Provision Your Network

- Provisioning, on page 1
- Onboarding Devices with Plug and Play Provisioning, on page 1
- Add a Device to a Site, on page 16
- Tag Devices, on page 17
- Tag Devices Using Rules, on page 17
- Edit Device Tags, on page 18
- Provisioning Devices, on page 18
- Check the LAN Automation Status, on page 46
- Delete a Device After Provisioning, on page 47
- Fabric Sites and Fabric Domains, on page 47
- Multi-Site Fabric Domain, on page 48
- Transit Sites, on page 48
- Configuring Fabric Domains, on page 49

Provisioning

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

Provisioning devices includes the following aspects:

- Onboarding devices with Plug and Play, which adds them to the inventory.
- Deploying the required settings and policies to devices in inventory.
- Adding devices to sites.
- Creating fabric domains and adding devices to the fabric.

Onboarding Devices with Plug and Play Provisioning

Plug and Play provisioning provides a way to automatically and remotely provision and onboard new network devices with minimal network administrator and field personnel involvement.

Using Plug and Play provisioning, you can do the following:
Provision devices by assigning a site, deploying site settings, installing a device software image, and applying a custom onboarding configuration.

Plan devices before their installation by entering device information and choosing provisioning operations. When the device comes online, it contacts Cisco DNA Center and Plug and Play provisions and onboards the device automatically.

Provision unclaimed network devices, which are new devices that appear on the network, without prior planning.

Synchronize the device inventory from the Cisco Plug and Play Connect cloud portal in a Cisco Smart Account to Plug and Play, so that all the devices appear in Cisco DNA Center.

Display the detailed onboarding status of network devices.

**Prerequisites**

Before using Plug and Play provisioning, do the following:

- Set your Cisco credentials in the main Cisco DNA Center settings by using **System Settings > Settings > Cisco Credentials**. For more information, see "Configure Cisco Credentials" in the *Cisco Digital Network Architecture Center Administrator Guide*.

- Accept the End User License Agreement (EULA) in the main Cisco DNA Center settings by using **System Settings > Settings > Device EULA Acceptance**. For more information, see "Accept the License Agreement" in the *Cisco Digital Network Architecture Center Administrator Guide*.

The following sections describe typical use cases and workflows for Plug and Play provisioning.

**Planned Provisioning**

An administrator can plan the provisioning of a new site or other group of network devices as follows:

1. Define the site within the network hierarchy. See *About Network Hierarchy*.
2. Define network profiles for the types of devices you are deploying. See *Create Network Profiles*.
3. Optionally, ensure that software images for the devices to be provisioned are uploaded and marked as golden in the Image Repository. See *Import a Software Image*.
4. Optionally, define Onboarding Configuration templates to be applied to devices. Such templates contain basic network configuration commands to onboard a device so that it can be managed on the network. In most cases, such templates are not necessary, unless you need to customize the Day-0 configuration. See *Create Templates to Automate Device Configuration Changes*.
5. Add details about planned devices one at a time or in bulk with a CSV file. See *Add or Edit a Device*, on page 8 or *Add Devices in Bulk*, on page 9.
6. Devices boot up and are automatically provisioned.

**Unclaimed Provisioning**

If a new network device is added to the network before it can be planned, it is labeled as an unclaimed device. An unclaimed device can be added manually by an administrator, or automatically through one of the discovery methods described in *Controller Discovery Prerequisites*, on page 3. An administrator can provision the device, as follows:
1. Find the device on the devices list by filtering on unclaimed devices or searching for it by name. See View Devices, on page 6.

2. Claim the device by assigning a site, image, configuration template, or profile. See Provision a Device With Plug and Play, on page 12.

Cisco Smart Account Synchronization and Provisioning

Network devices can be automatically registered through a Cisco Smart Account with the Cisco Plug and Play Connect cloud service. An administrator can synchronize the device inventory from Cisco Plug and Play Connect to Cisco DNA Center Plug and Play, so that all the devices appear in Cisco DNA Center. These devices can then be claimed and provisioned.

1. Register a Smart Account and virtual account to synchronize with. See Register or Edit a Virtual Account Profile, on page 10.

2. Synchronize the device inventory from the Smart Account. See Add Devices from a Smart Account, on page 11.

3. Find the device on the devices list by filtering on unclaimed devices or searching for it by name. See View Devices, on page 6.

4. Claim the device by assigning a site, image, configuration template, or profile. See Provision a Device With Plug and Play, on page 12.

5. Devices boot up and are automatically provisioned.

Controller Discovery Prerequisites

Plug and Play automates device onboarding and requires that devices must be able to discover and contact the Cisco DNA Center controller. Devices must be able to automatically discover the controller in one of the following ways:

• DHCP—See DHCP Controller Discovery, on page 3.

• DNS—See DNS Controller Discovery, on page 4.

• Cisco Plug and Play Connect cloud service—See Plug and Play Connect Controller Discovery, on page 5.

DHCP Controller Discovery

When a Cisco network device first starts up with no startup configuration, it attempts to discover the Cisco DNA Center controller by using DHCP option 43.

The prerequisites for the DHCP discovery method are as follows:

• New devices can reach the DHCP server.

• The DHCP server is configured with option 43 for Cisco Plug and Play. This option informs the network device of the IP address of the Cisco DNA Center controller.

When the DHCP server receives a DHCP discover message from the device, with option 60 containing the string “ciscopnp”, it responds to the device by returning a response that contains the option 43
The Cisco Plug and Play IOS Agent in the device extracts the Cisco DNA Center controller IP address from the response and uses this address to communicate with the controller.

DHCP option 43 consists of a string value that is configured as follows on a Cisco router CLI that is acting as a DHCP server:

```
ip dhcp pool pnp_device_pool <-- Name of DHCP pool
network 192.168.1.0 255.255.255.0 <-- Range of IP addresses assigned to clients
default-router 192.168.1.1 <-- Gateway address
option 43 ascii "5A1N;B2;I172.19.45.222;J80" <-- Option 43 string
```

The option 43 string has the following components, delimited by semicolons:

- **5A1N;**—Specifies the DHCP suboption for Plug and Play, active operation, version 1, no debug information. It is not necessary to change this part of the string.
- **B2;**—IP address type:
  - B1 = hostname
  - B2 = IPv4 (default)
- **Ixxx.xxx.xxx.xxx;**—IP address or hostname of the Cisco DNA Center controller (following a capital letter i). In this example, the IP address is 172.19.45.222.
- **Jxxxx;**—Port number to use to connect to the Cisco DNA Center controller. In this example, the port number is 80. The default is port 80 for HTTP and port 443 for HTTPS.
- **K4;**—Transport protocol to be used between the device and the controller:
  - K4 = HTTP (default)
  - K5 = HTTPS
- **TrustpoolBundleURL;**—Optional parameter that specifies the external URL of the trustpool bundle if it is to be retrieved from a different location than the default, which is the Cisco DNA Center controller, which gets the bundle from the Cisco InfoSec cloud (http://www.cisco.com/security/pki/). For example, to download the bundle from a TFTP server at 10.30.30.10, you would specify the parameter like this: Tftp://10.30.30.10/ios.p7b
  
  If you are using trustpool security and you do not specify the T parameter, the device retrieves the trustpool bundle from the Cisco DNA Center controller.
- **Zxxx.xxx.xxx.xxx;**—IP address of the NTP server. This parameter is mandatory when using trustpool security to ensure that all devices are synchronized.

See the *Cisco IOS Command Reference* for additional details on DHCP configuration.

If DHCP option 43 is not configured, the device cannot contact the DHCP server, or this method fails for another reason, the network device attempts discovery using using DNS. For more information, see *DNS Controller Discovery*, on page 4.

**DNS Controller Discovery**

If DHCP discovery fails to get the IP address of the Cisco DNA Center controller, the network device falls back on the DNS lookup method. Based on the network domain name returned by the DHCP server, it
constructs a fully qualified domain name (FQDN) for the controller, using the preset hostname `pnpserver`. The NTP server name is based on the preset hostname `pnptpserver`.

For example, if the DHCP server returns the domain name “customer.com”, the network device constructs the controller FQDN of `pnpserver.customer.com`. It then uses the local name server to resolve the IP address for this FQDN. The NTP server name FQDN would be `pnptpserver.customer.com`.

The prerequisites for the DNS discovery method are as follows:

• New devices can reach the DHCP server.

• The Cisco DNA Center controller is deployed with the hostname “pnpserver”.

• The NTP server is deployed with the hostname `pnptpserver`.

### Plug and Play Connect Controller Discovery

In situations where using the DHCP or DNS discovery methods is not an option, the Cisco Plug and Play Connect cloud service allows devices to discover the IP address of the Cisco DNA Center controller. When the network device boots up, if it cannot locate the controller through DHCP or DNS, then it tries Plug and Play Connect by contacting `devicehelper.cisco.com` to obtain the IP address of the appropriate controller that is defined for your organization. To secure the communications, the first thing that the device does when contacting Plug and Play Connect is to download and install the Cisco trustpool bundle.

The following steps summarize how to use Cisco Plug and Play to deploy a Cisco network device by using Plug and Play Connect for discovery.

#### Before you begin

Cisco network devices are running Cisco IOS images that support Cisco Plug and Play and have connectivity to the Cisco Plug and Play Connect cloud service.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>The network administrator configures the controller profile for the appropriate Cisco DNA Center controller for your organization by using Plug and Play Connect in the Cisco Smart Account web portal. For more information, see the Smart Account documentation in the web portal.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>If you order plug and play network devices through Cisco Commerce Workspace (CCW), these network devices are automatically registered with Plug and Play Connect as long as a Cisco Smart Account is assigned to the order and you include the NETWORK-PNP-LIC option for each device that you want to use with Cisco Plug and Play. This option causes the device serial number and PID to be automatically registered in your Smart Account for plug and play. If you have specified a default controller, then the devices are automatically assigned to that controller when the order is processed.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Alternatively, you can manually add devices in the Plug and Play Connect web portal.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Register the Cisco DNA Center controller as a controller for Cisco Plug and Play Connect in a Cisco Smart Account, for redirection services. See Register or Edit a Virtual Account Profile, on page 10. This step is required if you order plug and play network devices through CCW and these network devices are automatically registered with Plug and Play Connect through your Smart Account.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Synchronize the device inventory from the Smart Account in the Cisco Plug and Play Connect cloud portal to Cisco DNA Center Plug and Play.</td>
</tr>
</tbody>
</table>
Devices registered in the Plug and Play Connect web portal are synced to the controller and appear in the plug and play device list with a source of SmartAccount.

**Step 6** Claim the newly synced devices. See Provision a Device With Plug and Play, on page 12.

**Step 7** The device installer installs and powers up the Cisco network device.

**Step 8** The device discovers the Cisco DNA Center controller by querying the Plug and Play Connect service, identifies itself by serial number to Plug and Play in Cisco DNA Center, then is provisioned according to what was planned for it during the claim process.

---

**Note**
The device will fail to contact Plug and Play Connect if the device cannot synchronize with the predefined NTP servers `time-pnp.cisco.com` or `pool.ntp.org`. To resolve this problem, either unblock NTP traffic to these two host names, or map these two NTP host names to local NTP server addresses on the DNS server.

---

**View Devices**

This procedure shows how to view devices from the Plug and Play tab, how to perform actions on them, and how to add new devices.

---

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

**Step 2** Click the Plug and Play tab.

The table lists all of the devices (see Table 1: Device Information, on page 7). You can use the Filter option to find specific devices. Click Refresh to refresh the device list.

**Step 3** Click the name of a device.

A window with the device details is displayed.

**Step 4** Click the Details, History, and Configuration or Stack tabs to view the different types of information for the device. Some tabs have additional links that you can click for more information.

The Stack tab appears only for a switch stack device.

**Step 5** Click the following actions at the top of the dialog box to perform specific tasks on the device. Available actions depend on the device state.

- **Refresh**—Refreshes the device state information.
- **Claim**—Claims and provisions the device. See Provision a Device With Plug and Play, on page 12.
- **Edit**—Edits the device. See Add or Edit a Device, on page 8.
- **Reset**— Resets the device if it is in an error state. See Reset a Device, on page 16.
- **Delete**—Deletes the device. See Delete a Device, on page 15.

**Step 6** To perform an action on multiple devices, click the check box next to each device in the table view and choose an action from the Actions drop-down menu.

**Step 7** Click Add to add a new device.
See the following for more information about adding devices in different ways: Add or Edit a Device, on page 8, Add Devices in Bulk, on page 9, or Add Devices from a Smart Account, on page 11.

The Device table displays the information shown in Table 1: Device Information, on page 7 for each device. All of the columns support sorting. Click the column header to sort the rows in ascending order. Click the column header again to sort the rows in descending order.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the device. Click this link to open the device details window. A stack icon indicates a switch stack.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Device serial number.</td>
</tr>
<tr>
<td>Product ID</td>
<td>Device product ID.</td>
</tr>
<tr>
<td>Source</td>
<td>Source of the device entry:</td>
</tr>
<tr>
<td></td>
<td>• User—User added the device through the GUI or API.</td>
</tr>
<tr>
<td></td>
<td>• Network—Unclaimed device that has contacted the controller.</td>
</tr>
<tr>
<td></td>
<td>• SmartAccount—Device was synced from a SmartAccount.</td>
</tr>
<tr>
<td>State</td>
<td>Source of the device entry:</td>
</tr>
<tr>
<td></td>
<td>• Unclaimed—Device has not been provisioned.</td>
</tr>
<tr>
<td></td>
<td>• Planned—Device has been claimed but has not yet contacted the server.</td>
</tr>
<tr>
<td></td>
<td>• Onboarding—Device onboarding is in progress.</td>
</tr>
<tr>
<td></td>
<td>• Provisioned—Device is successfully onboarded and added to inventory.</td>
</tr>
<tr>
<td></td>
<td>• Error—Device had an error and could not be provisioned.</td>
</tr>
<tr>
<td>Onboarding State</td>
<td>Onboarding state of the device.</td>
</tr>
<tr>
<td>Site</td>
<td>Site with which the device is associated.</td>
</tr>
<tr>
<td>Last Contact</td>
<td>Last date and time the device contacted Plug and Play.</td>
</tr>
</tbody>
</table>
Add or Edit a Device

This procedure shows how to add or edit a device from the **Plug and Play** tab. Alternatively, you can edit a device from the device details window by clicking **Edit**.

Table 2: Device Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial Number</td>
<td>Device serial number (read only if you are editing a device).</td>
</tr>
<tr>
<td>Product ID</td>
<td>Device product ID (read only if you are editing a device).</td>
</tr>
<tr>
<td>Device Name</td>
<td>Device name.</td>
</tr>
<tr>
<td>Enable SUDI Authorization</td>
<td>Enables secure unique device identifier (SUDI) authorization on devices that support it.</td>
</tr>
<tr>
<td>SUDI Serial Numbers</td>
<td>Devices that support SUDI have two serial numbers: the chassis serial number and the SUDI serial number (called the License SN on the device label). Enter one or more comma-separated SUDI serial numbers in this field when adding a device that uses SUDI authorization. This field appears only if <strong>Enable SUDI Authorization</strong> is checked.</td>
</tr>
<tr>
<td>This Device Represents a Stack</td>
<td>Device represents a stack (this item is read only if you are editing a device). Applicable only for supported stackable switches.</td>
</tr>
</tbody>
</table>

Before you begin

If the device requires credentials, be sure that the global device credentials are set in the **Design > Network Settings > Device Credentials** page. For more information, see **Configure Global CLI Credentials**.

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

**Step 2**  Click the **Plug and Play** tab.
The table lists all of the devices. You can use the Filter option to find specific devices.

**Step 3** Add or edit a device as follows:
- To add a device, click Add and the Add Devices dialog is displayed.
- To edit a device, check the check box next to the name of the device you want to edit and click Actions > Edit in the menu bar above the device table. The Edit Device dialog is displayed.

**Step 4** Set the fields as needed, referring to Table 2: Device Fields, on page 8 for more information.

**Step 5** Save the settings by doing one of the following:
- If you are adding a device and will claim it later, click Add Device.
- If you are adding a device and want to claim it immediately, click Add + Claim. For more information on claiming a device, see Provision a Device With Plug and Play, on page 12.
- If you are editing a device, click Edit Device.

---

**Add Devices in Bulk**

This procedure shows how to add devices in bulk from a CSV file.

---

**Note** If you add a device that already exists in Plug and Play, there is no change to the existing device.

---

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

**Step 2** Click the Plug and Play tab.

**Step 3** Click Add.

The Add Devices dialog is displayed.

**Step 4** Click the Bulk Devices tab.

**Step 5** Click Download File Template to download the sample file.

**Step 6** Add the information for each device to the file and save the file.

**Step 7** Upload the CSV file by doing one of the following actions:
- Drag and drop the file to the drag and drop area.
- Click where it says "click to select" and select the file.

**Step 8** Click Import Devices.

The devices in the CSV file are listed in a table.

**Step 9** Check the box next to each device to import, or click the check box at the top to select all devices.

**Step 10** Add the devices by doing one of the following:
- To add the devices and claim them later, click Add Devices.
Register or Edit a Virtual Account Profile

This procedure lets you register the Cisco DNA Center controller as the default controller for Cisco Plug and Play Connect in a Cisco Smart Account, for redirection services. Also, this lets you synchronize the device inventory from the Cisco Plug and Play Connect cloud portal to Cisco DNA Center Plug and Play.

**Table 3: Virtual Account Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Smart Account</td>
<td>Cisco Smart Account name.</td>
</tr>
<tr>
<td>Select Virtual Account</td>
<td>Virtual account name. Virtual accounts are subaccounts within a Cisco Smart Account.</td>
</tr>
<tr>
<td>Use as Default Controller Profile</td>
<td>Check this check box to register this Cisco DNA Center controller as the default controller in the Cisco Plug and Play Connect cloud portal.</td>
</tr>
<tr>
<td>Controller IP or FQDN</td>
<td>IP address or fully qualified domain name of this Cisco DNA Center controller.</td>
</tr>
<tr>
<td>Profile Name</td>
<td>Controller profile name.</td>
</tr>
</tbody>
</table>

**Before you begin**

Set the Cisco Smart Account credentials in the main Cisco DNA Center settings by using **System Settings > Settings > Cisco Credentials**. For more information, see "Configure Cisco Credentials" in the *Cisco Digital Network Architecture Center Administrator Guide*.

**Step 1**
From the Cisco DNA Center home page, click **System Settings > Settings > Cisco Credentials**.

**Step 2**
Click the **PnP Connect** tab.

The table lists all of the registered Plug and Play Connect virtual account profiles.

**Step 3**
Either add or edit a virtual account profile, as follows:

- To register a virtual account, click **Add**. The register virtual account dialog is displayed.
- To edit a registered virtual account profile, click the radio button next to the name of the profile that you want to edit and click **Edit Profile** in the menu bar above the table. The edit virtual account dialog is displayed.

**Step 4**
Set the fields as needed by referring to the preceding table.

**Step 5**
Save the settings by doing one of the following:

- If you are registering a new virtual account profile, click **Register**.
- If you are editing a virtual account profile, click **Change**.
What to do next
Synchronize the device inventory from the Cisco Plug and Play Connect cloud portal to Cisco DNA Center Plug and Play. For more information, see Add Devices from a Smart Account, on page 11.

Add Devices from a Smart Account

This task allows you to synchronize the device inventory from a Smart Account in the Cisco Plug and Play Connect cloud portal to Cisco DNA Center Plug and Play.

The Virtual Accounts table displays the information shown in Table 4: Virtual Accounts Information, on page 11 for each profile.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Accounts</td>
<td>Virtual account name.</td>
</tr>
<tr>
<td>Smart Accounts</td>
<td>Smart account that the virtual account is associated with.</td>
</tr>
<tr>
<td>Sync Status</td>
<td>Status of the last synchronization process</td>
</tr>
</tbody>
</table>

Before you begin
Before you can synchronize the device inventory from the Cisco Plug and Play Connect cloud portal, you must register a virtual account. See Register or Edit a Virtual Account Profile, on page 10.

Step 1 From the Cisco DNA Center home page, choose Provision > Devices.
Step 2 Click the Plug and Play tab.
Step 3 Click Add.

The Add Devices dialog is displayed.

Step 4 Click the Smart Account Devices tab.
Step 5 Click the radio button next to the name of the Plug and Play Connect virtual account profile from which you want to add devices.
Step 6 Click Sync to synchronize the device inventory from Cisco Plug and Play Connect in this virtual account to Cisco DNA Center Plug and Play.

Added devices appear in the Plug and Play Devices table with the source set to SmartAccount.

What to do next
Claim the newly synchronized devices. For more information on claiming a device, see Provision a Device With Plug and Play, on page 12.
Provision a Device With Plug and Play

Provisioning or claiming a device provisions it by deploying an image and an onboarding configuration to it, or a network profile for wireless devices, and adding it to the inventory. If you claim a device that has not yet booted for the first time, then you are planning the device so that it is automatically provisioned when it boots up.

The workflow for provisioning a device varies depending on the type of device, as follows:

- **Switches and Routers**—See Provision a Switch or Router Device, on page 12
- **Wireless Access Points and Sensors**—See Provision a Wireless or Sensor Device, on page 14

Provision a Switch or Router Device

Claiming a device provisions it by assigning it to a site, installing an image, deploying the site settings and onboarding configuration to it, and adding it to the inventory. If you claim a device that has not yet booted for the first time, then you are planning the device so that it is automatically provisioned when it boots up.

This procedure shows how to claim a device from the main Plug and Play tab. Alternatively, you can claim a device from the device details window by clicking Claim.

**Before you begin**

- Ensure that the devices being provisioned can discover and contact Cisco DNA Center. For more information, see Controller Discovery Prerequisites, on page 3.
- Define the site within the network hierarchy. See About Network Hierarchy.
- Define network profiles for the devices. See Create Network Profiles.
- Optionally, ensure that software images for the devices to be provisioned are uploaded and marked as golden in the Image Repository, if you want to deploy images. See Import a Software Image.

**Note**

The image deployment process used by Plug and Play during Day-0 provisioning is not the same as that used when updating a device image later, which is described in Provision a Software Image. During Plug and Play provisioning, there are no device prechecks, auto flash cleanup, or post-checks done, as it is expected that devices are in the factory default state.

- Optionally, define Onboarding Configuration templates to be applied to devices. Such templates contain basic network configuration commands to onboard a device so that it can be managed on the network. In most cases, such templates are not necessary, unless you need to customize the Day-0 configuration. See Create Templates to Automate Device Configuration Changes.

**Step 1**

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

**Step 2**

Click the Plug and Play tab.

The table lists all of the devices. You can use the Filter or Find option to find specific devices.

**Step 3**

Check the check box next to one or more devices that you want to claim.
Step 4 Click Actions > Claim in the menu bar above the device table.
The Claim Devices window opens, showing the first step, Site Assignment.

Step 5 From the Site drop-down list, choose a site to assign to each device.
To apply the same site to all devices, click the Apply to all check box.

Step 6 Click Next.
The Configuration window appears.

Step 7 (Optional) In the Image drop-down list, choose a golden software image to apply to the device.
If you do not want to deploy an image, check the Skip golden image upgrade check box.

Step 8 (Optional) In the Template drop-down list, choose an onboarding configuration template to apply to the device.
Click the eye icon next to a selected template to view the template.

Step 9 (Optional) In the Select a Top of Stack serial Number drop-down list, choose the serial number of the top of stack switch, if you want to renumber the stack.
This item appears only for switches that support stacking, and only if they are connected as shown in the image.

Step 10 (Optional) In the Select a License Level drop-down list, choose the stack license level.
This item appears only for switches that support stacking.

Step 11 If you selected multiple devices to provision, click the next device in the list at the left side of the window and repeat the configuration steps, until you have done this for all devices.

Step 12 Click Next.
The Advanced Configuration window appears.

Step 13 For each device, specify the values for the parameters that were defined in the template, if the device was assigned a configuration template.
Enter the values for each parameter in the fields for each device. A red asterisk indicates required fields.

Step 14 To specify parameter values in bulk, do the following:
a) Click Export to save the CSV template file.
b) Add the values for each of the parameters to the file and save the file.
c) Click Import.
d) Drag and drop the file to the drag and drop area, or click where it says "click to select" and select the file.
e) Click Import.

Step 15 If you selected multiple devices to provision, click the next device in the list at the left side of the window and enter the parameter values, until you have done this for all devices.

Step 16 Click Next.
The Summary window appears, where you can view details about the device, image, and configuration templates.

Step 17 Click the Day-0 Configuration Preview section to expand it and check that the configuration preview was successful.
If the preview was not successful, you should resolve any issues before claiming the device, to avoid provisioning errors. You may need to go back to the Advanced Configuration step and change parameter values, change the template, revisit the Design area to update network design settings, or resolve any network connectivity issues.
Step 18 If you selected multiple devices to provision, click the next device in the list at the left side of the window and check if the configuration preview was successful, until you have done this for all devices.

Step 19 Click **Claim** to claim the devices and start the provisioning process.

---

**Provision a Wireless or Sensor Device**

Claiming a device provisions it by assigning a network profile to the device and adding it to the inventory. If you claim a device that has not yet booted for the first time, you are planning the device so that it is automatically provisioned when it boots up.

This procedure explains how to claim a device from the main **Plug and Play** tab. Alternatively, you can claim a device from the device details window by clicking **Claim**.

**Before you begin**

- Ensure that the devices being provisioned can discover and contact Cisco DNA Center. For more information, see Controller Discovery Prerequisites, on page 3.
- Define the site within the network hierarchy. See About Network Hierarchy.
- For provisioning a wireless access point device, ensure that the wireless LAN controller that is managing the wireless access point has been added to the inventory and assigned to the site where the wireless device is to be assigned. This is not needed for a Mobility Express access point.
- For provisioning a sensor device, ensure that the sensor is reachable through the Cisco DNA Center enterprise IP address (private/enp9s0). A DHCP option 43 string makes the device reachable in unclaimed mode in Cisco DNA Center, however, to claim the device, it must be reachable from the interface enp9s0 IP address. In the DHCP server, configure the NTP server (DHCP option 42) and the vendor-specific DHCP option 43 with ASCII value "5A1D;B2;K4;1172.16.x.x;J80", where 172.16.x.x is the virtual IP address of Cisco DNA Center associated with the enp9s0 interface.
- Define wireless radio frequency profiles for wireless access point devices, except for Mobility Express access points. See Create a Wireless Radio Frequency Profile.
- Define wireless sensor device profiles for wireless sensor devices. See Create a Wireless Sensor Device Profile.
- For Mobility Express access points, define an IP address pool and a management interface. See Configure IP Address Pools.

---

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

**Step 2** Click the **Plug and Play** tab.

The table lists all of the devices. You can use the **Filter** or **Find** option to find specific devices.

**Step 3** Check the check box next to one or more devices that you want to claim.

**Step 4** Choose **Actions** > **Claim** in the menu bar above the device table.

The **Claim Devices** window opens, showing the first step, **Site Assignment**.

**Step 5** From the **Site** drop-down list, choose a site to assign to each device.
To apply the same site to all devices, click the **Apply to all** check box. Wireless devices can be assigned only to floors within a building, not to the building itself.

**Step 6**  
Click **Next**.  
The **Configuration** window appears.

**Step 7**  
For a wireless sensor device, in the **Sensor Profile** drop-down list, choose the sensor device profile to assign to the device.

**Step 8**  
If you selected multiple devices to provision, click the next device in the list at the left side of the window and repeat the profile selection, until you have done this for all devices.

**Step 9**  
Click **Next**.  
The **Advanced Configuration** window appears.

**Step 10**  
Click **Next**.  
The **Summary** window appears, where you can view details about the device and configuration.

**Step 11**  
Click the **Day-0 Configuration Preview** section to expand it and check that the configuration preview was successful.

If the preview was not successful, you should resolve any issues before claiming the device, to avoid provisioning errors. Ensure that the wireless LAN controller that is managing the device has been added to the inventory and assigned to the site where the wireless device is assigned. You may need to resolve any network connectivity issues.

**Step 12**  
Click **Claim** to claim the devices and start the provisioning process.

---

**Delete a Device**

Deleting a device removes it from the Plug and Play database but does not reset the device. Use **Reset** if you want to reset a device that is in the Error state.

This procedure shows how to delete a device from the **Plug and Play** tab. Alternatively, you can delete a device from the device details window by clicking **Delete**.

---

**Note**  
If a device is in the Provisioned state, it can be deleted only from the **Inventory** tab.

---

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

**Step 2**  
Click the **Plug and Play** tab.  
The table lists all of the devices. You can use the **Filter** or **Find** option to find specific devices.

**Step 3**  
Check the check box next to one or more devices that you want to delete.

**Step 4**  
Click **Actions > Delete** in the menu bar above the device table.  
A confirmation dialog box is displayed.

**Step 5**  
Click **Delete** to confirm that you want to delete the devices.
Reset a Device

Resetting a device applies only to devices in the Error state and reloads the device, but does not remove it from the Plug and Play database. Use **Delete** if you want to delete a device.

---

**Note**

If the saved configuration on the device is the factory default or a similar minimal configuration, then this option causes the device to restart the provisioning process. However, if the device has a previously saved startup configuration, then this could prevent the device from restarting the provisioning process and it will need to be reset to factory defaults.

This procedure shows how to reset a device from the **Plug and Play** tab. Alternatively, you can reset it from the device details window by clicking **Reset**.

---

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

### Step 2
Click the **Plug and Play** tab.

The table lists all of the devices. You can use the **Filter** or **Find** option to find specific devices.

### Step 3
Check the check box next to one or more devices that you want to reset.

### Step 4
Click **Actions > Reset** in the menu bar above the device table.

A confirmation dialog box is displayed.

### Step 5
Choose one of the following options:

- **Reset and keep current claim parameters**—Keep the current claim parameters and the device goes to the Planned state.
- **Reset and remove all claim parameters**—Remove the current claim parameters and the device goes to the Unclaimed state.

### Step 6
Click **Reset**.

---

### Add a Device to a Site

### 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.

### Step 3
From the **Action** menu, choose **Assign Device to Site**.

### Step 4
In the **Find Site** field, enter the name of the site to which you want to associate the device. If you selected multiple devices to add to the same site, click **All Same Site**.

### Step 5
Click **Assign**.
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.

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 17 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.

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.
**Edit Device Tags**

You can edit device tags that you previously created.

**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 as SSIDs, wireless interfaces, and wireless radio frequency profiles. For more information, see Configure Global Wireless Settings.

• Discover devices in your network by running Discovery so that the discovered devices are listed on the Inventory window.

• Make sure that the Cisco Wireless Controller is added to a site. For more information, see Add a Device to a Site, on page 16.

---

**Note**
You cannot make manual configuration changes to a Cisco Wireless Controller that is managed by Cisco DNA Center. You must perform all configurations from the Cisco DNA Center user interface.

---

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

The **Devices > Inventory** window appears.

**Step 2**
All the 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**.

The **Assign Site** window appears.

**Step 5**
In the **Find Site** field, enter the name of the site to which you want to associate the wireless controller. To assign multiple controllers to the same site, check the **All Same Site** check box.

**Step 6**
Click **Next**.

The **Configuration** window appears.

**Step 7**
Select a role for the wireless controller: **Active Main WLC** or **Guest Anchor WLC**.

**Step 8**
Click **Select Managed AP locations** to choose AP locations that are managed by the wireless controller.

**Step 9**
In the **Managed AP Location** window, check the check box next to the site name. You can either select a parent site or the individual sites. If you select a parent site, all the children under the parent site are also selected. You can uncheck the check box to deselect a particular site.

Inheritance of managed AP locations allows you to automatically choose a site along with the buildings and floors under that site. One site can be managed by only one wireless controller.

**Step 10**
Click **Save**.

**Step 11**
For an active main wireless controller, you must configure the interface and VLAN details. Under the **Interface and VLAN Configuration** area, click **+ Add**.

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

**Step 12**
From the **Interface Name** drop-down list, choose the interface name.

**Step 13**
In the **VLAN ID** field, enter a value for the VLAN.

**Step 14**
In the **Interface IP Address** field, enter a value for the interface IP address.

**Step 15**
In the **Interface Net Mask (in bits)** field, enter the subnet mask of the interface.
Provision a Cisco Wireless Controller

Step 16  In the Gateway IP Address field, enter the IP address of the gateway.
Step 17  From the LAG/Port Number drop-down list, choose the link aggregation or the port number.
Step 18  Click OK.
Step 19  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 20  Click Next.

The Advanced Configuration window appears, where you can enter values for predefined template variables.

Step 21  You can search for the device or the template in the Devices panel.
Step 22  Enter a value for the predefined template variable in the wlanid field.
Step 23  Click Next.

The Summary window displays the following information:

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

Step 24  Click Deploy to provision the controller.
- To deploy the device immediately, click the Now radio button, and click Apply.
- To schedule the device deployment for a later date and time, click the Later radio button and define the date and time of the deployment.

Step 25  The Status column in the Device Inventory window shows SUCCESS after a successful deployment.

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

Step 26  After the devices are deployed successfully, the Provision Status changes from Configuring to Success.
Step 27  On the Provision > Device Inventory window, click See Details in the Provision Status column for a device to get more information about network intent or to view a list of actions.
Step 28  Click See Details under Device Provisioning.
Step 29  Click View Details under Deployment of network intent, and click the device name.
Step 30  Expand the Configuration Summary area to view the operation details, feature name, and the management capability.

The configuration summary also displays any error that occurred while provisioning the device.

Step 31  Expand the Provision Summary area to view details of the exact configuration that is sent to the device.
Provision Routing and NFV Profiles

Before you begin

Make sure that you have defined the following global network settings before provisioning a NFV profile:

• 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.

• SP profiles. For more information, see Configure Service Provider Profiles.

Note

When provisioning Cisco Firepower Threat Defense Virtual through the NFV provisioning flow, the default credential username is retained and the password is updated based on the settings in the credential profile assigned to the site in Network Settings.

---

Step 1

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

The Device Inventory window appears.

Step 2

Click the Plug and Play tab.

• Check the check box next to one or more devices that you want to claim.

• Select Claim from Actions drop-down list.

• The Claim Device dialog opens. From the Select a site drop-down list, choose a site to assign it to the device.

• Click Close.

For more information, see Onboarding Devices with Plug and Play Provisioning, on page 1.

Step 3

Click the Inventory tab.

To provision a NFVIS device, do the following:

• Check the check box next to the NFVIS device. From the Actions drop-down list, choose provision.

• Review the details in the Confirm Profile window, and click Next.

• Review the details in the Router WAN Configuration window. Click on O and enter the WAN IP address. Review the details in the +Edit Services window. Click Next.

Note

You have to configure vManage settings in system setting page, before provisioning vEDGE related service. For more information see the section Configure vManage Properties in Cisco Digital Network Architecture Center Administrator Guide.

• Review the details in the ENCS Integrated Switch Configuration window, and click Next.
**Provision a Cisco AP—Day 1 AP Provisioning**

**Before you begin**

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

---

**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 the discovered devices are displayed.

**Step 3**

Check the check box adjacent the AP device name that you want to provision.

**Step 4**

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

**Step 5**

The **Assign Site** window appears.

**Step 6**

Assign an AP to the site.

**Step 7**

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 8**

Click Next.

---

**Provision Your Network**

**Step 4**

Click **Deploy** to provision the device.

The **Provision Status** column in the **Device Inventory** window shows **SUCCESS** after a successful deployment. Click **SUCCESS** to see detailed Provisional log status.
The Configuration window appears.

**Step 9**
By default, the custom 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 10**
Click Deploy to provision the AP.
You are prompted with a message that creation or modification of an AP group in progress.

**Note**
After completion, these devices will get rebooted.

**Step 11**
Click OK.
The Status column in the Device Inventory window shows SUCCESS if the deployment is successful.

---

### Provision a Brownfield Device

**Before you begin**

**Note**
Brownfield support is available on Cisco AireOS Wireless Controller devices and not for Cisco Catalyst 9800 Series Wireless Controller devices.

With the 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.

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

The Device Inventory window appears.

**Step 2**
Click the Inventory tab.
All discovered devices 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.
In the Configure Interface and VLAN window, configure the required fields, and click OK.

Click Next.

The Summary window displays the following information:

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

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 Cisco Wireless Controller.

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.

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.

Create SSIDs for a guest wireless network with external web authentication and central web authentication along with configuring Cisco Identity Services Engine. For more information, see Create SSIDs for a Guest Wireless Network.

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

Provision a foreign wireless controller as the active main wireless controller. See Provision a Cisco Wireless Controller, on page 18.

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 18.

Configure 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.

Configure and Provision a Cisco Catalyst 9800 Series Wireless Controller

Cisco Catalyst 9800 Series Wireless Controller Overview

The Cisco Catalyst 9800 Series Wireless Controller is the next generation of wireless controllers built for intent-based networking. The Cisco Catalyst 9800 Series Wireless Controller is Cisco IOS XE based and integrates the RF excellence from Aironet with the intent-based networking capabilities of Cisco IOS XE to create the best-in-class wireless experience for your organization.
The Cisco Catalyst 9800 Series Wireless Controller is built on a modular operating system and uses open, programmable APIs that enable automation of day-0 and day-N network operations.

The Cisco Catalyst 9800 Series Wireless Controller is available in multiple form factors:

- Catalyst 9800-40 Wireless Controller
- Catalyst 9800-80 Wireless Controller
- Catalyst 9800-CL Cloud Wireless Controller—deployable on private cloud (ESXi, KVM, Cisco ENCS) and manageable by Cisco DNA Center
- Catalyst 9800 Embedded Wireless Controller for Catalyst 9300 Switch

The following table lists the supported virtual and hardware platforms for the Cisco Catalyst 9800 Series Wireless Controller:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Catalyst 9800-80 Wireless Controller</td>
<td>Supports up to 6000 access points and 64,000 clients.</td>
</tr>
<tr>
<td></td>
<td>Supports up to 80 Gbps throughput and occupies a 2 - rack unit space.</td>
</tr>
<tr>
<td></td>
<td>Modular wireless controller with up to 100-GE uplinks and seamless software updates.</td>
</tr>
<tr>
<td>Cisco Catalyst 9800-40 Wireless Controller</td>
<td>A fixed wireless controller with seamless software updates for mid-sized organizations and campus deployments.</td>
</tr>
<tr>
<td></td>
<td>Supports up to 2000 access points and 32,000 clients.</td>
</tr>
<tr>
<td></td>
<td>Supports up to 40 Gbps throughput and occupies a 1-rack unit space.</td>
</tr>
<tr>
<td></td>
<td>Provides four 1-GE or 10-GE uplink ports.</td>
</tr>
<tr>
<td>Cisco Catalyst 9800-CL Cloud Wireless Controller—supports Cisco Catalyst 9800-CL for private cloud</td>
<td>Cisco Catalyst 9800-CL Cloud Wireless Controller is the next generation of enterprise-class virtual wireless controllers built for high availability and security.</td>
</tr>
<tr>
<td></td>
<td>A virtual form factor of Cisco Catalyst 9800-CL Cloud Wireless Controller can be deployed in a private cloud (supports ESXi, KVM, and Cisco ENCS).</td>
</tr>
<tr>
<td>Cisco Catalyst 9800-CL Cloud Wireless Controller</td>
<td>Cisco Catalyst 9800-CL Cloud Wireless Controller brings the wired and wireless infrastructure together with consistent policy and management.</td>
</tr>
<tr>
<td></td>
<td>This deployment model supports only Cisco SD-Access, which is a highly secure solution for small campuses and distributed branches. The embedded controller supports access points (APs) only in Fabric mode.</td>
</tr>
</tbody>
</table>

The following table lists the host environments supported by the Cisco Catalyst 9800 Series Wireless Controller:
Installing the .ova file of C9800-CL using ESXi vSphere does not work. This is not limited to the C9800 ova but affects other products. Cisco and VMware are actively working to fix the issue. Contact your Cisco account representative to see if the problem is fixed. There are issues specific to VMware 6.5 and C9800-CL OVA file deployment in which deployment fails with the warning "A required disk image was missing" and the error "Failed to deploy VM: postNFCData failed: Cannot POST to non-disk files.”

To install C9800-CL on VMware ESXi 6.5, do one of the following: 1) Install the .iso file of C9800-CL using the ESXi embedded GUI (ESXI 6.5 client version 1.29.0 is tested and required). 2) Install the .ova file of C9800-CL using the OVF tool.

The following table lists the NFVIS versions supported in Cisco DNA Center:

<table>
<thead>
<tr>
<th>NFVIS Version</th>
<th>Device Platform</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>• 3.7.1</td>
<td>• ENCS 5400</td>
<td></td>
</tr>
<tr>
<td>• 3.8.1</td>
<td>• UCS-E</td>
<td></td>
</tr>
<tr>
<td>• 3.9.1</td>
<td>• UCS-C</td>
<td></td>
</tr>
<tr>
<td>• 3.9.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 3.10.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 3.10.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 3.7.1</td>
<td>ENCS 5100</td>
<td>Cisco 5100 Enterprise Network Compute System (ENCS) does not support NFVIS 3.10.x</td>
</tr>
<tr>
<td>• 3.8.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 3.9.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 3.9.2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Cisco Enterprise NFVIS devices support N-1 to N upgrade path only. For example, upgrade from Cisco Enterprise NFVIS Release 3.8.x to Cisco Enterprise NFVIS 3.9.x only is supported. Upgrade from Cisco Enterprise NFVIS Release 3.8.x to Cisco Enterprise NFVIS Release 3.10.x is not supported.
Workflow to Configure a Cisco Catalyst 9800 Series Wireless Controller in Cisco DNA Center

1. Install Cisco DNA Center.
   For more information, see Cisco Digital Network Architecture Center Installation Guide.

2. For information on software image upgrade, see Software Image Upgrade Support for Cisco Catalyst 9800 Series Wireless Controller, on page 30.

3. Log in to Cisco DNA Center user interface, and verify if the applications you need are in the Running state.
   To verify, from Cisco DNA Center home page, click the gear icon ☰, and then choose System Settings > App Management > Packages & Updates.

4. Integrate Cisco Identity Services Engine with Cisco DNA Center. After integration, any devices that Cisco DNA Center discovers along with relevant configurations and data is pushed to Cisco ISE.

   You must enable NETCONF and set the port to 830 to discover Catalyst 9800 Series Wireless Controllers. NETCONF provides a mechanism to install, manipulate, and delete configurations of network devices.
   For more information, see Discover Your Network Using CDP, or Discover Your Network Using an IP Address Range.
   You need to add the wireless management IP address manually.
   While performing discovery using the Cisco Discovery Protocol (CDP) or IP address range on the Discovery page, choose Use Loopback from the Preferred Management IP drop-down list to specify the device's loopback interface IP address.

6. Make sure that the discovered devices appear in the Device Inventory page and are in Managed state.
   For more information, see About Inventory and Display Information About Your Inventory.
   You must wait for the devices to move to a Managed state.

7. To verify the assurance connection with the Catalyst 9800 Series Wireless Controller, use the following commands:
   • `#show crypto pki trustpoints | sec DNAC-CA`

      Trustpoint DNAC-CA
      Subject Name:
      cn=kube-ca
      Serial Number (hex): 00E**************
      Certificate configured.

   • `#show crypto pki trustpoints | sec sdn-network`

      Trustpoint sdn-network-infra-iwan:
      Subject Name:
      cn=sdn-network-infra-ca
      Serial Number (hex): 378**************
      Certificate configured.

   • `#show telemetry ietf subscription all`

      Telemetry subscription brief
<table>
<thead>
<tr>
<th>ID</th>
<th>Type</th>
<th>State</th>
<th>Filter type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1011</td>
<td>Configured</td>
<td>Valid</td>
<td>tdl-uri</td>
</tr>
<tr>
<td>1012</td>
<td>Configured</td>
<td>Valid</td>
<td>tdl-uri</td>
</tr>
<tr>
<td>1013</td>
<td>Configured</td>
<td>Valid</td>
<td>tdl-uri</td>
</tr>
</tbody>
</table>

- **#show telemetry internal connection**

  Telemetry connection

  Address | Port | Transport | State | Profile
  --------------|------|------------|-------|-------------
  IP address 25103 | tls-native | Active | sdn-network-infra-iwan |

- **#show network-assurance summary**

  Network-Assurance: True
  Server Url: https://10.***.***.***
  ICap Server Port Number: 3***
  Sensor Backhaul SSID:
  Authentication: Unknown

8. Configure TACACS server while configuring authentication and policy servers.

   Configuring TACACS is not mandatory if you have configured user name locally on the Catalyst 9800 Series Wireless Controller.

9. Design your network hierarchy by adding sites, buildings, and floors so that later you can easily identify where to apply design settings or configurations.

   You can either create a new network hierarchy or if you have an existing network hierarchy on Cisco Prime Infrastructure, you can import into Cisco DNA Center.

   To import and upload an existing network hierarchy, see Upload an Existing Site Hierarchy.

   To create a new network hierarchy, see Create a Site in a Network Hierarchy, Add Buildings, and Add a Floor to a Building.

10. Add the location information of APs, and position them on the floor map to get coverage heatmap visualization.

    For more information, see Add, Position, and Delete APs.

11. Define network settings, such as AAA (Cisco ISE is configured for Network and Client Endpoint), Netflow Collector, NTP, DHCP, DNS, syslog, and SNMP traps. These network servers become the default for your entire network. You can add a TACACS server while adding a AAA server.

    For more information, see About Global Network Settings, Configure Global Network Servers, and Add AAA server.

12. Create a wireless radio frequency profile with the parent profile as custom.

    For more information, see Create a Wireless Radio Frequency Profile.

13. Create IP address pools at the global level.

    Cisco DNA Center uses IP address pools to automate the configuration and deployment of SD-Access networks. While adding IP address pool, make sure that the Overlapping check box is not checked. Overlapping allows users to identify overlapping subnets within their network. This enables these addresses to be used in multiple places which would be denied otherwise.

    To create an IP address pool, see Configure IP Address Pools.
You must reserve an IP address pools for the building that you will be provisioning. For more information, see Provision a LAN Underlay.

14. Create an enterprise and guest wireless networks. Define the global wireless settings once and then Cisco DNA Center pushes configurations to various devices across geographical locations. Designing a wireless network is a two-step process. First, you must create SSIDs on the Wireless page. Then, associate the created SSID to a wireless network profile. This profile helps you to construct a topology, which is used to deploy devices on a site.

For more information, see Create SSIDs for an Enterprise Wireless Network and Create SSIDs for a Guest Wireless Network.

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

16. Configure the following on the Policy window for the Catalyst 9800 Series Wireless Controller:

   • Create a virtual network. The virtual network segments your physical network into multiple logical networks. For more information, see Virtual Networks and Create a Virtual Network.

   • Create a group-based access control policy, and add a contract. For more information, see Create a Group-Based Access Control Policy.

17. Configure high availability.

   For more information, see Configure High Availability for Cisco Catalyst 9800 Series Wireless Controller, on page 31.

18. Provision the Catalyst 9800 Series Wireless Controller with configurations added during the design phase.

   For more information, see Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 34.

Software Image Upgrade Support for Cisco Catalyst 9800 Series Wireless Controller

Before you begin

   • Discover the Cisco Catalyst 9800 Series Wireless Controller.

   Enable NETCONF and set the port to 830 to discover the Cisco Catalyst 9800 Series Wireless Controller. NETCONF enables wireless services on the controller and provides a mechanism to install, manipulate, and delete the configuration of network devices.

   For more information, see Discover Your Network Using CDP, or Discover Your Network Using an IP Address Range.

   • Make sure that the devices appear in the device inventory and are in the Managed state.

   For more information, see About Inventory and Display Information About Your Inventory.

---

**Step 1** From Cisco DNA Center home page, choose Design > Image Repository or click Image Repository.

**Step 2** Import the Cisco Catalyst 9800 Series Wireless Controller software image from your local computer or from a URL.

For more information, see Import a Software Image.

**Step 3** Assign the software image to a device family.
For more information, see Assign a Software Image to a Device Family.

**Step 4**
You can mark a software image as golden by clicking star for a device family or for a particular device role.
For more information, see Specify a Golden Software Image.

**Step 5**
To provision a software image, from Cisco DNA Center home page, click Provision.
  - Select the Cisco Catalyst 9800 Series Wireless Controller whose image you want to upgrade.
  - From the Actions drop-down, choose Update OS Image.
For more information, see the Provision a Software Image.

---

**Information About High Availability**

High availability (HA) allows you to reduce the downtime of wireless networks that occurs because of the failover of controllers. You can configure high availability of Cisco Catalyst 9800 Series Wireless Controllers through Cisco DNA Center.

**Configure High Availability for Cisco Catalyst 9800 Series Wireless Controller**

**Before you begin**
Note the prerequisite tasks for configuring High Availability (HA) on Cisco Catalyst 9800 Series Wireless Controller:

  - Both the devices are running the same software version and have active software image on the primary controller.
  - The service port and the management port of controller 1 and controller 2 are configured.
  - The redundancy port of controller 1 and controller 2 are physically connected.
  - Preconfigurations such as interface configurations, route addition, ssh line configurations, netconf-yang configurations are completed on the controller appliance.
  - The management interface of controller 1 and controller 2 are in the same subnet.
  - The discovery and inventory of controller 1 and controller 2 are successful from Cisco DNA Center.
  - The devices are reachable and are in Managed state.

---

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

**Step 2**
Click the desired controller name to configure as a primary controller.

**Step 3**
Click the High Availability tab.
The selected controller by default becomes the primary controller and the Primary C9800 field is grayed out.

**Step 4**
From the Select Primary Interface and Secondary Interface drop-down lists, choose the interface that is used for HA connectivity.
The HA interface serves the following purposes:
• Enables communication between the controller pair before the IOSd boots up.
• Provides transport for IPC across the controller pair.
• Enables redundancy across control messages exchanged between the controller pair. The control messages can be HA role resolution, keepalives, notifications, HA statistics, and so on.

Step 5
From the **Select Secondary C9800** drop-down list, choose the secondary controller to create a HA pair.

Step 6
Enter the **Redundancy Management IP** and **Peer Redundancy Management IP** addresses in the respective fields.

**Note**
The IP addresses used for redundancy management IP and peer redundancy management IP should be configured in the same subnet as the management interface of the controller. Ensure that these IP addresses are unused IP addresses within the subnet range.

Step 7
In the **Netmask** field, enter the netmask address.

Step 8
Click **Configure HA**.

The HA configuration is initiated at the background using the CLI commands. First, the primary controller is configured. On success, the secondary controller is configured. Both the devices reboot once the HA is enabled. This process may take up to 2.5 minutes to complete.

Step 9
After the HA is initiated, the **Redundancy Summary** under **High Availability** tab displays the **Sync Status** as **HA Pairing is in Progress**. When Cisco DNA Center finds that the HA pairing is successful, the **Sync Status** becomes **Complete**.

This is triggered by the inventory poller or by manual resynchronization. By now, the secondary controller is deleted from Cisco DNA Center. This flow indicates successful HA configuration on the controller.

Step 10
To manually resynchronize the controller, on the **Provision > Inventory** window, select the controller that you want to synchronize manually.

Step 11
From the **Actions** drop-down list, choose **Resync**.

Step 12
The following is the list of actions that occur after the process is complete:

• Controller 1 and controller 2 are configured with redundancy management, redundancy units, and Single sign-on (SSO). The devices reboot in order to negotiate their role as an active controller or a standby controller. Configuration is synchronized from active to standby.

• On the **Show Redundancy Summary** window, you can see these configurations:
  • SSO is enabled
  • Controller 1 is in active state
  • Controller 2 is in standby state

---

**Commands to Configure High Availability on Cisco Catalyst 9800 Series Wireless Controllers**

**Step 1**
Use the following commands to configure HA on primary for the Cisco Catalyst 9800 Series Wireless Controller:

• Run the `chassish-interface GigabitEthernet <redundancy interface num> local-ip <redundancy ip> <netmask> remote-ip <peer redundancy ip>` command to configure the HA chassis interface.
This example shows how to configure a HA chassis interface:

```
chassis ha-interface GigabitEthernet 3 local-ip 1.1.1.2 255.255.255.0 remote-ip 1.1.1.3
```

- Run the `reload` command to reload devices for the changes to become effective.

**Step 2**

Use the following commands to configure HA on secondary for the Cisco Catalyst 9800 Series Wireless Controller:

- Run the `chassis ha-interface GigabitEthernet <redundancy interface num> local-ip <redundancy ip> <netmask> remote-ip <peer redundancy ip>` command to configure the HA chassis interface.

This example shows how to configure a HA chassis interface:

```
chassis ha-interface GigabitEthernet 2 local-ip 1.1.1.3 255.255.255.0 remote-ip 1.1.1.2
```

**Step 3**

Run the `chassis clear` command to clear or delete all the HA-related parameters, such as local IP, remote IP, HA interface, mask, timeout, and priority.

**Note**  
Reload the devices for changes to take effect by running the `reload` command.

**Step 4**

Use the following commands to configure HA on primary for Cisco Catalyst 9800-40 Wireless Controller and Cisco Catalyst 9800-80 Wireless Controller devices:

- Run the `chassis ha-interface local-ip <redundancy ip> <netmask> remote-ip <peer redundancy ip>` command to configure the HA chassis interface.

This example shows how to configure a HA chassis interface:

```
chassis ha-interface local-ip 1.1.1.2 255.255.255.0 remote-ip 1.1.1.3
```

- Run the `reload` command to reload devices for the changes to become effective.

**Step 5**

Use the following commands to configure HA on secondary for Cisco Catalyst 9800-40 Wireless Controller and Cisco Catalyst 9800-80 Wireless Controller devices:

- Run the `chassis ha-interface local-ip <redundancy ip> <netmask> remote-ip <peer redundancy ip>` command to configure the HA chassis interface.

This example shows how to configure a HA chassis interface:

```
chassis ha-interface local-ip 1.1.1.3 255.255.255.0 remote-ip 1.1.1.2
```

**Step 6**

Run the `chassis clear` command to clear or delete all the HA-related parameters, such as local IP, remote IP, HA interface, mask, timeout, and priority.

**Note**  
Reload the devices for changes to take effect by running the `reload` command.

---

**Commands to Verify Cisco Catalyst 9800 Series Wireless Controllers High Availability**

Use the following commands to verify the high availability configurations from Cisco Catalyst 9800 Series Wireless Controllers:

- Run the `config redundancy mode sso` command to check the HA-related details.
• Run the `show chassis` command to view chassis configurations about the HA pair, including the MAC address, role, switch priority, and current state of each controller device in the redundant HA pair.

• Run the `show ip interface brief` command to view the actual operating redundancy mode running on the device, and not the configured mode as set by the platform.

• Run the `show redundancy states` command to view the redundancy states of the active and standby controllers.

• Run the `show redundancy summary` command to check the configured interfaces.

• Run the `show romvar` command to verify high availability configuration details.

---

**Provision a Cisco Catalyst 9800 Series Wireless Controller**

**Before you begin**

Before provisioning a Cisco Catalyst 9800 Series Wireless Controller, make sure that you have completed the steps in *Workflow to Configure a Cisco Catalyst 9800 Series Wireless Controller in Cisco DNA Center*, on page 28.

---

**Step 1**

From the Cisco DNA Center home page, choose **Provision**.

The Devices > Inventory window appears with a list of discovered devices.

**Step 2**

Check the check box next to the Catalyst 9800 Series Wireless Controller name that you want to associate to a site.

**Step 3**

From the Actions drop-down list, choose **Provision > Assign Device to Site**.

**Step 4**

In the Assign Device to Site window, click **Choose a Site** to assign a site for the Catalyst 9800 Series Wireless Controller device.

**Step 5**

In the Add Sites window, click the check box next to the site name to associate a Catalyst 9800 Series Wireless Controller.

You can either select a parent site or the individual sites. If you select a parent site, all the children under the parent site are also selected. You can uncheck the check box to deselect an individual site.

**Step 6**

Click **Save**.

**Step 7**

Click **Apply**.

**Step 8**

Provision the device with the configurations that were added during the design phase.

**Step 9**

Choose **Provision > Devices > Inventory**.

**Step 10**

Check the check box next to the Catalyst 9800 Series Wireless Controller name that you want to provision.

**Step 11**

From the Actions drop-down list, choose **Provision > Provision**.

**Step 12**

In the Assign Site window, click **Next**.

The Configuration window appears.

**Step 13**

Select a wireless controller role for the Catalyst 9800 Series Wireless Controller device: **Active Main WLC**.

**Step 14**

Click **Select Primary Managed AP Locations** to select a managed AP location for the primary controller.

**Step 15**

Click **Select Secondary Managed AP Locations** to select a managed AP location for the secondary controller.

**Step 16**

You can either select a parent site or the individual sites. If you select a parent site, all the children under the parent site are also selected. You can uncheck the check box to deselect a particular site.
Inheritance of managed AP locations allows you to automatically choose a site along with the buildings and floors under that particular site. One site is managed by only one wireless controller.

**Step 17**  
Click **Save**.

**Step 18**  
For an active main wireless controller, you need to configure interface and VLAN details.

**Step 19**  
Under the **Assign Interface** area, do the following:

- **VLAN ID**: Enter a value for the VLAN ID.
- **IP Address**: Enter the interface IP address.
- **Gateway IP Address**: Enter the gateway IP address.
- **Subnet Mask (in bits)**: Enter the interface net mask details.

*Note* Assigning an IP address, gateway IP address, and subnet mask is not required for the Catalyst 9800 Series Wireless Controller.

**Step 20**  
Click **Next**.

The **Advanced Configuration** window appears, where you enter values for the predefined template variables.

**Step 21**  
Search for the device or the template in the **Devices** panel.

**Step 22**  
Enter a value for the predefined template variable in the **wlanid** field.

**Step 23**  
Click **Next**.

**Step 24**  
On the **Summary** window, review the following configurations:

- Device Details
- Network Setting
- SSID
- Managed Sites
- Interfaces
- Advanced Configuration

**Step 25**  
Click **Deploy** to provision the Catalyst 9800 Series Wireless Controller.

- To deploy the device immediately, click the **Now** radio button and click **Apply**.
- To schedule the device deployment for a later date and time, click the **Later** radio button and define the date and time of the deployment.

**Step 26**  
To verify configurations that are pushed from Cisco DNA Center to the device, use the following commands on the Catalyst 9800 Series Wireless Controller device:

- `#show wlan summary`
- `#show run | sec line`
- `#show running-configuration`

**Step 27**  
Once the devices are deployed successfully, the **Provision Status** changes from **Configuring** to **Success**.
Step 28  In the Inventory window, click See Details in the Provision Status column against a device to get more information about network intent or to view a list of actions.

Step 29  Click See Details under Device Provisioning.

Step 30  Click View Details under Deployment of network intent, and click the device name.

Step 31  Click and expand the device name.

Step 32  Expand the Configuration Summary area to view the operation details, feature name, and the management capability. The configuration summary also displays any error that occurred while provisioning device with reasons for failure.

Step 33  Expand the Provision Summary area to view details of the exact configuration that is sent to the device.

Step 34  Provision the AP.

For more information, see Provision a Cisco AP—Day 1 AP Provisioning, on page 22.

Step 35  Configure and deploy application policies on the Catalyst 9800 Series Wireless Controller. For more information, see Create an Application Policy, Deploy an Application Policy, and Edit an Application Policy.

You must provision Catalyst 9800 Series Wireless Controller devices before deploying an application policy.

For Catalyst 9800 Series Wireless Controller devices, two different policies with different business relevance for two different SSIDs do not work. Always the last deployed policy takes precedence when you are setting up the relevance.

For Catalyst 9800 Series Wireless Controller devices, changing the default business relevance for an application does not work in FlexConnect mode.

You can apply an application policy only on a nonfabric SSID.

---

Configure and Provision a Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9k Series Switches

Supported Hardware Platforms

<table>
<thead>
<tr>
<th>Device Role</th>
<th>Platforms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Embedded Wireless Controller</td>
<td>Cisco Catalyst 9300 Series Switches</td>
</tr>
<tr>
<td>Fabric Edge</td>
<td>Cisco Catalyst 9300 Series Switches</td>
</tr>
<tr>
<td></td>
<td>Cisco Catalyst 3600 Series Switches</td>
</tr>
<tr>
<td></td>
<td>Cisco Catalyst 3850 Series Switches</td>
</tr>
<tr>
<td>APs</td>
<td>Cisco 802.11ac Wave 2 APs:</td>
</tr>
<tr>
<td></td>
<td>• Cisco Aironet 1810 Series OfficeExtend Access Points</td>
</tr>
<tr>
<td></td>
<td>• Cisco Aironet 1810W Series Access Points</td>
</tr>
<tr>
<td></td>
<td>• Cisco Aironet 1815i Access Point</td>
</tr>
<tr>
<td></td>
<td>• Cisco Aironet 1815w Access Point</td>
</tr>
<tr>
<td></td>
<td>• Cisco Aironet 1815m Access Point</td>
</tr>
<tr>
<td>Device Role</td>
<td>Platforms</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------</td>
</tr>
<tr>
<td></td>
<td>• Cisco 1830 Aironet Series Access Points</td>
</tr>
<tr>
<td></td>
<td>• Cisco Aironet 1850 Series Access Points</td>
</tr>
<tr>
<td></td>
<td>• Cisco Aironet 2800 Series Access Points</td>
</tr>
<tr>
<td></td>
<td>• Cisco Aironet 3800 Series Access Points</td>
</tr>
<tr>
<td></td>
<td>• Cisco Aironet 4800 Series Access Points</td>
</tr>
<tr>
<td></td>
<td>Cisco 802.11ac Wave 1 APs</td>
</tr>
<tr>
<td></td>
<td>• Cisco Aironet 1700 Series Access Points</td>
</tr>
<tr>
<td></td>
<td>• Cisco Aironet 2700 Series Access Points</td>
</tr>
<tr>
<td></td>
<td>• Cisco Aironet 3700 Series Access Points</td>
</tr>
</tbody>
</table>

**Preconfiguration**

Make sure that the following commands are present if the switch is already configured with `aaa new-model`:

```bash
aaa new-model
aaa authentication login default local
aaa authorization exec default local
aaa session-id common
```

This is required for NETCONF configuration. These configurations are not required if you are using automated underlay for provisioning.

**Workflow to a Configure Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Switches**

1. Install Cisco DNA Center.  
   See the [Cisco Digital Network Architecture Center Installation Guide](#).

2. Log in to the Cisco DNA Center user interface, and verify if the applications you need are in the **Running** state.
   To verify, from Cisco DNA Center home page, click the gear icon 🔄, and then choose **System Settings > Software Updates > Installed Apps**.

3. Integrate Cisco Identity Services Engine with Cisco DNA Center. Once Cisco ISE is registered with Cisco DNA Center, any device that Cisco DNA Center discovers, along with relevant configurations and other data, is pushed to Cisco ISE.

4. Discover Cisco Catalyst 9000 Series Switch and edge switches.
   You must enable NETCONF and set the port to 830 to discover the device.
   You do not have to enable NETCONF to discover the edge switches.
   For more information, see [Discover Your Network Using CDP](#), or [Discover Your Network Using an IP Address Range](#).
Change the Preferred Management IP to Use Loopback.

5. Make sure that the devices appear in the device inventory and are in Managed state.
   For more information, see About Inventory and Display Information About Your Inventory.
   You must wait for all the devices to get into a managed state.

6. Design your network hierarchy which represents your network's geographical location. You create site, buildings, and floors so that later you can easily identify where to apply design settings or configurations.
   You can either create a new network hierarchy or if you have an existing network hierarchy on Cisco Prime Infrastructure, you can import it into Cisco DNA Center.
   To import and upload an existing network hierarchy, see the Upload an Existing Site Hierarchy.
   To create a new network hierarchy, see the Create a Site in a Network Hierarchy, Add Buildings, and Add a Floor to a Building.

7. For a non fabric network, add and position APs on a floor map to get coverage heatmaps visualization during the design phase.
   For a fabric network, you cannot place APs on a floor map during the design time. The APs are on-boarded after adding devices to a fabric network.
   For more information, see Add, Position, and Delete APs.

8. Define network settings such as AAA (Cisco ISE is configured for Network and Client Endpoint), Netflow Collector, NTP, DHCP, DNS, syslog, and SNMP traps. These network servers become the default for your entire network.
   For more information, see About Global Network Settings, Configure Global Network Servers and Add AAA server.

9. Configure device credentials such as CLI, SNMP, and HTTPS credentials.
   For more information, see About Global Device Credentials, Configure Global CLI Credentials, Configure Global SNMPv2c Credentials, Configure Global SNMPv3 Credentials, and Configure Global HTTPS Credentials.

10. Configure IP address pools at the global level.
    These IP addresses are used for end clients and APs. While adding IP pool, make sure that the Overlapping check box is not checked. Overlapping allows users to identify overlapping subnets within their network. This enables these addresses to be used in multiple places which would be denied otherwise.
    To configure an IP address pool, see Configure IP Address Pools.
    To reserve an IP address pools for the building that you will be provisioning, see Provision a LAN Underlay.

11. Create enterprise and guest wireless networks. Define global wireless settings once and then Cisco DNA Center pushes configurations to various devices across geographical locations.
    Designing a wireless network is a two-step process. First, you must create SSIDs on the Wireless page. Then, associate the created SSID to a wireless network profile. This profile helps you to construct a topology, which is used to deploy devices on a site.
    For more information, see Create SSIDs for an Enterprise Wireless Network and Create SSIDs for a Guest Wireless Network.
12. Create a network profile. For more information, see Create a Wireless Sensor Device Profile.

13. Configure the following on the Policy page:
   - Create a virtual network. The virtual network segments your physical network into multiple logical networks. For more information, see Virtual Networks and Create a Virtual Network.
   - Create a group-based access control policy, and add a contract. For more information, see Create a Group-Based Access Control Policy.

14. Provision Cisco Catalyst 9000 Series Switch and the edge node switches with configurations added during the design phase.
   - Create a fabric domain.
   - Add devices to fabric network by creating a CP+Border+Edge or CP+Border.
   - Enable embedded wireless capabilities on the devices.
   - Onboard APs in the fabric domain.

Once the devices are deployed successfully, the deploy status changes from Configuring to Success. For more information, see Provision Embedded Wireless on Cisco Catalyst 9300 Series Switches, on page 39.

Provision Embedded Wireless on Cisco Catalyst 9300 Series Switches

Before you begin
Before provisioning a Cisco Catalyst 9300 Series Switch, ensure that you have completed the steps that are mentioned here: Workflow to a Configure Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Switches, on page 37.

---

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

The Inventory page displays all the discovered devices and the edge switches. These devices are displayed as WLC Capable devices.

**Step 2**
Check the check box next to the Catalyst 9300 Series Switch device and an edge switch that you want to associate to a site.

**Step 3**
From the Actions drop-down list, choose Add to Site.

**Step 4**
In the Assign Device to Site window, click Choose a site.

**Step 5**
In the Choose a site window, check the check box next to the site to associate the device.

**Step 6**
Click Save.

**Step 7**
Click Apply.

**Step 8**
Next step is to provision Catalyst 9300 Series Switch and the edge node with configurations that were added during the design phase.

**Step 9**
Choose Provision > Devices > Inventory.

**Step 10**
Check the check box adjacent the device name that you want to provision.

**Step 11**
From the Actions drop-down list, choose Provision.
Step 12: Click Next.

Step 13: In the Summary window, verify the configurations, and click **Deploy** to provision the device.

Step 14: To provision the edge switch, check the check box adjacent the edge switch that you want to provision.

Step 15: From the **Actions** drop-down list, choose **Provision**.

Step 16: Click Next.

Step 17: In the Summary window, verify the configurations, and click **Deploy**.

Once the devices are deployed successfully, the **Provision Status** changes from **Configuring** to **Success**.

Step 18: To add devices to a fabric domain, from the Cisco DNA Center home page, choose **Provision > Fabric**.

Step 19: Create a fabric LAN. For more information, see **Create a Fabric Domain**, on page 49.

Step 20: Add an IP transit network.

IP transit network is used in a regular IP network to connect to an external or to connect two or more fabric sites. For more information, see **Create an IP Transit Network**, on page 48.

Step 21: Add devices and associate virtual networks to a fabric domain. For more information, see **Add a Device to a Fabric**, on page 51.

Step 22: Add Cisco Catalyst 9300 Series Switch as a control plane, a border node, and an edge node or a control plane and a border node.

Click the device and choose **Add as CP+Border+Edge** or **Add as CP+Border**.

In the dialog box that appears, configure the following:

- 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.

- In the **Local Autonomous Number** field, enter the local autonomous number for the device.

- From the **Select the IP Pool** drop-down list, choose the IP address pool which should be part of the virtual network. Cisco DNA Center uses this IP pool to configure the automatic border handoff from the fabric.

- Check the **Connected to the Internet** check box to select this border node to advertise Internet services on to other fabric borders.

- From the **Select Transit** drop-down list, click **Add** to choose a transit network to enable on the border device.

- Click **Add Interface**.

The **Add Interface** dialog box appears.

- From the **External Interface** drop-down list, choose the interface connecting from a fabric network to IP transit network

- In the **Remote AS Number** field, enter the autonomous system number for the device.

- Expand the **Virtual Network** drop-down list, and check the virtual network check box. This virtual network should be advertised by the border to the remote peer. You can select one, multiple, or all virtual networks.
Provision Embedded Wireless on Cisco Catalyst 9300 Series Switches

- Click Save.
- Click Add.
- Click Save.

A success message saying Devices updated to fabric domain successfully is displayed.

Step 23
Click the edge switch and choose Add to Fabric.

Step 24
Click Save.

Step 25
To enable embedded wireless on the device, click the device which is added as a CP+Border+Edge or CP+Border, and choose Enable Embedded Wireless.

If you have not installed the wireless package on Cisco Catalyst 9300 Series Switch before enabling the wireless functionality, Cisco DNA Center displays a warning message saying 9800-SW image is necessary for turning on the capability. Click "OK" to import the 9800-SW image manually.

Step 26
Click OK to install the image manually.

Step 27
On the Download Image window, click Choose File to navigate to a software image stored locally or Enter image URL to specify an HTTP or FTP source from which to import the software image.

Step 28
Click Import.

The progress of the import is displayed.

Step 29
Click Activate image on device.

A warning message saying Activate image on device will reboot the device. Are you sure you want to reboot the device? appears.

Step 30
Click Yes.

The device reboots and comes online once the device package upgrade is complete.

Step 31
In the dialog box that appears, the AP locations which are managed by the controllers are displayed. You can change, remove, or reassign the site here.

Step 32
Click Next.

Step 33
Review details on the Summary window, and click Save.

Step 34
On the Modify Fabric Domain window, click Now to commit the changes, and click Apply to apply the configurations.

Step 35
Next step is to onboard APs in a fabric domain.

Step 36
From Cisco DNA Center home page, click the Provision tab.

Step 37
Click the Fabric tab.

A list of fabric domains is displayed.

Step 38
Select the fabric domain that was created, and click the Host Onboarding tab to enable IP pool for APs.

Step 39
Select the authentication template that is applied for devices in the fabric domain. These templates are predefined configurations that are retrieved from Cisco Identity Service Engine (ISE). After selecting the authentication template, click Save.

Step 40
Under Virtual Networks, click INFRA_VN to associate one or more IP pools with the selected virtual network.

Step 41
Check the IP Pool Name check box that was created for APs during the design phase.

Step 42
Click Update to save the setting.
AP gets the IP address from the specified pool, which is associated with the AP VLAN and registers with the Cisco Wireless Controller through one of the discovery methods.

**Step 43** Specify wireless SSIDs within the network that hosts can access. Under Wireless SSID section, you can select the guest or enterprise SSIDs and assign address pools, and click Save.

**Step 44** Manually trigger resynchronization by performing an Inventory > Resync to see the APs on Cisco DNA Center for embedded wireless.

**Step 45** The discovered APs are now displayed under Inventory in the Provision page and the Status is displayed as Not Provisioned.

**Step 46** Provision the AP.

For more information, see Provision a Cisco AP—Day 1 AP Provisioning, on page 22.

---

**Fabric in a Box with Catalyst 9800 Embedded Wireless on Cisco Catalyst 9k Series Switches**

**Information About Fabric in a Box**

Cisco Catalyst 9300 Series Switches have the capability to host fabric edge, control plane, border, and embedded wireless functionalities on a single switch, which you can configure using Cisco DNA Center.

With this feature, configurations at the small site locations are simplified and the cost to deploy Cisco SD-Access is reduced.

For information on how to add CP+Border+Edge nodes on Cisco Catalyst 9300 Series Switches, see Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 34.

**Scale Information**

This table shows the device scalability information.

<table>
<thead>
<tr>
<th>Fabric Constructs</th>
<th>Cisco Catalyst 9300 Series Switches</th>
<th>Cisco Catalyst 9400 Series Switches</th>
<th>Cisco Catalyst 9500 Series Switches</th>
<th>Cisco Catalyst 9500-H Series Switches</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Networks</td>
<td>256</td>
<td>256</td>
<td>256</td>
<td>256</td>
</tr>
<tr>
<td>Local End Points/Hosts</td>
<td>4K</td>
<td>4K</td>
<td>4K</td>
<td>4K</td>
</tr>
<tr>
<td>SGT/DGT Table</td>
<td>8K</td>
<td>8K</td>
<td>8K</td>
<td>8K</td>
</tr>
<tr>
<td>SGACLs (Security ACEs)</td>
<td>5K</td>
<td>18K</td>
<td>18K</td>
<td>18K</td>
</tr>
</tbody>
</table>
Provision a 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 16.)

• 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 feature.

Note: LAN Automation is blocked if the discovered site is configured with CLI credentials that has a username "cisco".

---

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, choose 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) From the LAN Automation drop-down list, choose LAN Automation.

c) In the LAN Automation dialog box, complete the following fields:

- **Primary Site**: Select your Primary Device from this site.
- **Peer Site**: This site is used for selection of Peer Device. Note that this site can be different from the Primary Site.
- **Primary Device**: Select the primary device that Cisco DNA Center uses as the starting point to discover and provision new devices.
- **Peer Device**: Select the peer device.
- **Choose Primary Device Ports**: Ports to be used to discover and provision new devices.
- **Discovered Device Site**: All newly discovered devices are assigned to this site. This site can be different from Primary and Peer Sites.
- **IP Pool**: IP address pool that was reserved for LAN automation. (See Step 1.)
- **ISIS Domain Password**: A user-provided IS-IS password 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 default domain password is used. If both primary and secondary seeds have domain passwords, ensure that they match.
- **Enable Multicast**: LAN automation creates a multicast tree from seed devices as RPs and discovered devices as subscribers.
- **Device Name Prefix**: Name prefix for the devices being provisioned. As Cisco DNA Center provisions each device, it prefixes the device with the text that you provide and adds a unique number at 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 discovered devices using a CSV file that contains a mapping between serial numbers and hostnames. If the discovered device is a stack, all serial numbers of the stack are provided in the CSV file.

Here is a sample CSV file:

```plaintext
standalone-switch,FCW2212L0NF
stack-switch,FCW2212E00Y,FCW2212L0GV
```

d) Click **Start**.

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

**Step 3**

Monitor and review the progress of the devices being provisioned.

a) From the Provision > Devices > Inventory tab, click LAN Automation > LAN Auto Status.

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

**Note** The provisioning process might take several minutes for 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 Inventory.

**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.

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.

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 and transit site. Multiple fabric sites are connected to each other using a transit site.

There are two types of transit sites:

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

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

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

Transit Sites

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

- IP transit: Uses a regular IP network to connect to an external network or to connect two or more fabric sites.
- SDA transit: Uses LISP/VxLAN encapsulation to connect two fabric sites. The SDA transit area may be defined as a portion of the fabric that has its own Control Plane Nodes, but does not have Edge or Border Nodes. However, it can work with a fabric that has an external border. Using SDA transit, an end-to-end policy plane is maintained using SGT group tags.

Create an IP Transit Network

To add a new IP transit network:

Step 1 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:
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 SD-Access as the transit type.
Step 7  Enter the Site for the Transit Control Plane for the transit network. Choose at least one transit map server.
Step 8  Enter the Transit Control Plane for the transit network.
Step 9  Repeat Step 7 and Step 8 for all map servers that you want to add.
Step 10 Click Save.

What to do next

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

Configuring Fabric Domains

Fabrics Overview

A fabric 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.

The 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.

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.

Step 1  From the Cisco DNA Center home page, click Provision.
Step 2  Click the Fabric tab.
**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:

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

For more information, see [SD-Access 1.2.x 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 current state of user intent for Virtual Network on Cisco DNA Center.
Configure a Fabric Domain

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

Add a Device to a Fabric

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

Note

It is optional to designate the devices in a fabric domain as control plane nodes or border nodes. You might have devices that do not 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.

Note

Currently, Cisco Wireless Controller communicates only with two control plane nodes.

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

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

Before you begin

Provision the device. To provision a device, click the Provision tab and choose Devices. The topology displays 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.
Add Device as a Border Node

Step 1: From the Cisco DNA Center homepage, click Provision. The window displays all the 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>Adds the selected device as a control plane and a border node and an edge node.</td>
</tr>
<tr>
<td>Add to Fabric</td>
<td>Adds a distribution or access device to the fabric domain.</td>
</tr>
<tr>
<td>Add as CP</td>
<td>Adds 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>Adds 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>Adds the selected device as a control plane and a border node.</td>
</tr>
<tr>
<td>Enable Guests</td>
<td>Allows 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 Enable.</td>
</tr>
<tr>
<td>Note</td>
<td>Ensure that you have created a guest virtual network in the Policy application. See Create a Virtual Network.</td>
</tr>
</tbody>
</table>

View Device Info         | Displays the details of the selected device.                                |

Step 4: Click Save.

What to do next

Once 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 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 a Device to a Fabric, on page 51.

To add a device as a border node:
Step 1  From the Cisco DNA Center homepage, 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. An external border node connects to unknown networks such as the internet and/or transit area.
      • **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.

**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.

**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.

**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.

**Step 1**

From the Cisco DNA Center home page, choose Design > Network Settings > IP Address Pools. A list of all IP address pools is displayed.

**Step 2**

Click Add and specify the multicast addresses to form the pool:

- **IP Pool Name**: Enter a name for the multicast IP address pool.
- **Subnet/Mask**: Enter the subnet IP address and subnet mask for the multicast pool.
- **Gateway IP Address**: Enter the IP address of the gateway.

**Step 3**

Click Save.

**Step 4**

To enable multicast in multiple virtual networks, create a separate IP multicast pool for each virtual network. (Repeat Step 2 and Step 3.)
Native Fabric Multicast

Note

For a brownfield deployment of Native Multicast, manually configure the underlay multicast commands. If you enable multicast using LAN Automation, the multicast commands are configured during discovery of devices.

To enable and disable native fabric multicast on a fabric site:

---

**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 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**
By default, native multicast is disabled for a site. To enable native multicast for a site, click the gear box next to the listed fabric and choose **Enable Native Multicast for IPv4**. Save the fabric.

**Step 4**
To disable native multicast for a fabric site, click the gear box next to the listed fabric and choose **Disable Native Multicast for IPv4**. Save the fabric.

---

Add a Device as a Rendezvous Point

**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.

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

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.

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.
Add a Device as a Redundant Rendezvous Point