



Provision Your Network

- [Provisioning, on page 1](#)
- [Onboard Devices with Plug and Play Provisioning, on page 1](#)
- [Provision Wireless Devices, on page 23](#)
- [Provision Routing and NFV Profiles, on page 74](#)
- [Provision Firewall Profiles, on page 76](#)
- [Provision a LAN Underlay, on page 78](#)
- [Delete a Device After Provisioning, on page 82](#)

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 the inventory.
- Adding devices to sites.
- Creating fabric sites and adding devices to the fabric.

Cisco DNA Center provisioning supports only IBNS 2.0, which changes the AAA configuration and converts all relevant authentication commands to their Class-Based Policy Language (CPL) control policy equivalents. Because the CPL conversion disables the conversion CLI **authentication display [legacy|new-style]**, we recommend that you back up your current configuration. Also, plan your change management windows to support AAA configuration updates (aligned with IBNS 2.0).

Onboard 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 the Cisco Smart Account credentials in the main Cisco DNA Center settings by using **System > Settings > Smart Account**.
- Accept the End User License Agreement (EULA) in the main Cisco DNA Center settings by using **System > Settings > Device EULA Acceptance**.
- Ensure that Cisco network devices to be provisioned have a supported software release and are in a factory default state. If you are using a network device that was previously configured or is in an unknown state, see the device clean-up and reset details in the [Network Plug and Play Troubleshooting Guide for Cisco DNA Center](#).

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. 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 many cases, such templates are not necessary unless you need to customize the Day 0 configuration. See [Create Templates to Automate Device Configuration Changes](#).
3. Define network profiles for the types of devices you are deploying. See [Create Network Profiles](#).
4. Define the device credentials (CLI and SNMP) for the devices you are deploying. If you are using SNMPv2c, both Read and Write credentials must be provided. See [About Device Credentials](#).
5. 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](#).
6. Add details about planned devices one at a time or in bulk with a CSV file. See [Add or Edit a Device, on page 9](#) or [Add Devices in Bulk, on page 10](#).
7. 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 7](#).
2. Claim the device by assigning a site, image, configuration template, or profile. See [Provision a Device with Plug and Play, on page 13](#).

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 with which to synchronize. See [Register or Edit a Virtual Account Profile, on page 11](#).
2. Synchronize the device inventory from the Smart Account. See [Add Devices from a Smart Account, on page 12](#).
3. Find the device on the devices list by filtering on unclaimed devices or searching for it by name. See [View Devices, on page 7](#).
4. Claim the device by assigning a site, image, configuration template, or profile. See [Provision a Device with Plug and Play, on page 13](#).
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 5](#).
- 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 information. 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;K4;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.
 - Jxxx—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 DNS. For more information, see [DNS Controller Discovery, on page 5](#).

If the Cisco DNA Center system certificate has an FQDN-only SAN field, you must edit the DHCP pool on the seed device to contain the Option 43 string with FQDN, B2 to B1, dns-server, and domain-name before starting PnP.

If the DHCP pool relies on Cisco switches or routers, a sample configuration is as follows:

```
ip dhcp pool PnP_Pool
network 214.2.64.0/255.255.0
default-router 214.2.64.1
option 43 ascii "5A1D;B1;K4;I<FQDN>;J80"
domain-name sitdns.com
dns-server 17.1.104.100
```

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 pnpntpserver.

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 pnpntpserver.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 pnpntpserver.

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.

-
- Step 1** 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.
- Step 2** 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.

- Step 3** Alternatively, you can manually add devices in the Plug and Play Connect web portal.
- Step 4** 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 11](#).
- 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.
- Step 5** Synchronize the device inventory from the Smart Account in the Cisco Plug and Play Connect cloud portal to Cisco DNA Center Plug and Play.
- 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 13](#).
- 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.

Plug and Play Deployment Guidelines


Follow these recommendations when using Plug and Play:

- **Device bring up order:** In general, routing and upstream devices should be brought up first. Once the router and all upstream devices are up and provisioned, switches and downstream devices can be brought up. The Plug and Play agent in a device attempts to auto-discover the Cisco DNA Center controller only during initial device startup. If at this time, the device cannot contact the controller, device provisioning fails, so upstream devices should be provisioned first.
- **Cisco Router Trunk/Access Port Configuration:** Typical branch networks include routers and switches. One or more switches are connected to the WAN router and other endpoints like IP phones and access points connect to the switches. When a switch connects to an upstream router, the following deployment models are supported for Plug and Play:
 - Downstream switch is connected to the router using a switched port on the router. In this type of connection, the switched port on the router can be configured as a trunk or access port.
 - Downstream switch is connected to the router using a routed port on the router. In this case, the routed port can support multiple VLANs using sub-interfaces. During the Plug and Play process, the switch would automatically configure its port as a trunk port. In a large branch scenario, it becomes necessary to carry multiple VLANs between the router and the downstream switch. To support this use case, the switch must be connected to a routed port.

- **Non-VLAN 1 configuration:** Plug and Play supports devices using VLAN 1 by default. If you want to use a VLAN other than 1, adjacent upstream devices must use supported releases and you must configure the following global CLI command on the upstream device to push this CLI to the upcoming Plug and Play device: **pnpp startup-vlan x**. When you execute this command on an adjacent upstream device, the VLAN membership change does not happen on that device. However, the active interfaces on the upcoming Plug and Play device that are connected to the upstream device are changed to the specified VLAN. This guideline applies to both routers and switches and should be used only for trunk mode scenarios and not access mode.

View Devices

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

-
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon () and choose **Provision > Plug and Play**.
- Step 2** View the devices in the table. The **Devices** table shows all the Plug and Play devices.
- Step 3** In the **Device Status** area, click **Unclaimed**, **Error**, **Provisioned**, or **All**.
- **Unclaimed:** Shows the devices that are not claimed and the devices that are being claimed.
 - **Error:** Shows the devices in which error appears while being claimed.
 - **Provisioned:** Shows the devices that are claimed.
 - **All:** Shows all the devices.
- Step 4** From the **Focus** drop-down list, choose **Basic** or **Default**.
- **Basic:** Shows the **Device Name**, **Serial Number**, **Product ID**, **IP Address**, **Source**, **State**, **Site**, and **Last Contact** details of the devices.
 - **Default:** Shows the **Device Name**, **Serial Number**, **Product ID**, **IP Address**, **Source**, **State**, **Onboarding Progress**, **Site**, **Last Contact**, **Smart Account**, **Virtual Account**, and **Created** details of the devices.
- Step 5** From the **Auto-Refresh** drop-down list, choose **30 s**, **1 min**, **5 min**, or **10 min** to auto refresh the **Devices** table in the specified time span or choose **Off** to turn off auto refresh.
- Step 6** Click the Gear icon to customize the appearance of the **Devices** table.
- In the **Table Settings** slide-in pane, do the following:
- a. Click **Table Appearance**, choose **Default** or **Compact** under **Table Density**, and enable **Table Striping** if you want striping in alternate rows.
 - b. Click **Enable Table Columns** and choose the columns that you want to see in the table.
 - c. Click **Apply**.
 - d. Click **Reset All Settings** if you want to reset the table settings.
- Step 7** Click the Search or Filter icon to find specific devices.
- Step 8** Click **Refresh Now** to refresh the **Devices** table manually.
- Step 9** For devices with status as **Error**, hover your cursor over the progress bar on the **Onboarding Progress** column to view the error.
- For more information about error, click the name of the device and view the error details in the **History** tab.
- Step 10** Click the name of a device.

A slide-in pane with the device details is displayed.

Step 11 Click the **Details**, **History**, and **Configuration** or **Stack** tabs to view the different types of information for the device. The **Stack** tab appears only for a switch stack device.

Step 12 Choose a device in the **Devices** table and perform any of the following options from the **Actions** drop-down list:

- **Claim:** See [Provision a Device with Plug and Play, on page 13](#).
- **Edit:** See [Add or Edit a Device, on page 9](#).
- **Reset:** See [Reset a Device, on page 23](#).
- **Delete:** See [Delete a Device, on page 22](#).

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

Step 13 Click **Add Device** to add a new device.

See the following topics for more information about adding devices in different ways:

- [Add or Edit a Device, on page 9](#)
- [Add Devices in Bulk, on page 10](#)
- [Add Devices from a Smart Account, on page 12](#)

The **Devices** table displays the information shown in the following table for each device. Some of the columns support sorting. Click the column header to sort the rows in ascending order, if sorting is supported. Click the column header again to sort the rows in descending order.

The Device table displays the information shown in the following table for each device. Some of the columns support sorting. Click the column header to sort the rows in ascending order, if sorting is supported. Click the column header again to sort the rows in descending order.

Table 1: Device Information

Column	Description
#	Row number.
Device Name	Hostname of the device. Click this link to open the device details window. A stack icon indicates a switch stack.
Serial Number	Device serial number.
Product ID	Device product ID.
IP Address	Device IP address.
Source	Source of the device entry: <ul style="list-style-type: none"> • User: User added the device through the GUI or API. • Network: Unclaimed device that has contacted the controller. • SmartAccount: Device was synced from a Smart Account.

Column	Description
State	<ul style="list-style-type: none"> • Unclaimed: Device has not been provisioned. • Planned: Device has been claimed but has not yet contacted the server. • Onboarding: Device onboarding is in progress. • Provisioned: Device is successfully onboarded and added to inventory. • Error: Device had an error and could not be provisioned.
Onboarding State	Onboarding state of the device. Click on the progress bar to go to the device history.
Site	Site with which the device is associated.
Last Contact	Last date and time the device contacted Plug and Play.
Smart Account	Cisco Smart Account with which the device is associated.
Virtual Account	Virtual Account (within the Cisco Smart Account) with which the device is associated.
Created	Date and time when the device was added to Plug and Play.

Add or Edit a Device

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

Table 2: Device Fields

Field	Description
Serial Number	Device serial number (read only if you are editing a device).
Product ID	Device product ID (read only if you are editing a device).
Device Name	Device name.
Enable SUDI Authorization	Enables secure unique device identifier (SUDI) authorization on devices that support it.
SUDI Serial Numbers	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 Enable SUDI Authorization is checked.
This Device Represents a Stack	Device represents a stack (this item is read only if you are editing a device). Applicable only for supported stackable switches.

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** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision > Plug and Play**.
- Step 2** View the devices in the table.
- You can filter on device state by using one of the **Device State** buttons, or use the **Filter** option to find specific devices. Click **Refresh** to refresh the device list.
- Step 3** Add or edit a device as follows:
- To add a device, click **Add Devices** and then click **Single Device**.
 - 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 the preceding table 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 13](#).
 - 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.

-
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision > Plug and Play**.
- Step 2** Click **Add Device**.
- The **Add Devices** dialog is displayed.
- Step 3** Click **Bulk Devices**.
- Step 4** Click **Download File Template** to download the file template.
- See the file template for information on which fields are mandatory and optional for different devices.
- Step 5** Add the information for each device to the file and save the file. Note that certain fields are required, depending on the device type.
- Step 6** 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 7** Click **Import Devices**.
- The devices in the CSV file are listed in a table.

Step 8 Check the box next to each device to import, or click the check box at the top to select all devices.

Step 9 Add the devices by doing one of the following:

- To add the devices and claim them later, click **Add Devices**.
- To add the devices and claim them immediately, click **Add + Claim**. For more information on claiming a device, see [Provision a Device with Plug and Play, on page 13](#).

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

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

Before you begin

Set the Cisco Smart Account credentials in the main Cisco DNA Center settings by using **System > Settings > Smart Account**.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon () and choose **System > Settings > PnP Connect**.

Step 2 View the virtual accounts in the table.

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 **Register**. 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 Virtual Account Fields 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 12](#).

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 following information for each profile.

Table 4: Virtual Accounts Information

Column	Description
Virtual Accounts	Virtual account name
Smart Accounts	Smart account that the virtual account is associated with
Sync Status	Status of the last synchronization process
Sync Result	Result of the last synchronization process

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 11](#). You can go directly to the PnP Connect settings page by clicking the **PnP Connect** link in the **Add Devices > Smart Account Devices** dialog.

-
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon () and choose **Provision > Plug and Play**.
- Step 2** Click **Add Device**.
The **Add Devices** dialog is displayed.
- Step 3** Click **Smart Account Devices**.
- Step 4** If you need to enter a Cisco.com ID (Cisco.com ID shows as Not Associated), follow these steps:
- Click the **Add** link.
 - Enter the Cisco.com username and password.
 - Click **Save For Later** if you want to save the credentials permanently in Cisco DNA Center, or leave this check box unchecked to use these credentials one time only.
 - Click **Submit**.
- 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.

If you need to register a PnP Connect virtual account profile, click the **PnP Connect** link. If you need to add Cisco.com credentials, click the **Add** link next to **Cisco.com ID**. If you want to change the Cisco ID, click the **Not me?** link.

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 13](#).

Provision a Device with Plug and Play

Provisioning or claiming a device deploys an image and an onboarding configuration to the device. In the case of wireless devices, a network profile is configured. The device is then added to the inventory. If you claim a device that has not yet booted for the first time, you are planning the device configuration so that it is automatically provisioned when it boots up.

When provisioning or claiming a device, Cisco DNA Center does the following:

1. Deploys an image to the device.
2. Deploys an onboarding configuration for physically connected devices or a network profile for wireless devices.
3. Adds the device to the inventory.

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 13](#)
- Wireless LAN controllers, access points, and sensors: See [Provision a Wireless or Sensor Device, on page 17](#)

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.

When a device is claimed, some system configuration CLI commands from Cisco DNA Center are pushed to the device first, before the Onboarding Configuration (Day-0) template that you have defined. If your Onboarding Configuration template has any of the same CLI commands, these will override the system configuration, since they are applied last. The CLI commands pushed by the system include the following:

- Device credentials (CLI and SNMP)
- Enable SSH v2 and SCP server
- Disable HTTP and HTTPS servers
- For switches, vtp mode transparent is enabled



Note When Device Controllability is enabled for a device (it is enabled by default), additional configurations are pushed to the device when it is added to the inventory or assigned to a site. For more information, see the Device Controllability section in the [Cisco DNA Center Administrator Guide](#).

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

Before you begin

- Ensure that Cisco network devices to be provisioned have a supported software release and are in a factory default state. If you are using a network device that was previously configured or is in an unknown state, see the device clean-up and reset details in the [Network Plug and Play Troubleshooting Guide for Cisco Digital Network Architecture Center](#).
- 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 the CLI and SNMP credentials for the devices. If you are using SNMPv2c, you must provide both Read and Write credentials. See [About Device Credentials](#).
- 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. See [Create Templates to Automate Device Configuration Changes](#).



Note You can use the `ip http client source-interface` CLI command in the Onboarding Configuration template, which makes Cisco DNA Center use that IP address as the management IP address for device, especially for the scenario of multiple IPs or VRFs.

- Define network profiles for the devices. See [Create Network Profiles](#).

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

Step 2 View the devices in the table.

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, **Assign Site**. If, instead, you see a window that shows mandatory tasks such as defining a site and defining device credentials, you must click on **Add Site** to define a site, and **Add device credentials** to define device credentials. These are prerequisites for the claim process and, once these tasks are completed, you can return to claiming a device by clicking **Refresh** in this window.

Step 5 (Optional) Change the device hostname, if needed, in the first column.

Step 6 From the **Select a Site** drop-down list, choose a site to assign to each device.

To apply the same site as the first device to all other devices, click the **Apply Site to All** check box. To assign the site from any device to some other devices, click **Assign this Site to Other Devices**, choose the devices, and click **Assign**.

Step 7 Click **Next**.

The **Assign Configuration** window appears.

Step 8 (Optional) Make global changes to the device table as follows:

- a) Change which columns are displayed in the table by clicking the 3 dots at the right end of the table headings and choosing the desired columns. Click **Apply** to save the changes.
- b) Click **Clear Device Certificates** to clear any device certificates configured for devices. Click the check box for each device you want to clear the certificate from, and click **Clear**.
- c) Click **Clear Images** to clear the default images configured for devices. Click the check box for each device you want to clear the image from, and click **Clear**.
- d) Click **Clear Templates** to clear the default templates configured for devices. Click the check box for each device you want to clear the template from, and click **Clear**.
- e) Click **Clear License Levels** to clear the license levels configured for devices. Click the check box for each device you want to clear the license level from, and click **Clear**.
- f) You can apply an image or template from one device to other devices by clicking the 3 dots in the **Actions** column next to a device and choosing **Apply Image to Other Devices** or **Apply Template to Other Devices**. For stacked devices, you can apply the device license level to other devices by clicking **Apply License Level to Other Devices**.

Step 9 In the **Configuration** column, click on **Assign** for the device that you want to configure and follow these steps:

- a) View the device configuration summary and click **Cancel** if no changes are needed.
- b) (Optional) Check the check box **Apply the PKCS12 device certificate on the device** to deploy a PKCS12 certificate to the device. This option is available only for routers.
- c) (Optional) In the **Device Name** field, change the device hostname, if needed.
- d) (Optional) In the **Image** drop-down list, choose a golden software image to apply to the device. If there is only one golden image for this device type in the image repository, it is chosen by default.
- e) (Optional) In the **Template** drop-down list, choose an onboarding configuration template to apply to the device. If there is only one onboarding configuration template for this device type defined, it is chosen by default.

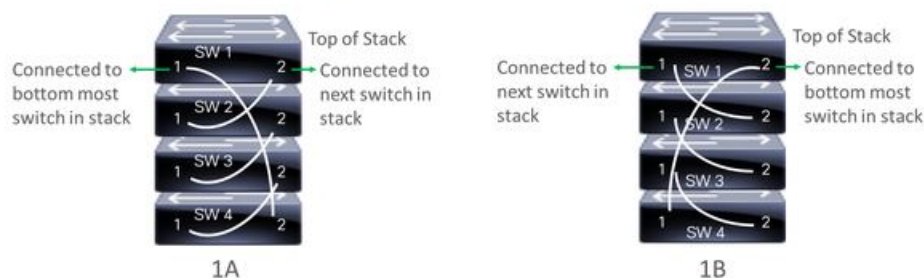
Click **Preview** next to a selected template to view the template.

- f) (Optional) In the **Select a Cabling Scheme** drop-down list, choose the stack cabling scheme, 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 one of the following cabling schemes.

Figure 1: Cabling Schemes

Supported Stack Switch Wiring Schemes:



- g) (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.

- h) (Optional) In the **Select a License Level** drop-down list, choose the stack license level.

This item appears only for switches that support stacking.

- i) If you made any changes, click **Save**, otherwise, click **Cancel** to return to the list and configure other devices.

Step 10 If you selected multiple devices to provision, click **Assign** for the next device in the list and repeat the configuration steps, until you have done this for all devices.

Step 11 Click **Next**.

The **Provision Templates** window appears, where you can specify the values for parameters that were defined in the template.

Step 12 Click on the name of a device that you want to configure and follow these steps:

- a) 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.

- b) If you want to copy the running configuration to the startup configuration on the selected device, check the box **Copy running config to startup config**.

- c) 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 13 To specify parameter values for all devices in bulk, do the following:

- Click **Export** to save the CSV template file.
- Add the values for each of the parameters to the file and save the file.
- Click **Import**.
- Drag and drop the file to the drag and drop area, or click where it says "**click to select**" and select the file.
- Click **Import**.

Step 14 Click **Next**.

The **Summary** window appears, where you can view details about the devices and their configuration preview status.

Step 15 Check the **Day-0 Config** column for each device to see if the configuration preview was successful.

If the preview shows an error, you can click on the **Actions** link in the error message above the table to see what actions you need to take. You can click on an action to open a new tab with the window where a change is needed. You must resolve any issues before claiming the device, to avoid provisioning errors. You may need to go back to the **Provision Templates** step and change parameter values, change the template, revisit the **Design** area to update network design settings, or resolve any network connectivity issues. Once you have resolved the problem, you can go back to this tab and click the radio button **Retrying getting Day-0 configuration preview for failed device(s)**, and click **OK**.

- Step 16** You can click the link in the **Day-0 Config** column to see more information about the device, its configuration, and any configuration preview errors.
- Step 17** Click **Claim**.
A confirmation dialog box is displayed.
- Step 18** Click **Yes** to claim the devices.

What to do next

To complete the provisioning process, after the device is added to the inventory, go to the **Inventory** tab, select the device and click **Actions > Provision > Provision Device**. Proceed through all the steps and click **Deploy** in the **Summary** step. In the **Summary**, you can see the remaining network settings that will be pushed to the device. For more information, see [Provision Wireless Devices, on page 23](#). This process is required if you intend to push the network settings that you may have configured in the **Design** area. During Plug and Play provisioning, only the device credentials and the Onboarding Configuration are pushed to the device; no other network settings are pushed until provisioning is completed from **Inventory**. Additionally, the device is added to ISE by Cisco DNA Center as a AAA client for RADIUS and TACACS, if these are configured.

Provision a Wireless or Sensor Device

Claiming a wireless device provisions it by assigning a configuration 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.



Note When Device Controllability is enabled for a device (it is enabled by default), additional configurations are pushed to the device when it is added to the inventory or assigned to a site. For more information, see the Device Controllability section in the [Cisco DNA Center Administrator Guide](#).

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

Before you begin

- Ensure that Cisco network devices to be provisioned have a supported software release and are in a factory default state. If you are using a network device that was previously configured or is in an unknown state, see the device clean-up and reset details in the [Network Plug and Play Troubleshooting Guide for Cisco DNA Center](#).
- 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 the CLI and SNMP credentials for the devices. See [About Device Credentials](#).
- 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.
- Optionally, ensure that the software images for any Cisco Catalyst 9800-CL 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.

- 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 ACSII value "5A1D;B2;K4;I172.16.x.x;J80", where 172.16.x.x is the virtual IP address of Cisco DNA Center associated with the enp9s0 interface.
- Define wireless radio frequency profiles for wireless access point devices, except for Mobility Express access points. See [Create a Wireless Radio Frequency Profile](#).
- For Mobility Express access points, define an IP address pool and a management interface. See [Configure IP Address Pools](#).

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

Step 2 View the devices in the table.

You can use the **Filter** or **Find** option to find specific devices.

Step 3 Check the check box next to one or more wireless 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, **Assign Site**. If, instead, you see a window that shows mandatory tasks such as defining a site and defining device credentials, you must click on **Add Site** to define a site, and **Add device credentials** to define device credentials. These are prerequisites for the claim process and, once these tasks are completed, you can return to claiming a device by clicking **Refresh** in this window.

Step 5 (Optional) Change the device name, if needed, in the first column.

Step 6 (Optional) Change the device type, if needed, in the second column. You can choose AP (Access Point) or ME (Mobility Express), depending on which mode the device is using.

Choosing the wrong mode causes an error provisioning the device. This item does not appear for wireless LAN controller or sensor devices.

- Step 7** From the **Select a Site** drop-down list, choose a site and floor to assign to each device. Access point devices must be assigned to a floor with a wireless controller.
- To apply the same site as the first device to all other devices, click the **Apply Site to All** check box. To assign the site from any device to some other devices, click **Assign this Site to Other Devices**, choose the devices, and click **Assign**. Wireless devices can be assigned only to floors within a building, not to the building itself.
- Step 8** Click **Next**.
The **Assign Configuration** window appears.
- Step 9** (Optional) You can change which columns are displayed in the table by clicking the 3 dots at the right end of the table headings and choosing the desired columns. Click **Apply** to save the changes.
- Step 10** In the **Configuration** column, click on **Assign** for the device that you want to configure and follow these steps:
- View the device configuration summary and click **Cancel** if no changes are needed.
 - (Optional) In the **Device Name** field, change the device name, if needed.
 - For an access point device, in the **Radio Frequency Profile** drop-down list, choose a radio frequency profile to apply to the device. This may be set if you designated one profile as a default.
 - For a wireless LAN controller, enter values in the following fields: **Wireless management IP**, **Subnet mask**, **Gateway**, **IP interface name**, and optionally, **VLAN ID**.
 - For a Mobility Express device, enter values in the following fields: **Wireless management IP**, **Subnet mask**, and **Gateway**.
 - For a wireless sensor device, in the **Sensor Settings** drop-down list, choose the sensor device profile (backhaul) to apply to the device.
- Note** For Cisco Aironet 1800s Active Sensor, older than Software Release 1.3.1.2, make sure that you do not choose the sensor device profile **CiscoProvisioningSSID**. Instead, choose your own SSID for Backhaul purposes.
- If you made any changes, click **Save**, otherwise, click **Cancel** to return to the list and configure other devices.
 - You can apply a configuration that you assigned to one device to other devices of the same type by clicking **Apply ... to Other Devices** in the **Actions** column.
- Step 11** If any devices are a Cisco Catalyst 9800-CL Wireless Controller, click **Assign** next to **Image** in the **Configuration** column and follow these steps:
- (Optional) In the **Image** drop-down list, choose a golden software image to apply to the device. If there is only one golden image for this device type in the image repository, it is chosen by default.
 - Click **Save**.
- Step 12** If you selected multiple devices to provision, click **Assign** for the next device in the list and repeat the configuration, until you have done this for all devices.
- Step 13** Click **Next**.
The **Summary** window appears, where you can view details about the devices and configuration.
- Step 14** Check the **Day-0 Config** column for each device to see if the configuration preview was successful.
- If the preview shows an error, you can click on the **Actions** link in the error message above the table to see what actions you need to take. You can click on an action to open a new tab with the window where a change is needed. You must resolve any issues before claiming the device, to avoid provisioning errors. You may need to go back to the **Assign Configuration** step and change the configuration, revisit the **Design** area to update network design settings, or resolve any network connectivity issues. Once you have resolved the problem, you can go back to this tab and click the radio button **Retrying getting Day-0 configuration preview for failed device(s)**, and click **OK**. Ensure that the wireless LAN controller that is managing a device has been added to the inventory and assigned to the site where the wireless device is assigned.

- Step 15** Click **Claim**.
A confirmation dialog box is displayed.
- Step 16** Click **Yes** to claim the devices and start the provisioning process.
-

What to do next

To complete the provisioning process, after the device is added to the inventory, go to the **Inventory** tab, select the device and click **Actions > Provision > Provision Device**. Proceed through all the steps and click **Deploy** in the **Summary** step. In the **Summary**, you can see the remaining network settings that will be pushed to the device. For more information, see [Provision Wireless Devices, on page 23](#). This process is required if you intend to push the network settings that you may have configured in the **Design** area. During Plug and Play provisioning, only the device credentials and the Onboarding Configuration are pushed to the device; no other network settings are pushed until provisioning is completed from **Inventory**. Additionally, the device is added to ISE by Cisco DNA Center as a AAA client for RADIUS and TACACS, if these are configured.

Provision a Cisco DNA Traffic Telemetry Appliance

This procedure shows how to claim a Cisco DNA Traffic Telemetry Appliance from the Plug and Play Devices list.

Before you begin

- Ensure that Cisco network devices to be provisioned have a supported software release and are in a factory default state. If you are using a network device that was previously configured or is in an unknown state, see the device clean-up and reset details in the [Network Plug and Play Troubleshooting Guide for Cisco Digital Network Architecture Center](#).
- Ensure that the devices being provisioned can discover and contact Cisco DNA Center.
- Define the site within the network hierarchy. See [About Network Hierarchy](#).
- Define the CLI and SNMP credentials for the devices. If you are using SNMPv2c, you must provide both Read and Write credentials. See [About Device Credentials](#).




Note SNMPv3 Limitations:

- Supports SHA for Auth and AES128 for privacy.
 - Does not support MD5.
-
- If you want to deploy images, ensure that the software images for the devices to be provisioned are uploaded and marked as golden in the Image Repository. See [Import a Software Image](#).



Note The image deployment process that Plug and Play uses during Day-0 provisioning is not the same as the deployment process used when updating a device image later. For information, see [Provision a Software Image](#). During provisioning, Plug and Play performs no device prechecks, auto flash cleanup, or postchecks. Device must be in the factory default state.

- Define network profiles for the devices. See [Create Network Profile for Cisco DNA Traffic Telemetry Appliance](#).

-
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon () and choose **Provision > Plug and Play**.
- Step 2** View the devices in the table.
- You can use the **Filter** or **Find** option to find the Cisco DNA Traffic Telemetry Appliance.
- 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, **Assign Site**. If instead, you see a window that shows mandatory tasks such as defining a site and defining device credentials, you must click **Add Site** to define a site, and **Add device credentials** to define device credentials. These mandatory tasks are prerequisites for the claim process. After these tasks are completed, you can return to claiming a device by clicking **Refresh** in this window.
- Step 5** (Optional) Change the device hostname, if needed, in the first column.
- Step 6** From the **Select a Site** drop-down list, choose a site to assign to each device.
- To apply the same site as the first device to all other devices, click the **Apply Site to All** check box. To assign the site from any device to some other devices, click **Assign this Site to Other Devices**, choose the devices, and click **Assign**.
- Step 7** Click **Next**.
The **Assign Configuration** window appears.
- Step 8** In the **Configuration** column, click **Assign** for the device that you want to configure and follow these steps:
- a) View the device configuration summary and, if no changes are needed, click **Cancel**.
 - b) (Optional) In the **Device Name** field, change the device hostname, if needed.
 - c) (Optional) In the **Image** drop-down list, choose a golden software image to apply to the device. If there is only one golden image for this device type in the image repository, it is chosen by default.
 - d) If you made any changes, click **Save**. Otherwise, click **Cancel** to return to the list and configure other devices.
- Step 9** If you selected multiple devices to provision, click **Assign** for the next device in the list. Repeat the configuration steps, until you have configured all devices.
- Step 10** Click **Next**.
The **Summary** window appears, where you can view details about the devices and their configuration preview status.
- Step 11** Check the **Day-0 Config** column for each device to see if the configuration preview was successful.
- If the preview shows an error, you can click the **Actions** link in the error message above the table to see what actions you need to take. You can click an action to open a new tab with the window where a change is needed. To avoid provisioning errors, you must resolve any issues before claiming the device. You may need to revisit the **Design** area to update network design settings or resolve any network connectivity issues. After you resolve the problem, return to

this tab and click the **Retrying getting Day-0 configuration preview for failed device(s)** radio button. Then click **OK**.

Step 12 You can click the link in the **Day-0 Config** column to see more information about the device, its configuration, and any configuration preview errors.

Step 13 Click **Claim**.

A confirmation dialog box is displayed.

Step 14 Click **Yes** to claim the devices.

What to do next

To complete the provisioning process, after the device is added to the inventory, go to the **Inventory** tab, select the device and click **Actions > Provision > Provision Device**. Proceed through all the steps and click **Deploy** in the **Summary** step. In the **Summary** window, you can see the remaining network settings that are pushed to the device. For more information, see [Provision Wireless Devices, on page 23](#). This process is required if you intend to push the network settings that you may have configured in the **Design** area. During Plug and Play provisioning, only the device credentials and the Onboarding Configuration are pushed to the device; no other network settings are pushed until provisioning is completed from **Inventory**.

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 Devices list. 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 In the Cisco DNA Center GUI, click the **Menu** icon () and choose **Provision > Plug and Play**.

Step 2 View the devices in the table.

You can filter on device state by using one of the **Device State** buttons, or use the **Filter** option to find specific devices. Click **Refresh** to refresh the device list.

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 **Yes** to confirm that you want to delete the devices.

Reset a Device

Resetting a device applies only to devices in the Error state and resets its state to Unclaimed 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. On wireless and sensor devices, only the device state is reset and the device is not reloaded.

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

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

Step 2 View the devices in the table.

You can filter on device state by using one of the **Device State** buttons, or use the **Filter** option to find specific devices. Click **Refresh** to refresh the device list.

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**.

Provision Wireless Devices

The following sections provide information about how to provision various Cisco wireless devices.

About Wireless Devices and Country Codes

Controllers and access points are designed for use in many countries with varying regulatory requirements. The radios within the access points are assigned to a specific regulatory domain at the factory (such as -E for Europe), but the country code enables you to specify a particular country of operation within that regulatory domain (such as FR for France or ES for Spain). Configuring a country code ensures that each radio's broadcast frequency bands, interfaces, channels, and transmit power levels are compliant with country-specific regulations.

Cisco DNA Center provisions controllers with country codes according to the site they are assigned. In the case of controllers, they can be assigned to more than one site. So, they can be assigned more than one country code. During provisioning, Cisco DNA Center assigns sites to the controller along with the sites' country codes. For example, a controller that manages both India and US sites is assigned the IN and US country codes.

When access points are provisioned, they are assigned to a floor. If the access point is a ROW AP, Cisco DNA Center gets the country code for the site and assigns it to the AP. Any additional APs on the same floor are assigned the same country code.

The country code information is displayed on the device 360 page for controllers and access points.

For a complete list of country codes supported per product, see

<https://www.cisco.com/c/dam/assets/prod/wireless/wireless-compliance-tool/index.html>.

Provision a Cisco AireOS Controller

Before you begin

- Make sure that you have defined the following global network settings before provisioning a Cisco Wireless Controller:
 - Network servers, such as AAA, DHCP, and DNS.
For more information, see [Configure Global Network Servers](#).
 - Device credentials, such as CLI, SNMP, HTTP, and HTTPS.
For more information, see [Configure Global CLI Credentials](#), [Configure Global SNMPv2c Credentials](#), [Configure Global SNMPv3 Credentials](#), and [Configure Global HTTPS Credentials](#).
 - IP address pools.
For more information, see [Configure IP Address Pools](#).
 - Wireless settings, such as SSIDs, wireless interfaces, and wireless radio frequency profiles.
For more information, see [Configure Global Wireless Settings](#).
- Make sure that you have the Cisco Wireless Controller in your inventory. If not, use the **Discovery** feature to discover the controller.
- Make sure that the Cisco Wireless Controller is added to a site. For more information, see [Add a Device to a Site](#).
- You cannot reuse any pre-existing VLANs on devices. Provisioning fails if Cisco DNA Center pushes the same VLAN that already exists on the device.
- You cannot make any configuration changes to the wireless controller that is being managed by the Cisco DNA Center manually. You must perform all configurations from the Cisco DNA Center GUI.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision > Network Devices > Inventory**. The **Inventory** window appears, with the discovered devices listed.

Step 2 Expand the **Global** site in the left pane, and select the site, building, or floor that you are interested in.

The available devices in the selected site is displayed in the **Inventory** window.

- Step 3** From the **DEVICE TYPE** list, click the **WLCs** tab, and from the **Reachability** list, click the **Reachable** tab to get the list of wireless controllers that are discovered and reachable.
- Step 4** Check the check box next to the device name that you want to provision.
- Step 5** From the **Actions** drop-down list, choose **Provision > Provision Device**.
The **Assign Site** window appears.
- Step 6** Click **Choose a site** to assign a site for the wireless controller.
- Step 7** In the **Add Sites** window, check the check box next to the site name to associate the wireless controller, and click **Save**.
- Step 8** Click **Apply**.
- Step 9** Click **Next**.
The **Configuration** window appears.
- Step 10** Select a role for the wireless controller: **Active Main WLC** or **Guest Anchor WLC**.
- Step 11** Click **Select Primary Managed AP Locations** to select the managed AP location for the wireless controller.
- Step 12** 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, the children under that parent site automatically gets selected.
- Note** Inheritance of managed AP locations allows you to automatically choose a site along with the buildings and floors under that site. One wireless controller can manage only one site.
- Step 13** Click **Save**.
- Step 14** Under **Interface and VLAN Configuration**, click + **Add** and configure the interface and VLAN details for an active main wireless controller.
Interface and VLAN configuration is applicable for nonfabric wireless controller provisioning only.
The **Configure Interface and VLAN** window appears.
- Step 15** From the **Interface Name** drop-down list, choose the interface name.
- Step 16** In the **VLAN ID** field, enter a value for the VLAN.
- Step 17** In the **Interface IP Address** field, enter a value for the interface IP address.
- Step 18** In the **Interface Net Mask (in bits)** field, enter the subnet mask for the interface.
- Step 19** In the **Gateway IP Address** field, enter the gateway IP address.
- Step 20** From the **LAG/Port Number** drop-down list, choose the link aggregation or the port number.
- Step 21** Click **OK**.
- Step 22** (Optional) For a guest anchor wireless controller, change the VLAN ID configuration by changing the **VLAN ID** under **Assign Guest SSIDs to DMZ site**.
- Step 23** Under **Mobility Group**, click **Configure** to configure the wireless controller as the mobility peer.
The **Configure Mobility Group** side panel appears.
- Step 24** From the **Mobility Group Name** drop-down list, you can either add a new mobility group by clicking +, or choose a mobility group from the existing mobility groups.
The existing mobility peers information is loaded from the intent available in the Cisco DNA Center.
- Step 25** In the **RF Group Name** text box, enter a name for the RF group.
- Step 26** Under **Mobility Peers**, click **Add** to configure the wireless controller as a mobility peer.

- Step 27** From the **Device Name** drop-down list, choose the controller.
- After the device is provisioned, Cisco DNA Center creates a mobility group in the device, assigns the RF group, and configures all ends of peers. The mobility group configuration is deployed automatically to all the selected peer devices.
- Step 28** Click **Save**.
- Step 29** To reset the mobility group name and the RF group name, you can do one of the following:
- In the **Configure Mobility Group** side panel, choose **default** from the **Mobility Group Name** drop-down list.
 - On the **Provision > Configuration** page, under **Mobility Group**, click **Reset**.
- This automatically sets the **RF Group Name** to **default** and removes all peers. After provisioning, the mobility on the device is set and the device is removed from all other peers.
- Step 30** Click **Next**.
- The **Model Configuration** window appears.
- Step 31** In the **Devices** pane, you can either search for a model config design by entering its name in the **Find** field, or expand the device and select a model config design.
- The selected model config design appears in the right pane.
- Step 32** Check the check box next to the **Design Name** that you want to provision, and click **Configure** to edit the model config design.
- You cannot edit all the configurations at this step.
- Step 33** After making the necessary changes, click **Apply**.
- Step 34** Click **Next**.
- The **Advanced Configuration** window appears, where you can enter values for predefined template variables.
- Step 35** Search for the device or the template in the **Devices** panel.
- Step 36** Enter a value for the predefined template variable in the **wlanid** field.
- Step 37** Click **Next**.
- The **Summary** window displays the following information:
- **Device Details**
 - **Network Settings**
 - **SSID**
 - **Managed Sites**
 - **Interfaces**
 - **Advanced Configuration**
 - **Mobility Group Configuration**
 - **Model Config**
- Step 38** Click **Deploy** to provision the controller.
- Step 39** In the **Provision Devices** window, do the following to preview the CLI configuration:

- Click **Generate Configuration Preview** radio button.
- In the **Task Name** field, enter a name for the CLI preview task and click **Apply**.
- In the **Task Submitted** message, click the **Work Items** link.
Note If you didn't notice the **Task Submitted** message, click the **Menu** icon (☰) and choose **Activities > Work Items**.
- In the **Work Items** window, click the CLI preview task for which you submitted the configuration preview request.
- View the CLI configuration details and click **Deploy**.
- To immediately deploy the device, 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.
- In the **Information** pop-up, do the following:
 - Click **Yes**, if you want to delete the CLI preview task from the **Work Items** window.
 - Click **No**, if you want to retain the task in the **Work Items** window.
Note The CLI task will be marked as completed in the **Work Items** window. You can view the CLI configuration for this task but you cannot deploy it again.

Step 40 Provision the secondary controller.

Step 41 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 42 After the devices are deployed successfully, the **Provision Status** changes from **Configuring** to **Success**.

Step 43 In the **Device Inventory** window, click **See Details** in the **Provision Status** column to get more information about the network intent or to view a list of actions that you need to take.

Step 44 Click **See Details** under **Device Provisioning**.

Step 45 Click **View Details** under **Deployment of network intent**, and click the device name.

Step 46 Expand the **Configuration Summary** area to view the operation details, feature name, and the management capability. The configuration summary also displays any errors that occurred while provisioning the device.

Step 47 Expand the **Provision Summary** area to view details of the exact configuration that is sent to the device.

Configure Cisco Wireless Controller High Availability from Cisco DNA Center

Cisco Wireless Controller High Availability (HA) can be configured through Cisco DNA Center. Currently, both the formation and breaking of wireless controller HA is supported; switchover options are not supported.

Prerequisites for Configuring Cisco Wireless Controller High Availability

- The discovery and inventory features of wireless controller 1 and wireless controller 2 must be successful. The devices must be in Managed state.

- The service ports and the management ports of wireless controller 1 and wireless controller 2 must be configured.
- The redundancy ports of wireless controller 1 and wireless controller 2 must be physically connected.
- The management address of wireless controller 1 and wireless controller 2 must be in the same subnet. The redundancy management address of wireless controller 1 and wireless controller 2 must also be in the same subnet.
- Manually configure the following boot variables on the wireless controller:

```

config t
boot system bootflash::<device_iosxe_image_filename>
config-register 0x2102

show boot. (IOSXE cli)

BOOT variable = bootflash:<device_iosxe_image_filename>,12;
Configuration register is 0x2102

```

Configure Cisco Wireless Controller HA

- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision > Network Devices > Inventory**. The **Inventory** window appears, with the discovered devices listed.
- Step 2** Check the check box next to the controller name that you want to configure as the primary controller.
- Step 3** From the **Actions** drop-down list, choose **Provision > Configure WLC HA**. The **High Availability** page appears.
- Step 4** Enter the **Redundancy Management IP** and the **Peer Redundancy Management IP** address in the respective text boxes.
- 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 Cisco Wireless Controller. Ensure that these IP addresses are unused IP addresses within that subnet range.
- Step 5** From the **Select Secondary WLC** drop-down list, choose the secondary controller.
- Note** When you select secondary controller, based on the wireless management interface IP subnet of primary controller, redundancy management IP auto populates and an **i** icon appears on the top of **High Availability** window, saying **Please make sure the Redundancy Management IP and Peer Redundancy Management IP are not assigned to any other network entities. If used, kindly change the IP accordingly and configure.**
- Step 6** Click **Configure HA**. The HA configuration is initiated in the background using the CLI commands. First, the primary wireless controller is configured. On success, the secondary wireless controller is configured. After the configuration is complete, both wireless controllers reboot. This process may take up to 2.5 minutes to complete.
- Step 7** To verify the HA configuration, on the **Devices > Inventory** page, click the device that you configured as a HA device.
- Step 8** Click the **Wireless Info** tab. The **Redundancy Summary** displays the **Sync Status** as **In Progress**. When Cisco DNA Center finds that HA pairing succeeded, the **Sync Status** changes to **Complete**.

This is triggered by the inventory poller or by manual resynchronization. By now, the secondary wireless controller (wireless controller 2) is deleted from Cisco DNA Center. This flow indicates successful HA configuration on the wireless controller.

What Happens During or After the High Availability Process is Complete

1. Cisco wireless controller 1 and wireless controller 2 are configured with redundancy management, redundancy units, and SSO. The wireless controllers reboot in order to negotiate their role as active or stand by. Configuration is synced from active to stand by.
2. On the **Show Redundancy Summary** window, you can see these configurations:
 - SSO is Enabled
 - Wireless Controller is in Active state
 - Wireless Controller is in Hot Stand By state
3. The management port of the active wireless controller is shared by both the controllers and will be pointing to active controller. The user interface, Telnet, and SSH on the stand by wireless controller will not work. You can use the console and service port interface to control the stand by wireless controller.

Commands to Configure and Verify High Availability

Cisco DNA Center sends the following commands to configure Cisco Wireless Controller HA.

Cisco DNA Center sends the following commands to wireless controller 1:

- **config interface address redundancy-management 198.51.100.xx peer-redundancy-management 198.51.100.yy**
- **config redundancy unit primary**
- **config redundancy mode sso**

Cisco DNA Center sends the following commands to wireless controller 2:

- **config interface address redundancy-management 198.51.100.yy peer-redundancy-management 198.51.100.xx**
- **config redundancy unit secondary**
- **config port adminmode all enable**
- **config redundancy mode sso**

Enter the following commands to verify the HA configuration from the wireless controller:

- To check HA-related details: **config redundancy mode sso**
- To check the configured interfaces: **show redundancy summary**

Disable High Availability Configured Brownfield Device from Cisco DNA Center

The Cisco DNA Center disable high-availability feature is supported on Cisco Catalyst 9800 Series Wireless Controllers and Cisco AireOS Controllers.

Before you begin

Ensure that the high availability brownfield device is configured outside of Cisco DNA Center.

-
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision > Device > Inventory**.
The **Inventory** window appears, with the discovered devices listed.
- Step 2** Check the check box next to the name of the wireless controller that has the high-availability feature that you want to disable.
- Step 3** From the **Actions** drop-down list, choose **Provision > Configure WLC HA**.
The **High Availability** page appears.
High Availability page shows the **REDUNDANCY SUMMARY** of selected wireless controller configured from outside Cisco DNA Center.
- Step 4** In the **Warning** window, click **OK**.
A success message appears at the bottom of the screen indicating that high availability has been successfully disabled for the selected wireless controller.
-

Provision a Cisco AP—Day 1 AP Provisioning

Before you begin

Make sure that you have Cisco APs in your inventory. If not, use the Discovery feature to discover APs. For more information, see [Discover Your Network](#).

-
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision > Network Devices > Inventory**.
The **Inventory** window displays the device information that is gathered during the Discovery process.
- Note** You can either search for a site by entering its name or expand **Global** to select the site. Devices that are available in the selected site are displayed in the **Inventory** window.
To filter the devices based on various criteria, such as **Device Family** or **Reachability Status**, click **Filter**, make your selections, then click **Apply**.
- Step 2** Check the check box next to the AP that you want to provision.
- Step 3** From the **Action** drop-down list, choose **Provision > Provision Device**.
- Step 4** In the **Assign Site** step, configure the following parameters:
- Click **Choose a floor** and assign an AP to the site.
 - In the **Choose a floor** slide-in pane, select the floor where the AP resides, and click **Save**.

c) Click **Next**.

Step 5 In the **Configuration** step, configure the following parameters:

a) Click **Advanced Configuration** to configure radio antenna profiles on antenna slots.

Note Advanced configuration is supported on Cisco Catalyst 9130AXE Unified Access Points with Cisco Catalyst 9800 Series Wireless Controller software release 17.6 or later.

b) Configure the beam selection value for AP radio slot 1 and slot 2 from the **Slot 1** and **Slot 2** drop-down list.

c) Click **Save**.

d) In the **RF Profile** drop-down list, leave the default setting or choose a different value from the list. The options are **High**, **Typical**, and **Low**.

The default RF profile is the custom profile that you marked as default under **Design > Network Settings > Wireless > Wireless Radio Frequency Profile**.

e) In the **Mesh Role** drop-down list, choose **Root** or **Mesh**.

f) Click **Next**.

Step 6 In the **Summary** step, review the device details, and click **Deploy** to provision the AP.

The **Provision Device** slide-in pane appears.

Step 7 In the **Provision Device** slide-in pane, do the following:

- To immediately deploy the device, 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.
- To preview the CLI configuration, click the **Generate Configuration Preview** radio button.

Step 8 You are prompted with a message that creation or modification of an AP group is in progress, and then a message that APs will reboot after provisioning. Click **OK**.

The **Last Sync Status** column in the **Inventory** window shows **SUCCESS** for a successful deployment.

Enable ICMP Ping on APs in FlexConnect Mode

You can enable Internet Control Message Protocol (ICMP) ping on APs that are in FlexConnect mode and in an unreachable state. Cisco DNA Center uses the ICMP to ping FlexConnect APs that are in unreachable state every five minutes to enhance reachability and then updates the reachability status in the **Inventory** window.

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

Step 2 Check the **Enable ICMP ping for unreachable access points in FlexConnect mode** check box to enable the ICMP ping.

Step 3 Click **Save**.

A success message saying ICMP Ping status updated successfully appears.

Cisco DNA Center starts pinging FlexConnect APs that are disassociated from Cisco Wireless Controller but are reachable. You can view the reachability status in the **Inventory** window.

Step 4 To view the reachability status, choose **Provision > Inventory**.

Step 5 The **Reachability** column shows **Ping Reachable** when the device is reachable by the ICMP ping.

Day 0 Workflow for Cisco AireOS Mobility Express APs

Before you begin

The Cisco Mobility Express wireless network solution comprises at least one 802.11ac Wave 2 Cisco Aironet Series access point with an in-built, software-based wireless controller managing other APs in the network. The AP acting as the wireless controller is referred to as the *primary AP*. The other APs in the Cisco Mobility Express network, which are managed by this primary AP, are referred to as *subordinate APs*.

- Design your network hierarchy with sites, buildings, floors, and so on. For more information, see [Create a Site in a Network Hierarchy](#), [Add a Building](#), and [Add a Floor to a Building](#).
- Define the device credentials, such as CLI, SNMP, HTTP, and HTTPS at the global level. The credentials that are defined at the global level are inherited by the sites. For more information, see [Configure Global CLI Credentials](#), [Configure Global SNMPv2c Credentials](#), and [Configure Global SNMPv3 Credentials](#).
- Create WLANs, interfaces, and RF profiles.
- Configure the DHCP server with Option #43 or Option #60. This is the IP address of the Cisco DNA Center Plug and Play server. Using this IP address, the APs contact the PnP server and download the configuration.
- Make sure that you have Mobility Express APs in the inventory. If not, discover them using the Discovery feature. For more information, see [Discover Your Network Using CDP](#), [Discover Your Network Using an IP Address Range](#), and [About Inventory](#).
- The APs should be in the factory reset state without any Cisco Wireless Controller configurations.

Step 1 The Cisco Mobility Express contacts the DHCP server and connects to the Cisco DNA Center Plug and Play server.

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

Step 3 The Mobility Express AP starts the PnP agent and contacts the PnP server.

Note If you have a set of Mobility Express APs in the network, they go through an internal protocol. The protocol selects one Mobility Express AP, which will be configured on the Cisco Wireless Controller as the primary AP to reach the PnP server.

Step 4 Find the unclaimed AP in the **Provision > Network Devices > Plug and Play** tab.

The table lists all the unclaimed devices. The **State** column shows as **Unclaimed**. Use the **Filter** or **Find option** to find specific devices.

You must wait for the **Onboarding Status** to become **Initialized**.

Step 5 To claim the AP, check the check box next to the AP device name.

- Step 6** Choose **Actions > Claim** in the menu bar above the device table.
The **Claim Devices** window appears.
- Step 7** In the **Site Assignment** window, choose a site from the **Site** drop-down list.
Claiming the selected AP to this particular site also applies the associated configurations.
- Step 8** Click **Next**.
- Step 9** To configure a device, click the device name in the **Configuration** window.
- Step 10** In the **Configuration for device name** page, assign the static IP details for the device:
- **Management IP**
 - **Subnet Mask**
 - **Gateway**
- Step 11** Click **Save**.
- Step 12** Click **Next**.
The **Summary** page appears.
- Step 13** Click **Claim** in the **Summary** page.
After the Mobility Express AP is claimed, the IP address configured is assigned to the Mobility Express AP.
The claimed device, which is an AP, and the wireless controller are now available under **Provision > Device Inventory > Inventory**.
- Step 14** (Optional) Add devices in bulk from a CSV file.
For more information, see [Add Devices in Bulk, on page 10](#).
When you bulk import Mobility Express APs through a CSV, all the Mobility Express APs appear on the **Devices > Plug and Play** page. Based on the VRRP protocol, only one Mobility Express AP among the imported ME APs becomes the primary AP. The remaining APs become subordinate APs. After claiming the primary AP, you don't need to claim the subordinate APs. Cisco DNA Center does not clear the subordinate APs from the Plug and Play page. You must delete those subordinate APs manually from the **Devices > Plug and Play** page.
- Step 15** To provision the Cisco Wireless Controller, see [Provision a Cisco AireOS Controller, on page 24](#).
-

Brownfield Support for Cisco AireOS Controllers

Before you begin

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

This procedure shows how to provision a brownfield Cisco AireOS Controller with Cisco DNA Center.


- 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** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision > Network Devices > Inventory**.
The **Inventory** window appears, with the discovered devices listed.
- Step 2** 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 3** Check the check box next to the wireless controller device name that you want to provision.
- Step 4** From the **Action** drop-down list, choose **Provision > Learn Device Config**.
- Step 5** Associate a site to the controller in the **Assign Site** step:
- Click **Choose a site** to assign a site to the controller.
 - In the **Choose a site** slide-in pane, select a site to which you want to associate the wireless controller, and click **Save**.
 - Click **Next**.
- Step 6** The **Resolve Conflict** step shows any conflicting configurations in Cisco DNA Center that you need to resolve.
- Step 7** Click **Next**.
- Step 8** The **Design Object** window lists all the learned configurations.
- Click **Network** in the left pane.
The right pane displays network 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.
 - **DHCP Server** details.
 - Enter the **Shared Secret** for the AAA server.
 - Click **Wireless** in the left pane.
The right pane lists the enterprise SSIDs, guest SSIDs, antenna radio profiles, and wireless interface details.
For an SSID with a preshared key (PSK), enter the **passphrase key**.
 - 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
 - Click **Next**.
The **Network Profile** window lists the network profile or site profile that is created based on the AP and WLAN combination.
 - Click **Save**.
A message saying **Brownfield Configuration is Successful** is displayed.

Step 9 Choose **Design > Network Profiles** to assign a site to the network profile.

Step 10 In the **Network Profiles** window, configure the following:

- a) Click **Assign Site** to add sites to the selected profile.
- b) In the **Add Sites to Profile** window, choose a site from the drop-down list, and click **Save**.

Step 11 In the Cisco DNA Center GUI, click the **Menu** icon () and choose **Provision > Network Devices > Inventory**.

- a) Click **Filter** to locate the device that you want to provision.

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

- b) Check the check box next to the controller device name that you want to provision.
- c) From the **Action** drop-down list, choose **Provision**.
- d) Review the details in the **Assign Site** window, and click **Next**.

The **Configurations** step appears.

- e) Under **Interface and VLAN Configuration**, click **+Add** to configure interface and VLAN details.
- f) In the **Configure Interface and VLAN** window, configure the required fields, and click **OK**.
- g) Click **Next**.


Step 12 Review the **Summary** step which displays the following information:

- **Device Details**
- **Network Setting**
- **SSID**
- **Managed Sites**
- **Interfaces**

Step 13 Click **Deploy**.

Step 14 In the **Provision Devices** slide-in pane, do the following to preview the CLI configuration:

- Click the **Generate Configuration Preview** radio button.
- In the **Task Name** field, enter a name for the CLI preview task and click **Apply**.
- In the **Task Submitted** pop-up, click the **Work Items** link.

Note If you missed the **Task Submitted** pop-up, click the **Menu** icon () and choose **Activities > Work Items**.

- In the **Work Items** window, click the CLI preview task for which you submitted the configuration preview request.
- View the CLI configuration details and click **Deploy**.
- To immediately deploy the device, 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.
- In the **Information** pop-up, do the following:
 - Click **Yes** if you want to delete the CLI preview task from the **Work Items** window.
 - Click **No** if you want to retain the task in the **Work Items** window.

Note The CLI task will be marked as completed in the **Work Items** window. You can view the CLI configuration for this task, but you cannot deploy it again.

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 Hyper-V) and manageable by Cisco DNA Center.
- Catalyst 9800 Embedded Wireless Controller for Catalyst 9300 Series Switches, Catalyst 9400 Series Switches, and Catalyst 9500H Series Switches.
- Cisco Catalyst 9800-L Wireless Controller: Provides seamless software updates for small- to mid-size enterprises. The Cisco Catalyst 9800-L Wireless Controller is available in two variations. You can choose between copper and fiber uplinks, which gives you flexibility in your network.

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

Platform	Description
Cisco Catalyst 9800-80 Wireless Controller	Supports up to 6000 access points and 64,000 clients. Supports up to 80 Gbps throughput and occupies a 2-rack unit space. Modular wireless controller with up to 100-GE uplinks and seamless software updates.
Cisco Catalyst 9800-40 Wireless Controller	A fixed wireless controller with seamless software updates for mid-sized organizations and campus deployments. Supports up to 2000 access points and 32,000 clients. Supports up to 40 Gbps throughput and occupies a 1-rack unit space. Provides four 1-GE or 10-GE uplink ports.

Platform	Description
Cisco Catalyst 9800-CL Cloud Wireless Controller	<p>Cisco Catalyst 9800-CL Cloud Wireless Controller can be deployed in a private cloud or a public cloud as Infrastructure as a Service (IaaS).</p> <p>Cisco Catalyst 9800-CL Cloud Wireless Controller is the next generation of enterprise-class virtual wireless controllers built for high availability and security.</p> <p>A virtual form factor of Cisco Catalyst 9800-CL Cloud Wireless Controller for private cloud supports ESXi, KVM, Cisco ENCS, and Hyper-V hypervisors.</p>
Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches	<p>Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches bring the wired and wireless infrastructure together with consistent policy and management.</p> <p>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.</p>
Cisco Catalyst 9800-L Wireless Controller	<p>Cisco Catalyst 9800-L Wireless Controller provides seamless software updates for small to mid-size enterprises. The Cisco Catalyst 9800-L Wireless Controller is available in two variations. You can choose between copper and fiber uplinks, which gives you flexibility in your network.</p> <ul style="list-style-type: none"> • Cisco Catalyst 9800-L Copper Series Wireless Controller (9800-L-C RJ45) • Cisco Catalyst 9800-L Fiber Series Wireless Controller 9800-L-F SFP)

The following table lists the host environments supported by the Cisco Catalyst 9800 Series Wireless Controller:

Host Environment	Software Version
VMware ESXi	<ul style="list-style-type: none"> • VMware ESXi vSphere 6.0 • VMware ESXi vSphere 6.5¹ • VMware ESXi vCenter 6.0 • VMware ESXi VCenter 6.5
KVM	<ul style="list-style-type: none"> • Linux KVM based on Red Hat Enterprise Linux 7.1 and 7.2 • Ubuntu 14.04.5 LTS, Ubuntu 16.04.5 LTS
NFVIS	Cisco ENCS 3.8.1 and 3.9.1

¹ 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 Cisco Enterprise Network Function Virtualization Infrastructure Software (NFVIS) versions supported in Cisco DNA Center:



Note Cisco Enterprise NFVIS devices support the N-1 to N upgrade path only. For example, upgrade from Cisco Enterprise NFVIS 3.11.x to Cisco Enterprise NFVIS 3.12.x only is supported. Upgrade from Cisco Enterprise NFVIS 3.11.x to Cisco Enterprise NFVIS 4.1.x is not supported.

Cisco Enterprise NFVIS Version	Enterprise Network Compute System Device Platform	Notes
4.1.2	ENCS 5400	Cisco DNA Center supports the following NFVIS upgrade paths: NFVIS v3.11.1 > 3.11.2 > 3.11.3 > 3.12.3 > 4.1.1 > 4.1.2. Cisco Enterprise NFVIS 3.12.1 is not supported on any versions of Cisco DNA Center. Upgrade to Cisco Enterprise NFVIS 3.12.1 from Cisco Enterprise NFVIS 3.11.x using Cisco DNA Center is not supported. Upgrade to Cisco Enterprise NFVIS 3.12.2 from Cisco Enterprise NFVIS 3.12.1 using Cisco DNA Center is not supported. Upgrade to Cisco Enterprise NFVIS 3.12.2 from 3.11.2 is supported using Cisco DNA Center. Cisco Enterprise NFVIS 3.12.2 is supported on Cisco DNA Center.
4.1.1	UCS-E	
3.12.3	UCS-C	
3.11.3		
3.11.2		
3.11.1		
3.12.2	ENCS 5100	Cisco 5100 ENCS does not support Cisco Enterprise NFVIS 3.10.x.
3.11.3		
3.11.2		
3.11.1		

Workflow to Configure a Cisco Catalyst 9800 Series Wireless Controller in Cisco DNA Center

1. Install Cisco DNA Center.
For more information, see the [Cisco DNA Center Installation Guide](#).
2. For information on software image upgrade, see [Software Image Upgrade Support for Cisco Catalyst 9800 Series Wireless Controller, on page 41](#).
3. Log in to the Cisco DNA Center GUI and verify that the applications you need are in the **Running** state.
In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **System Settings > Software Updates > Installed Apps**.
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 are pushed to Cisco ISE.
5. Discover the Cisco Catalyst 9800 Series Wireless Controller.
You must enable NETCONF and set the port to 830 to discover the Cisco Catalyst 9800 Series Wireless Controller. 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 must add the wireless management IP address manually.

While performing discovery using the Cisco Discovery Protocol (CDP) or an IP address range in the **Discovery** window, 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 Cisco 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

  ID           Type      State      Filter type
  -----
  1011         Configured Valid      tdl-uri
  1012         Configured Valid      tdl-uri
  1013         Configured Valid      tdl-uri
```

- **#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 a TACACS server while configuring authentication and policy servers.

Configuring TACACS is not mandatory if you have configured the username locally on the Cisco 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 it 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 a Building](#), and [Add a Floor to a Building](#).

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

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 [Manage 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.

To create an IP address pool, see [Configure IP Address Pools](#).

You must reserve an IP address pool for the building that you are provisioning. For more information, see [Provision a LAN Underlay](#).

14. Create enterprise and guest wireless networks. Define the global wireless settings once; Cisco DNA Center then pushes the configurations to various devices across geographical locations.

Designing a wireless network is a two-step process. First, you must create SSIDs, and 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](#). For information about other wireless settings, see [Configure Global Wireless Settings](#).

15. Configure the backhaul settings. For more information, see [Manage Backhaul Settings](#).

16. Configure the following in the **Policy** window for the Cisco 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](#).
- Create a group-based access control policy and add a contract. For more information, see [Create Group-Based Access Control Policy](#).

17. Configure high availability.
For more information, see [Configure High Availability for the Cisco Catalyst 9800 Series Wireless Controller, on page 42](#).
18. Provision the Cisco Catalyst 9800 Series Wireless Controller with the configurations added during the design phase.
For more information, see [Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 55](#).
19. Configure and deploy application policies on the Cisco Catalyst 9800 Series Wireless Controller.
For more information, see [Create an Application Policy](#), [Deploy an Application Policy](#), and [Edit an Application Policy](#).



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

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

For Cisco 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.

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 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 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design > Image Repository**.

The **Inventory** window appears, with the discovered devices listed.

Step 2 Import 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** Provision the software image.
- In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision > Device > Inventory**.
- Step 6** In the **Inventory** window, check the check box next to the Cisco Catalyst 9800 Series Wireless Controller whose image you want to upgrade.
- Step 7** From the **Actions** drop-down list, choose **Software Image > Update Image**.
- For more information, see [Provision a Software Image](#).
-

Configure High Availability for the Cisco Catalyst 9800 Series Wireless Controller

Before you begin

Configuring High Availability (HA) on the Cisco Catalyst 9800 Series Wireless Controller involves the following prerequisites:

- Both the Cisco Catalyst 9800 Series Wireless Controller devices are running the same software version and have active software image on the primary Catalyst 9800 Series Wireless Controller.
 - The service port and the management port of Catalyst 9800 Series Wireless Controller 1 and Catalyst 9800 Series Wireless Controller 2 are configured.
 - The redundancy port of Catalyst 9800 Series Wireless Controller 1 and Catalyst 9800 Series Wireless Controller 2 are physically connected.
 - Preconfigurations such as interface configurations, route addition, ssh line configurations, netconf-yang configurations are completed on the Catalyst 9800 Series Wireless Controller appliance.
 - The management interface of Catalyst 9800 Series Wireless Controller 1 and Catalyst 9800 Series Wireless Controller 2 are in the same subnet.
 - The discovery and inventory of Catalyst 9800 Series Wireless Controller 1 and Catalyst 9800 Series Wireless Controller 2 devices are successful from Cisco DNA Center.
 - The devices are reachable and are in **Managed** state.
-

- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision > Network Devices > Inventory**. The **Inventory** window appears, with the discovered devices listed.
- Step 2** To view devices available in a particular site, expand the **Global** site in the left pane, and select the site, building, or floor that you are interested in.
- All the devices available in that selected site is displayed in the **Inventory** window.
- Step 3** From the **Device Type** list, click the **WLCs** tab, and from the **Reachability** list, click the **Reachable** tab to get the list of wireless controllers that are discovered and reachable.

- Step 4** In the Inventory window, click the desired Cisco Catalyst 9800 Series Wireless Controller name to configure as a primary controller.
- Step 5** Click the **High Availability** tab.
- The selected Catalyst 9800 Series Wireless Controller by default becomes the primary controller and the **Primary C9800** field is grayed out.
- Step 6** 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 7** From the **Select Secondary C9800** drop-down list, choose the secondary controller to create a HA pair.
- Note** When you select secondary controller, based on the wireless management interface IP subnet of primary controller, redundancy management IP auto populates and an **i** icon appears on the top of **High Availability** window, saying **Please make sure the Redundancy Management IP and Peer Redundancy Management IP are not assigned to any other network entities. If used, kindly change the IP accordingly and configure.**
- Step 8** 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 Cisco Catalyst 9800 Series Wireless Controller. Ensure that these IP addresses are unused IP addresses within the subnet range.
- Step 9** In the **Netmask** field, enter the netmask address.
- Step 10** 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 11** 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 **SyncStatus** becomes **Complete**.
- This is triggered by the inventory poller or by manual resynchronization. By now, the secondary controller (Catalyst 9800 Series Wireless Controller 2) is deleted from Cisco DNA Center. This flow indicates successful HA configuration in the Catalyst 9800 Series Wireless Controller.
- Step 12** To manually resynchronize the controller, on the **Provision > Inventory** window, select the controller that you want to synchronize manually.
- Step 13** From the **Actions** drop-down list, choose **Resync**.
- Step 14** The following is the list of actions that occur after the process is complete:

- Catalyst 9800 Series Wireless Controller 1 and Catalyst 9800 Series Wireless 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
 - Catalyst 9800 Series Wireless Controller 1 is in active state
 - Catalyst 9800 Series Wireless Controller 2 is in standby state

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 for the Cisco Catalyst 9800 Series Wireless Controller through Cisco DNA Center.

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

Step 1 Use the following commands to configure HA on primary for 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 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 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 Controller:

- 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.

N+1 High Availability

Overview of N+1 High Availability

Cisco DNA Center supports N+1 High Availability (HA) on Cisco Wireless Controller and Cisco Catalyst 9800 Series Wireless Controller platforms.

N+1 HA with HA-SKU is supported on the Cisco 2504, 5500, 7500, and 8500 Series of standalone wireless controllers and WiSM2 controllers.

The N+1 HA architecture provides redundancy for controllers across geographically separated data centers with low-cost deployments.

N+1 HA allows a single Cisco Wireless Controller to be used as a backup controller for multiple primary controllers. These wireless controllers are independent of each other and do not share configuration or IP addresses on any of their interfaces.

Cisco DNA Center supports primary and secondary controller configurations for N+1 HA.

N+1 HA is configured at the AP level, not at the global level. Configurations are pushed directly to the AP.

When a primary wireless controller resumes operation, the APs fall back automatically from the backup wireless controller to the primary wireless controller if the AP fallback option is enabled.



Note The primary and secondary controllers must be of the same device type. For example, if the primary device is a Catalyst 9800 Series Wireless Controller, the secondary device must also be a Catalyst 9800 Series Wireless Controller.

APs with higher priority on the primary controller always connect first to the backup controller, even if they have to push out the lower priority APs.

The N+1 HA configuration has the following limitations:


- Auto provisioning of a secondary controller is not supported because of the VLAN ID configuration.
- You must reprovision the secondary controller manually with the latest design configuration if you made any changes to the primary controller.
- Cisco DNA Center does not support fault tolerance.
- Access Point Stateful Switch Over (AP SSO) functionality is not supported for N+1 HA. The AP Control and Provisioning of Wireless Access Points (CAPWAP) state machine is restarted when the primary controller fails.

Prerequisites for Configuring N+1 High Availability from Cisco DNA Center

- Discover primary and the secondary controller by running the **Discovery** feature.
For more information, see [Discover Your Network Using CDP](#), or [Discover Your Network Using an IP Address Range](#).
- Make sure that the wireless controllers are reachable and in the managed state.
For more information, see [About Inventory](#) and [Display Information About Your Inventory](#).
- Verify the network connectivity between devices. If the primary controller goes down, the AP should be able to join the secondary controller as per the N+1 configuration.
- Create two buildings to manage the primary and secondary locations for both devices. For example, create two buildings, *Building A* and *Building B*, where Building A is the primary managed location for controller-1 and also the secondary managed location for controller-2, and Building B is configured only as a primary managed location for controller-2.
For more information, see [Create a Site in a Network Hierarchy](#), [Add a Building](#), and [Add a Floor to a Building](#).
- Add and position APs on a floor map to get a coverage heatmap visualization during the design phase.
For more information, see [Add, Position, and Delete APs](#).
- Create two SSIDs and associate them as the backhaul SSIDs.
For more information, see [Create SSIDs for an Enterprise Wireless Network](#) and [Create SSIDs for a Guest Wireless Network](#).

Configure N+1 High Availability from Cisco DNA Center

This procedure shows how to configure N+1 High Availability (HA) on Cisco Wireless Controller and Cisco Catalyst 9800 Series Wireless Controller.

-
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon () and choose **Provision > Network Devices > Inventory**.
The **Inventory** window appears, with the discovered devices listed.
- Step 2** Check the check box next to the desired controller to provision it as a primary controller.
- Step 3** From the **Actions** drop-down list, choose **Provision > Provision**.
The **Assign Site** window appears.
- Step 4** Click **Choose a site** to assign a primary managed AP location for the primary controller.
- Step 5** In the **Choose a site** window, select a site and click **Save**.
- Step 6** Click **Next**.
The **Configuration** window appears, which displays the primary AP managed location for the primary device.
- Step 7** Add or update the managed AP locations for the primary controller by clicking **Select Primary Managed AP Locations**.
- Step 8** In the **Managed AP Location** window, check the check box next to the site name, and click **Save**.
You can either select a parent site or the individual sites.
- Step 9** Configure the interface and VLAN details.
- Step 10** Under **Configure Interface and VLAN** area, configure the IP address and subnet mask details, and click **Next**.
- Step 11** In the **Advanced Configuration** window, configure values for the predefined template variables, and click **Next**.
- Step 12** In the **Summary** window, verify the managed AP locations for the primary controller and other configuration details, and click **Deploy**.
- 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 13** Next, provision the secondary controller.
- Step 14** On the **Inventory** window, check the check box next to the desired controller to provision it as a secondary controller.
- Step 15** From the **Actions** drop-down list, choose **Provision > Provision**.
The **Assign Site** window appears.
- Step 16** Click **Choose a site** to assign the managed AP location for the secondary controller.
The managed AP location for the secondary controller should be same as the managed AP location of the primary controller.
- Step 17** In the **Choose a site** window, check the check box next to the site name to associate the secondary controller, and click **Save**.
- Step 18** Click **Next**.
The **Configuration** window appears, which displays the primary AP managed and secondary AP managed locations for the secondary device.

- Step 19** Add or update the managed AP locations for the secondary controller by clicking **Select Secondary Managed AP Locations**.
- Step 20** In the **Managed AP Location** window, check the check box next to the site name, and click **Save**.
You can either select a parent site or the individual sites.
- Step 21** Configure the interface and VLAN details for the secondary controller.
- Step 22** Under the **Configure Interface and VLAN** area, configure the IP address and subnet mask details for the secondary controller, and click **Next**.
- Step 23** In the **Advanced Configuration** window, configure values for the predefined template variables, and click **Next**.
- Step 24** In the **Summary** window, verify the managed AP locations for the secondary controller and other configuration details and click **Deploy**.
- 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** To verify the managed locations of the primary and secondary controllers, click the device name of the controllers that you provisioned on the **Provision > Network Devices > Inventory** window.
- Step 26** In the **Device details** window, click the **Managed ap locations** tab to view the primary and secondary managed location details.
- Step 27** Provision the AP for the primary controller.
- Step 28** On the **Network Devices > Inventory** window, check the check box next to the AP that you want to provision.
- Step 29** From the **Action** drop-down list, choose **Provision > Provision**.
- Step 30** In the **Assign Site** window, click **Choose a Floor** to select the floor from the primary managed location.
- Step 31** Click **Next**.
The **Configuration** window appears.
- Step 32** By default, the custom RF profile that you marked as the default under **Design > 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.
- Step 33** Click **Next**.
- Step 34** In the **Summary** window, review the details.
- Step 35** Click **Deploy** to provision the primary AP.
- Step 36** You are prompted with a message that creation or modification of an AP group is in progress.
You are prompted with a message stating `After provisioning AP(s) will reboot. Do you want to continue?`.
- Step 37** Click **OK**.
When deployment succeeds, the **Last Sync Status** column in the **Device Inventory** window shows `SUCCESS`.
-

Mobility Configuration Overview

The mobility configuration in Cisco DNA Center allows you to group a set of Cisco Wireless Controllers into a mobility group for a seamless roaming experience of wireless clients.

By creating a mobility group, you can enable multiple wireless controllers in a network to dynamically share information and forward traffic when inter-controller or inter-subnet roaming occurs. Mobility groups enable you to limit roaming between different floors, buildings, or campuses in the same enterprise by assigning different mobility group names to different wireless controllers within the same wireless network.

Cisco DNA Center allows you to create mobility groups between various platforms such as Cisco Catalyst 9800 Series Wireless Controller and Cisco AireOS Controllers.

Mobility configuration has the following guidelines and limitations:

- You cannot select multiple controllers for configuring mobility on the **Provision** page.
- You cannot create mobility groups with the group name as default. This resets the mobility and RF group names as default and deletes all the peers.
- You cannot configure a mobility group name on the anchor controller.
- You must reboot the wireless controller manually if there is change to the virtual IP address when configuring mobility groups on Cisco AireOS Controllers.
- Wireless controllers with the same mobility group name are automatically grouped into a single mobility group and are added as peers to each other.
- When configuring mobility groups on Cisco AireOS Controllers, if the wireless controllers do not have the IP address 192.0.2.1, Cisco DNA Center pushes the virtual IP address 192.0.2.1 to all the wireless controllers.
- Do not explicitly add guest anchor controllers to the mobility group. The provisioned guest anchor controllers do not appear in the drop-down list while adding peers in the mobility configuration page.
- If you provision a wireless controller as a guest anchor, ensure that it is not added to the mobility group.

Mobility Configuration Workflow

Here is the workflow that you can follow to configure mobility on Cisco Wireless Controller:

- To configure mobility, you must provision a wireless controller with mobility group name, RF group name, and mobility peers.
- The configuration that is applied during the wireless controller provisioning is automatically replicated to all the mobility peers configured in that group.
- Resynchronize the wireless controllers to get the latest tunnel status.

Mobility Configuration Use Cases

The following use cases explain the steps to configure mobility between controllers.

Use Case 1

Cisco Wireless Controller 1, wireless controller 2, and wireless controller 3 are newly added to Cisco DNA Center with the mobility group name as Default and is not provisioned yet.

1. Provision the wireless controller 1 by configuring mobility group name, RF group name, and adding wireless controller 2 and wireless controller 3 as peers.
2. Provision the wireless controller 2.
In the **Provision** window, the mobility configuration is automatically populated for wireless controller 2 with the group name and peers.
3. Provision the wireless controller 3.
4. After provisioning all wireless controllers, resynchronize the wireless controllers to receive the latest tunnel status.

Use Case 2

Cisco Wireless Controller 1, wireless controller 2, and wireless controller 3 with different mobility group names are already added to Cisco DNA Center and are provisioned.

1. Provision the wireless controller 1 by configuring mobility group name, RF group name, and adding wireless controller 2 and wireless controller 3 as peers.
2. The mobility configuration is automatically replicated across other peers, such as wireless controller 2 and wireless controller 3.
 - After the successful provisioning of wireless controller 1, the wireless controller 2 and wireless controller 3 are added as peers on the wireless controller 1.
 - The wireless controller 1 and wireless controller 3 are added as peers on wireless controller 2.
 - The wireless controller 1 and wireless controller 2 are added as peers on wireless controller 3.

Configure Mobility Group

- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision > Network Devices > Inventory**.
The **Inventory** window appears, which lists all the discovered devices.
- Step 2** Choose **Provision > Network Devices > Inventory**.
- Step 3** Check the check box next to the Catalyst 9800 Series Wireless Controller name for which you want to configure mobility.
- Step 4** From the **Actions** drop-down list, choose **Provision > Provision WLC Mobility**.
The **Configure Mobility Group** panel appears.
For more information, see [Mobility Configuration Overview, on page 49](#).
- Step 5** From the **Mobility Group Name** drop-down list, you can either add a new mobility group by clicking +, or choose from the existing mobility groups.
The existing mobility peers information is loaded from the intent available in the Cisco DNA Center.
- Step 6** In the **RF Group Name** text box, enter a name for the RF group.
- Step 7** To enable or disable Cipher configuration for mobility, click the **DTLS High Cipher Only** button on.
Cipher configuration is applicable for Cisco Catalyst 9800 Series Wireless Controller Release 17.5 or later. You need to manually reboot the device for changes to take effect.

- Step 8** To manually reboot the device after making changes in the DTLS (Data Datagram Transport Layer Security) cipher configuration to take effect after provision, click the **Restart for DTLS Ciphers to take effect** button on.
- Step 9** To enable DTLS data encryption, click the **Data Link Encryption** button on.
- Step 10** Under **Mobility Peers**, click **Add** to configure a mobility peer.
- Step 11** From the **Device Name** drop-down list, choose the controller.
- After the device is provisioned, the Cisco DNA Center creates a mobility group in device, assigns the RF group, and configures all ends of peers. The mobility group configuration is deployed automatically to all the selected peer devices.
- Step 12** Click **Save**.
- Step 13** You can reset the mobility group name and the RF group name using one of the following methods:
- In the **Configure Mobility Group** panel, choose **default** from the **Mobility Group Name** drop-down list.
 - On the **Provision > Configuration** page, under **Mobility Group**, click **Reset**.

This automatically sets the **RF Group Name** to **default** and removes all peers. Once you provision, the mobility on the device is set and the device is removed from all other peers.

About DTLS Ciphersuites

Ciphersuites are a set of encryption and integrity algorithms designed to protect radio communication on your wireless LAN.

You can configure multiple DTLS (Data Datagram Transport Layer Security) Ciphersuites on Cisco Catalyst 9800 Series Wireless Controller, Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches, and Cisco Embedded Wireless Controller on Catalyst Access Points platforms running Release 17.5 or later.

Configure Multiple DTLS Ciphersuites

You can configure DTLS Ciphersuites either at the global level or at the site level.

Before you begin

- Make sure that the Device Controllability feature is enabled on the **System > Settings > Device Settings > Device Controllability** page.
- Discover Cisco Catalyst 9800 Series Wireless Controllers in your network using the **Discovery** functionality so that the discovered devices are listed in the Inventory window.

-
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design > Network Settings > Wireless**.
- Step 2** In the left tree menu, select **Global** to configure all sites with the same DTLS Ciphersuite configuration.
- In the left tree menu, select a site to configure DTLS Ciphersuites at the site level. The DTLS Ciphersuite configuration will be pushed to the controller available on that particular site.
- Step 3** Uncheck the **Skip DTLS Ciphersuite Config** check box to configure Ciphersuites as part of Device Controllability.
- Step 4** Configure either default Ciphersuites or custom Ciphersuites.
- By default, the **Default** Ciphersuite is selected.

The Default Ciphersuite box shows the list of default Ciphersuites and these Ciphersuites are configured as default on the device. You cannot change the priority of these default ciphersuites.

Step 5 To configure custom Ciphersuites, click the **Custom** button.

Custom Ciphersuite overrides the default Ciphersuites with priority.

Step 6 From the **Version** drop-down list, choose the DTLS version.

Based on the DTLS version, Cisco DNA Center shows the available Ciphersuites.

Step 7 Click the blue button next to the Ciphersuite if you do not want to apply any of the Ciphersuites.

Step 8 To change the priority of Ciphersuites, hold and drag each Ciphersuite.

Step 9 Click **Save**.

The message `DTLS Ciphersuite Config Saved successfully` is displayed.

Step 10 To apply the Ciphersuite configuration, you must provision the device.

For more information, see [Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 55](#).

About N+1 Rolling AP Upgrade

The rolling AP upgrade feature is supported on the Cisco Catalyst 9800 Series Wireless Controller in an N+1 High Availability setup. This feature helps you upgrade software images on the APs associated with the Cisco Catalyst 9800 Series Wireless Controller in your wireless LAN network. To achieve the zero downtime, it is possible to upgrade APs in a staggered way using the N+1 Rolling AP upgrade feature.

The primary controller identifies the candidate APs through the radio resource management neighbor AP map. The upgrade process starts with the software image downloading to the primary controller while the image is predownloaded to the candidate APs. After the candidate APs have been upgraded and rebooted, they join the secondary controller in a staggered manner. After all the APs have joined the secondary controller, the primary controller reboots. The APs rejoin the primary controller in a staggered manner after it is rebooted.

Here are the prerequisites for configuring Rolling AP Upgrade:

- An N+1 High Availability setup with two wireless controllers, one as the primary controller and the other one as the secondary.
- The primary and the N+1 controllers have the same configuration and managing the same location in the network.
- The N+1 controller is already running the Golden image so that rolling AP upgrade works with zero downtime.

Golden images are standardized images for network devices and Cisco DNA Center automatically downloads the images from Cisco.com. Image standardization helps in device security and optimal device performance.

- The N+1 controller is reachable and in **Managed** state in Cisco DNA Center.
- Both the controllers are part of the same mobility group and a mobility tunnel is established between the primary and N+1 controller. The upgrade information between the primary and N+1 controllers are exchanged through the mobility tunnel.




Note If you have a cyclic N+1 HA deployment, where *wireless controller 1* is N+1 for *wireless controller 2* and *wireless controller 2* is N+1 for *wireless controller 1*, you cannot perform a rolling AP upgrade on both devices. Instead, one controller must go through a normal upgrade. You can perform a rolling AP upgrade on the other controller after the first controller is upgraded without the rolling AP upgrade.

Workflow to Configure Rolling AP Upgrade

This procedure shows how to configure rolling AP upgrade on Cisco Catalyst 9800 Series Wireless Controller.



Note N+1 rolling AP upgrade is supported on fabric and nonfabric deployments.

-
- Step 1** Install Cisco DNA Center.
For more information, see the [Cisco Digital Network Architecture Center Installation Guide](#).
- Step 2** Log in to the Cisco DNA Center GUI and verify that the applications you need are in the **Running** state.
In the Cisco DNA Center GUI, click the **Menu** icon () and choose **System > Software Updates > Installed Apps**.
- Step 3** Discover the wireless controller using the Discovery feature.
You must enable NETCONF and set the port to 830 to discover the Catalyst 9800 Series Wireless Controller. 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](#).
- Step 4** Make sure that the discovered devices appear in the **Device Inventory** window and are in the **Managed** state.
For more information, see [About Inventory](#) and [Display Information About Your Inventory](#).
You must wait for devices to move to a **Managed** state.
- Step 5** 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 it 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 a Building](#), and [Add a Floor to a Building](#).
- Step 6** Add the location information of APs, and position them on the floor map to visualize the heatmap coverage.
For more information, see [Add, Position, and Delete APs](#).
- Step 7** Provision the primary controller with primary managed AP location, rolling AP upgrade enabled, and mobility group configured with the secondary controller as its peer.
To do this, choose **Provision > Network Devices > Inventory**, and check the check box next to the primary controller name.

- Step 8** Configure the N+1 controller as the mobility peer in the Mobility Group configuration.
For more information, see [Mobility Configuration Overview, on page 49](#).
- Step 9** Provision the N+1 HA controller by configuring the primary controller's primary managed AP location as the N+1 controller's secondary managed AP location. This configures the secondary controller as the N+1 controller.
For more information, see [Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 55](#).
- Step 10** Provision the APs that are associated with the primary controller.
- Step 11** Import the software images to repository.
For more information, see [Import a Software Image](#).
- Step 12** Assign the software image to a device family.
For more information, see [Assign a Software Image to a Device Family](#).
- Step 13** Mark the software image as golden by clicking the star for a device family or a device role.
For more information, see [Specify a Golden Software Image](#).
- Step 14** Before upgrading the image, make sure that the image readiness checks are successful for both devices.
Also make sure that the status of the **N+1 Device Check** and the **Mobility Tunnel Check** has a green tick mark.
- To do the image update readiness check, choose **Provision > Network Devices > Software Images**.
 - From the **Focus** drop-down list, choose Software Images. Select the device whose image you want to upgrade.
 - If the prechecks are successful for a device, the **Status** link in the **Image Precheck Status** column has a green tick mark. If any of the upgrade readiness prechecks fail for a device, the Image Precheck Status link has a red mark, and you cannot update the OS image for that device. Click the **Status** link and correct any errors before proceeding.
- Step 15** Initiate the upgrade on the primary controller.
- Step 16** On the Software Images page, check the check box next to the primary controller.
- Step 17** From the **Actions** drop-down list, choose **Software Image > Update Image**.
For more information, see [Provision a Software Image](#).
- Step 18** To monitor the progress of the image upgrade, click **In Progress** in the **Software Image** column.
The **Device Status** page displays the following information:
- **Distribution Operation:** Provides information about the image distribution process. The image gets copied from the Cisco DNA Center to the primary device. The activate operation starts after the distribution process is complete.
 - **Activate Operation:** Provides the activate operation details. The rolling AP upgrade starts during this process.
 - **Rolling AP Upgrade Operation:** Provides a summary of the rolling AP upgrade, such as whether the rolling AP upgrade task is complete, the number of APs pending, the number of rebooting APs, and the number of APs that have joined the N+1 controller.
- Click **View AP Status** to view details about the primary controller, N+1 controller, device names, current status, and iterations.
-

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 38](#).

-
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision > Network Devices > Inventory**. The **Inventory** window appears, which lists all the discovered devices.
- Step 2** Check the check box next to the Catalyst 9800 Series Wireless Controller name that you want to provision.
- Step 3** From the **Actions** drop-down list, choose **Provision > Provision Device**.
- Step 4** In the **Assign Site** window, click **Assign Site** to associate with a site.
- Step 5** In the **Add Sites** window, check 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 **Next**.
The **Configuration** window.
This automatically sets the **RF Group Name** to **default** and removes all peers. Once you provision, the mobility on the device is set and the device is removed from all other peers.
-

Brownfield Support for Cisco Catalyst 9800 Series Wireless Controller

With Cisco DNA Center, you can add and provision brownfield devices such as the Cisco Wireless Controller and the Cisco Catalyst 9800 Series Wireless Controller to the network. Brownfield refers to devices that belong to existing sites with pre-existing infrastructure.

This section provides information on provisioning a brownfield Cisco Catalyst 9800 Series Wireless Controller with the Cisco DNA Center.

Before you begin

- Make sure that you have Cisco Catalyst 9800 Series Wireless Controller in the inventory. If you do not, discover devices using the Discovery feature.

To discover the Cisco Catalyst 9800 Series Wireless Controller, you must enable NETCONF and set the port to 830. For more information, see [About Discovery](#).

- Ensure that the Catalyst 9800 Series Wireless Controller is reachable and in **Managed** state on the **Inventory** window. For more information, see [About Inventory](#).
- 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, import it into Cisco DNA Center.

For more information about importing and uploading an existing network hierarchy, see [Upload an Existing Site Hierarchy](#).

For more information about creating a new network hierarchy, see [Create a Site in a Network Hierarchy](#), [Add a Building](#), and [Add a Floor to a Building](#).

-
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision > Network Devices > Inventory**. The **Inventory** window, which lists all the discovered devices that are available in the network, appears.
- Step 2** Check the check box next to the Catalyst 9800 Series Wireless Controller that you want to provision.
- Step 3** From the **Action** drop-down list, choose **Provision > Learn Device Config**.
- Step 4** Configure the following parameters in the **Assign Site** step:
- Click **Choose a site** to assign a site to the Catalyst 9800 Series Wireless Controller.
 - In the **Choose a site** window, select the location to which you want to associate the Catalyst 9800 Series Wireless Controller, and click **Save**.
 - Click **Next**.
- Step 5** The **Resolve Conflict** step shows the configurations that are available on the Cisco DNA Center and the Catalyst 9800 Series Wireless Controller. The conflicting configurations that you need to resolve are highlighted with a red box around them.
- The **Choose this config in Cisco DNA Center** section shows the available configurations in Cisco DNA Center, while the **Choose this config in Device** section shows the available configurations on the Catalyst 9800 Series Wireless Controller device.
- To retain the Cisco DNA Center configuration, from the **Choose this config** section, select the configuration that you want to retain by clicking the respective red box. This overwrites the device configuration.

For example, if the Cisco DNA Center is using Open as the authentication type for an SSID, and the device is using wpa2_enterprise as the authentication type, you can decide the configuration that you want to retain. To retain the Cisco DNA Center configuration, from the **Choose this config** section, select Open. Retaining the Cisco DNA Center configuration overwrites the device configuration.


To retain the device configuration, from the **Choose this config in Device** section, select the configuration that you want to retain by clicking the respective red box. Note that retaining the device configuration overwrites the Cisco DNA Center configuration.
 - Click **OK** in the **Warning** dialog box.
 - Click **Next**.

The **Design Object** window lists the configurations learned by the device.
- Step 6** Configure the following in the **Design Object** step:
- Click **Network** in the left pane. The right pane displays network configurations that were learned as part of the device configuration learning process, and shows the following information:
 - **AAA Server** details.
 - **Systems Settings**, with details about the IP address and protocol of the AAA server.
 - **DHCP Server**, with details about all the DHCP servers available in the device.
 - **NTP Server**, with details about all the NTP servers available in the device.

- Enter the **Shared Secret** for the AAA server.
- b) Click **Wireless** in the left pane. This displays the enterprise SSIDs, guest SSIDs, wireless interfaces, antenna radio profiles, and RF profiles that are present on the device.
For an SSID with a preshared key (PSK), you must provide the **Passphrase key**.
- c) Click **Ignored Config** in the left pane.
This displays the conflicting and the existing configurations on the Cisco DNA Center. The discarded configuration entries are available under the following categories:
 - Duplicate design entity
 - Unknown device configuration for radio policy
- d) Click **Next**.


Step 7 Review the **Network Profile** step which lists the network profile or site profile that is created based on the AP and WLAN combination, and click **Save**.

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

Step 8 In the Cisco DNA Center GUI, click the **Menu** icon () and choose **Design > Network Profiles** to assign a site to the network profile.

Step 9 In the **Network Profiles** window, configure the following:

- a) Click **Assign Site** to add sites to the selected profile.
- b) In the **Add Sites to Profile** slide-in pane, check the check box next to the site to associate this profile.
- c) Click **Save**.

Step 10 In the Cisco DNA Center GUI, click the **Menu** icon () and choose **Provision > Network Devices > Inventory**.

Step 11 Click **Filter** to locate the device that you want to provision.

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

Step 12 Check the check box next to the Catalyst 9800 Series Wireless Controller name that you want to provision.

Step 13 From the **Action** drop-down list, choose **Provision > Provision Device**.

Step 14 Review the details in the **Assign Site** step, and click **Next**.

Step 15 In the **Configuration** step, configure the following:

- a) Under **Interface and VLAN Configuration**, click **+Add** to configure interface and VLAN details.
- b) In the **Configure Interface and VLAN** window, configure the required fields, and click **OK**.
- c) Click **Next**.

Step 16 Review the **Summary** step which displays the following information:

- **Device Details**
- **Network Setting**
- **SSID**
- **Managed Sites**
- **Rolling AP Upgrade**
- **Interfaces**

- Step 17** Click **Deploy** to provision the device.
- a) You are prompted to deploy the device immediately or to schedule the deployment for a later time.
- To deploy the device now, click the **Now** radio button, and click **Apply**.
- To schedule device deployment for a later date and time, click the **Later** radio button, and define the date and time of the deployment.
- Step 18** Next, provision the AP.
- For more information, see [Provision a Cisco AP—Day 1 AP Provisioning, on page 30](#).

Day 0 Workflow for Cisco Embedded Wireless Controller on Catalyst Access Points

The Cisco Embedded Wireless Controller on Catalyst Access Points (EWC-APs) is the next-generation Wi-Fi solution, which combines the Cisco Catalyst 9800 Series Wireless Controller with Cisco Catalyst 9100 Series Access Points, creating the best-in-class wireless experience for the evolving and growing organization.

Before you begin

- Design your network hierarchy with sites, buildings, floors, and so on.
For more information, see [Create a Site in a Network Hierarchy](#), [Add a Building](#), and [Add a Floor to a Building](#).
- Define the device credentials, such as CLI, SNMP, HTTP, and HTTPS at the global level. The credentials that are defined at the global level are inherited by the sites.
For more information, see [Configure Global CLI Credentials](#), [Configure Global SNMPv2c Credentials](#), and [Configure Global SNMPv3 Credentials](#).
- Create wireless SSIDs, wireless interfaces, and wireless Radio Frequency profiles.
For more information, see [Create SSIDs for an Enterprise Wireless Network](#), [Create SSIDs for a Guest Wireless Network](#), [Create a Wireless Interface](#), and [Create a Wireless Radio Frequency Profile](#).



Note For Cisco Embedded Wireless Controller on Catalyst Access Points, only Flex-based SSID creation is supported.

- Configure the DHCP server with Option #43 on the switch where the Cisco Embedded Wireless Controller on Catalyst Access Points is connected. This is IP address of the Cisco DNA Center Plug and Play server. Using this IP address, the APs contact the PnP server and download the configuration.
- Make sure that you have the Cisco Embedded Wireless Controller on Catalyst Access Points in the inventory. If not, discover them using the Discovery feature. For more information, see [Discover Your Network Using CDP](#), [Discover Your Network Using an IP Address Range](#), and [About Inventory](#).
- The APs should be in the factory reset state without any Cisco Wireless Controller configurations.

The Cisco Embedded Wireless Controller on Catalyst Access Points is available in multiple form factors:

- Cisco Embedded Wireless Controller on Catalyst 9115AX Access Points

- Cisco Embedded Wireless Controller on Catalyst 9117AX Access Points
- Cisco Embedded Wireless Controller on Catalyst 9120AX Access Points
- Cisco Embedded Wireless Controller on Catalyst 9130AX Access Points

-
- Step 1** The Cisco Embedded Wireless Controller on Catalyst Access Points contacts the DHCP server.
In response, the DHCP server provides the IP address along with Option #43, which contains the IP address of the Cisco Plug and Play server.
- Step 2** Based on Option #43, the Cisco Embedded Wireless Controller on Catalyst Access Points turns on the Plug and Play agent and contacts the Cisco DNA Center Plug and Play server.
- Note** If you have a set of Cisco Embedded Wireless Controller on Catalyst Access Points in the network, they go through an internal protocol. The protocol selects one Cisco Embedded Wireless Controller on Catalyst Access Points, which is configured on the Cisco Wireless Controller as the primary AP to reach the PnP server.
- Step 3** Find the unclaimed Cisco Embedded Wireless Controller on Catalyst Access Points in the **Provision > Network Devices > Plug and Play** tab.
The table lists all the unclaimed devices. The **State** column shows as **Unclaimed**. Use the **Filter** or **Find option** to find specific devices.
You must wait for the onboarding status to become **Initialized** under the **Onboarding State** column.
- Step 4** To claim the Cisco Embedded Wireless Controller on Catalyst Access Points, check the check box next to the AP device name.
- Step 5** Choose **Actions > Claim** in the menu bar above the device table.
The **Claim Devices** window appears.
- Step 6** In the **Site Assignment** window, choose a site from the **Site** drop-down list.
Claiming the selected AP to this particular site also applies the associated configurations.
- Step 7** Click **Next**.
- Step 8** To configure a device, click the device name in the **Configuration** window.
- Step 9** In the **Configuration for device name** page, assign the static IP details for the device:
- **Management IP**
 - **Subnet Mask**
 - **Gateway**
- Step 10** Click **Save**.
- Step 11** Click **Next**.
The **Summary** page appears.
- Step 12** Click **Claim** in the **Summary** page.

After the Cisco Embedded Wireless Controller on Catalyst Access Points is claimed, the IP address configured is assigned to the Cisco Embedded Wireless Controller.

The claimed device, which is a Cisco Embedded Wireless Controller with internal AP, is now available under **Provision > Network Devices > Inventory**.

- Step 13** To provision the additional controller, see [Provision a Cisco AireOS Controller, on page 24](#).
- Step 14** To bulk import devices from a CSV file, see [Add Devices in Bulk, on page 10](#).
- Step 15** To add devices manually, see [Add or Edit a Device](#).

Migrate Cisco AireOS Controller to Cisco Catalyst 9800 Series Wireless Controller Using Cisco DNA Center

Before you begin

- Design your network hierarchy by adding sites, buildings, and floors.
- Discover the Cisco Catalyst 9800 Series Wireless Controller by running the discovery feature and add it to the Inventory. Make sure that the device status is reachable and in managed state.

You must enable NETCONF and set the port to 830 to discover the Catalyst 9800 Series Wireless Controller. NETCONF provides a mechanism to install, manipulate, and delete configurations of network.
- Discover the Cisco AireOS Controllers and add it to the Inventory. Make sure that the device status is reachable and in managed state.

-
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision > Network Devices > Inventory**.
The **Inventory** window appears, which lists the discovered devices.
- Step 2** Check the check box next to the Cisco AireOS Controller.
- Step 3** From the **Action** drop-down list, choose **Provision > Assign Device to Site**.
- Step 4** In the **Assign Device to Site** window, click **Choose a Site**.
- Step 5** In the **Add Sites** window, check the check box next to the site name to associate a Cisco AireOS Controller.
- Step 6** Click **Save**.
- Step 7** From the **Action** drop-down list, choose **Provision > Learn Device Config** to learn the configuration from the Cisco AireOS Controller device.
- Step 8** In the **Assign Site** window, click **Next**.
- Step 9** The **Resolve Conflict** window shows any conflicting configurations in Cisco DNA Center that you need to resolve. Click **Next**.
- Step 10** In the **Design Object** window, click **Next**.
- Step 11** In the left pane, click **Network**.
The right pane displays network configurations that were learned as part of the device configuration learning process, and shows the following information:
- AAA server details.

- Systems settings, with details about the IP address and protocol of the AAA server. Enter the shared secret for the AAA server, because the passwords are encrypted and Cisco DNA Center cannot learn passwords.
- DHCP server, with details about all the DHCP servers available in the device.
- NTP server, with details about all the NTP servers available in the device.

Step 12 Click **Next**.

Step 13 In the left pane, click **Wireless**.

The **Wireless** window displays the enterprise SSIDs, guest SSIDs, wireless interfaces, and RF profiles that are present on the device.

Step 14 For an SSID with a preshared key (PSK), enter the passphrase key.

Step 15 In the left pane, click **Discarded Config**.

This displays the conflicting and the existing configurations on Cisco DNA Center. The discarded configuration entries are available under the following categories:

- Duplicate design entity
- Unknown device configuration for radio policy

Step 16 Click **Next**.

Step 17 The **Network Profile** window lists the network profile or site profile that is created based on the AP and WLAN combination.

Step 18 Click **Save**.

A success message is displayed.

Step 19 Choose **Design > Network Settings > Wireless** to view the SSID and interface configurations that Cisco DNA Center has learned from the Cisco AireOS Controller.

Step 20 Choose **Design > Network Profiles** to assign a site to the network profile.

Step 21 In the **Network Profiles** window, click **Assign Site** to add sites to the selected profile.

Step 22 In the **Add Sites to Profile** window, choose a site from the drop-down list, and click **Save**.

Step 23 Click the **Provision** tab.

Step 24 Check the check box next to the Cisco Catalyst 9800 Series Wireless Controller that you want to provision.

Step 25 From the **Action** drop-down list, choose **Provision**.

Step 26 Click **Choose a site** to assign a site for the Cisco Catalyst 9800 Series Wireless Controller.

Step 27 In the **Choose a site** window, check the check box next to the site name to associate a Catalyst 9800 Series Wireless Controller.

Step 28 Click **Next**.

The **Configuration** window appears.

Step 29 Select a role for the Cisco Catalyst 9800 Series Wireless Controller as **Active Main WLC**.

Step 30 Click **Select Primary Managed AP Locations** to configure a managed AP location for the primary controller.

Step 31 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, the children under that parent site are automatically selected.

Step 32 Click **Save**.

Step 33 Click **Next**.

Step 34 The summary window shows the configurations that will be pushed to the Cisco Catalyst 9800 Series Wireless Controller from the Cisco AireOS Controller.

Review the following details:

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

Step 35 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 36 After the devices are deployed successfully, the **Provision Status** changes from **Configuring** to **Success**.

Step 37 In the **Device Inventory** window, click **See Details** in the **Provision Status** column to get more information about the network intent or to view a list of actions that you need to take.

Step 38 To manually resynchronize the Cisco Catalyst 9800 Series Wireless Controller, on the **Provision > Inventory** window, select the controller that you want to manually synchronize.

Step 39 From the **Actions** drop-down list, choose **Resync**.

Step 40 Provision the AP.

Configure and Provision a Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches

Supported Hardware Platforms

Device Role	Platforms
Embedded Wireless Controller	Cisco Catalyst 9300 Series Switches Cisco Catalyst 9400 Series Switches Cisco Catalyst 9500H Series Switches
Fabric Edge	Cisco Catalyst 9300 Series Switches Cisco Catalyst 9400 Series Switches Cisco Catalyst 9500H Series Switches Cisco Catalyst 3600 Series Switches

Device Role	Platforms
	Cisco Catalyst 3850 Series Switches
APs	<p>Cisco 802.11ac Wave 2 APs:</p> <ul style="list-style-type: none"> • Cisco Aironet 1810 Series OfficeExtend Access Points • Cisco Aironet 1810W Series Access Points • Cisco Aironet 1815i Access Point • Cisco Aironet 1815w Access Point • Cisco Aironet 1815m Access Point • Cisco 1830 Aironet Series Access Points • Cisco Aironet 1850 Series Access Points • Cisco Aironet 2800 Series Access Points • Cisco Aironet 3800 Series Access Points • Cisco Aironet 4800 Series Access Points <p>Cisco 802.11ac Wave 1 APs</p> <ul style="list-style-type: none"> • Cisco Aironet 1700 Series Access Points • Cisco Aironet 2700 Series Access Points • Cisco Aironet 3700 Series Access Points

Preconfiguration

On the Cisco Catalyst 9800 Series Wireless Controller, make sure that the following commands are present if the switch is already configured with **aaa new-model**:

```
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 an automated underlay for provisioning.

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

1. Install Cisco DNA Center.
For more information, see the [Cisco DNA Center Installation Guide](#).
2. Log in to the Cisco DNA Center GUI and verify that the applications you need are in the **Running** state.
In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **System > Software Updates > Installed Apps**.

3. Integrate Cisco Identity Services Engine with Cisco DNA Center. After 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 Switches and the edge switches.

You must enable NETCONF and set the port to 830 to discover Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches.

Do not enable NETCONF to discover the edge switches.

For more information, see [Discover Your Network Using CDP](#) and [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](#).

Ensure that the devices are in the **Managed** state.
6. Design your network hierarchy, which represents your network's geographical location. You create 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 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 a Building](#), and [Add a Floor to a Building](#).
7. For a nonfabric network, add and position APs on a floor map to get heatmap visualization during the design phase.

For a fabric network, you cannot place APs on a floor map during the design time. The APs are onboarded 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.

You can configure upto six AAA servers on the **Wireless** page during the SSID creation.

For more information, see [Manage Global Network Settings](#), [Configure Global Network Servers](#), and [Add AAA server](#).
9. Configure device credentials such as CLI, SNMP, and HTTPs.

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.

To configure an IP address pool, see [Configure IP Address Pools](#).

To reserve an IP address pool for the building that you are provisioning, see [Provision a LAN Underlay](#).

11. Create enterprise and guest wireless networks. Define global wireless settings once and Cisco DNA Center then 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. Configure backhaul settings. For more information.
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](#).
 - Create a group-based access control policy, and add a contract. For more information, see [Create Group-Based Access Control Policy](#).
14. Provision Cisco Catalyst 9000 Series Switches and the edge node switches with the configurations added during the design phase.
 - Create a fabric site.
 - Add devices to the fabric network by creating a CP+Border+Edge or CP+Border.
 - Enable embedded wireless capabilities on the Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches.
 - Onboard APs in the fabric site.


After the devices are deployed successfully, the deploy status changes from **Configuring** to **Success**.

Provision Embedded Wireless on Cisco Catalyst 9000 Series Switches

Before you begin

Before provisioning a Cisco Catalyst 9800 Embedded Wireless Controller on Catalyst 9000 Series Switches, ensure that you have completed the steps in [Workflow to Configure Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Switches, on page 63](#).

This procedure explains how to provision embedded wireless on Cisco Catalyst 9300 Series Switches, Cisco Catalyst 9400 Series Switches, and Cisco Catalyst 9500H Series Switches.

-
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon () and choose **Provision > Network Devices > Inventory**. The **Inventory** window appears, with the discovered devices listed.
 - Step 2** Check the check box next to the Catalyst 9000 Series Switch device and an edge switch 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** step, configure the following:
 - a) Click **Choose a site**.

- b) In the **Choose a site** slide-in pane, check the check box next to the site to associate the device.
- c) Click **Save**.
- d) Click **Apply**.

The next step is to provision the Catalyst 9000 Series Switch and the edge node with the configurations that were added during the design phase.

Step 5

In the **Devices > Inventory** window, check the check box next to the device name that you want to provision.

- a) From the **Actions** drop-down list, choose **Provision > Provision Device**.
- b) Click **Next**.
- c) In the **Summary** step, verify the configurations, and click **Deploy**.
- d) In the **Provision Devices** window, do the following to preview the CLI configuration:

- Click **Generate Configuration Preview** radio button.
- In the **Task Name** field, enter a name for the CLI preview task and click **Apply**.
- In the **Task Submitted** pop-up, click the **Work Items** link.

Note If you missed the **Task Submitted** pop-up, click the **Menu** icon (☰) and choose **Activities > Work Items**.

- In the **Work Items** window, click the CLI preview task for which you submitted the configuration preview request.
- View the CLI configuration details and click **Deploy**.
- To immediately deploy the device, 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.
- In the **Information** pop-up, do the following:
 - Click **Yes** if you want to delete the CLI preview task from the **Work Items** window.
 - Click **No** if you want to retain the task in the **Work Items** window.

Note The CLI task will be marked as completed in the **Work Items** window. You can view the CLI configuration for this task, but you cannot deploy it again.

Step 6

To provision the edge switch, check the check box next to the edge switch that you want to provision.

- a) From the **Actions** drop-down list, choose **Provision**.
- b) Click **Next**.
- c) In the **Summary** window, verify the configurations, and click **Deploy**.

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

Step 7

To add devices to a fabric site, in the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision > Fabric Sites**.

Step 8

Create a fabric site. For more information, see [Add a Fabric Site](#).

Step 9

Add an IP transit network.

Step 10

Add devices and associate virtual networks to a fabric site.

Step 11

Add the Cisco Catalyst 9000 Series Switch as a control plane, a border node, and an edge node or a control plane and a border node.

- a) Click the device and choose **Add as CP+Border+Edge** or **Add as CP+Border**.
- b) Click the edge node and choose **Add to Fabric**.
- c) Click **Save**.

Step 12 To enable embedded wireless on the device, click the device that is added as a **Edge**, **CP+Border+Edge** or **CP+Border**, and click the **Embedded Wireless**.

- a) If you have not installed the wireless package on Cisco Catalyst 9000 Series Switches 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.
- b) Click **OK** to install the image manually.
- c) 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.
- d) Click **Import**.

The progress of the import is displayed.

- e) 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.

- f) Click **Yes**.

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

- g) In the dialog box that appears, the AP locations that are managed by the controllers are displayed. You can change, remove, or reassign the site here.

- h) Click **Next**.

Step 13 Review the details on the **Summary** step, and click **Save**.

Step 14 On the **Modify Fabric** step, click **Now** to commit the changes, and click **Apply** to apply the configurations. The next step is to onboard APs in a fabric site.

Step 15 In the Cisco DNA Center GUI, click the **Provision** tab.

Step 16 Click the **Fabric** tab.

A list of fabric sites is displayed.

Step 17 Select the fabric site that was created, and click the **Host Onboarding** tab to enable IP pool for APs.

Step 18 Select the authentication template that is applied for devices in the fabric site. These templates are predefined configurations that are retrieved from Cisco ISE. After selecting the authentication template, click **Save**.

Step 19 Under **Virtual Networks**, click **INFRA_VN** to associate one or more IP pools with the selected virtual network.

Step 20 Under **Virtual Network**, click the guest virtual networks to associate IP pools for the selected guest virtual network.

Step 21 Check the **IP Pool Name** check box that was created for APs during the design phase.

Step 22 Click **Update** to save the setting.

The 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 23 Specify wireless SSIDs within the network that hosts can access. Under the **Wireless SSID** section, select the guest or enterprise SSIDs and assign address pools, and click **Save**.

Step 24 Manually trigger resynchronization by performing an **Inventory > Resync** to see the APs on Cisco DNA Center for embedded wireless.

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

Step 25 Provision the AP.

For more information, see [Provision a Cisco AP—Day 1 AP Provisioning, on page 30](#).

Step 26 Configure and deploy application policies. For more information, see [Create an Application Policy](#), [Deploy an Application Policy](#), and [Edit an Application Policy](#).

Provision the Catalyst 9300 Series Switches and Cisco Catalyst 9500H Series Switches before deploying an application policy.

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.

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.

Fabric in a Box with Catalyst 9800 Embedded Wireless on Cisco Catalyst 9000 Series Switches

Information About Fabric in a Box

Cisco Catalyst 9000 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 9000 Series Switches, see [Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 55](#).

Scale Information

This table shows the device scalability information.

Fabric Constructs	Cisco Catalyst 9300 Series Switches	Cisco Catalyst 9400 Series Switches	Cisco Catalyst 9500 Series Switches	Cisco Catalyst 9500-H Series Switches
Virtual Networks	256	256	256	256
Local End Points/Hosts	4K	4K	4K	4K
SGT/DGT Table	8K	8K	8K	8K
SGACLs (Security ACEs)	5K	18K	18K	18K

Inter-Release Controller Mobility Introduction

Inter-Release Controller Mobility (IRCM) supports seamless mobility and wireless services across different Cisco Wireless Controllers with different software versions.

Cisco DNA Center supports guest anchor feature for the following device combinations:

- Configuration of a Cisco AireOS controller as a foreign controller with a Cisco AireOS controller as an anchor controller.
- Configuration of a Cisco AireOS controller as a guest anchor controller with a Cisco Catalyst 9800 Series Wireless Controller as a foreign controller.
- Configuration of a Cisco Catalyst 9800 Series Wireless Controller as a foreign controller with a Cisco Catalyst 9800 Series Wireless Controller as an anchor controller.

Configuring IRCM on controller devices has the following limitations:

- Configuration of a Cisco AireOS controller as a foreign controller and Cisco Catalyst 9800 Series Wireless Controller as an anchor controller is not supported.
- Configuration of a fabric guest anchor is not supported.
- Configuration of multiple anchor controllers and one foreign controller is not supported.
- Only guest SSID is supported.
- Broadcast of a nonguest anchor SSID in a guest anchor mode is not supported.
- Mobility tunnel is not encrypted.

Guest Anchor Configuration and Provisioning

Follow these steps to configure a guest anchor Cisco Wireless Controller.



Note Guest anchor configuration is not supported on the Cisco Catalyst 9800 Series Wireless Controller.

-
- Step 1** Design a network hierarchy, with sites, buildings, floors, and so on. For more information, see [Create a Site in a Network Hierarchy](#), [Add a Building](#), and [Add a Floor to a Building](#).
 - Step 2** Configure network servers, such as AAA, DHCP, and DNS servers. For more information, see [Configure Global Network Servers](#) and [Add Cisco ISE or Other AAA Servers](#).
 - Step 3** Create SSIDs for a guest wireless network with external web authentication and central web authentication along with configuring Cisco Identity Services Engine. For more information, see [Create SSIDs for a Guest Wireless Network](#).
 - Step 4** Discover the wireless controller using the Cisco Discovery Protocol (CDP) or an IP address range and that the devices are in the **Devices > Inventory** window and are in the **Managed** state. For more information, see [About Discovery](#).
 - Step 5** Provision a foreign wireless controller as the active main wireless controller. See [Provision a Cisco AireOS Controller, on page 24](#).
 - Step 6** Choose the role for the wireless controller as guest anchor and provision the guest anchor controllers. For more information, see [Provision a Cisco AireOS Controller, on page 24](#).

- Step 7** 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](#).
-

IRCM: Cisco AireOS Controller and Cisco Catalyst 9800 Series Wireless Controller

Before you begin

- Discover the Cisco Catalyst 9800 Series Wireless Controller and Cisco AireOS Controllers.
You must enable NETCONF and set the port to 830 to discover the Catalyst 9800 Series Wireless Controller. 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](#).
- Design your network hierarchy by adding sites, buildings, and floors so that later you can easily identify where to apply design settings or configurations.
To create a new network hierarchy, see [Create a Site in a Network Hierarchy](#), [Add a Building](#), and [Add a Floor to a Building](#).
- Add the location information of APs, and position them on the floor map to visualize the heatmap coverage.
For more information, see [Add, Position, and Delete APs](#).
- 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 [Manage Global Network Settings](#), [Configure Global Network Servers](#), and [Add AAA server](#).
- Create SSIDs for a guest wireless network.
For more information, see [Create SSIDs for a Guest Wireless Network](#).
- The WLAN profile name of the foreign controller and anchor controller should be the same for mobility.

-
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision > Network Devices > Inventory**. The **Inventory** window appears, with the discovered devices listed.
- Step 2** Check the check box next to the Catalyst 9800 Series Wireless Controller that you want to provision as a foreign controller.
- Step 3** From the **Actions** drop-down list, choose **Provision > Provision**.
- Step 4** In the **Assign 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, check the check box next to the site name to associate a Catalyst 9800 Series Wireless Controller.
- Step 6** Click **Save**.

- Step 7** Click **Apply**.
- Step 8** Click **Next**.
- Step 9** Select a role for the Catalyst 9800 Series Wireless Controller as **Active Main WLC**.
- Step 10** For an active main wireless controller, you need to configure interface and VLAN details.
- Step 11** 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 12** Click **Next**.
- Step 13** In the **Summary** window, review the configurations details.
- Step 14** Click **Deploy** to provision the Catalyst 9800 Series Wireless Controller as a foreign controller.
- Step 15** On the **Devices > Inventory** window, check the check box next to the Cisco AireOS Controller that you want to provision as a guest anchor controller.
- Step 16** Repeat Step 3 through Step 8.
- Step 17** Select a role for the Cisco AireOS Controller as **Guest Anchor**.
- Step 18** For a guest anchor wireless controller, you need to configure interface and VLAN details.
- Step 19** Repeat Step 11 through Step 14.
-

Provision a Meraki Device

This procedure explains how to provision SSIDs to Cisco Meraki devices managed by a Meraki dashboard.

Before you begin

- Integrate the Meraki dashboard with Cisco DNA Center. See [Integrate the Meraki Dashboard](#).
- Create the SSID. See [Create SSIDs for an Enterprise Wireless Network](#).



Note The Meraki dashboard supports the following types of SSIDs:

- Open: This SSID corresponds to Open in the Meraki dashboard.
- WPA2 Personal: This SSID corresponds to the preshared key with WAP2 in the Meraki dashboard.
- WPA2 Enterprise: This SSID corresponds to WAP-2 Encryption with Meraki authentication or My Radius server in the Meraki dashboard. If you have defined AAA or Cisco ISE servers for client and endpoint authentication at the building level in Cisco DNA Center, the configuration will be provisioned to **my Radius server** in the Meraki dashboard. Otherwise, **Meraki Radius** will be used for authentication by the Meraki devices.

For every SSID, you can choose an interface name. If you choose the **Management** interface in Cisco DNA Center and the VLAN ID is 0, the configuration is not supported in the Meraki dashboard and VLAN tagging is disabled in the Meraki dashboard. If you create a custom interface for the SSID in Cisco DNA Center, an AP tag is created with the custom interface name and VLAN ID in the Meraki dashboard.

-
- Create the network profile and assign it to the sites for which the SSID is provisioned.



Note The Network Hierarchy **Sites > Buildings** in Cisco DNA Center corresponds to the **Organization > Network** in the Meraki dashboard. We recommend that you choose **Buildings** in the **Add Sites to Profile** window in the workflow.



Note Cisco DNA Center creates the Meraki network and provisions the SSIDs to the network. The Meraki dashboard provisions the Meraki network configuration to the Meraki devices.

-
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision**.
The **Network Devices > Inventory** window appears, listing all discovered devices.
- Step 2** To view the Meraki dashboard, expand the **Global** site in the left pane, and select a building.
All Meraki dashboards available in the selected building are displayed.
- Step 3** Check the check box next to the Meraki dashboard name that you want to provision.
- Step 4** From the **Actions** drop-down list, choose **Provision > Provision Device**.
The **Assign Site** window appears, where you can view the Meraki dashboard and the associated building.
- Step 5** To change the associated building, click **Choose a site**.
- Step 6** In the **Choose a site** window, select a building and click **Save**.

Step 7 Click **Next**.

The **Configuration** window appears. You can view the managed building in the Primary location.

Step 8 Click **Select Secondary Managed AP Locations** to select the secondary managed location for the Meraki dashboard.

Step 9 In the **Managed AP Location** window, check the check box next to the building name.

Step 10 Click **Save**.

Step 11 Click **Next**.

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

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

Note Meraki deployment supports a maximum of 15 SSIDs in each network.

Step 12 Click **Deploy**.

Step 13 In the **Provision Devices** window, do the following to preview the CLI configuration:

- Click the **Generate Configuration Preview** radio button.
- In the **Task Name** field, enter a name for the CLI preview task and click **Apply**.
- In the **Task Submitted** pop-up, click the **Work Items** link.
- **Note** If you missed the **Task Submitted** pop-up, click the **Menu** icon (☰) and choose **Activities > Work Items**.
- In the **Work Items** window, click the CLI preview task for which you submitted the configuration preview request.
- View the CLI configuration details and click **Deploy**.
- To immediately deploy the device, 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.
- In the **Information** pop-up, do the following:
 - Click **Yes** if you want to delete the CLI preview task from the **Work Items** window.
 - Click **No** if you want to retain the task in the **Work Items** window.

Note The CLI task will be marked as completed in the **Work Items** window. You can view the CLI configuration for this task, but you cannot deploy it again.

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

Provision Routing and NFV Profiles

Before you begin

Make sure that you have defined the following global network settings before provisioning routing and NFV profiles:

- 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** In the Cisco DNA Center GUI, click the **Menu** icon (\equiv) and choose **Provision**.
The **Network Devices > Inventory** window appears, and all the discovered devices are listed in this window.
- Step 2** To view devices available in a particular site, expand the Global site in the left pane, and select the site, building, or floor that you are interested in.
All the devices available in that selected site are displayed in the **Inventory** window.
- Step 3** From the **Device Type** list, click the **Routers** tab, and from the **Reachability** list, click the **Reachable** tab to get a list of devices that are discovered and reachable.
- Step 4** Check the check box next to the device name that you want to provision.
- Step 5** Click **Assign** under the site; the **Assign Device to Site** window appears. Click **Choose a Site**.
- Step 6** From the **Actions** drop-down list, choose **Provision > Provision Device**.

To provision an NFVIS device, do the following:

- Review the details in the **Confirm Profile** window, and click **Next**.
- Review the details in the **Router WAN Configuration** window. Click **O** and enter the WAN IP address. Review the details in the **+Edit Services** window. Click **Next**.

Note You must configure vManage settings in the System Settings page before provisioning vEdge-related services. For more information, see [Configure vManage Properties in the Cisco DNA Center Administrator Guide](#).

- Review the details in the **ENCS Integrated Switch Configuration** window, and click **Next**.

- Review the details in the **Custom Configuration** window, and click **Next**.
- Review the details in the **Summary** page.

To provision a router, do the following:

- Review the details in the **Confirm Profile** window, and click **Next**.
- Review the details in the **Router WAN Configuration** window.
 - If you selected Gigabit Ethernet as the line interface, click **O** and enter the WAN IP address if you select a static IP address. If you select DHCP, enter the IP address from the DHCP server. If the primary WAN is already configured using PnP, you can select **Do not Change** and select the interface that is configured as the primary WAN from the drop-down list.
 - If you selected cellular as the line interface, click **O**, choose **IP Negotiated**, select the **Interface Name** from the drop-down list, and enter the **Access Point Name (APN)**. Depending on your service provider, check the **PAP** or **CHAP** check box.
 - Enter the **IP SLA Address** for the backup WAN interface when you have multiple service providers.

This window does not appear if you are provisioning a virtual router.

- Review the details in the **Router LAN Configuration** window, and click **Next**.
You can now select one L3 interface or one or multiple L2 interfaces from the **Interface(s)** drop-down list.
- Review the details in the **Integrated Switch Configuration** window, and click **Next**.
- Review the details in the **Summary** page.

Step 7 Click **Deploy**.

Step 8 In the **Provision Devices** window, do the following to preview the CLI configuration:

- Click the **Generate Configuration Preview** radio button.
 - In the **Task Name** field, enter a name for the CLI preview task and click **Apply**.
 - In the **Task Submitted** pop-up, click the **Work Items** link.
- Note** If you missed the **Task Submitted** pop-up, click the **Menu** icon (☰) and choose **Activities > Work Items**.
- In the **Work Items** window, click the CLI preview task for which you submitted the configuration preview request.
 - View the CLI configuration details and click **Deploy**.
 - To immediately deploy the device, 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.
 - In the **Information** pop-up, do the following:
 - Click **Yes** if you want to delete the CLI preview task from the **Work Items** window.
 - Click **No** if you want to retain the task in the **Work Items** window.

Note The CLI task will be marked as completed in the **Work Items** window. You can view the CLI configuration for this task, but you cannot deploy it again.

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

VPC Inventory Collection

After successful cloud inventory collection, the **Cloud** tab in the **Provision** section provides a view of the collected AWS VPC Inventory. The navigation on the left can be expanded to show the cloud regions for a cloud profile or access key. You can filter the left navigation items by keyword and click to see the VPCs just for the selected region or access key.

In the VPC Inventory view you can also click on a VPC to see more details about it, like the subnets and virtual instances in that VPC and some more details about them. AWS VPC inventory collection is scheduled to occur at the default interval for all inventory collection and can also be triggered on demand by using the **Sync** action from the gear menu for a cloud access key. The status of the inventory collection can be viewed by clicking on **Show Sync Status** in the **VPC Inventory** view.

Provision Firewall Profiles

This procedure explains how to provision a Firepower Threat Defense (FTD) device managed by Firepower Management Center (FMC).

Before you begin

- Integrate FMC with Cisco DNA Center. See [Integrate Firepower Management Center](#).
- Create a site in a network hierarchy. See [Create a Site in a Network Hierarchy](#).
- Create a network profile for firewall and assign it to a site for which the FTD device is provisioned. See [Create Network Profiles for Firewall](#).

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision > Network Devices > Inventory**. The Inventory page displays the device information that is gathered during the discovery process.

Step 2 Check the check box next to the FTD device that you want to provision and click **Assign** under the **Site** column.

Step 3 In the **Assign Device to Site** window, click **Choose a Site**.

Step 4 In the **Choose a Site** window, select a site from the hierarchy and click **Save**.

Step 5 Click **Next**.

Step 6 Click **Now** to assign the device to site immediately or click **Later** to schedule at a specific time.

Step 7 Click **Assign**.

Note You can view the status of assigning device to site in **Activities > Tasks**.

Step 8 From the **Actions** drop-down list, choose **Provision > Provision Device**.

The **Provision Firewall Profile** window appears.

Step 9 Review the details in the **Confirm Profile** page and click **Next**.

Step 10 Review the details in the **Firewall Type** page and click **Next**.

The **FTD Configuration** page appears.

Step 11 If you have associated a routed mode firewall with the site, do the following:

- a) Expand the **Outside Interface** area, choose an outside interface from the **Select Physical Interface** drop-down list, and choose **Static IP** or **DHCP** radio button.
 - **Static IP**: Enter the IP address and a subnet mask.
 - **DHCP**: The IP address is obtained from DHCP.
- b) Expand the **Inside Interface** area, choose an inside interface from the **Select Physical Interface** drop-down list, and choose **Static IP** or **DHCP** radio button.
 - **Static IP**: Enter the IP address and a subnet mask.
 - **DHCP**: The IP address is obtained from DHCP.

Step 12 If you have associated a transparent mode firewall with the site, do the following:

- a) Expand the **Outside Interface** area and choose an outside interface from the **Select Physical Interface** drop-down list.
- b) Expand the **Inside Interface** area and choose an inside interface from the **Select Physical Interface** drop-down list.
- c) Expand the **Bridge Virtual Interface** area, and do the following:
 - **Bridge Group Number**: Enter a bridge group number. The valid number is from 1 to 250.
 - **IP**: Enter the IP address of the FTD device.
 - **Subnet Mask**: Enter a subnet mask.

Step 13 Click **Next**.

The **Summary** page appears. This page summarizes the device specifications.

Step 14 Review the details in the **Summary** page and click **Deploy**.

The **Provision Firewall device(s)** dialog box appears.

Step 15 Click **Now**, **Later**, or **Generate configuration preview** radio button.

- **Now**: Starts the provision immediately.
- **Later**: Schedules the provisioning at a specific time.
- **Generate configuration preview**: Generates preview which can be later used to deploy on selected devices.

Step 16 Click **Apply**.

Note You can view the status of provisioning firewall device in **Activities > Tasks**. If you have chosen **Generate configuration preview** in the **Provision Firewall device(s)** dialog box, you can view the status in **Activities > Work Items**.

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](#).)
- 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".

- If you have a Cisco Catalyst 9400 Switch configured in the network, ensure that the following operations are done on the switch for LAN automation to automatically enable the 40G port:
 - [Day-0 Configuration](#) is performed on the switch.
 - A 40G Quad Small Form-Factor Pluggable (QSFP) transceiver is inserted in either port 9 or port 10 of the Supervisor, and the ports numbered 1 to 8 on the Supervisor do not have a 10G or 1G Small Form-Factor Pluggable (SFP) transceiver inserted in them. If there are dual supervisor engines, ensure that the 40G QSFP is inserted in port 9.
- For more information on the Catalyst 9400 Series Supervisor, see [Cisco Catalyst 9400 Series Supervisor Installation Note](#).

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 or larger.

- In the Cisco DNA Center GUI, click the **Menu** icon () and choose **Design > Network Settings > IP Address Pools**.
- From the **Network Hierarchy** pane, choose a site.
- Click **Reserve** and complete the following fields in the **Reserve IP Pool** window to reserve all or part of an available global IP address pool, for the specific site:
 - **IP Address Pool Name:** Unique name for the reserved IP address pool.
 - **Type:** Type of IP address pool. For LAN automation, choose **LAN**.

- **IP Address Space:** Check **IPv4** or **IPv6** to create an address pool. To create a dual-stack pool, check both **IPv4** and **IPv6** check boxes.
- **Global IP Pool:** IPv4 address pool from which you want to reserve all or part of the IP addresses.
Note LAN automation uses only the IPv4 subnet.
- **Prefix length / Number 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 that you want to reserve.
- **Gateway:** Gateway IP address.
- **DHCP Server(s):** DHCP server(s) IP address(es).
- **DNS Server(s):** DNS Server(s) IP address(es).

d) Click **Reserve**.

Step 2

Discover and provision the devices.

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

All the discovered devices are displayed.

b) Click **Actions > Provision > LAN Automation**.

c) In the **LAN Automation** window, 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.
- **SELECTED PORTS OF PRIMARY DEVICE:** Ports to be used to discover and provision new devices. Click **Modify Selections** to enter the port numbers.
- **Discovered Device Site:** All newly discovered devices are assigned to this site. This site can be different from Primary and Peer Sites.
- **Main IP Pool:** IP address pool that was reserved for LAN automation. (See Step 1.)
- **Link Overlapping IP Pool:** IP address pool that is shared with other sites, is used to specifically configure the /31 IP addresses on point-to-point links in the underlay.

A link overlapping IP pool can be a subpool that is inherited from a parent site or a subpool that is defined in any other site.

A link overlapping IP pool allows you to overlap /31 IP addresses in a multisite deployment. Hosts in different sites will be able to reuse IP addresses on the /31 links.

If you choose to define a link overlapping IP pool, the addresses defined in the **Main IP Pool** field are used for Management IPs (like loopback address, VLAN address, and so on).

- **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:** Check this check box to enable underlay native 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.
- **Choose a File:** Click **Browse** to choose a hostname map File. Configures user-provided names for discovered devices using the chosen 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:

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

- d) Click **Start**.

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

LAN automation configures an IP address on the seed device of VLAN 1. If this VLAN 1 IP address of the seed device is not reachable from Cisco DNA Center, an error message is displayed on the LAN Automation Status window. Hover your cursor over the **See Details** link on this window to see the error details and possible remedial actions.

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

- a) Click **Actions > Provision > LAN Automation Status**.

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

Note The provisioning of new devices may take several minutes.

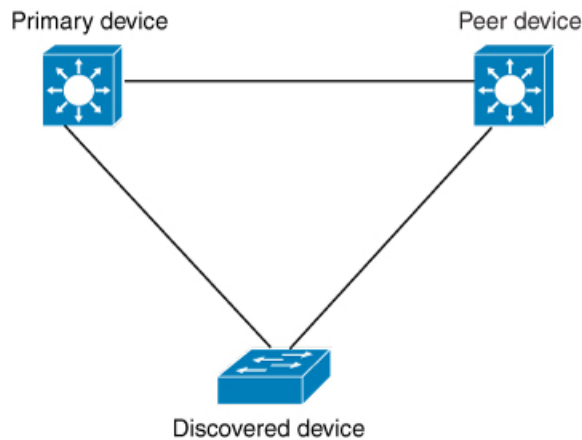
- b) After all devices have been discovered, added to Inventory, and are in Managed state, click **Stop** in the **LAN Automation Status** window.

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.



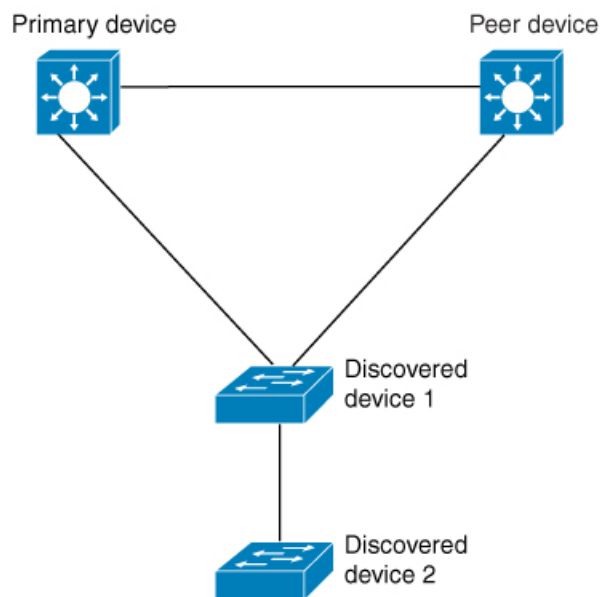
355771

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



355772

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** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision > Inventory**.
All discovered devices are displayed.
- Step 2** Choose **Actions > Provision > LAN Automation Status**.
The **LAN Automation Status** window displays the status of all running or completed LAN automation jobs.
-

Delete a Device After Provisioning

- If you are deleting a device that is already been added to the fabric site, remove it from the fabric site 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** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision > Network Devices > Inventory**.
The **Inventory** window appears, with the discovered devices listed.
- 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**.
-