Onboard and Provision Devices with Plug and Play

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 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.

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. We recommend that you define the site within the network hierarchy. See Network Hierarchy Overview.

2. 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-zero configuration. See Create Templates to Automate Device Configuration Changes.

> **Note** Day-zero templates do not support Interactive commands.

3. Define network profiles for the types of devices you are deploying. See Network Profiles Overview.

4. We recommend that you define the device credentials (CLI and SNMPv2c/SNMPv3) for the devices you are deploying. If you are 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 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 11 or Add Devices in Bulk, on page 12.

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 Plug and Play Provisioning 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 8.

2. Claim the device by assigning a site, image, configuration template, or profile. See Provision a Device with Plug and Play, on page 15. 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 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 13.

2. Synchronize the device inventory from the Smart Account. See Add Devices from a Smart Account, on page 14.

3. Find the device on the devices list by filtering on unclaimed devices or searching for it by name. See View Devices, on page 8.

4. Claim the device by assigning a site, image, configuration template, or profile. See Provision a Device with Plug and Play, on page 15.

5. Devices boot up and are automatically provisioned.

Plug and Play Provisioning Prerequisites

Before using Plug and Play provisioning, make sure the required prerequisites are met for all device types. In addition, if you are deploying wireless or sensor devices, make sure those prerequisites are met. Other prerequisites are optional, but if you decide to do them, they must be done before you use Plug and Play to provision devices.

Prerequisites for All Devices

Make sure all device types meet the following prerequisites:

- Make sure devices can automatically discover the Cisco DNA Center controller in one of the following ways:

  - DHCP: See DHCP Controller Discovery, on page 5.

  - DNS: See DNS Controller Discovery, on page 6.

  - Cisco Plug and Play Connect cloud service: See Plug and Play Connect Controller Discovery, on page 6.

- Set the Cisco.com credentials in the main Cisco DNA Center settings by using **System** > **Settings** > **Cisco.com Credentials**.

  If needed, set the Cisco Smart Account credentials in **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 *Network Plug and Play Troubleshooting Guide for Cisco DNA Center*.

Prerequisites for Wireless or Sensor Devices

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

- For wireless AP devices, ensure that the Cisco Wireless Controller that is managing the wireless APs has been added to the inventory 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 and Add AP Groups, Flex Groups, Site Tags, and Policy Tags to a Network Profile.

- For sensors, 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.

Optional Prerequisites

The following prerequisites are optional, but help to automate the Plug and Play provisioning process:

- Define the site within the network hierarchy. See Network Hierarchy Overview.

- Define the CLI and SNMP credentials for the devices. See Global Device Credentials Overview.

Note You can claim wireless devices 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 Cisco DNA 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.

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)

- I*xxx.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.

- J*xxxx*—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

- • T*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.

- • Z*xxx.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 6.

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 214.2.64.0255.255.255.0
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 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 13.

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 15.

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 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:

- 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: **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 the following topics:

Step 1   Click the menu icon (☰) and choose **Provision** > **Plug and Play**.

The **Plug and Play** window displays a table with the following device information:

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.
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.

Column	Description
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 following 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 the following 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.

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. 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 Configure Global CLI Credentials.

Step 1   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 15.
- 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   Click the menu icon (☰) and choose **Provision** > **Plug and Play**.

Step 2   Click **Add Devices**.

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 .

Register or Edit a Virtual Account Profile

For redirection services, in a Cisco Smart Account, register Cisco DNA 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 Cisco DNA 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

Field	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 address or fully qualified domain name of this Cisco DNA 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.

Step 1   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 register or edit a virtual account profile, as follows:

- 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 the following:

- 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 Cisco DNA Center Plug and Play. For more information, see Add Devices from a Smart Account, on page 14.

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.
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 13. 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 Click the menu icon (☰) and choose **Provision** > **Plug and Play**.

Step 2 Click **Add Devices**.

Step 3 Click **Smart Account Devices**.

Step 4 If you need to enter a Cisco.com ID (Cisco.com ID shows as Not Associated), do the following:

a) Click the **Add** link.

b) Enter the Cisco.com username and password.

c) 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.

d) Click **Submit**.

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

When you claim a device, you begin the process of provisioning it. When a device is provisioned, Cisco DNA Center performs the following actions:

1. Deploys an image to the device.

2. Deploys system configuration CLI commands that configure the following 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 on boarding configuration template that corresponds to the type of device:

    - For wired devices, Cisco DNA Center deploys the on boarding configuration (day-zero) template that you defined.

    - For wireless devices, Cisco DNA Center deploys a configuration based on the network profile assigned to the site.

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

4. Pushes the Netconf configuration on port 830 during device on boarding. The Netconf port information is saved in the global credentials and network settings.

   Note   If the device is not assigned to a site during claiming process, Netconf will not be configured in the device.

   Automatic Netconf enablement support is available only for Cisco Catalyst 9000 Series switches running Cisco IOS-XE 17.3 or later.

5. Adds the device to the inventory.

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*.

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, as follows:

- Switches and routers: See Provision a Switch or Router Device, on page 16

- Cisco Wireless Controllers, access points, and sensors: See Provision a Wireless or Sensor Device, on page 19

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.

Step 1   Click the menu icon (☰) and 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 gets 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 the following:

a) Change the device hostname, if needed.

b) Assign a site by doing any of the following:

- 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**.

c) Click **Next**.

Step 6 In the **Assign Configuration** window, do the following:

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 Step 7. Otherwise, change or configure any of the following 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.

- **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 to proceed further.

- **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 and 5000 Series Switches.

   Note   To choose **IP Services**, accept the End User License Agreement (EULA) in **System** > **Settings** > **Device EULA Acceptance**.

- **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 the following cabling schemes.

  Figure 1: Cabling Schemes
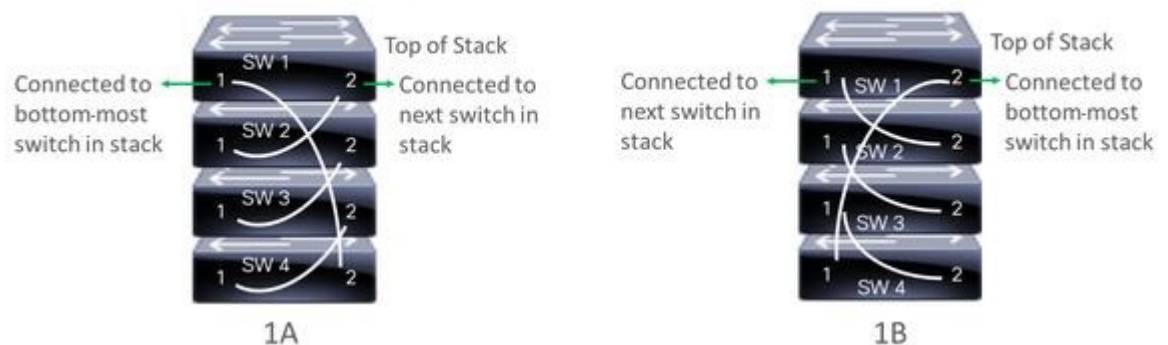
- **Select a Top of Stack Serial Number**: The top-of-stack serial number autopopulates with the user-entered stack member serial number. If you don't want to use the autopopulated serial number, click the serial number, and in the **Select a Top of Stack Serial Number** field, click the drop-down arrow. 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 preceding image.

For a *planned device*, the top-of-stack serial number is set as the default.

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.

- **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 is displayed only for switches that support stacking.

c) Click **Save**.

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

- **Clear Device Certificates**: Choose this option and check the check box adjacent 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 adjacent 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 adjacent 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 adjacent 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, proceed to Step 8. To configure template parameter values for devices one at a time, from the **Provision Templates** window, do the following:

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, do the following:

a) Click **Export** to save the CSV template file.

b) Add the values for each of the parameters to the file and save the file.

c) Click **Import**.

d) Drag and drop the file to the drag-and-drop area, or click "**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 was successful.

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, you can return to **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 22.

Provision a Wireless or Sensor Device

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

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

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

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 are prerequisites for the claim process and, after 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 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 Cisco Wireless Controller or sensor devices.

Step 7 From the **Select a Site** drop-down list, choose a site and floor to assign to each device. AP devices must be assigned to a floor with a wireless controller.

To apply the same site as the first device to all other devices, check 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.

Note Cisco DNA Center does not configure this site as the AP location during AP PnP onboarding. You can configure the AP location using the **Configure Access Points** workflow. For more information, see Configure AP Workflow.

Step 8 Click **Next**.
The **Assign Configuration** window opens.

Step 9 (Optional) You can change which columns are displayed in the table by clicking the settings icon (⚙) in the top-right corner of the table and choosing the desired columns. Click **Apply** to save the changes.

Step 10 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 click **Cancel** if no changes are needed.

   b) (Optional) In the **Device Name** field, change the device name, if needed.

   c) For an AP 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.

   d) For a wireless controller, enter values in the following fields: **Wireless management IP**, **Subnet mask**, **Gateway**, **IP interface name**, and optionally, **VLAN ID**.

   e) For a Mobility Express device, enter values in the following fields: **Wireless management IP**, **Subnet mask**, and **Gateway**.

   f) 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 earlier than 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.

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

   h) 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 (Optional) For a wireless sensor device, to assign a software image, do the following:

   a. In the **Image** column, click **Assign**.

   b. From the **Image** drop-down list, choose a golden software image.

   c. Click **Save**.

Step 12 If any devices are a Cisco Catalyst 9800-CL Wireless Controller, click **Assign** next to **Image** in the **Configuration** column and follow these steps:

   a) (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.

   b) Click **Save**.

Step 13   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 14   Click **Next**.

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

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 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 16   Click **Claim**.

Step 17   In the confirmation dialog box, click **Yes** to claim the devices and start the provisioning process.

What to do next

If you have configured network settings, provision these settings on the devices. For more information, see .

Provision a Cisco DNA Traffic Telemetry Appliance

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

Before you begin

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

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

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, check 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, click the **Actions** link in the error message above the table to see what actions you need to take. 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, click **Retrying getting Day-0 configuration preview for failed device(s)**, and click **OK**.

Step 12   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**.

Step 14   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 information, see Complete the Provisioning Process, on page 22.

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, Cisco DNA Center configures the device on Cisco ISE as a AAA client for RADIUS or TACACS.

For wireless and sensor device, 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 the following procedures:

• Provision a Switch or Router Device, on page 16

• Provision a Wireless or Sensor Device, on page 19

• Configure network settings. For information, see Configure Network Settings.

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

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.

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