioning a sensor device is applicable only for Cisco Aironet 1800s Active Sensors.

- Make sure that the sensor device in your inventory is in an UNCLAIMED state.
- Make sure that you have created a profile for the sensor device. See Create a Wireless Sensor Device Profile.
- Make sure that Cisco Aironet 1800s Active Sensor is reachable through the Cisco DNA Center's enterprise IP address (private/enp9s0). A DHCP option 43 string makes the device reachable in unclaimed mode in Cisco DNA Center. To claim the device, the device must have reachability to interface enp9s0's IP address.
- In the DHCP server, make sure that you configure the NTP server (DHCP option 42) and the vendor-specific DHCP option 43 with the ASCII value "5A1D;B2;K4;I172.16.x.x;J80", where 172.16.x.x is the virtual IP address of Cisco DNA Center associated with the enp9s0 interface.

Procedure

Step 1: From the Cisco DNA Center home page, choose Provision > Devices.
The Device Inventory window appears.

Step 2: Click the Unclaimed Devices tab.
All unclaimed devices are displayed.

Step 3: Check the check box next to the sensor device that you want to provision.
Three tabs appear above the list of unclaimed devices.

Step 4: Click the Claim Device tab.
The Claim Device window appears, providing the serial number and device information.

Step 5: From the Choose a floor drop-down list, choose the floor where the sensor device is located.

Step 6: From the Sensor Select SSID Profile drop-down list, choose the profile name to associate to the sensor device.

Step 7: Click Assign.
Provisioning starts, and the sensor device appears in the device inventory.
If the provisioning succeeds, the Provision Status column in the Device Inventory window shows Success.
Provision LAN Underlay

Use LAN automation to provision a LAN underlay.

Before you begin

• Configure your network hierarchy. (See Add a Device to a Site, on page 1.)
• Make sure you have defined the following global network settings:
  • Network servers, such as AAA, DHCP, and DNS servers. (See Configure Global Network Servers.)
  • Device credentials such as CLI, SNMP, HTTP, and HTTPS credentials. (See Configure Global CLI Credentials, Configure Global SNMPv2c Credentials, Configure Global SNMPv3 Credentials, and Configure Global HTTPS Credentials.)
  • IP address pools. (See Configure IP Address Pools.)
• Make sure that you have at least one device in your inventory. If not, discover devices using the Discovery function.

Procedure

Step 1 Reserve an IP address pool for the site that you will be provisioning.

Note The size of the LAN automation IP address pool must be at least 25 bits of netmask in size or larger.

a) From the Cisco DNA Center home page, choose Design > Network Settings > IP Address Pools.
b) From the Network Hierarchy pane, select a site.
c) Click Reserve IP Pool and complete the following fields to reserve all or part of an available global IP address pool for the specific site:
  • IP Pool Name—Unique name for the reserved IP address pool.
  • Type—Type of IP address pool. For LAN automation, choose LAN.
  • Global IP Pool—IP address pool from which you want to reserve all or part of the IP addresses.
  • CIDR Notation/No. of IP Addresses—IP subnet and mask address used to reserve all or part of the global IP address pool or the number of IP addresses you want to reserve.
  • Gateway IP Address—Gateway IP address.
  • DHCP Servers—DHCP server(s) IP address(es).

d) Click Reserve.

Step 2 Discover and provision devices.

a) From the Cisco DNA Center home page, choose Provision > Devices > Inventory.
   All the discovered devices are displayed.
b) Click the Topology View icon.
c) Right-click one of the discovered devices and choose Discover and Provision New Devices.
d) From the **LAN Automation** dialog box, complete the following fields:

- **Site**—Site ID and associated settings that Cisco DNA Center uses for LAN automation.
  
  You can make different site selections for seed and discovered devices. LAN automation provides flexibility in site selection for seeds and discovered devices, which can belong to different sites.

- **Primary Device**—IP address of the device that Cisco DNA Center uses as the starting point to discover and provision new devices.

- **Peer Device**—IP address of the peer device.

- **Choose Primary Device Ports**—Ports to be used to discover and provision new devices.

- **IP Pool**—IP address pool that was reserved for LAN automation. (See Step 1.)

- **ISIS Password**—A user-provided IS-IS password for when LAN automation starts. If the password already exists on the seed device, it is reused and is not overwritten. If no user-provided password is entered and there is no existing IS-IS password on the device, the static IS-IS password 'cisco' is configured.

- **Enable Multicast**—LAN automation creates a multicast tree from seed devices as RPs and discovered devices as subscribers.

- **Device Name Prefix**—Text that describes the devices being provisioned. As Cisco DNA Center provisions each device, it names the device with the text that you provide and adds a unique number to the end. For example, if you enter Access as the name prefix, as each device is provisioned, it is named Access-1, Access-2, Access-3, and so on.

- **Hostname Map File**—Configures user-provided names for discovery devices using a CSV file that contains a mapping between serial numbers and hostnames. If the discovery device is a stack, all serial numbers of the stack are provided in the CSV file.


e) Click **Start**.

Cisco DNA Center begins to discover and provision the new devices.

**Step 3** Monitor and review the progress of devices being provisioned.

a) From the **Provision > Devices > Inventory** tab, click **Status**.

The **LAN Automation Status** dialog box displays the progress of the devices being provisioned.

**Note** The process can take several minutes for all of the new devices to be provisioned.

b) After all devices have been discovered, added to Inventory, and are in Managed state, click **Stop** in the **LAN Automation Status** dialog box.

The LAN automation process is complete, and the new devices are added to the Device Inventory.

**What to do next**

To review the LAN automation configurations, from the Cisco DNA Center home page, choose **Network Plug and Play > Configurations**.
Peer Device in LAN Automation Use Case

Provision a Dual-Homed Switch

You must always select a peer device to provision the dual-homed switch.

Cisco DNA Center configures the DHCP server on the primary device. Because Cisco DNA Center understands that the discovered device is connected to both the primary and peer devices, it configures two Layer 3 point-to-point connections when the LAN automation task is stopped. One connection is established between the discovered device and the primary device; the other connection is established between the discovered device and the peer device.

Note

If the link between the primary and the peer device is not configured before the LAN automation job is executed, you must select the interface of the primary device that connects to the peer device as part of the LAN automation configuration in Cisco DNA Center.
LAN Automation’s Two-Hop Limitation

For the preceding topology, Cisco DNA Center configures the following links:

- A point-to-point Layer 3 routed connection from Discovered device 1 to Primary device
- A point-to-point Layer 3 routed connection from Discovered device 1 to Peer device
- A point-to-point Layer 3 routed connection from Discovered device 1 to Discovered device 2

Consider the scenario where a device—named Discovered device 3—is directly connected below Discovered device 2. The connection between Discovered device 2 and Discovered device 3 is not configured as part of the LAN automation job, because it is more than two hops away from Primary device.

Check the LAN Automation Status

You can view the status of in-progress LAN automation jobs.

Before you begin

You must have created and started a LAN automation job.

Procedure

Step 1 From the Cisco DNA Center home page, choose Provision > Devices.
Step 2 Click the Inventory tab.
   All discovered devices are displayed.
Step 3 Click LAN Auto Status.
The status of any running or completed LAN automation jobs is displayed.

## Delete a Device After Provisioning

- If you are deleting a device that is already been added to the fabric domain, remove it from the fabric domain and then delete it from the **Provision** menu.
- You cannot delete a provisioned device from the **Inventory** window. Instead, you must delete provisioned devices from the **Provision** menu.

### Procedure

**Step 1**
From the Cisco DNA Center home page, choose **Provision > Devices**.

The **Device Inventory** window appears.

**Step 2**
Click the **Inventory** tab, which lists all discovered and provisioned devices.

**Step 3**
Check the check box next to the device that you want to delete.

**Note**
APs are deleted only when the controller to which they are connected is deleted.

**Step 4**
From the **Action** drop-down list, choose **Delete Device**.

**Step 5**
At the confirmation prompt, click **OK**.

## Fabric Sites and Fabric Domains

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

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

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

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

There are two types of transit sites:

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

Multi-Site Fabric Domain

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

The transit site consists of control plane nodes that help interconnect multiple fabric sites.

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

Transit Sites

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

• IP transit: Used in a regular IP network to connect to an external network or to connect two or more fabric sites.

• SDA transit: Used in LISP/VxLAN encapsulation to connect two fabric sites. The SDA transit area may be defined as a portion of the fabric that has its own Control Plane Nodes, Border Nodes, but does not have Edge Nodes.

Using SDA transit, an end-to-end policy plane is maintained using SGT group tags.

Create an IP Transit Network

To add a new IP transit network:

Procedure

Step 1 From the Cisco DNA Center home page, click Provision.
Step 2 Click the Fabric tab.
Step 3 Click the Add Fabric Domain or Transit tab.
Step 4 Choose Add Transit from the pop-up.
Step 5 Enter a transit name for the network.
Step 6 Choose IP-Based as the transit type.
The routing protocol is set to BGP by default.
Step 7 Enter the autonomous system number (ASN) for the transit network.
Step 8  Click Save.

Create an SDA Transit Network

To add a new SDA transit network:

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>From the Cisco DNA Center home page, click <strong>Provision</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click the <strong>Fabric</strong> tab.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click the <strong>Add Fabric Domain or Transit</strong> tab.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Choose <strong>Add Transit</strong> from the pop-up.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Enter a transit name for the network.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Choose <strong>SD-Access</strong> as the transit type.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Enter the <strong>Site for the Transit Control Plane</strong> for the transit network. Choose at least one transit map server.</td>
</tr>
<tr>
<td>Step 8</td>
<td>Enter the <strong>Transit Control Plane</strong> for the transit network.</td>
</tr>
<tr>
<td>Step 9</td>
<td>Repeat Step 7 and Step 8 for all map servers that you want to add.</td>
</tr>
<tr>
<td>Step 10</td>
<td>Click <strong>Save</strong>.</td>
</tr>
</tbody>
</table>

What to do next

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

Configuring Fabric Domains

Fabric Overview

A fabric domain is a logical group of devices that is managed as a single entity in one or multiple locations. Having a fabric 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 lets you add devices to a fabric network. These devices can be configured to act as control plane or border devices within the fabric network.
Before You Begin

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

Create a Fabric Domain

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

Procedure

- **Step 1**: From the Cisco DNA Center home page, click **Provision**.
- **Step 2**: Click the **Fabric** tab.
- **Step 3**: Click the **Add Fabric Domain or Transit** tab.
- **Step 4**: Choose **Add Fabric** from the pop-up.
- **Step 5**: Enter a fabric name.
- **Step 6**: Choose one fabric site.
- **Step 7**: Click **Add**.

Configure a Fabric Domain

You can add devices and associate virtual networks to a fabric domain, and add multicast address pools.

Add Devices to a Fabric

After you have created a fabric domain, you can add fabric sites, and then add devices to the fabric site. You can also specify whether the devices should act as a control plane node, a border node, or both.

Note

It is optional to designate the devices in a fabric domain as control plane nodes or border nodes. You may have devices that do not play these roles. However, every fabric domain must have at least one control plane node device and one border node device. In the current release for wired fabric, you can add up to six control plane nodes for redundancy.

There are three steps to add and configure devices to a fabric domain:

1. Select the devices.
2. Specify devices to act as control plane nodes.
3. Specify devices to act as border nodes.

To add a device to the fabric:
**Before you begin**

You must provision the device. To provision a device, click the **Provision** tab and choose **Devices**. Before you add a device to the fabric, you must perform the pre-verification check by clicking the **Pre-Verification** tab. The pre-verification check can be done only for devices that have been assigned roles. The pre-verification procedure performs a check on the **Hardware Version** and **Software Version** of the device. The result shows whether the device passed the test, failed the test, or is not supported.

**Procedure**

**Step 1**
From the Cisco DNA Center home page, click **Provision**. The screen displays all provisioned fabric domains.

**Step 2**
From the list of fabric domains, choose a fabric. The screen displays all devices in the network that have been inventoried. You can view devices in the topology view or list view. In the topology view, any device that is added to the fabric is shown in blue.

**Step 3**
Click a device and choose one of the options displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add as CP+Border+Edge</td>
<td>Add the selected device as a control plane and a border node and an edge node.</td>
</tr>
<tr>
<td>Add to Fabric</td>
<td>Add a distribution or access device to the fabric domain.</td>
</tr>
<tr>
<td>Add as CP</td>
<td>Add a core or distribution device as a control plane node. This allows the fabric access device to communicate with the control plane device.</td>
</tr>
<tr>
<td>Add as Border</td>
<td>Add a core device as a border node. This allows the fabric access device to communicate with the fabric border device.</td>
</tr>
<tr>
<td>Add as CP+Border</td>
<td>Add the selected device as a control plane and a border node.</td>
</tr>
<tr>
<td>Run Pre-Provisioning Check</td>
<td>Run a pre-provisioning check.</td>
</tr>
<tr>
<td>Enable Guests</td>
<td>In the pop-up window, enter the following options:</td>
</tr>
<tr>
<td></td>
<td>• Set as control plane: Check this check box if you want the device to act as a control plane.</td>
</tr>
<tr>
<td></td>
<td>• Set as a border node: Check this check box if you want the device to act as a border node.</td>
</tr>
<tr>
<td></td>
<td>• Select a guest virtual network: All guest virtual networks created are listed. Check the check box of the guest virtual network and click <strong>Enable</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Ensure that you have created a guest virtual network in the <strong>Policy</strong> application. See <strong>Create a Virtual Network</strong>.</td>
</tr>
<tr>
<td>View Device Info</td>
<td>Displays the details of the selected device.</td>
</tr>
</tbody>
</table>

**Step 4**
Click **Save**.
Add Device as a Border Node

When you are adding a device to a fabric, you can add it in various combinations to act as a control plane, border node, and edge node as explained in Add Devices to a Fabric, on page 18.

To add a device as a border node:

Procedure

**Step 1**  From the Cisco DNA Center home page, click **Provision**. A list of all provisioned fabric domains is shown.

**Step 2**  From the list of fabric domains, choose a fabric. The window displays all devices in the network that have been inventoried. You can view the devices in the topology view or list view. In the topology view, any device that is added to the fabric is shown in blue.

**Step 3**  Click a device and choose one of the options:

- **Add as CP+Border+Edge**: Add the selected device as a control plane and a border node and an edge node.
- **Add as Border**: Add a core device as a border node. This allows the fabric access device to communicate with the fabric border device.
- **Add as CP+Border**: Add the selected device as a control plane and a border node.

**Step 4**  A pop-up window appears with the name of the device that you want to add.

a) From the **Border to** field, click one of the radio buttons:

- **Rest of Company (Internal)**: Designate the device as a border for IP routes inside your company. A border exports fabric routes and imports outside routes.
- **Outside World (External)**: Designate the device as a default border for IP routes outside your company. A border exports fabric routes only.
- **Anywhere (Internal & External)**: Designate the device as a border for both internal and external IP routes. A border exports fabric routes and imports outside routes, except default-route.

b) Enter the **Local Autonomous Number** for the device.

c) From the **Select IP Address Pools** drop-down list, choose an IP address pool.

d) Check the **connected to the internet** check box to choose this border node to advertise internet services to other fabric borders.

e) Choose a transit network to enable on the border device:

- To enable SDA transit on the border, choose a user-created SDA transit domain from the **Select Transit** drop-down list. Click **Add**.

- To enable IP transit on the border, choose a user-created IP transit domain from the **Select Transit** drop-down list. Click **Add**.

Choose an IP pool from Design Hierarchy. The selected pool will be used to automate IP routing between the border node and IP peer. Click **Add Interface** to enter interface details on the next screen.
Choose **External Interface** from the drop-down list. Enter the **Remote AS Number**. Check the **Virtual Network** from the list. This virtual network should be advertised by the border to the remote peer. You can select one, multiple, or all virtual networks. Click **Save**.

**Step 5**
Click **Layer 2**. You will see a table of the virtual networks and the number of pools in each virtual network. Click one of the virtual networks.

If a check box in the virtual network list is not clickable, it indicates that the segments under the virtual network have been handed off to an external VLAN.

After you select a virtual network, the list of IP address pools present in the virtual network appears. A list of interfaces through which you can connect non-fabric devices is displayed.

Enter the **External VLAN** into which the fabric must be extended. A virtual network can only be handed off on a single interface. The same virtual network cannot be handed off via multiple interfaces.

Click **Save**.

**Step 6**
Click **Add**.

---

**Configure Host Onboarding**

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

In this tab, you can:

- Select an authentication template that will apply to the fabric. These templates are predefined configurations that are retrieved from the ISE. After selecting the authentication template, click **Save**.

- Associate IP address pools to virtual networks (default, guest, or user defined), and click **Update**. The IP address pools displayed are site-specific pools only.

- Specify wireless SSIDs within the network that hosts can access. You can select the guest or enterprise SSIDs and assign address pools, and click **Save**.

- Apply specific configurations for each port for each access device within the fabric domain.

- On an edge device, designate a port as a server port during port assignment. Select the port to assign and click **Assign**.

**Select Authentication Template**

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

**Procedure**

**Step 1**
From the **Auth Template** section, choose an authentication template:

- **Closed Authentication**: Any traffic prior to authentication is dropped, including DHCP, DNS, and ARP.
- **Easy Connect**: Security is added by applying an ACL to the switch port, to allow very limited network access prior to authentication. After a host has been successfully authenticated, additional network access is granted.
• No Authentication
• Open Authentication: A host is allowed network access without having to go through 802.1X authentication.

**Step 2** Click Save.

---

### Associate Virtual Networks to the Fabric Domain

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

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

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

**Procedure**

**Step 1** From the Virtual Networks section, click a virtual network.

**Step 2** Configure the virtual network.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Pool Name</td>
<td>From the list of IP address pools, choose the ones that should be part of the virtual network.</td>
</tr>
<tr>
<td>Traffic Type</td>
<td>Choose to send voice or data traffic through the virtual network.</td>
</tr>
<tr>
<td>Wireless Mgmt Pool</td>
<td>Choose whether the virtual network should be part of the wireless management pool of the fabric domain.</td>
</tr>
<tr>
<td>AP Provisioning Pool</td>
<td>Choose whether the virtual network should be part of the access point provisioning pool.</td>
</tr>
<tr>
<td>Layer-2 Extension</td>
<td>Enables Layer-2 MAC Address registration for the IP Pool and Layer-2 VNI.</td>
</tr>
<tr>
<td>Layer-2 Flooding</td>
<td>Layer 2 Flooding is disabled by default.</td>
</tr>
<tr>
<td>Groups</td>
<td>Choose which group the IP Pool should belong to.</td>
</tr>
<tr>
<td>Critical Pool</td>
<td>Displays whether the IP address pool assigned to this virtual network belongs to the critical IP address pool.</td>
</tr>
<tr>
<td>Auth Policy</td>
<td>Displays the authentication policy for the virtual network.</td>
</tr>
</tbody>
</table>

**Step 3** Click **Update** to save the settings. The settings you specify here will be deployed to all devices on the network.

**Step 4** After all the virtual networks have been configured, click **Save**.

---

### Configure Wireless SSIDs for the Fabric Domain

The Wireless SSID section allows you to specify wireless SSIDs within the network that the hosts can access.
Configure Ports Within the Fabric Domain

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

**Note**

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

**Procedure**

**Step 1**
From the Select Fabric Device section, choose the access device that you want to configure. The ports available on the device are displayed.

**Step 2**
Choose the ports on the device and specify the allowed IP address pool, the groups that have been provisioned, the voice or data pool, and the authentication type for the port.

**Step 3**
Click Save.

Multicast Overview

Multicast traffic is forwarded in different ways:

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

See IP Multicast Technology Overview.

Configure Multicast Settings

After devices are added to the fabric domain, you can create multicast IP address pools and rendezvous points (RPs). Applicable multicast configurations will be automated on all fabric devices operating in that fabric domain.

An RP is a router in a multicast network domain that acts as a shared root for a multicast shared tree.

Create a Multicast IP Address Pool

**Before you begin**

A multicast IP address pool is used for internal PIM communication within the fabric domain. There is an option to define multiple multicast pools, and each can be associated with a separate virtual network. There is a requirement that each virtual network must have a separate multicast IP address pool created and associated with it.
**Add a Device as a Rendezvous Point**

**Procedure**

**Step 1**
From the Cisco DNA Center home page, click the **Provision** tab. By default, the Devices window is shown.

**Step 2**
Click the Fabric tab. A list of fabric domains is shown.

**Step 3**
Choose a fabric. The Fabric - Devices window appears, showing all the devices in the network. Any device that is added to the fabric is highlighted in blue.

**Step 4**
Click the fabric device that you want to add as a rendezvous point, and choose **Enable Rendezvous Point**.

**Step 5**
Cisco DNA Center displays a list of virtual networks in the pop-up window. Expand Virtual Networks and choose an **IP multicast pool** by clicking the Plus button. Click Next.
Only a single IP address pool is currently supported for each virtual network for multicast. To enable multicast in multiple virtual networks, you must create multiple multicast IP address pools.

**Note**

Step 6: Associate the corresponding virtual network and click **Enable**.

Step 7: Click **Save** on the main screen. **Apply** the changes.

---

**Verify the Rendezvous Point**

**Procedure**

**Step 1**
From the Cisco DNA Center home page, click the **Provision** tab. By default, the **Devices** window is shown.

**Step 2**
Click the **Fabric** tab. A list of fabric domains is shown.

**Step 3**
Choose a fabric. The **Fabric - Devices** window appears, showing all devices in the network. Virtual networks that are enabled for IP multicast are marked with an **M**.
Add a Device as a Redundant Rendezvous Point

**Note**

Dual RP is supported only for EXTERNAL or INTERNAL BORDERNODE.

When a redundant RP is added to the network, the MSDP session is enabled. Each fabric device that hosts the RP creates two loopbacks per VRF: one for the RP, and one to establish an MSDP session.

**Procedure**

**Step 1**

From the Cisco DNA Center home page, click the **Provision** tab. By default, the **Devices** window is shown.

**Step 2**

Click the **Fabric** tab. A list of fabric domains is shown.

**Step 3**

Choose a fabric. The **Fabric - Devices** window appears, showing all devices in the network. Any device that is added to the fabric is highlighted in blue.

**Step 4**

Click the device that you want to add as a redundant RP and choose **Enable Rendezvous Point**.

Cisco DNA Center displays the list of virtual networks.

**Step 5**

Expand the **Virtual Networks** for which you want to add a redundant RP. A multicast IP address pool should be prepopulated. Click **Next**.

**Step 6**

Associate the virtual networks and click **Enable**.

**Step 7**

Click **Save** on the main screen. **Apply** the changes.