

Onboard and Provision Devices with Plug and Play

- Plug and Play provisioning overview, on page 1
- Plug and Play provisioning prerequisites, on page 3
- Plug and Play deployment guidelines, on page 9
- View devices, on page 10
- Add or edit a device, on page 12
- Add devices in bulk, on page 13
- Register or edit a virtual account profile, on page 14
- Add devices from a Smart Account, on page 15
- Provision a device with Plug and Play, on page 17
- Delete a device, on page 30
- Reset a device, on page 30

Plug and Play provisioning overview

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:

- 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 Catalyst 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 Catalyst Center.
- Display the detailed onboarding status of network devices.

These 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.

Note The planned state for APs is for only claiming the APs using zero-touch provisioning (ZTP) when the APs contact Catalyst Center through Plug and Play. This planning isn't applicable for provisioning the APs via the **Provision** > **Inventory** option when the APs directly associate with the wireless controller.

The steps for planned provisioning include:

1. We recommend that you define the site within the network hierarchy. See Network hierarchy.
2. Define the 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. Often, such templates aren't necessary unless you need to customize the day-zero configuration. See Create Templates to Automate Device Configuration Changes.

Note Day-zero templates don't support Interactive commands.

3. Define network profiles for the types of devices that you are deploying. See Network profiles overview.
4. We recommend that you define the device credentials (CLI and SNMPv2c/SNMPv3) for the devices that you're deploying. If you're using SNMPv2c, both Read and Write credentials must be provided.

Note Missing credentials will lead to the devices not being able to be added to the inventory after they are provisioned.

5. 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 12 or Add devices in bulk, on page 13.
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's 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 Plug and Play provisioning prerequisites, on page 3.

The steps for an administrator to provision the device include:

1. Find the device on the devices list by filtering on unclaimed devices or searching for it by name. See View devices, on page 10.
2. Claim the device by assigning a site, image, configuration template, or profile. See Provision a device with Plug and Play, on page 17. You can also claim the device without assigning a site.

Note Global device credentials are required for devices with no site assigned. Global device credentials at site level are required for devices with sites assigned.

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 Catalyst Center Plug and Play, so that all the devices appear in Catalyst 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 14.
2. Synchronize the device inventory from the Smart Account. See Add devices from a Smart Account, on page 15.
3. Find the device on the devices list by filtering on unclaimed devices or searching for it by name. See View devices, on page 10.
4. Claim the device by assigning a site, image, configuration template, or profile. See Provision a device with Plug and Play, on page 17.
5. Devices boot up and are automatically provisioned.

Device claim and management scenarios

- **Claimed devices**
  - When a device is claimed and managed, PnP profiles are removed from the device.
  - The device will not contact PnP again only after a factory reset.
- **Unclaimed devices in inventory**
  - If a user tries to claim a device through PnP that is already in inventory, the claim is blocked.
  - Catalyst Center reads inventory notifications and updates PnP to prevent duplicate claims.
- **Factory reset devices**
  - If a managed device is factory reset, it moves to the unclaimed state.
  - Catalyst Center checks for inventory presence and blocks new claims if the device is still in inventory.

Plug and Play provisioning prerequisites

Before using Plug and Play provisioning, ensure you have access to the sites and devices where you want to provision, along with the necessary permissions to perform Plug and Play provisioning. For more information, see User profile roles and permissions.

Ensure all device types meet the required prerequisites. Additionally, if you are deploying wireless or sensor devices, make sure those prerequisites are also met. Other prerequisites are optional, but if you choose to implement them, they must be completed before using Plug and Play to provision devices.

Prerequisites for all devices

Make sure all device types meet these prerequisites:

- Make sure devices can automatically discover the Catalyst Center controller in one of these ways:
  - DHCP: See DHCP controller discovery, on page 6.
  - DNS: See DNS controller discovery, on page 7.
  - Cisco Plug and Play Connect cloud service: See Plug and Play connect controller discovery, on page 8.
- Set the cisco.com credentials in the main Catalyst Center settings by using **System** > **Settings** > **Cisco.com Credentials**.

  If needed, set the Cisco Smart Account credentials in **System** > **Settings** > **Smart Account**.
- 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 *Network Plug and Play Troubleshooting Guide for Cisco Catalyst Center*.

Prerequisites for wireless or sensor devices

In addition to the previous prerequisites, make sure any wireless or sensor devices meet these requirements:

- For wireless AP devices, ensure that the Cisco Wireless Controller that is managing the wireless APs has been added to the inventory, provisioned, and assigned to the site where the wireless APs are going to be assigned. This requirement is not needed for Mobility Express APs.
- For wireless AP devices, define the wireless radio frequency profiles. See Create a wireless radio frequency profile. This requirement is not needed for Mobility Express APs.
- For Mobility Express APs, define an IP address pool and a management interface. See Configure IP address pools.
- For ROW APs, we recommend that you create an AP profile with the necessary country code and configure custom site tags. See Configure additional settings for an AP profile for Cisco IOS XE devices.
- For intent APs, you can configure the AP location for PnP onboarding in the **PnP AP Location** window using the **Configure AP Location** check box. This check box is unchecked by default. If necessary, check this check box to configure the site assigned during PnP claim as the AP location during PnP onboarding. For more information, see "Configure AP location for PnP onboarding" in the *Catalyst Center Administrator Guide*.
- For sensors, ensure that the sensor is reachable through the Catalyst Center enterprise IP address (private/enp9s0). A DHCP option 43 string makes the device reachable in unclaimed mode in Catalyst Center; however, to claim the device, it must be reachable from the interface enp9s0 IP address. In the DHCP server, configure the NTP server (DHCP option 42) and the vendor-specific DHCP option 43 with ASCII value "5A1D;B2;K4;I172.16.x.x;J80;", where 172.16.x.x is the virtual IP address of Catalyst Center associated with the enp9s0 interface.

- PnP supports DHCP option 43, DNS option, or devicehelper method for AP discovery. If an AP joins a wireless controller using DNS option, but DHCP option 43 is employed for PnP discovery, contention will occur.

Optional prerequisites for wireless controllers

Optional prerequisites that help to automate the Plug and Play provisioning process include:

- Define the site within the network hierarchy. See Network hierarchy.
- Define the CLI and SNMP credentials for the devices. See Configure global device credentials.



Note You can claim Cisco IOS XE wireless controllers using CLI, SNMPv2c, or SNMPv3 credentials. If you use SNMPv2c, provide both Read Only and Read Write credentials.

- 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-zero 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.

- 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 Catalyst Center use that IP address as the management IP address for the device, especially for the scenario of multiple IPs or VRFs.

- Define network profiles for the devices. See Network profiles overview.

System certificate requirements for Plug and Play

The PnP discovery process requires a valid system certificate to facilitate the secure transition from HTTP to HTTPS. If the system certificate is misconfigured, PnP discovery will fail. To ensure successful device discovery, verify these requirements:

- Ensure that the system certificate contains all necessary Subject Alternative Name (SAN) fields, including the SAN IP and SAN FQDN.

- The FQDN configured in the DHCP Option 43 string must match the FQDN present in the system certificate.
- Ensure that all hostnames defined in the system certificate are resolvable via your DNS infrastructure.

If there is a mismatch between the certificate configuration and the address provided during discovery, the device will be unable to establish a secure connection, resulting in a discovery failure.

DHCP controller discovery

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

The prerequisites for the DHCP discovery method include:

- New devices can reach the DHCP server.
- The DHCP server is configured with Option 43 for Cisco Plug and Play. When configuring DHCP Option 43, you can use either the Catalyst Center Enterprise IP or Enterprise Virtual IP (VIP) or the fully qualified domain name (FQDN). If using an FQDN, ensure that your DNS server is configured to resolve the hostname to the correct Catalyst Center cluster address.

  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 Catalyst Center controller IP address from the response and uses this address to communicate with the controller.

Note For lightweight APs, Option 60 doesn't contain the string `ciscopnp`. Instead, it contains the Vendor Class Identifier (VCI) of the lightweight AP. Make sure to set the DHCP server rules as needed so that Plug and Play can discover the lightweight AP. For more information, see Configure DHCP OPTION 43 for Lightweight Access Points.

DHCP Option 43 consists of a string value that is configured like this example 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 components, delimited by semicolons, including:

- 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)

- I*xxx.xxx.xxx.xxx*;—Enterprise IP or Enterprise VIP address or hostname of the Catalyst Center controller (following a capital letter i). While the Enterprise VIP configuration is optional for a single-node deployment, it is required for a three node cluster. In this example, the IP address is 172.19.45.222.
- J*xxxx*—Port number to use to connect to the Catalyst Center controller. You must use port 80 for HTTP.

Note After trusted certificate installation during PnP discovery, the device automatically switches to using port 443 for HTTPS.

- K4;—Transport protocol to be used between the device and the controller:
  - K4 = HTTP (default)
  - K5 = HTTPS
- T*TrustedCertificateBundleURL*;—Optional parameter that specifies the external URL of the trusted certificate bundle if it is to be retrieved from a different location than the default, which is the Catalyst 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 trusted certificate security and you do not specify the T parameter, the device retrieves the trusted certificate bundle from the Catalyst Center controller.
- Z*xxx.xxx.xxx.xxx*;—IP address of the NTP server. This parameter is mandatory when using trusted certificate 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 7.

If the Catalyst 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, it looks like this sample configuration:

```
ip dhcp pool PnP_Pool
network 214.2.64.0255.255.255.0
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 Catalyst 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 include:

- New devices can reach the DHCP server.
- The Catalyst 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 Catalyst 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 trusted certificate bundle.

These 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.

Procedure

Step 1 The network administrator configures the controller profile for the appropriate Catalyst 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 Catalyst 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 14.

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 Catalyst 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 17.

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

Step 8 The device discovers the Catalyst Center controller by querying the Plug and Play Connect service, identifies itself by serial number to Plug and Play in Catalyst 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 hostnames, or map these two NTP hostnames to local NTP server addresses on the DNS server.

Plug and Play deployment guidelines

Follow these recommendations when using Plug and Play for routers, switches, and wireless controllers:

- 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 Catalyst 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, these 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 this global CLI command on the upstream device to push this CLI to the upcoming Plug and Play device: **pnp 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

You can view information about devices in the **Plug and Play** window.

In addition, you can perform several tasks from this window. For information, see these topics:

- Add or edit a device, on page 12
- Add devices in bulk, on page 13
- Add devices from a Smart Account, on page 15
- Provision a device with Plug and Play, on page 17
- Reset a device, on page 30
- Delete a device, on page 30

Procedure

Step 1 From the main menu, choose **Provision** > **Plug and Play**.

The **Plug and Play** window displays a table with device information, including:

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: • 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	• Unclaimed: Device successfully completed initialization and is ready to be claimed or put in Planned state. • Planned: User provided device configuration or provisioning parameters and the device is ready to be provisioned. • Onboarding: Device onboarding is in progress. • Provisioned: Device is successfully onboarded and added to inventory. For APs and sensors, the state changes to Provisioned after the device is successfully assigned to a wireless controller. • Error: Device had an error and could not be provisioned.
Onboarding State	Onboarding state of the device: • Not Contacted: Device has not called in. A user might have added or reset the device. • Connecting: Device called in. • Initializing: Executing system workflow. Basic device information is collected. Stack license and version mismatches are corrected. • Initialized: System workflow completed. • Executing Workflow: Any tasks that are selected during the claim are applied in this state. Stacks support renumbering and license update based on the product and image version. • Executed Workflow: User workflow completed. • Connection Error: Could not install certificates to secure a connection. • Authentication Error: Could not verify the SUDI certificate. • Authorization Error: Could not verify the user-provided SUDI serial number. • Initialization Error: Error executing system workflow. • Workflow Execution Error: Error executing user workflow. • Executing Reset: Executing reset workflow. You must manually reset the errored device, which reloads the device. • Reset Execution Error: Error executing reset workflow. Click 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.

The Device table displays the information shown in the table for each device. Some of the columns support sorting.

Note

- Certain columns, such as **Device Name** and **Serial Number**, are displayed in the **Default** focus view.
- You can customize the **Devices** table to display or hide columns. Click the settings icon ( ) to display the **Table Settings** slide-in pane, and from the **Edit Table Columns** tab, choose which columns to display or hide. Click **Apply** to save the changes.

Step 2 From the **Plug and Play** window, you can control the display of device information in these ways:

- To sort the rows in ascending or descending order, click any column header with a carrot arrow icon .
- To display devices in a particular state, from the **Device Status** filter, choose **Unclaimed**, **Error**, **Provisioned** or **All**.
- To focus the view, from the **Focus** drop-down list, choose **Default** or **All**.
- To change when table information is refreshed, click the **Auto-Refresh** drop-down list and choose the desired auto-refresh time. By default, the devices table refreshes every 30 seconds.
- To find specific devices, use the **Filter** or **Find** option.
- To view device details, click the name of a device.

  To view additional details, from the window that opens, click the **Details**, **History**, or **Configuration** tabs. For a switch stack, you can also click the **Stack** tab. Some tabs have additional links that you can click for even more information.

Note To delete the stack member from a switch stack, under the **Stack** tab, check the check box next to the desired member and click **Delete Member**.

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.

Field	Description
Enable SUDI Authorization	Enables secure unique device identifier (SUDI) authorization on devices that support it. When enabled, when a device attempts to connect to a Plug and Play server, the server compares the serial number on the SUDI certificate with the user-provided serial number. When the serial numbers match, the device is verified and connects to the Plug and Play server.
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 Add global CLI credentials.

Procedure

Step 1 From the main menu, 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:

- 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 choose **Actions** > **Edit** in the menu bar above the device table. The **Edit Device** dialog displays.

Step 4 Set the fields as needed, referring to the preceding table for more information.

Step 5 Save the settings by doing one of these tasks:

- 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 17.
- 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.

Procedure

Step 1 From the main menu, choose **Provision** > **Plug and Play**.

Step 2 Click **Add Devices**.

The **Add Devices** dialog displays.

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.

Based on the device type, enter data in the mandatory fields.

Note If sites added through a file template are not present in the network hierarchy, they are removed.

For wireless controllers, Catalyst Center processes the data based on the IP address type: IPv4 address, IPv6 address, or both.

Step 6 Upload the CSV file using one of these options:

- Drag and drop the file into the drag-and-drop area.
- Click **Choose a file**, browse to the location of the CSV file, and click **Open**.

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 these tasks:

- 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 17.

Register or edit a virtual account profile

For redirection services, in a Cisco Smart Account, register Catalyst Center as a controller for Cisco Plug and Play Connect. This lets you add the device inventory from the Cisco Plug and Play Connect cloud portal to Cisco Plug and Play in Catalyst Center.

You can register a Smart Account, virtual account, and the relevant server profile information with the Plug and Play system and database. The devices in the registered virtual account are synchronized with the Plug and Play database.

Table 3: Virtual Account Fields

Option	Description
Select Smart Account	Cisco Smart Account name.
Select Virtual Account	Virtual account name. Virtual accounts are subaccounts within a Cisco Smart Account.
IP or **FQDN**	**IP**: IPv4 address, IPv6 address, or both types of IP addresses for this Catalyst Center controller. **FQDN**: The fully qualified domain name for this Catalyst Center controller.
Profile Name	Controller profile name.
Use as Default Controller Profile	*Default controller profile* means that any new device that is added to a virtual account, or any existing device that doesn't have a default controller assigned, will be assigned to this redirection profile.

Procedure

Step 1 From the main menu, 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 register or edit a virtual account profile:

- To register a virtual account, click **Register**. The Register Virtual Account pane 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**. The Edit Profile pane is displayed.

Step 4 Set the fields as needed.

Step 5 Save the settings by doing one of these tasks:

- If you are registering a new virtual account profile, click **Register**.
- If you are editing a virtual account profile, click **Save**.

What to do next

Synchronize the device inventory from the Cisco Plug and Play Connect cloud portal to Catalyst Center Plug and Play. For more information, see Add devices from a Smart Account, on page 15.

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 Catalyst Center Plug and Play.

The virtual accounts table displays information for each profile, including.

Table 4: Virtual accounts information

Column	Description
Virtual Accounts	Virtual account name
Smart Accounts	Smart account that the virtual account is associated with
Profile	Profile name
Controller	Controller IP address

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 14. You can go directly to the PnP Connect settings page by clicking the **PnP Connect** link in the **Add Devices** > **Smart Account Devices** dialog.

Procedure

Step 1 From the main menu, choose **Provision** > **Plug and Play**.

Step 2 Click **Add Devices**.

Step 3 Click **Smart Account Add** to open the **Add Devices from a Smart Account** slide-in pane.

Step 4 If you have already configured the cisco.com user, skip ahead to Step 5. If you haven't, complete these steps:

a) Open an Incognito/private window in your browser (to avoid using previously cached credentials).

b) Open another Catalyst Center GUI instance and log in.

c) Open another instance of the **Add Devices from a Smart Account** slide-in pane.

d) Complete one of these tasks:

If you...	Then...
completed a fresh installation of Catalyst Center 2.3.7.9,	configure a new cisco.com user by clicking the **Add** link in the **Cisco.com ID** field.
upgraded to Catalyst Center 2.3.7.9 and want to use the same cisco.com user that was configured previously,	reauthenticate that user by clicking the **Re-Authenticate** link in the **Cisco.com ID** field.
upgraded to Catalyst Center 2.3.7.9 and don't want to use the same cisco.com user as before,	delete the old cisco.com user and then configure a new one. 1. Click the **Delete** link in the **Cisco.com ID** field. 2. Confirm the operation by clicking **Delete** in the resulting dialog box. 3. Click the **Add** link in the **Cisco.com ID** field.

e) In the **Information** pop-up window, check one or both of these check boxes and then click **Authenticate**:

- (Mandatory) **I am in private or incognito mode**
- (Optional) **Save credentials**

f) In the **Activate your device** pop-up window, confirm that an activation code is displayed and then click **Next**.
g) In the **Log in** pop-up window, enter the cisco.com user's email address and then click **Next**.
h) In the **Verify with your password** pop-up window, enter the cisco.com user's password and then click **Verify**.

The **Device activated** pop-up window appears.

i) Close the **Device Activated** pop-up window.
j) Refresh the **Plug and Play** window, then click **Add Devices** > **Smart Account Add** to reopen the **Add Devices from a Smart Account** slide-in pane.
k) In the **Cisco.com ID** field, confirm that the email address you entered for the user displays. Also confirm that you see the **Change** link.

Step 5 Choose the Smart Account and virtual account that you want to register with Plug and Play.

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

Step 6 From the Devices table, choose the devices that you want to add, and then click **Add Devices**.

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

What to do next

Claim the newly added devices. For more information on claiming a device, see Provision a device with Plug and Play, on page 17.

Provision a device with Plug and Play

When you claim a device, the process of provisioning it begins. When a device is provisioned, Catalyst Center does these actions:

1. Deploys an image to the device.
2. Deploys system configuration CLI commands that configure these settings:
   - Device credentials (CLI and SNMP)
   - Enable SSH v2 and SCP server
   - Disable HTTP and HTTPS servers
   - For switches, vtp mode transparent is enabled
3. Deploys a device onboarding configuration template that corresponds to the type of device:
   - For wired devices, Catalyst Center deploys the onboarding configuration (day-zero) template that you defined.
   - For wireless devices, Catalyst Center deploys a configuration based on the network profile assigned to the site.

If your onboarding configuration template has any of the same system configuration CLI commands, the system configuration CLI commands are overridden, because the onboarding configuration template is applied to the device after the system configuration CLI commands.

4. Deploys Application Quality of Service (QoS) policy on the wired devices, if you configure QoS policy on the site to which the device is provisioned. For more information, see Create an application policy.
5. Pushes the NETCONF configuration on port 830 during device onboarding. The NETCONF port information is saved in the global credentials and network settings.

Note

- If NETCONF is pushed through incorrect port instead of the standard port 830, the device successfully completes onboarding but cannot be added to the inventory.
- If the device isn't assigned to a site during the claiming process, NETCONF isn't configured on the device.
- Automatic NETCONF enablement support is available for only:
  - Cisco Catalyst 9000 Series switches running Cisco IOS XE Release 17.3 or later and
  - Cisco Catalyst 9800 Series Wireless Controllers.

6. Application Telemetry and Controller-Based Application Recognition (CBAR) is enabled on the applicable network devices.
7. Adds the device to the inventory.
8. The PnP label trustpoint is removed automatically after the device successfully completes day-0 onboarding, is in managed state in the inventory, and is assigned to a site.

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

When you claim a device that has not yet booted for the first time, the device is automatically provisioned when it boots up. This process is referred to as device *planning*.

The procedure for provisioning a device depends on the type of device:

- Switches and routers: See Provision a switch or router device, on page 18
- Cisco Wireless Controllers, APs, and sensors: See Provision a wireless controller, on page 22

Provision a switch or router device

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

Make sure that the Plug and Play provisioning prerequisites have been met. For information, see Plug and Play provisioning prerequisites, on page 3.

Procedure

Step 1 From the main menu, choose **Provision** > **Plug and Play**.

Step 2 View the devices in the table.

From the **Focus** drop-down list, choose **Default** or **All** to view the devices.

By default, the devices table is refreshed every 30 seconds. Click the **Auto-Refresh** drop-down list and choose a refresh time.

Use the **Filter** or **Find** option to find specific devices.

Step 3 Check the check box next to the device or devices that you want to claim.

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

Step 5 (Optional) In the **Assign Site** window, do these steps:

a) Change the device hostname, if needed.

b) Assign a site by doing any of these tasks:

- To assign a different site to each device, click **Assign**, and from the **Select a Site** drop-down list, choose a site.
- To assign the same site as the first device to all other devices, in the **Actions** column, hover your cursor over the ellipsis icon ••• and choose **Apply Site to All**.
- To assign a site from any device to some other devices, in the **Actions** column, hover your cursor over the ellipsis icon ••• and choose **Assign this Site to Other Devices**, choose the devices, and click **Assign**.
- To clear the site assigned to the devices, click **Clear Site**.

Note If you do not assign a device to a site, you must choose a template for the device in Step 6, on page 19.

c) Click **Next**.

Step 6 In the **Assign Configuration** window, do these steps:

a) In the **Configuration** column, click **Assign** for the device that you want to configure.

b) If the device configuration doesn't need any changes, click **Cancel** and proceed to the next step. Otherwise, change or configure any of these settings:

- **Device Name**: Change the device hostname, if needed.
- **Image**: From this 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.

Note If the device software image version or golden tagged version is 17.14.1 or later, the device claim is blocked if the selected site is configured with MD5 authentication for SNMP credentials.

If a golden image is not available, and the images are tagged with a specific device role (such as Border, Core, and so on) for this device type in the image repository, the drop-down list displays the available images.

To claim the device, you must also configure SHA authentication for SNMP credentials, or the software image version must be earlier than 17.14.1. For information on how to configure SHA authentication, see Edit global device credentials.

- **Template**: From this drop-down list, choose an onboarding configuration template to apply to the device. If there is only one onboarding configuration template defined for this device type, it is chosen by default.

Note If you have not assigned the device to a site, you must choose a template for the device. The template that you choose must include the CLI commands necessary to configure the global device credentials on the device. Otherwise, the device is added to the inventory in an unmanaged state.

- **Apply the PKCS12 device certificate on the device**: Check this check box to deploy a PKCS12 certificate to the device. This option is available only for routers.
- **RTU License Level**: From this drop-down list, choose **Lanbase** or **IP Services**. This option is available only for Cisco Industrial Ethernet (IE) 4000 Series and 5000 Series switches.
- **Select a Cabling Scheme**: From this 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 these cabling schemes.

Figure 1: Cabling schemes



- **Select a Top of Stack Serial Number**: The top-of-stack serial number autopopulates with the user-entered stack member serial number. If you don't want to use the autopopulated serial number, click the serial number, and in the **Select a Top of Stack Serial Number** field, click the drop-down arrow. Click the **X** icon to deselect the serial number.

  This option appears only for switches that support stacking, and only if they are connected as shown in the cabling schemes image.

  For a *planned device*, the top-of-stack serial number is set as the default. If necessary, you can specify a different serial number.

  For an *unclaimed device*, the top-of-stack serial number is not set as the default. Choose the top-of-stack serial number from the drop-down list.

- **Select a License Level**: From this drop-down list, choose the stack license level. Click the **X** icon to deselect the license level.

  This item displays only for switches that support stacking.

c) Click **Save**.

d) From the **Clear Configuration** drop-down list, choose any of these options:

- **Clear Device Certificates**: Choose this option and check the check box next to each of the devices that you want to clear the certificate from, and click **Clear**.
- **Clear Images**: Choose this option and check the check box next to each of the devices that you want to clear the image from, and click **Clear**.
- **Clear Templates**: Choose this option and check the check box next to each of the devices that you want to clear the template from, and click **Clear**.
- **Clear License Levels**: Choose this option and check the check box next to each of the devices that you want to clear the license level from, and click **Clear**.

e) To apply an image or template from one device to other devices, in the **Actions** column, hover your cursor over the ellipsis icon ••• and choose **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**.

f) 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.

g) After you have configured all the devices, click **Next**.

Step 7 To configure template parameter values for all the devices in bulk, skip to the next step. To configure template parameter values for devices one at a time, from the **Provision Templates** window:

a) Click the name of the device that you want to configure.

b) If the device was assigned a configuration template, specify the values for the parameters that were defined in the template.

Enter the values for each parameter in the fields for each device. A red asterisk indicates a required field.

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

d) 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 the devices.

e) Click **Next**.

Step 8 To specify parameter values for all the devices in bulk, in the **Provision Templates** window:

a) Click **Export** to save the CSV template file.
b) Add the values for each of the parameters to the file and save the file.
c) Click **Import**.
d) Drag and drop the file to the drag-and-drop area, or click "**click to select**" and select the file.
e) Click **Import**.
f) Click **Next**.

Step 9 In the **Summary** window, view details about the devices and their configuration preview status.

Step 10 Verify the **Day-0 Config** column for each device to see whether the configuration preview succeeded.

If the preview shows an error, 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, resolve issues, if any, before claiming the device. You may need to go back to the **Provision Templates** step and change the parameter values, and the template, revisit the **Design** area to update network design settings, or resolve network connectivity issues, if any.

After you resolve the problem, return to the **Day-0 Config** column, click **Retrying getting Day-0 configuration preview for failed device(s)**, and click **OK**.

Step 11 Click a link in the **Day-0 Config** column to see more information about the device, its configuration, and configuration preview errors, if any.

Step 12 Click **Claim**.

Step 13 In the confirmation dialog box, click **Yes** to claim the devices.

What to do next

If you have configured network settings, provision these settings on the devices. For more information, see Complete the provisioning process, on page 29.

Provision a wireless controller

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

Before you begin

Make sure that the Plug and Play provisioning prerequisites have been met. For information, see Plug and Play provisioning prerequisites, on page 3.

Procedure

Step 1 From the main menu, choose **Provision** > **Plug and Play**.

Step 2 View the devices in the table.

You can use the search bar to find specific devices.

Step 3 Check the check box next to the device or devices that you want to claim.

Step 4 From the menu bar above the device table, choose **Actions** > **Claim**.

Step 5 (Optional) In the **Assign Site** window, do these steps:

a) Change the device hostname, if needed.

b) Assign a site by doing any of these tasks:

- To assign a different site to each device, click **Assign**, and from the **Select a Site** drop-down list, select a site.
- To assign the same site as the first device to all other devices, in the **Actions** column, hover your cursor over the ellipsis icon and select **Apply Site to All**.
- To assign a site from any device to some other devices, in the **Actions** column, hover your cursor over the ellipsis icon and select **Assign this Site to Other Devices**, select the devices, and click **Assign**.
- To clear the site assigned to the devices, click **Clear Site**.

If the wireless network profile associated with the assigned site has an onboarding template, Catalyst Center uses this template for PnP onboarding. For more information, see Add templates to a network profile.

c) Click **Next**.

Step 6 In the **Assign Configuration** window, do these steps:

a) In the **Configuration** column, click **Assign** for the device that you want to configure.

b) If the device configuration doesn't need any changes, click **Cancel** and continue to the next step. Otherwise, change or configure any of these settings:

- **Device Name**: Change the device hostname, if needed.
- **Image**: From this drop-down list, select 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.

Note If the device software image version or golden tagged version is 17.14.1 or later, the device claim is blocked if the selected site is configured with MD5 authentication for SNMP credentials.

To claim the device, you must also configure SHA authentication for SNMP credentials, or the software image version must be earlier than 17.14.1. For information on how to configure SHA authentication, see Edit global device credentials.

- **Template**: From this drop-down list, select an onboarding configuration template to apply to the device. If there is only one onboarding configuration template defined for this device type, it is chosen by default.

Note If you have not assigned the device to a site, you must choose a template for the device. The template that you choose must include the CLI commands necessary to configure the global device credentials on the device. Otherwise, the device is added to the inventory in an unmanaged state.

For more information about onboarding APs for non-intent-based network deployments, including Assurance use case and Per-Device Configurations, see Onboard APs using PnP for non-intent-based deployments.

- **Catalyst Wireless LAN Controller Settings**: For a Cisco Catalyst 9800 Series Wireless Controller, enter data in the required fields: **Wireless Management IP**, **Subnet Mask**, **Gateway**, **Wireless Management IP (IPv6)**, **Prefix**, **Gateway (IPv6)IP Interface Name**, and optionally **VLAN ID**.

Note The available fields vary based on the IP address type of the wireless controller. If the wireless controller has only the IPv4 address type, Catalyst Center displays the fields for IPv4 address. If it has only the IPv6 address type, Catalyst Center displays the fields for IPv6 address. If it has both IPv4 and IPv6 address types, Catalyst Center displays the fields for both IPv4 address and IPv6 address.

- For a Mobility Express device, enter values in these fields: **Wireless management IP**, **Subnet mask**, and **Gateway**.
- If you made any changes, click **Save**; otherwise, click **Cancel** to return to the list and configure other devices.

c) From the **Clear Configuration** drop-down list, select any these options:

- **Clear Device Certificates**: Select this option and check the check box next to each of the devices that you want to clear the certificate from, and click **Clear**.
- **Clear Images**: Select this option and check the check box next to each of the devices that you want to clear the image from, and click **Clear**.
- **Clear Templates**: Select this option and check the check box next to each of the devices that you want to clear the template from, and click **Clear**.
- **Clear License Levels**: Select this option and check the check box next to each of the devices that you want to clear the license level from, and click **Clear**.

d) To apply an image or template from one device to other devices, in the **Actions** column, hover your cursor over the ellipsis icon ••• and select **Apply Image to Other Devices** or **Apply Template to Other Devices**.

You can apply the device license level to other devices by clicking **Apply License Level to Other Devices**.

e) 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.

f) After you have configured all the devices, click **Next**.

Step 7 In the **Provision Templates** window, select the template from the **Devices** area, enter your domain name in the **domain** field, and click **Next**.

Step 8 In the **Summary** window, view details about the devices and their configuration preview.

Step 9 Check the **Device Configuration** column for each device to see if the configuration preview succeeded.

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. 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. After you have resolved the problem, you can go back to this tab, click **Retrying getting Day-0 configuration preview for failed device(s)**, and click **OK**. Ensure that the wireless controller that is managing a device has been added to the inventory and assigned to the site where the wireless device is assigned.

Step 10 In the **Device Configuration** column, click **Preview Configuration** to review the configuration.

Step 11 Click **Claim**.

Step 12 In the confirmation dialog box, click **Yes** to claim the devices and start the provisioning process.

Note If there is a conflicting operation for the selected site, to continue with the current configuration, you must either wait for the existing, scheduled, or pending-review operations to complete or discard the operations.

What to do next

If you have configured network settings, provision these settings on the devices. For more information, see Complete the provisioning process, on page 29.

Provision an AP or sensor device

Use this procedure to claim an AP or sensor 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

Make sure that the Plug and Play provisioning prerequisites have been met. For information, refer to Plug and Play provisioning prerequisites, on page 3.

Procedure

Step 1 Navigate to the **Plug and Play** to choose the required devices.

a) From the main menu, choose **Provision** > **Plug and Play**.

b) View the devices in the table.

You can use the search bar to find specific devices.

c) Check the check box next to the devices that you want to claim.

d) From the menu bar above the device table, choose **Actions** > **Claim**.

Step 2 (Optional) In the **Assign Site** window, do these steps:

a) Change the device hostname, if needed.

b) Assign a site by doing any of these tasks:

- To assign a different site to each device, click **Assign**, and from the **Select a Site** drop-down list, select a site.
- To assign the same site as the first device to all other devices, in the **Actions** column, hover your cursor over the ellipsis icon ••• and select **Apply Site to All**.
- To assign a site from any device to some other devices, in the **Actions** column, hover your cursor over the ellipsis icon ••• and select **Assign this Site to Other Devices**, select the devices, and click **Assign**.
- To clear the site assigned to the devices, click **Clear Site**.

If the wireless network profile associated with the assigned site has an onboarding template, Catalyst Center uses this template for PnP onboarding. For more information, refer to Add templates to a network profile.

Note In the **System** > **Settings** > **Device Settings** > **PnP AP Location** window:

- If the **Configure AP Location** check box is checked, Configure APs assigns this site as the AP location during PnP onboarding.
- If the **Configure AP Location** check box is unchecked, Catalyst Center does not configure this site as the AP location during PnP onboarding. You can configure the AP location using the **Configure Access Points** workflow. For more information, refer to Configure APs.

For more information, refer to "Configure AP location for PnP onboarding" in the *Cisco Catalyst Center Administrator Guide*.

c) Click **Next**.

Step 3 In the **Assign Configuration** window, do these steps:

a) In the **Configuration** column, click **Assign** for the device that you want to configure.

b) If the device configuration doesn't need any changes, click **Cancel** and continue to the next step. Otherwise, change or configure any of these settings:

- **Device Name**: Change the device hostname, if needed.
- **Template**: From this drop-down list, select an onboarding configuration template to apply to the device. If there is only one onboarding configuration template defined for this device type, it is chosen by default.

Note If you have not assigned the device to a site, you must choose a template for the device. The template that you choose must include the CLI commands necessary to configure the global device credentials on the device. Otherwise, the device is added to the inventory in an unmanaged state.

For more information about onboarding APs for non-intent-based network deployments, including Assurance use case and Per-Device Configurations, refer to Onboard APs using PnP for non-intent-based deployments.

- For an AP, select an AP zone from the **AP Zone** drop-down list. The **RF Profile** is auto-populated, and the SSID count appears based on the selected AP zone. When you select the default AP zone, choose the RF profile.
- For an AP, in the **Radio Frequency Profile** drop-down list, select a radio frequency profile to apply to the device. This may be set if you designated one profile as a default.

- For a sensor, in the **Sensor Settings** drop-down list, select the sensor device profile (backhaul) to apply to the device.

  Note For Cisco Aironet 1800s Active Sensor earlier than 1.3.1.2, make sure that you do not select the sensor device profile `CiscoProvisioningSSID`. Instead, select 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.

c) From the **Clear Configuration** drop-down list, select any these options:

- **Clear Device Certificates**: Select this option and check the check box next to each of the devices that you want to clear the certificate from, and click **Clear**.
- **Clear Images**: Select this option and check the check box next to each of the devices that you want to clear the image from, and click **Clear**.
- **Clear Templates**: Select this option and check the check box next to each of the devices that you want to clear the template from, and click **Clear**.
- **Clear License Levels**: Select this option and check the check box next to each of the devices that you want to clear the license level from, and click **Clear**.

d) To apply an image or template from one device to other devices, in the **Actions** column, hover your cursor over the ellipsis icon ••• and select **Apply Image to Other Devices** or **Apply Template to Other Devices**.

e) 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.

f) After you have configured all the devices, click **Next**.

Step 4 In the **Provision Templates** window, select the template from the **Devices** area, enter your domain name in the **domain** field, and click **Next**.

Note If device is assigned to a site, click **Next**.

Step 5 In the **Summary** window, view details about the devices and their configuration preview.

Step 6 Check the **Device Configuration** column for each device to verify if the configuration preview succeeded.

If the preview shows an error, you can click the **Actions** link in the error message above the table to verify what actions you need to take. You can click 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. After you have resolved the problem, you can go back to this tab, click **Retrying getting Day-0 configuration preview for failed device(s)**, and click **OK**. Ensure that the wireless controller that is managing a device has been added to the inventory and assigned to the site where the device is assigned.

Step 7 In the **Device Configuration** column, click **Preview Configuration** to review the configuration.

Step 8 Click **Claim**.

Step 9 In the confirmation dialog box, click **Yes** to claim the devices and start the provisioning process.

Note If there is a conflicting operation for the selected site, to continue with the current configuration, you must either wait for the existing, scheduled, or pending-review operations to complete or discard the operations.

What to do next

If you have configured network settings, provision these settings on the devices. For more information, refer to Complete the provisioning process, on page 29.

Provision StackWise Virtual Link switch

You can onboard a pair of connected switches as a single logical device with StackWise Virtual Link (SVL) support during PnP onboarding. Currently, SVL PnP onboarding is supported only for Catalyst 9500 Series switches .

Before you begin

- Ensure that both switches are directly connected.
- Connect the switches with links providing a minimum speed of 1 Gbps and ensure that the interface speeds are matched.
- Ensure that the switches are in an initialized state.

Procedure

Step 1 From the main menu, choose **Provision** > **Plug and Play**.

Step 2 Click **Claim a SVL switch**.

Step 3 In the **Claim as an SVL switch** Pop-up window, provide the values required for the SVL onboarding settings:

a. **Active Switch**: Choose one of the switches as active switch.

b. **Standby Switch**: Choose another switch as the standby switch.

c. **StackWise Virtual Link**: Choose the SVL links. You can choose up to eight SVL links.

d. **Dual-Active Detection Link**: Choose a dual-active detection link if available.

e. **Domain**: Assign a unique value for the domain.

Step 4 Click **Select Site** and choose the desired site for SVL switches.

Step 5 Click **Manage Template** and choose the template to be provisioned to the SVL switches.

Step 6 (Optional) Choose the standard image to be applied after SVL formation.

If the image versions on the devices differ, PnP enforces the selection of a standard image and applies it to both devices before SVL formation.

Step 7 Click **Claim**.

The PnP server creates the SVL and provisions the device.

Complete the provisioning process

During Plug and Play provisioning, only the device credentials and the onboarding configuration are pushed to the device. No other network settings are pushed. After Plug and Play provisioning is completed, you can complete the provisioning process by pushing the network settings that are configured in the **Design** area.

The network settings include AAA server settings, if these are configured. In the case of Cisco ISE, Catalyst Center configures the device on Cisco ISE as a AAA client for RADIUS or TACACS.

Note For Cisco Catalyst 9800 Series Wireless Controllers and Cisco Catalyst 9000 Series Switches, local AAA configurations are pushed to device when NETCONF is enabled during the day-zero configuration.

For wireless and sensor devices, the network settings include wireless settings, such as RF profiles and antenna radio profiles, if these are configured. For more information, see Wireless device provisioning overview.

Before you begin

- Ensure that the device has been provisioned (onboarded) using one of these procedures:
  - Provision a switch or router device, on page 18
  - Provision a wireless controller, on page 22
- Configure network settings. For information, see Configure Network Settings.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

Step 2 Select the device and choose **Actions** > **Provision** > **Provision Device**.

Step 3 Proceed through the steps in the workflow.

Step 4 In the **Summary** window, review the remaining network settings. To make any changes, click **Edit** next to the relevant category; otherwise, click **Deploy**.

Note If the device software image version or golden tagged version is 17.14.1 or later, the device claim is blocked if the selected site is configured with MD5 authentication for SNMP credentials.

To claim the device, you must also configure SHA authentication for SNMP credentials, or the software image version must be earlier than 17.14.1. For information on how to configure SHA authentication, see Edit global device credentials.

Step 5 (Optional) After deploying the configuration on the devices, the **Task Progress** bar displays the progress of the ongoing provisioning task under **Activities** > **Tasks** (which you can view by clicking the task name).

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 explains 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.
- If a device is in a transient state (such as Connecting or Executing), it cannot be deleted from the Plug and Play Devices list.

Procedure

Step 1 From the main menu, 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 From the menu bar above the device table, choose **Actions** > **Delete**.

Step 5 (Optional) For unclaimed devices, check the **Delete Plug and Play capabilities for this device in inventory** check box.

If you choose this option, Catalyst Center deletes the device profile, and the device does not reappear in PnP.

The device remains in inventory and can still be managed. You can re-enable PnP capabilities later.

Step 6 Click **Ok**.

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**.

Note If a device is in a transient state (such as Connecting or Executing), it cannot be reset.

Procedure

Step 1 From the main menu, 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 displays.

Step 5 Choose one of these 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**.