Understand Switch Onboarding through Catalyst Center Plug and Play

Contents

Introduction

Description

Audience

Requirements

Prerequisites

Plug and PlayConceptOverview

- 1. DHCP Discovery of PnP Server
- 2. DHCP Option 43 Format
  - Option 43 Field Definitions
- 3. DHCP Option 43 ConfigurationExamples
- 4. PnP startup VLANBehaviour

CatalystCenterCertificate Verification

- GUI Verification
- CLI Verification

Network Diagram

SwitchOnboardingMethods

- 1. Onboard using VLAN1
- 2. Onboard using custom VLAN
- 3. Onboard Switch using the management port
- 4. Switch Console logs

Onboarding Switch to CatalystCenterwithout Day-0 templates

- 1. To claim switches:
- 2. To name and map the switch:
- 3. AssignSoftwareImage orTemplate (optional):
- 4. Provision templates
- 5. Summary
- 6. Monitorthe ClaimingProcess

Onboarding Switch to CatalystCenterwith Day-0 templates

- 1. Create Day-0 orOnboardingTemplate
- 2. Add Template Details
- 3. Edit the Template
- 4. CreateNetwork Profile
- 5. Add template and edit network profile settings
- 6. Save the profile
- 7. Assign network profile to the site where switch/switches are to be onboarded
- 8. ClaimSwitches
- 9. Assign a name for the switch and assign to a site

10. Assign a Day-0 template
11. Provision templates
12. Summary
13. Monitor claim progress
Verification
Bulk ImportofDevicesinto CatalystCenterPlug and Play Inventory
1. Prerequisites
2. Bulk ImportProcedure
Troubleshooting
1. PnP Connectivity Validation
1.1. ICMPReachability
1.2. HTTPHELLO validation
1.3. HTTPScertificate retrieval
1.4. PnP profile status
2. DHCP Validation
2.1. Verify DHCP IP address assignment
2.2. Confirm Lease Server
2.3. Validate Option 43 using debug logs
Best Practices

Introduction

This document describes Catalyst Center Plug and Play for automated switch onboarding, the full lifecycle, discovery methods, and troubleshooting.

Description

Catalyst Center Plug and Play (PnP) automates Cisco Catalyst switch onboarding through the Cisco IOS® XE embedded PnP agent. This process enables secure discovery, authentication, and initial provisioning with minimal manual effort, significantly speeding up deployments and improving configuration consistency. By supporting scalable rollouts through standardized settings and optional Day-0 templates, PnP ensures a reliable deployment at scale.

The document outlines the complete onboarding lifecycle, including PnP workflows, discovery methods, onboarding options, and certificate validation. It also provides detailed guidance on device claiming, verification, troubleshooting, and industry best practices.

Audience

This document is intended for network administrators, deployment engineers, and system integrators who deploy and manage Cisco Catalyst switches through Catalyst Center.

Requirements

It is preferable that readers of this document have a basic working knowledge of these topics:

- Catalyst Center
- Cisco Catalyst switches
- Network automation and provisioning
- DHCP and DNS fundamentals

Prerequisites

Ensure that these prerequisites are met before starting the onboarding process:

- Catalyst Center 2.3.7.9 or later is installed and operational.
- Cisco Catalyst switches run a supported Cisco IOS XE release 16.12.x or later.
- Network connectivity is available between the Catalyst switches and Catalyst Center.
- The DHCP server is configured with Option 43 pointing to the Catalyst Center's enterprise interface IP address or FQDN.
- Switches are in factory-default (out-of-box) state, and the **pnpa service reset** command available on IOS XE 16.12.1 and later can be used to reset a switch to this state.

Plug and Play Concept Overview

Review these key concepts that explain how Catalyst Center Plug and Play onboards a new switch.

1. DHCP Discovery of PnP Server

When a factory-default Cisco Catalyst switch powers on, the PnP agent attempts to discover a Plug and Play controller (like Catalyst Center) using DHCP.

The discovery process use the standard DHCP exchange:

- DHCP Discover
- DHCP Offer
- DHCP Request
- DHCP Acknowledgement

If configured correctly, the DHCP server includes Option 43, which provides the switch with connection details for the PnP server.

2. DHCP Option 43 Format

The DHCP Option 43 value is a semicolon-separated ASCII string that specifies how the switch connects to the PnP server.

Example:

```
option 43 ascii 5A1N;B2;K4;I10.127.212.43;J80;
```

Option 43 Field Definitions

- 5A1N
  - 5 – PnP suboption
  - A – Active mode (device initiates communication)
  - 1 – PnP agent template version
  - N – Debug disabled (D enables debugging)
- B2 – PnP server IP address type
  - 1 – Hostname
  - 2 – IPv4 address
  - 3 – IPv6 address
- K4 – Transport protocol
  - 4 – HTTP
  - 5 – HTTPS
- I – PnP server IP address or FQDN
- J – TCP port number

Optional parameters include:

- T – Trustpool certificate bundle URL (mandatory for HTTPS)

- Z – NTP server IP address (mandatory when using Trustpool security)

3. DHCP Option 43 Configuration Examples

- **Example 1:** Option 43 IPv4 configuration: 10.127.212.43 [Catalyst Center enterprise interface IP address]

```
ip dhcp pool pnp_pool
  network 10.127.212.0 255.255.255.0
  option 43 ascii 5A1D;B2;K4;I10.127.212.43;J80;
  default-router 10.127.212.49
```

- **Example 2:** Option 43 hostname configuration: catc1.cisco.com [Catalyst Center FQDN]

```
ip dhcp pool pnp_pool
  network 10.127.212.0 255.255.255.0
  option 43 ascii 5A1D;B1;K4;Icatc1.cisco.com;J80;
  default-router 10.127.212.49
```

- **Example 3:** Option 43 IPv6 configuration: 2001:60:60:60::133 [Catalyst Center enterprise interface IPv6 address]

```
ipv6 dhcp pool pnp_pool
 address prefix 2001:70:70:70::/64
 link-address 2001:70:70:70::7/64
 vendor-specific 9
  suboption 16 ascii "ciscopnp"
  suboption 17 ascii "5A1D;B3;K4;I2001:60:60:60::133;J80"
```

4. PnP startup VLAN Behaviour

By default, a factory-reset switch uses VLAN 1 for PnP management. Cisco recommends using a dedicated management VLAN in production environments. This is the command to configure a Custom PnP Startup VLAN:

```
pnp startup-vlan <vlan-id>
```

This command must be configured on an upstream switch. The upstream switch communicates the PnP startup VLAN to the new switch using Cisco Discovery Protocol (CDP). The downstream switch then:

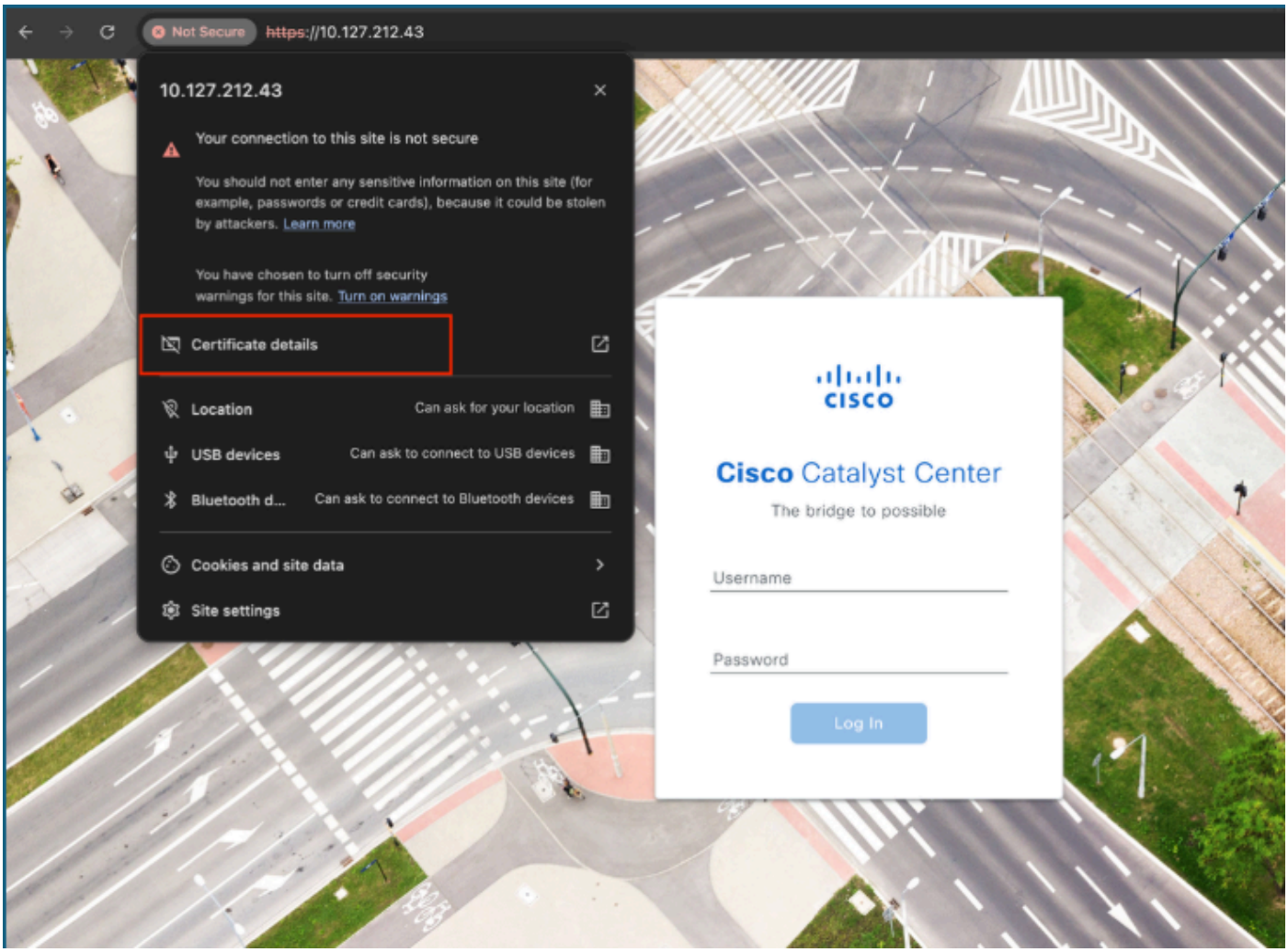
- Disables DHCP on VLAN 1
- Enables DHCP on the configured startup VLAN
- Updates the trunk to allow the new VLAN

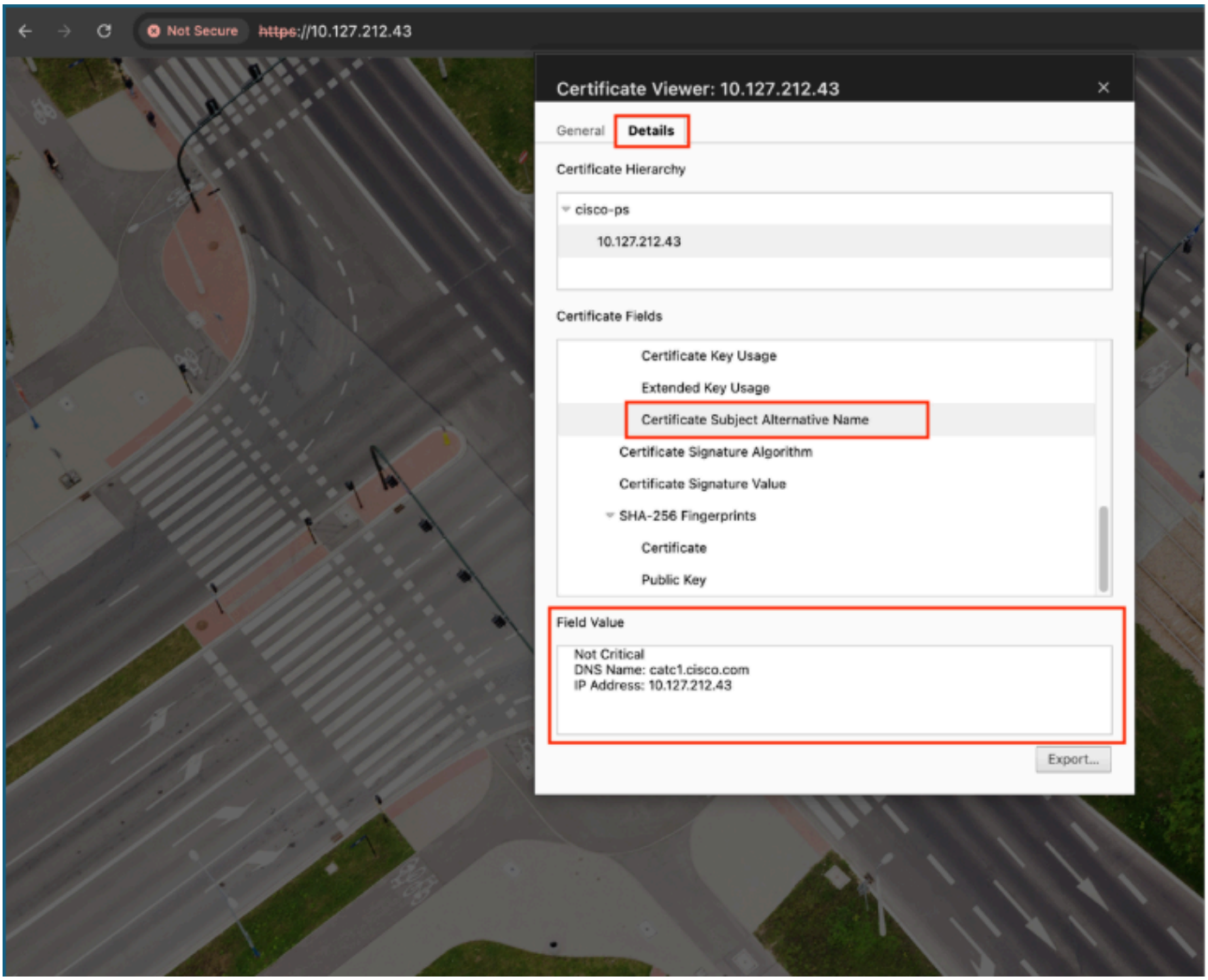
Catalyst Center Certificate Verification

Secure onboarding requires that the Catalyst Center SSL certificate includes the IP address or FQDN used by the switch in the Subject Alternative Name (SAN) field.

GUI Verification

1. Open the Catalyst Center login page in a browser
2. View site information
3. Open certificate details
4. Verify SAN entries under Extensions


Not Secure
https://10.127.212.43
10.127.212.43
Your connection to this site is not secure
You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more
You have chosen to turn off security warnings for this site. Turn on warnings
Certificate details
Location
Can ask for your location
USB devices
Can ask to connect to USB devices
Bluetooth d...
Can ask to connect to Bluetooth devices
Cookies and site data
Site settings
cisco
Cisco Catalyst Center
The bridge to possible
Username
Password
Log In



Note: If the SAN or Subject Alternative Name field contains:

- Only **DNS** Name – Configure the **DNS** name in the option 43 string.
- Only **IP Address** – Configure the **IP address** in the option 43 string.
- **Both** IP Address and DNS Name – Configure the **IP address** in the option 43 string.

CLI Verification

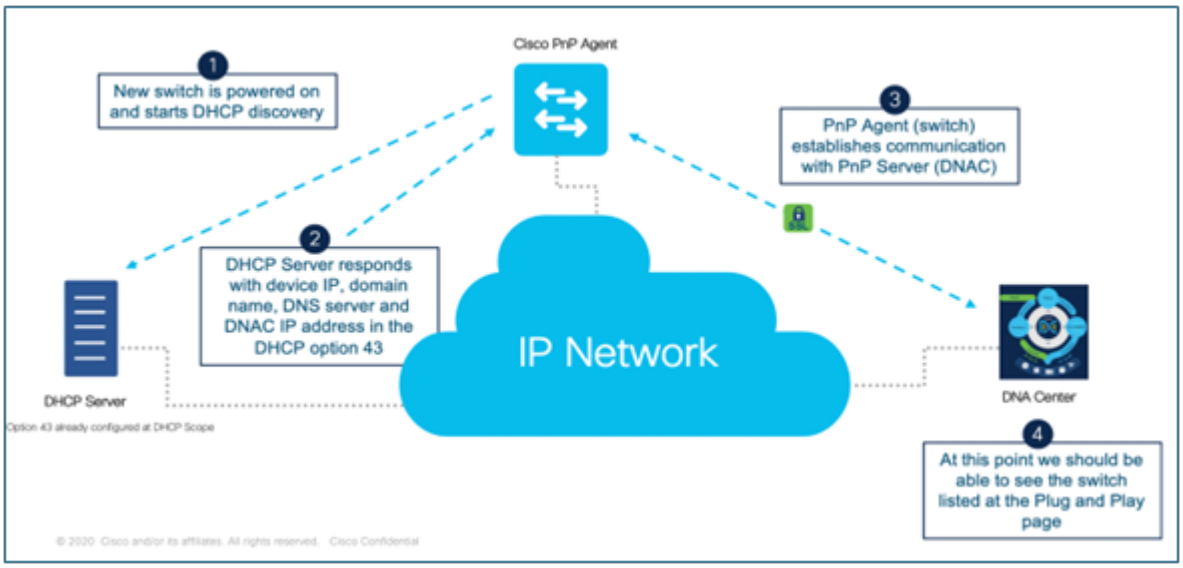
To verify this, we need the Catalyst Center IP address and a machine that can reach the Catalyst Center server. Run this command in the terminal or at the command prompt.

```
echo | openssl s_client -showcerts -servername <catc-ip-address> -connect <catc-ip-address>:443 2>/dev/
```

Verify that the SAN field contains the appropriate IP address or FQDN.

```
sitirkey@SITIRKEY-M-6PGJ netbox-docker % echo | openssl s_client -showcerts -servername 10.127.212.43 -connect 10.127.212.43:443 2>/dev/null | openssl x509 -inform
 pem -noout -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 7523967389788466058 (0x686a807a31f6eb8a)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=IN, ST=Karnataka, L=Bangalore, O=cisco, OU=cisco-ps, CN=cisco-ps, emailAddress=sitirkey@cisco.com
        Validity
            Not Before: Jan  5 14:51:00 2026 GMT
            Not After : Jan  5 14:51:00 2027 GMT
        Subject: CN=10.127.212.43
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:a5:ea:19:9e:b4:71:0d:97:fb:43:c5:ad:89:35:
                    69:2f:78:29:64:0a:b2:46:44:a7:89:98:a6:ff:71:
                    25:79:d2:53:0f:c0:c9:29:9d:c1:84:6a:16:4a:b4:
                    58:f5:46:ef:21:0a:79:71:b8:50:74:ff:29:86:cd:
                    6c:54:b6:91:62:8e:e4:20:5c:e9:38:66:84:40:97:
                    21:f8:73:27:49:2b:f3:09:86:08:1b:f5:d7:21:c8:
                    ad:8a:99:8e:55:9e:83:23:1e:f7:93:10:33:ee:08:
                    6b:2d:ad:57:7c:ba:af:21:44:67:d6:e4:b9:c5:e2:
                    88:b1:2f:ce:71:26:2a:68:ce:ea:29:65:6f:2b:47:
                    53:59:4d:5a:45:a3:03:1d:1c:fd:c9:58:f6:1d:c4:
                    49:b7:b9:36:0d:b7:6d:af:43:59:0c:ca:e0:d5:ef:
                    b7:86:92:31:bc:cd:66:e2:e8:ae:4c:68:7d:40:63:
                    45:c1:6a:e6:13:78:8e:cf:d5:42:07:04:2f:5f:80:
                    aa:ad:14:18:74:6f:47:f1:24:2b:93:47:a8:93:72:
                    8a:81:93:de:0b:41:b8:e7:5c:0a:10:e1:b2:46:06:
                    66:a7:9f:23:11:0d:e0:60:95:63:cb:ac:58:4f:6e:
                    04:a4:fd:d6:76:d4:5e:b4:e6:e4:25:50:04:30:07:
                    17:05
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage:
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 Subject Alternative Name:
                DNS:catc1.cisco.com, IP Address:10.127.212.43
    Signature Algorithm: sha256WithRSAEncryption
```

Network Diagram



Cisco PnP automates new device onboarding by enabling discovery, configuration, and management with minimal manual effort. When a new switch powers on, it sends a DHCP discovery request, and the DHCP server returns network details, including the Catalyst Center (PnP server) IP address through DHCP Option 43. Using this information, the switch's PnP agent securely connects to the PnP server over the IP network. After the connection is established, the device is authenticated and identified, then added to the Plug and

Play inventory, where administrators can apply configurations and complete provisioning quickly and consistently.

Switch Onboarding Methods

Review the various onboarding methods in this section through which a switch can be onboarded into the Plug and Play inventory of Catalyst Center.

1. Onboard using VLAN1

This method uses the default VLAN 1 for PnP management

Requirements

- VLAN 1 SVI is configured on the upstream switch.
- DHCP Server with Option 43 configured
- DNS resolution for the Catalyst Center FQDN

Procedure on the Upstream switch

Step 1. Configure VLAN 1's SVI.

```
config t
interface Vlan1
  ip address 10.127.212.49 255.255.255.0
```

Step 2. Configure a DHCP pool with Option 43 (Note: We can use the Option 43 parameter with either the IPv4 address or FQDN of Catalyst Center).

```
config t
ip dhcp pool pnp_pool
  network 10.127.212.0 255.255.255.0
  option 43 ascii 5A1D;B2;K4;I10.127.212.43;J80;
```

or

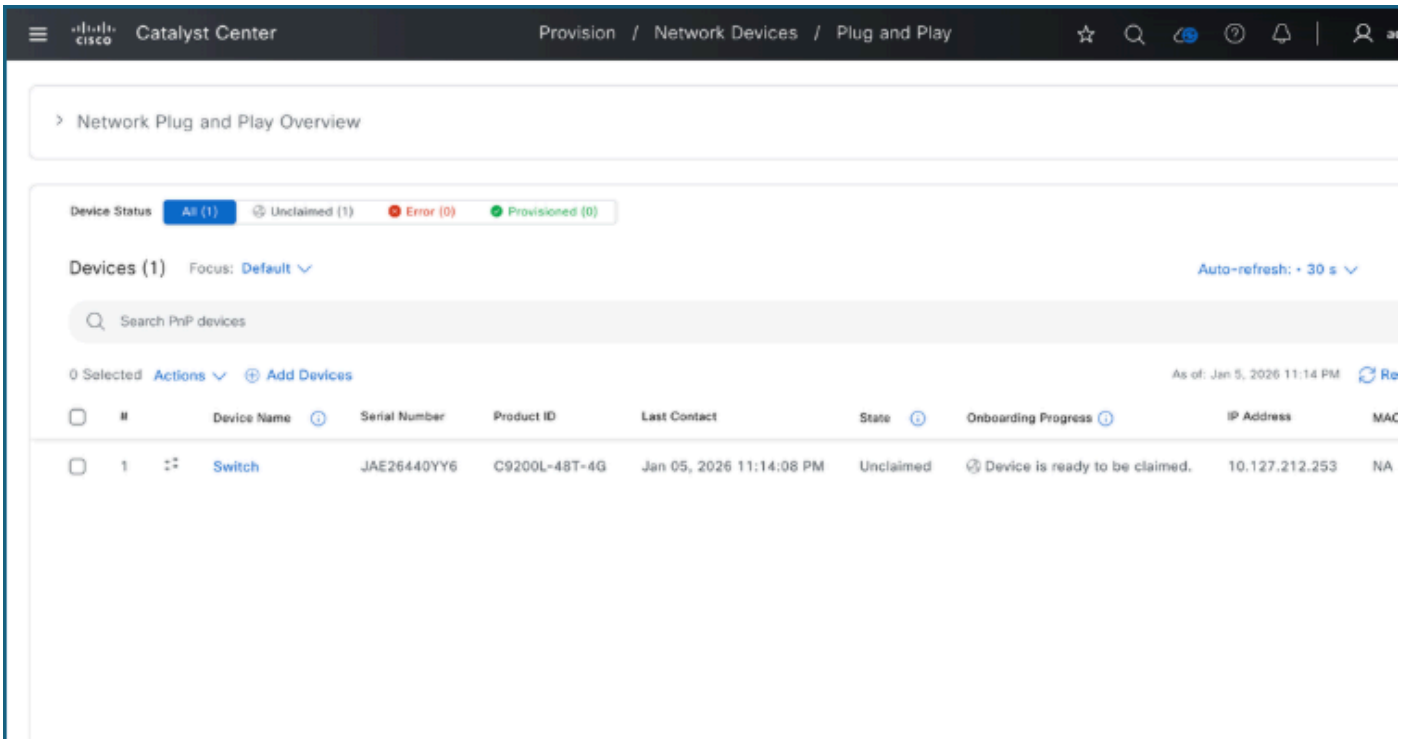
```
config t
```

```
ip dhcp pool pnp_pool
  network 10.127.212.0 255.255.255.0
  option 43 ascii5A1D;B1;K4;Icatc1.cisco.com;J80;
  default-router 10.127.212.49
  dns-server 10.127.212.1
```

Step 3. Configure a trunk interface to the new switch.

```
config t
interface GigabitEthernet1/0/5
  description PnP_Trunk
  switchport mode trunk
```

Step 4. Verify that the switch appears on Catalyst Center's **Provision** > **Plug and Play** page.



2. Onboard using custom VLAN

This method uses a dedicated VLAN for management.

Requirements

- Custom VLAN SVI configured on the upstream switch.

- DHCP Server with Option 43 configured.
- DNS resolution for the Catalyst Center FQDN.
- Trunk allows the custom VLAN along with any other VLANs necessary for other traffic.

Procedure on the upstream switch

Step 1. Configure the custom VLAN's SVI.

```
config t
interface Vlan302
  description PnP_Vlan
    ip address 10.127.212.49 255.255.255.0
```

Step 2. Configure a DHCP pool with Option 43 (Note: We can use the Option 43 parameter with either the IPv4 address or FQDN of Catalyst Center).

```
config t
ip dhcp pool pnp_pool
  network 10.127.212.0 255.255.255.0
  option 43 ascii 5A1D;B2;K4;I10.127.212.43;J80;
```

or

```
config t
ip dhcp pool pnp_pool
  network 10.127.212.0 255.255.255.0
  option 43 ascii 5A1D;B1;K4;Icatc1.cisco.com;J80;
  default-router 10.127.212.49
  dns-server 10.127.212.1
```

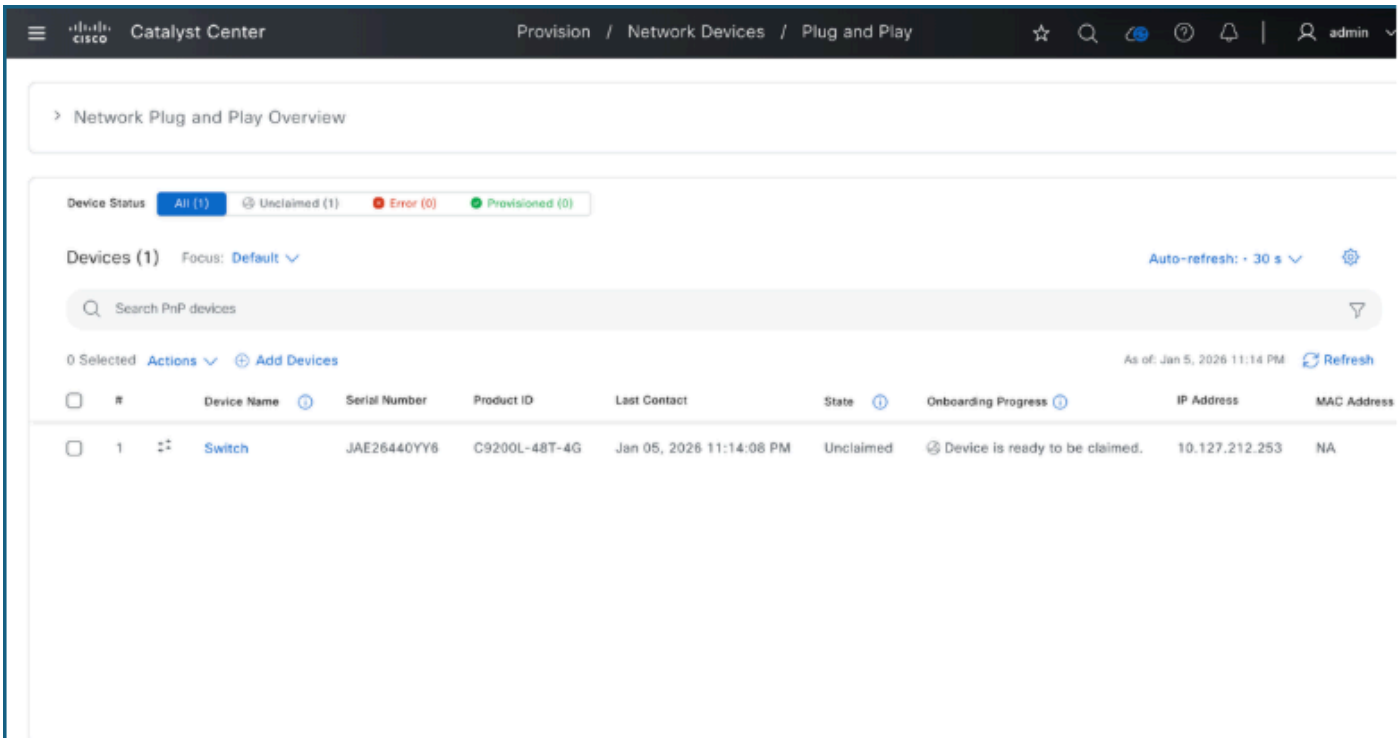
Step 3. Configure the custom VLAN as the PnP VLAN.

```
config t
pnp startup-vlan 302
```

Step 4. Configure the trunk interface to new switch.

```
config t
interface GigabitEthernet1/0/5
  description PnP_Trunk
  switchport mode trunk
  switchport trunk allowed vlan 302
```

Step 5. Verify that the switch appears on Catalyst Center's **Provision > Plug and Play** page.



3. Onboard Switch using the management port

This method leverages the management interface of the switch.

Requirements

- Custom VLAN SVI configured on the upstream switch
- DHCP Server with Option 43 configured
- DNS resolution for the Catalyst Center FQDN

Procedure on the upstream switch.

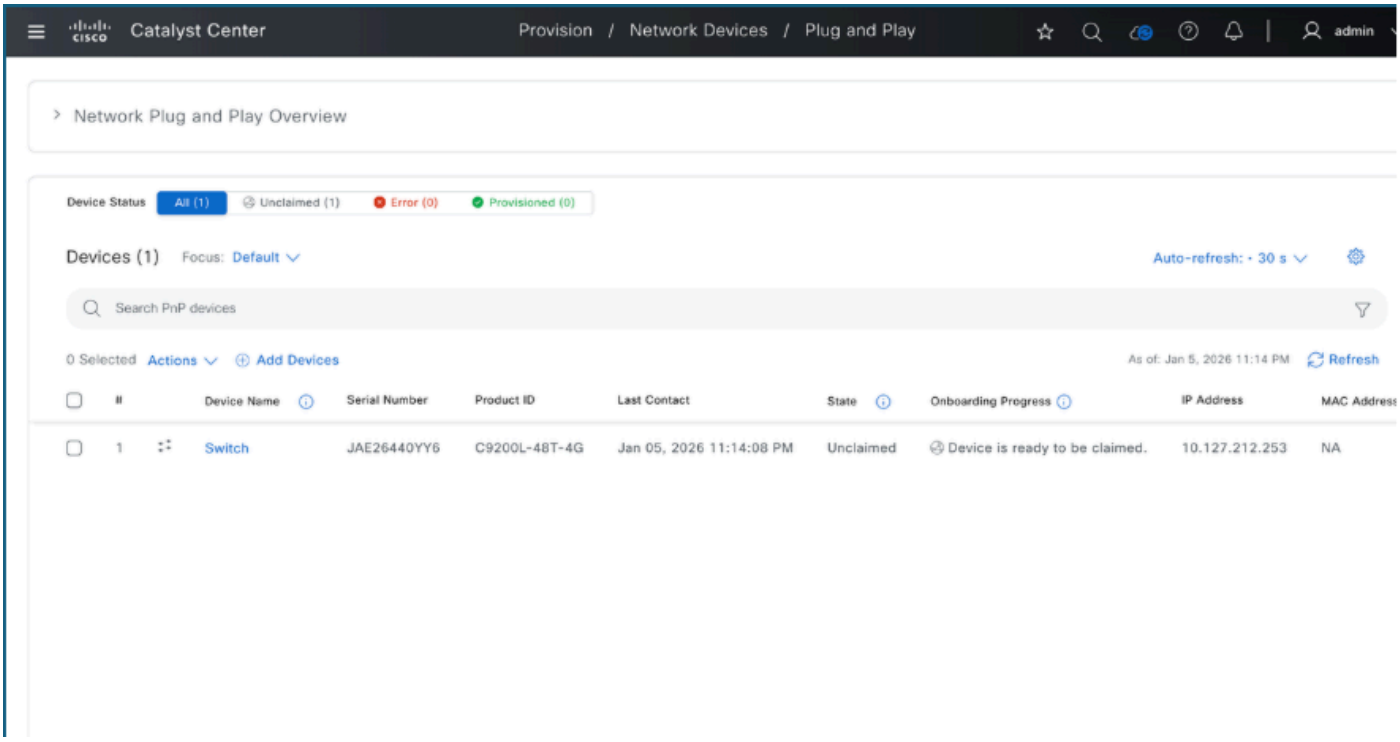
Step 1. Configure the VLAN's SVI.

```
config t
interface Vlan302
    ip address 10.127.212.49 255.255.255.0
    ip helper-address 10.127.212.1
```

Step 2. Configure the access interface to the new switch.

```
config t
interface GigabitEthernet1/0/5
  switchport mode access
  switchport access vlan 302
```

Step 3. Verify that the switch appears on Catalyst Center's **Provision** > **Plug and Play** page.



4. Switch Console logs

Here is what appears on the switch's console when DHCP is used for Plug and Play.

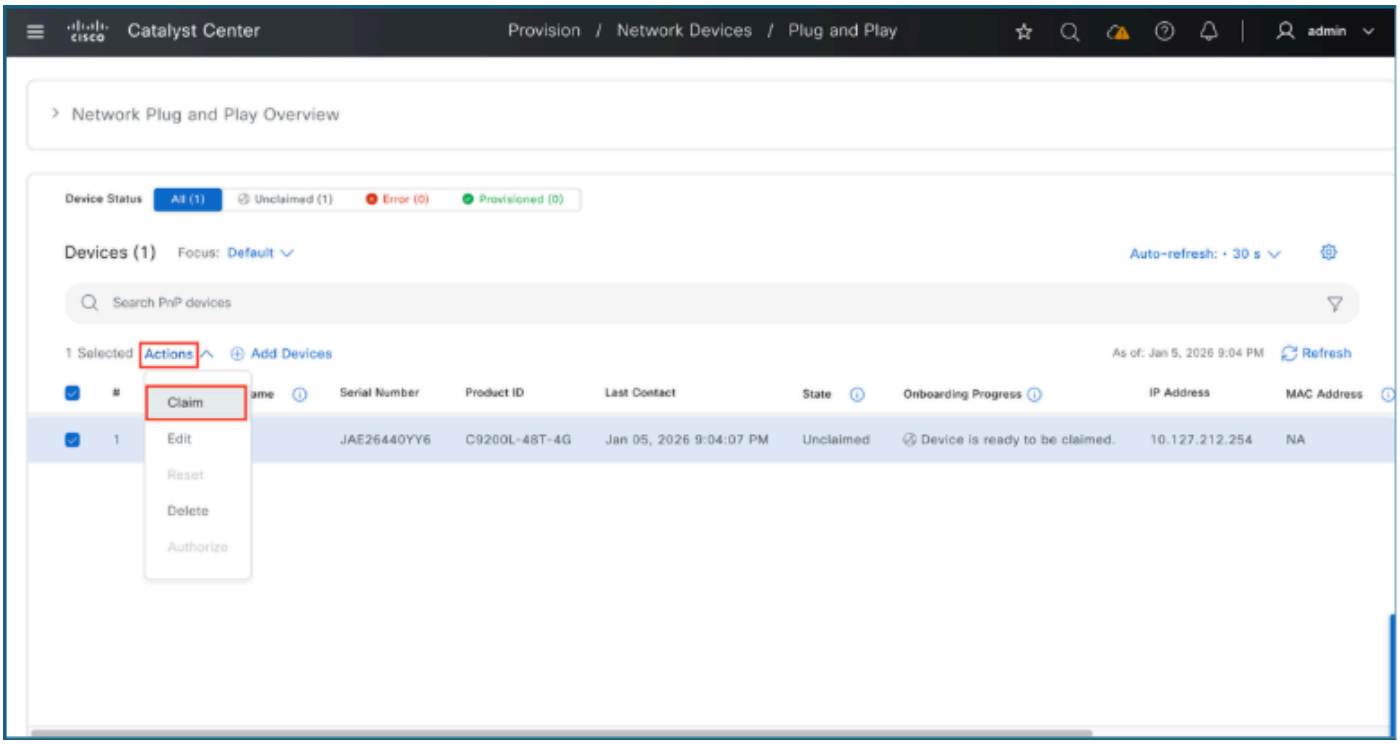
```
Base Ethernet MAC Address          : 44:64:3c:b1:2b:80
Motherboard Assembly Number        : 73-102066-04
Motherboard Serial Number          : JAE26440YY6
Model Revision Number              : D0
Motherboard Revision Number        : A0
Model Number                       : C9200L-48T-4G
System Serial Number               : JAE26440YY6



         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:


Press RETURN to get started!


*Jan  5 15:28:24.332: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named TP-self-signed-2360689995 has been generated or imported by crypto-engine
*Jan  5 15:28:24.366: %SSH-5-ENABLED: SSH 1.99 has been enabled
*Jan  5 15:28:24.540: %PKI-4-NOCONFIGAUTOSAVE: Configuration was modified.  Issue "write memory" to save new IOS PKI configuration
*Jan  5 15:28:24.543: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent Discovery from console as vty0
*Jan  5 15:28:24.895: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named TP-self-signed-2360689995.server has been generated or imported by crypto-engine
*Jan  5 15:28:26.546: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent Discovery from console as vty0
*Jan  5 15:28:26.546: %PNP-6-PNP_SAVING_TECH_SUMMARY: Saving PnP tech summary (pnp-tech-discovery-summary)... Please wait. Do not interrupt.
*Jan  5 15:28:27.574: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent Discovery from console as vty0
*Jan  5 15:28:28.589: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent Discovery from console as vty0
*Jan  5 15:28:29.604: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent Discovery from console as vty0
*Jan  5 15:28:33.230: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent Discovery from console as vty0
*Jan  5 15:28:31.023: %SYS-6-CLOCKUPDATE: System clock has been updated from 15:28:33 UTC Mon Jan 5 2026 to 15:28:31 UTC Mon Jan 5 2026, configured from console by vty0.
Jan  5 15:28:31.023: %PKI-6-AUTHORITATIVE_CLOCK: The system clock has been set.
Jan  5 15:28:31.032: %SYS-5-CONFIG_P: Configured programmatically by process XEP_pnp-zero-touch from console as vty0
Jan  5 15:28:31.034: %SMART_LIC-5-SYSTEM_CLOCK_CHANGED: Smart Agent for Licensing System clock has been changed
Jan  5 15:28:31.910: %PNP-6-PNP_TECH_SUMMARY_SAVED_OK: PnP tech summary (pnp-tech-discovery-summary) saved successfully.
Jan  5 15:28:31.910: %PNP-6-PNP_DISCOVERY_DONE: PnP Discovery done successfully (PnP-DHCP-IPv4)
Jan  5 15:28:33.405: %PKI-6-TRUSTPOINT_CREATE: Trustpoint: pnplabel created succesfully
Jan  5 15:28:33.419: %PKI-4-NOCONFIGAUTOSAVE: Configuration was modified.  Issue "write memory" to save new IOS PKI configuration
Jan  5 15:28:34.718: %SYS-5-CONFIG_P: Configured programmatically by process PnP reconnect profile from console as vty0
%Error opening tftp://255.255.255.255/network-confg (Timed out)
Jan  5 15:28:39.911: AUTOINSTALL: Tftp script execution not successful for Vl302.
Jan  5 15:29:35.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 15:29:35 UTC Mon Jan 5 2026 to 15:29:35 UTC Mon Jan 5 2026, configured from console by vty0.
Jan  5 15:29:35.000: %SYS-5-CONFIG_P: Configured programmatically by process XEP_pnp-zero-touch from console as vty0
Jan  5 15:29:35.001: %PNP-6-PNP_SAVING_TECH_SUMMARY: Saving PnP tech summary (pnp-tech-error-summary)... Please wait. Do not interrupt.
Jan  5 15:29:35.001: %SMART_LIC-5-SYSTEM_CLOCK_CHANGED: Smart Agent for Licensing System clock has been changed
Jan  5 15:29:38.651: %SYS-5-CONFIG_P: Configured programmatically by process XEP_pnp-zero-touch from console as vty0
Jan  5 15:29:39.651: %PNP-6-PNP_TECH_SUMMARY_SAVED_OK: PnP tech summary (pnp-tech-error-summary) saved successfully.
Jan  5 15:29:44.698: %SYS-5-CONFIG_P: Configured programmatically by process XEP_pnp-zero-touch from console as vty0
```

Onboarding Switch to Catalyst Center without Day-0 templates

To onboard a new switch into Catalyst Center's inventory, complete these required procedures once the device is visible and claimable on the Plug and Play page.

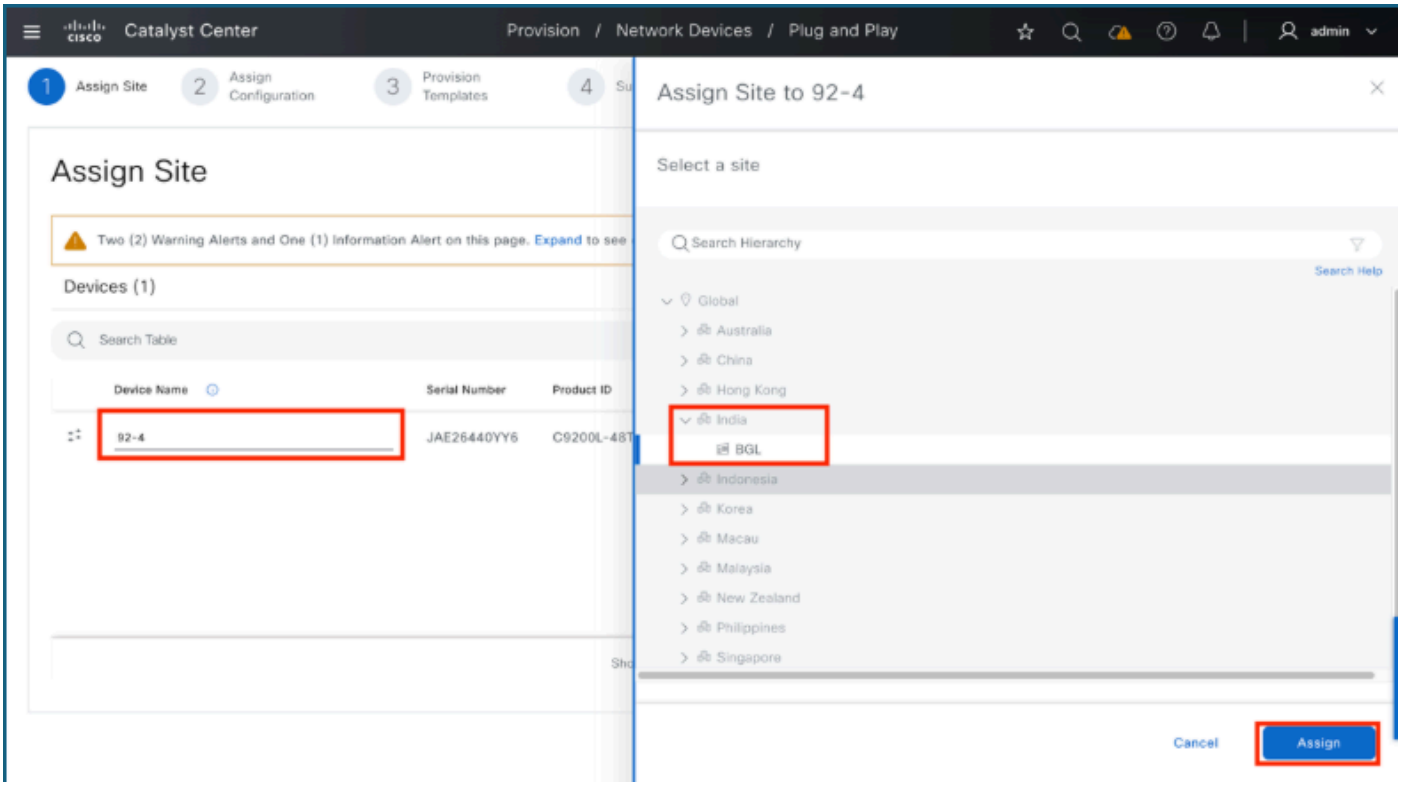
1. To claim switches:

- Select the checkboxes for the switches to be claimed.
- Navigate to Actions > Claim.



2. To name and map the switch:

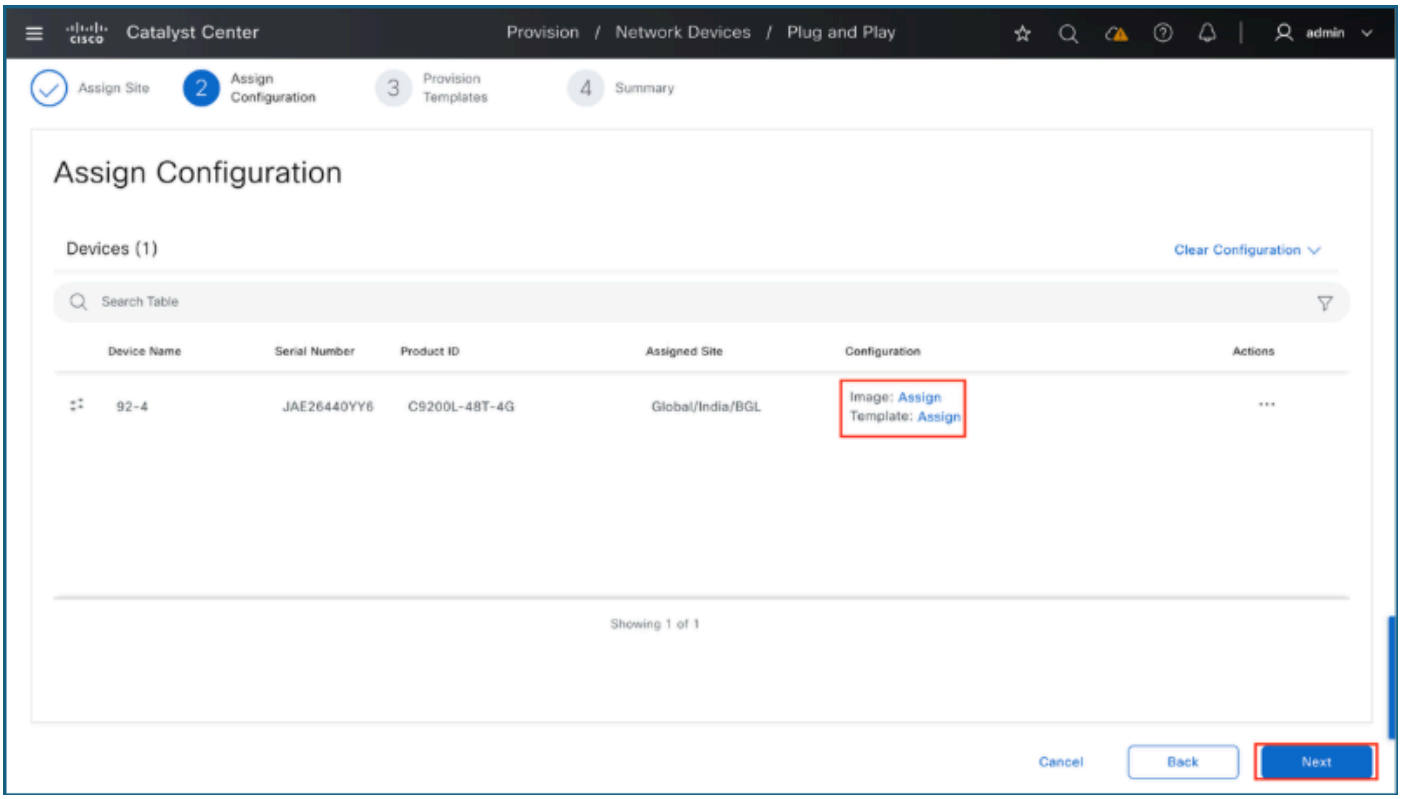
- Enter the name in the **Device Name** field and click **Assign.**
- Choose the correct site or building, click **Assign** again, and then click **Next.**



3. Assign Software Image or Template (optional):

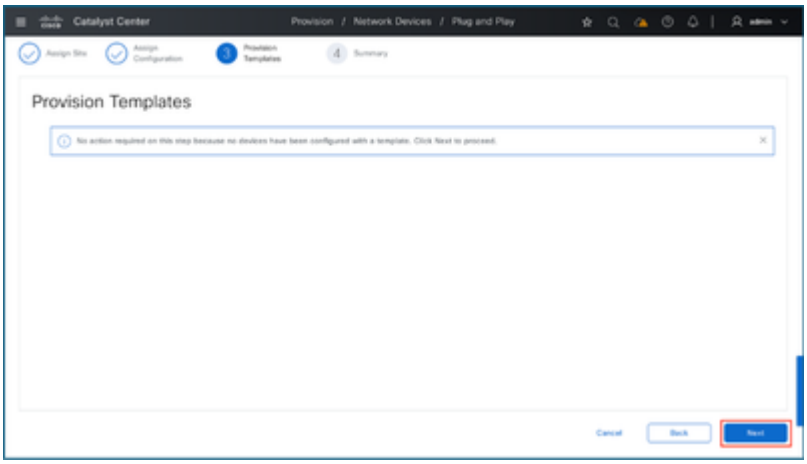
Use this step to upgrade the switch to a specific software version or apply a Day-0 configuration template.

- Click Assign next to **Image** to specify the software version.
- Click Assign next to **Template** to apply a template configuration.
- Click **Next** after the desired assignments are complete.



4. Provision templates

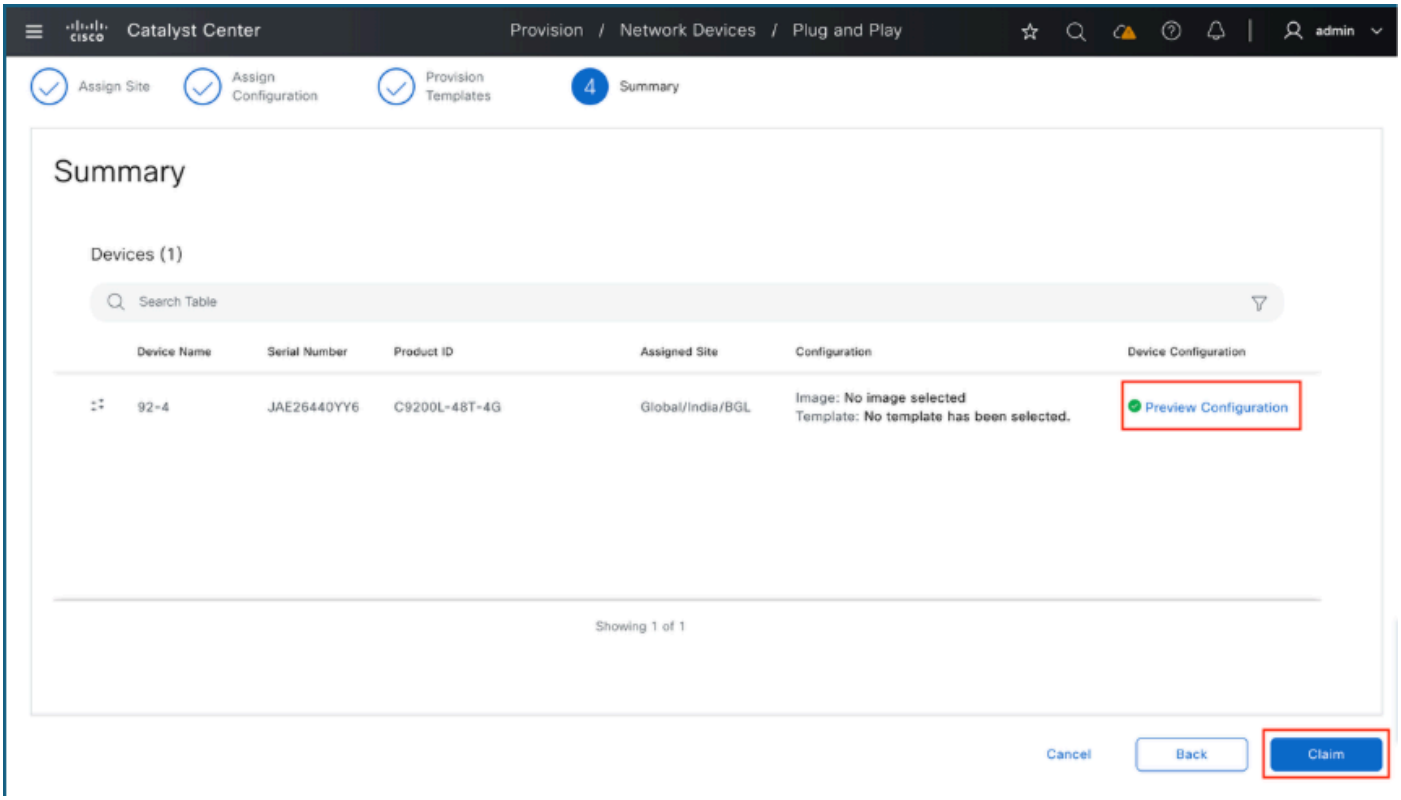
When claiming the device without the use of templates, bypass this configuration step by selecting **Next.**

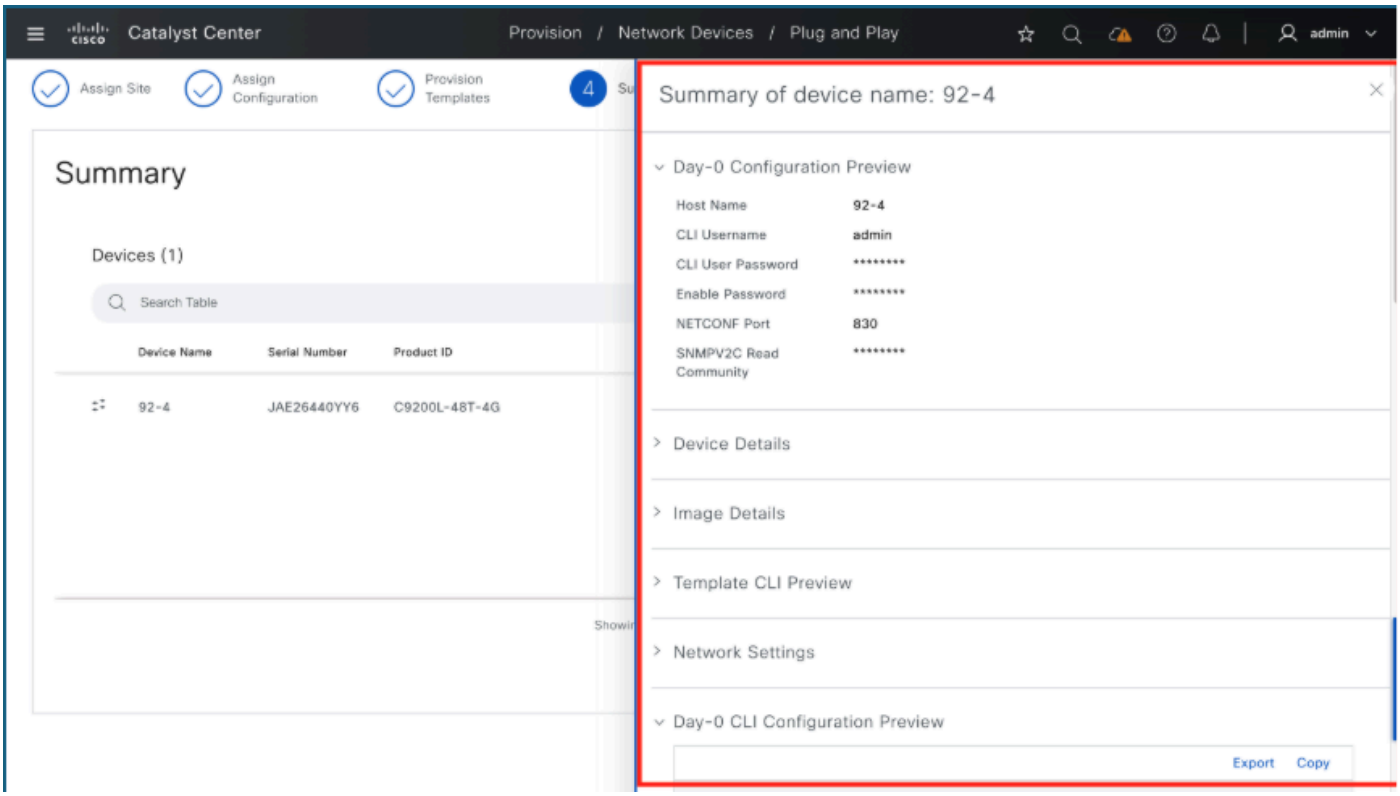


5. Summary

Use the Summary page to review the configuration before it is provisioned by Catalyst Center.

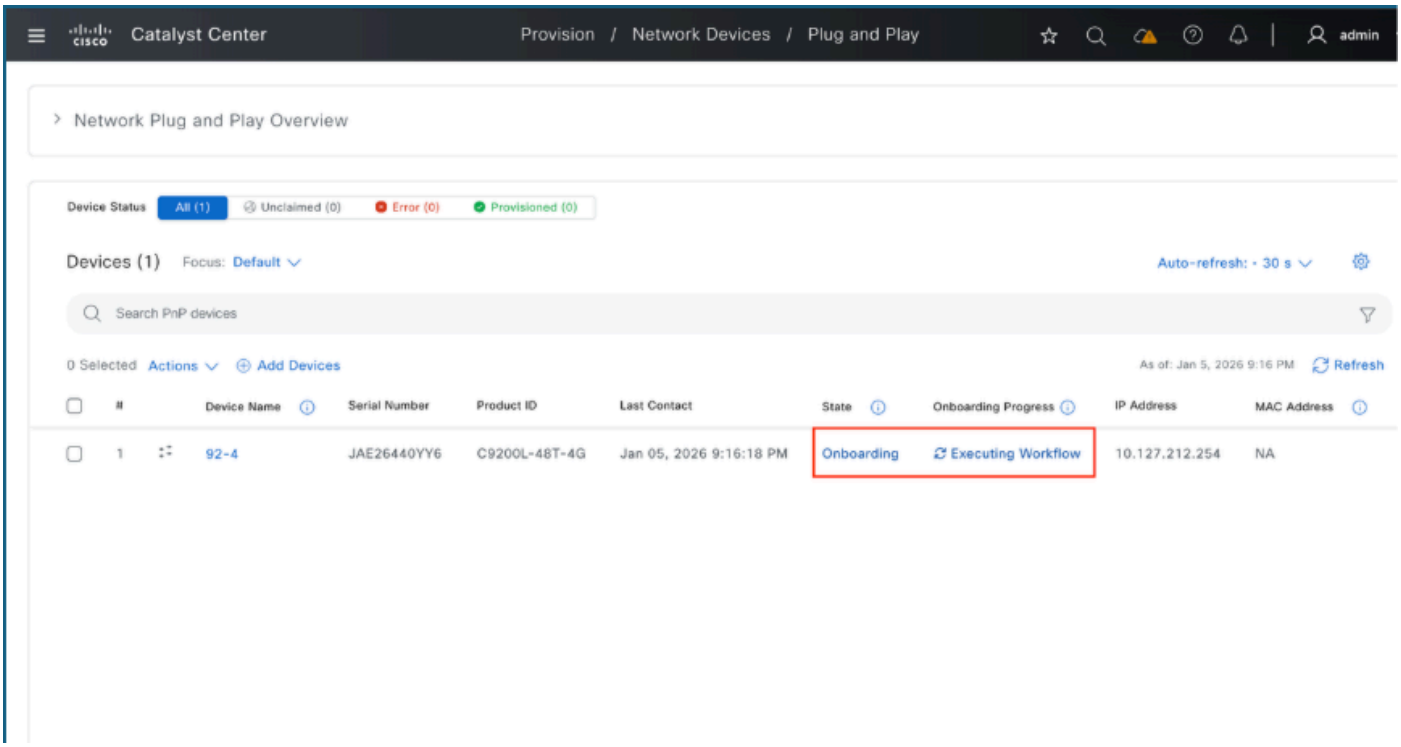
- Click **Preview Configuration**.
- Expand the individual sections to verify the settings.
- Once verified, click **Claim.**

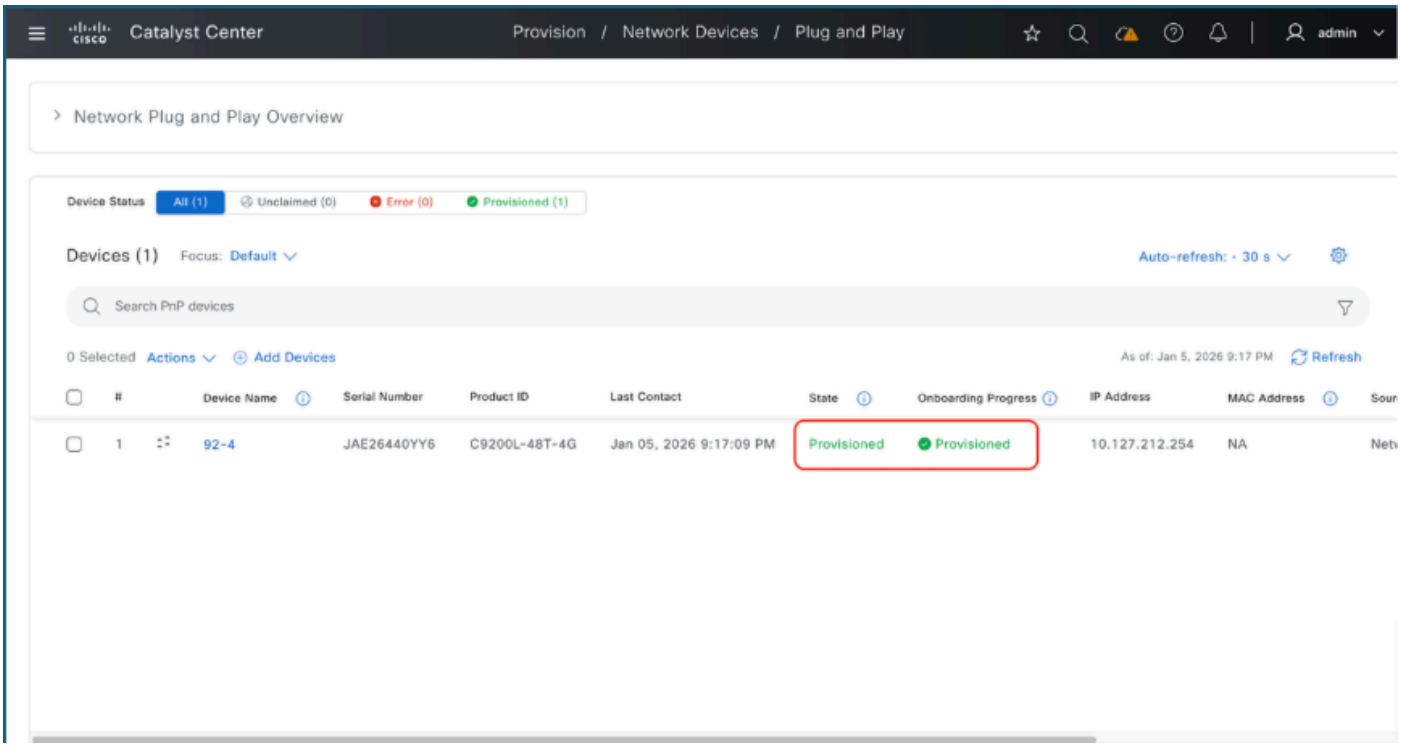




6. Monitor the Claiming Process

Upon initiating the claim, the interface returns to the Plug and Play dashboard. Monitor the device state, a transition to **Provisioned** indicates the switch has been successfully claimed and added into Catalyst Center's inventory.



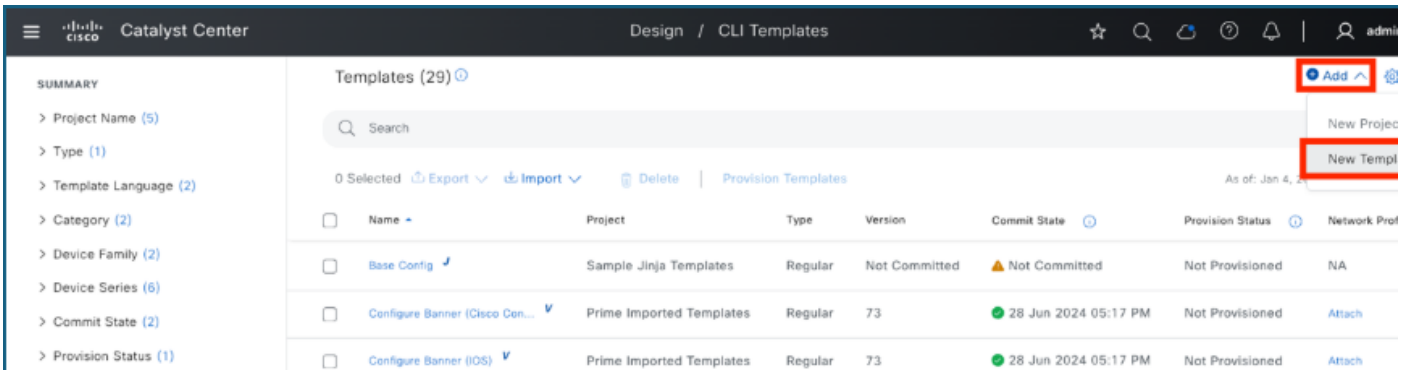


Onboarding Switch to Catalyst Center with Day-0 templates

When the new switch is ready to be claimed on Catalyst Center's Plug and Play page, apply a Day-0 template to include additional configuration during the claim process.

1. Create Day-0 or Onboarding Template

- Navigate to **Design** > **CLI Templates.**
- Select **Add** > **New Template.**

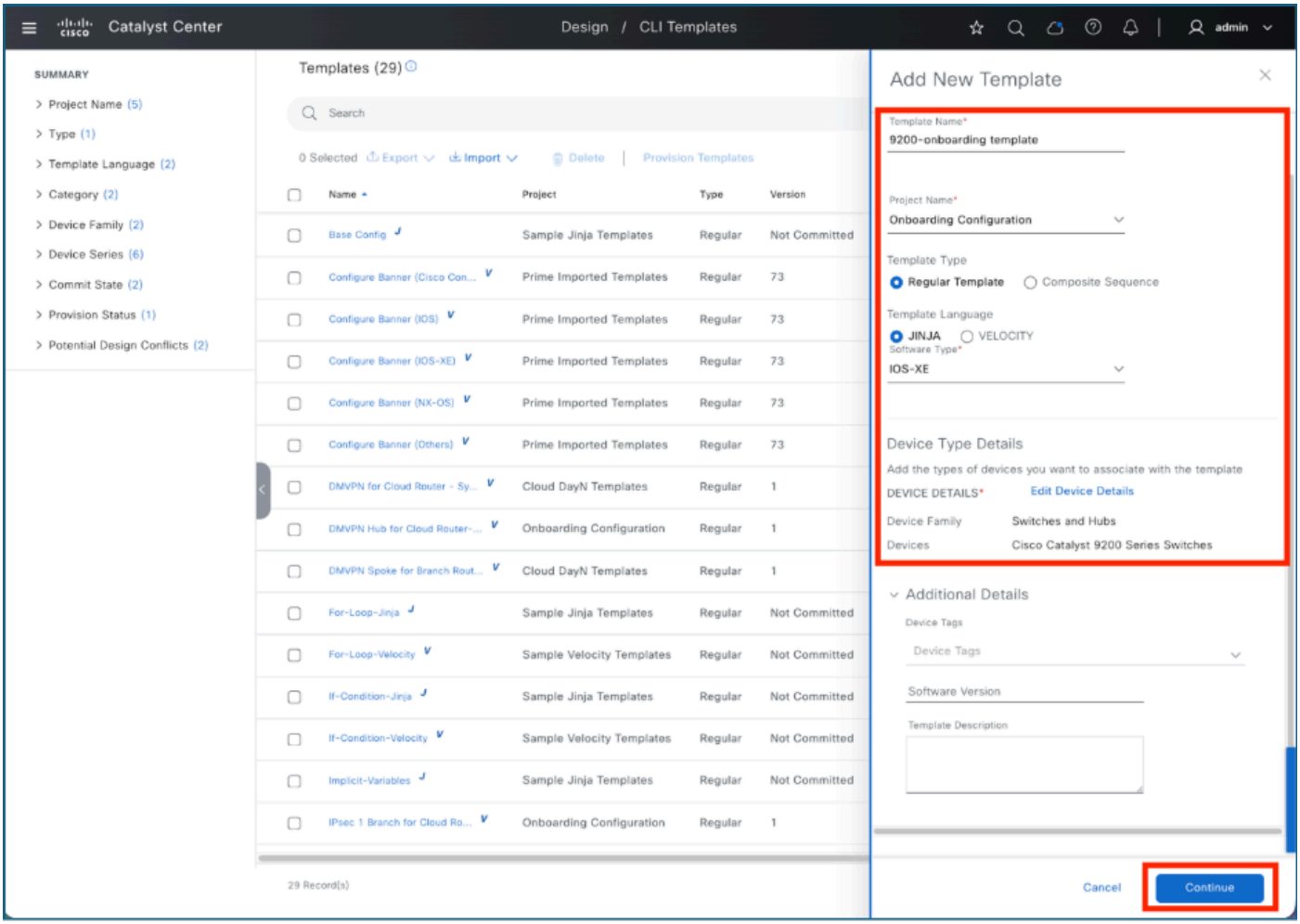


2. Add Template Details

In the side panel, enter these template specifications:

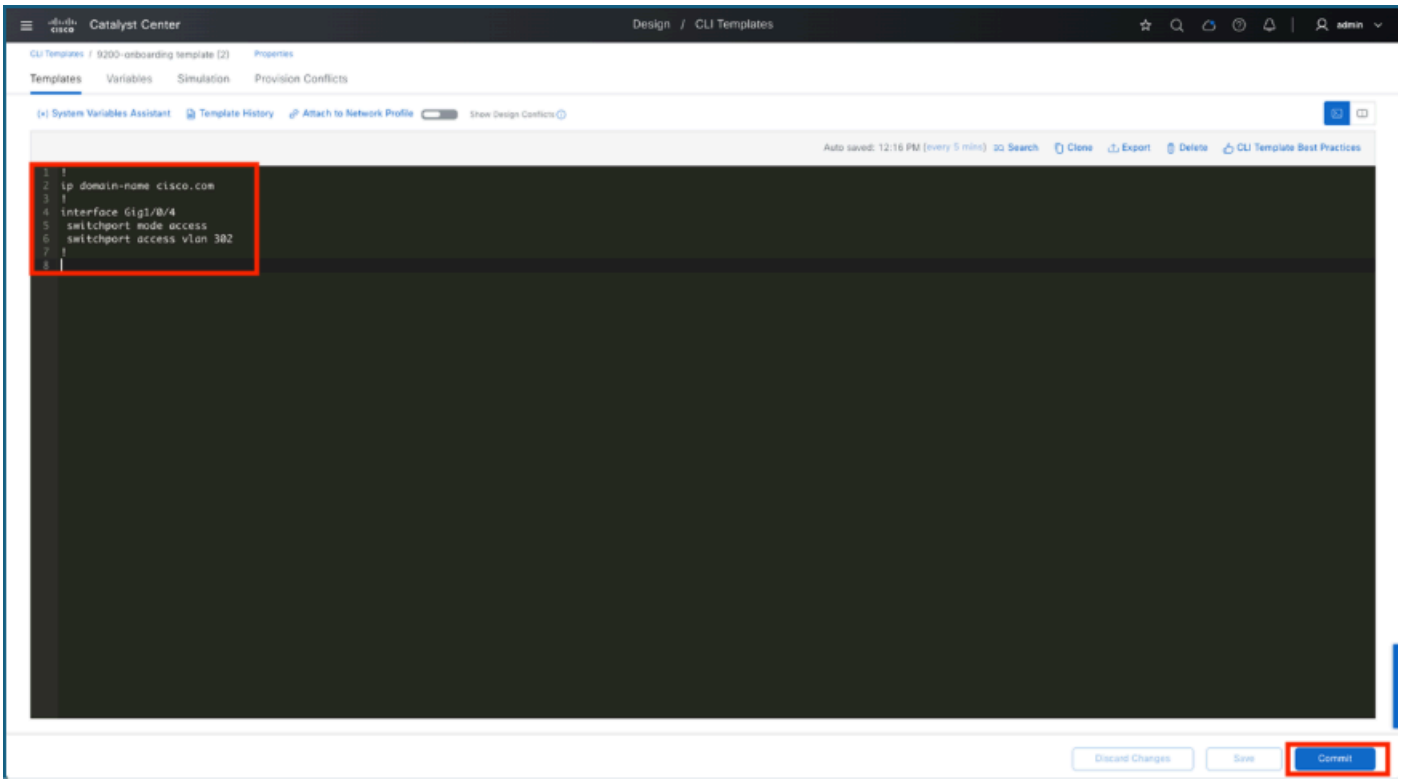
- **Template Name**
- **Project Name**: For Day-0 templates, always select **Onboarding Configuration.**

- **Template Type, Language,** and **Software Type**: Select the appropriate values from the menus.
- Click **Continue** to proceed.



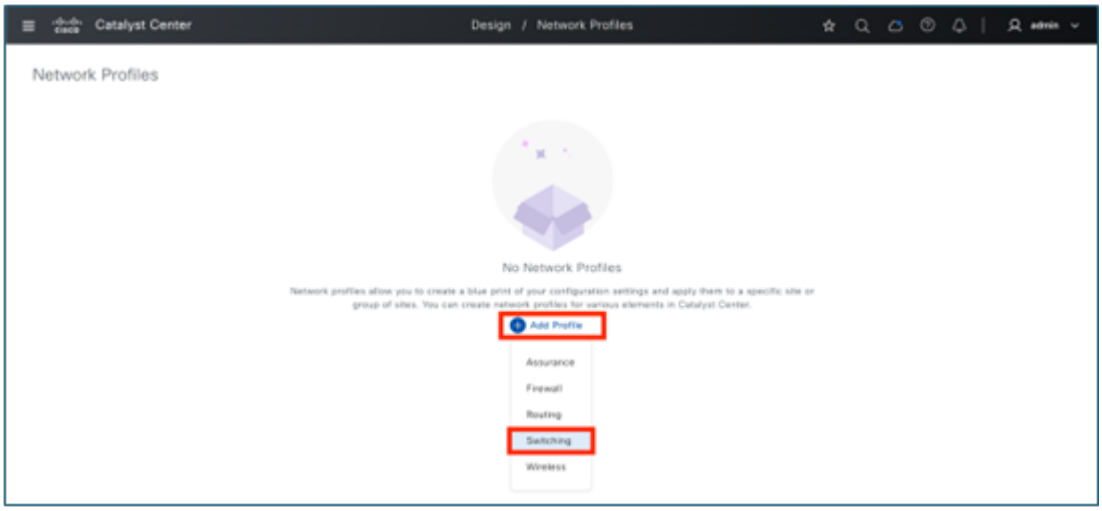
3. Edit the Template

Enter the configuration to be deployed to the switch in the CLI Template Editor. In this example a domain name and an access port are configured. After adding the configuration to the CLI Template Editor, click **Save** and then **Commit** to finalize the changes.



4. Create Network Profile

- Navigate to the **Design** menu and select **Network Profiles.**
- Click the **Add Profile** button.
- Choose the appropriate profile type from the list (for example, **Switching**).



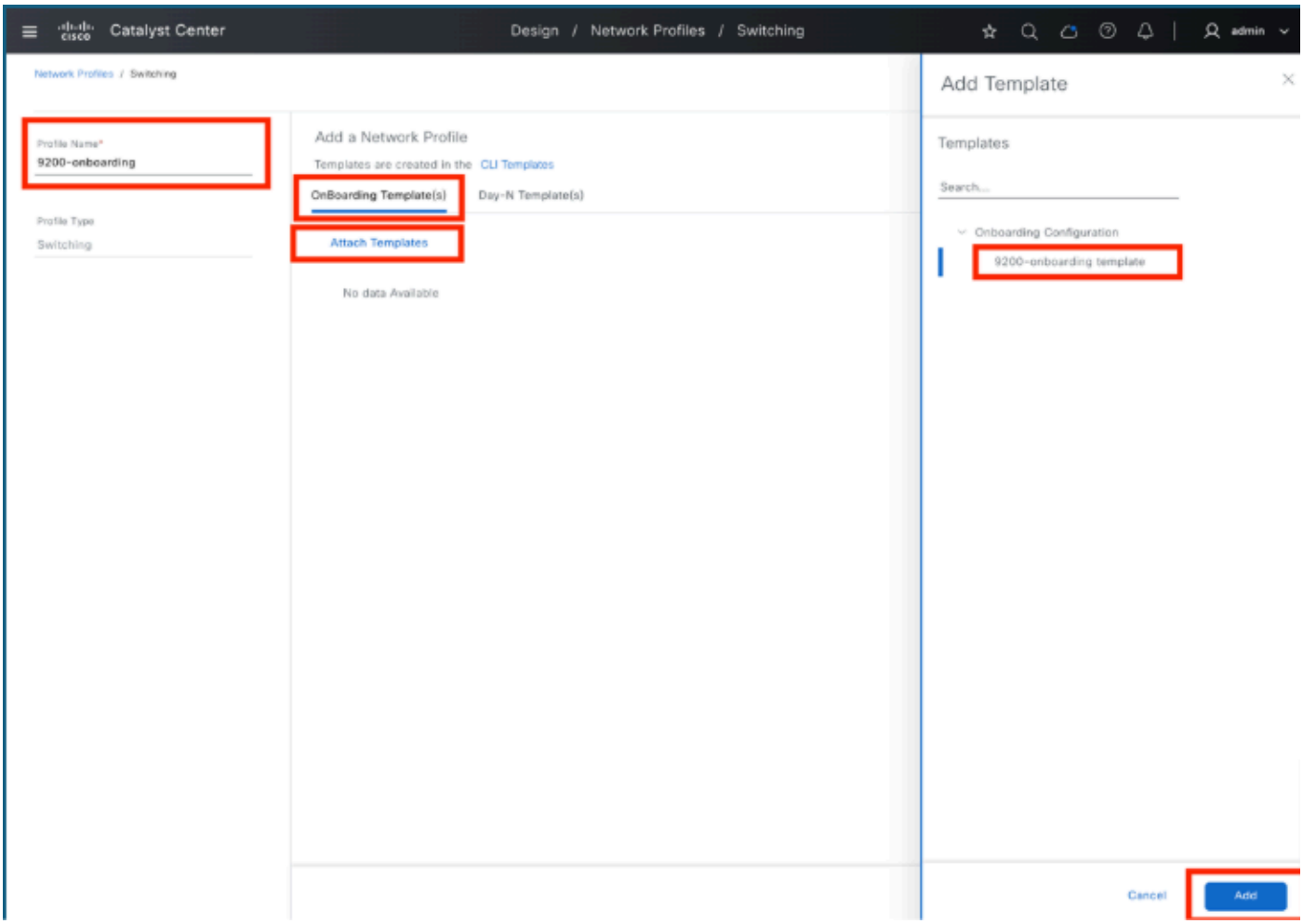
5. Add template and edit network profile settings

- **Enter a Profile Name:** Provide a name for the network profile.

- **Access Templates:** Click on **Onboarding Template(s)** and then select **Attach Templates.**

- **Choose Template:** Locate and select the required template from the **Onboarding Configuration** directory.

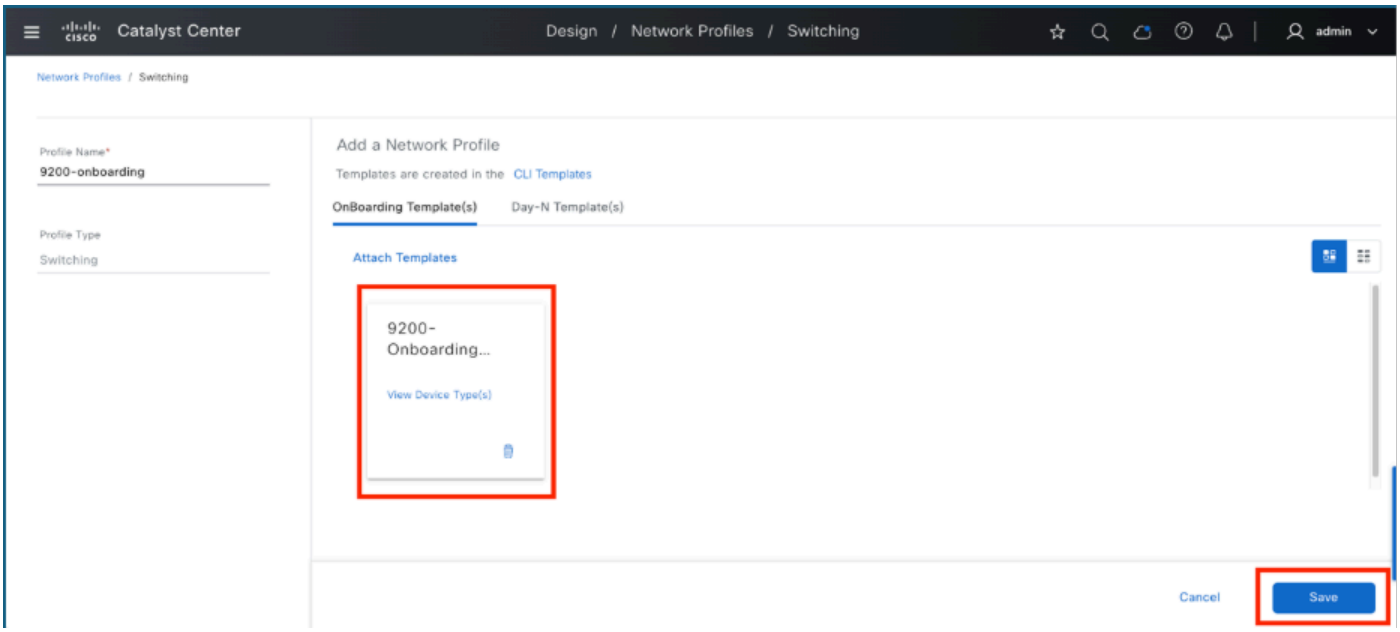
- **Finalize:** Click the **Add** button to complete the process.



6. Save the profile

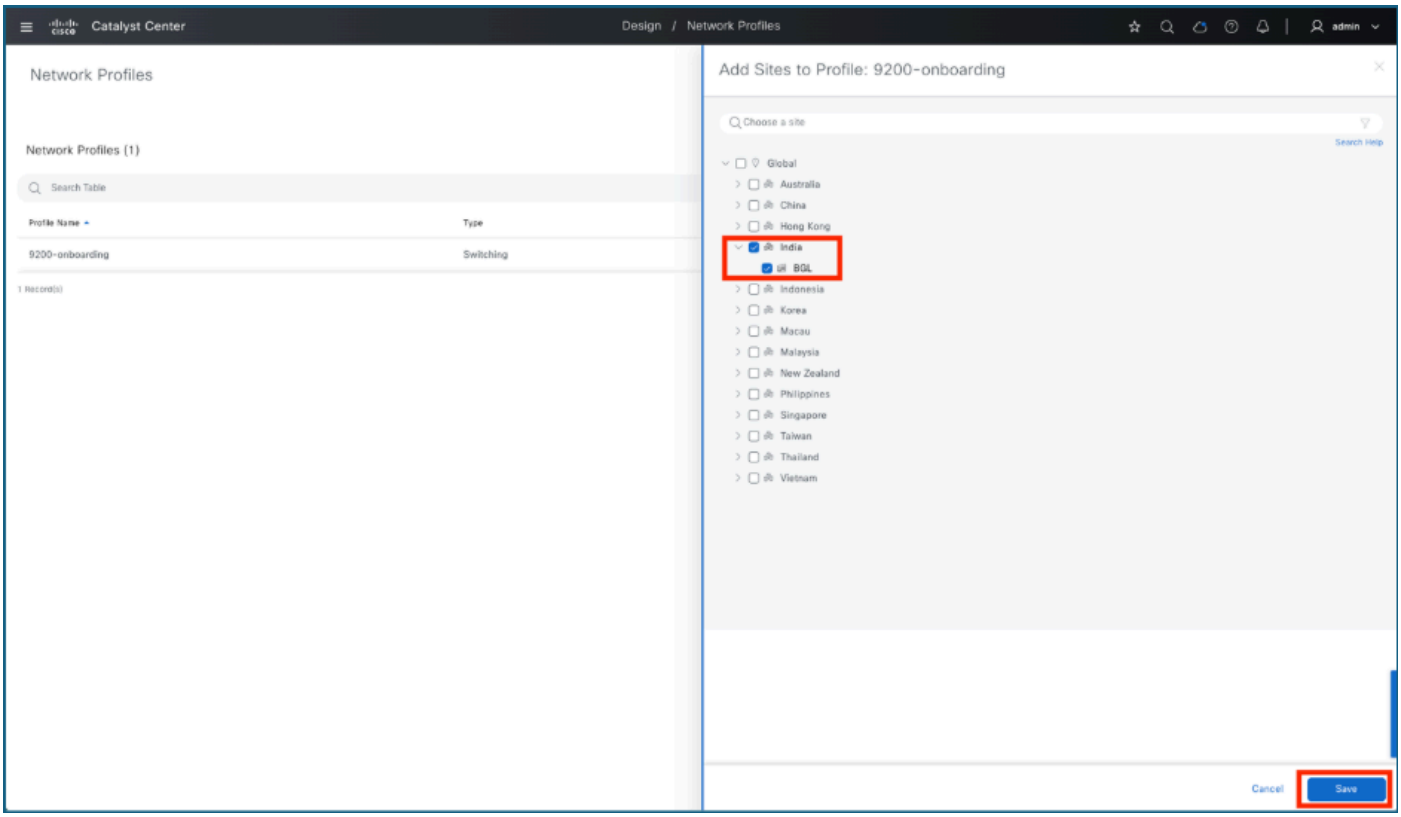
- **Verify Template:** After adding the template, ensure it appears in the list under **Onboarding Template(s).**

- **Save Profile:** Click **Save** button to finalize and store the profile settings.



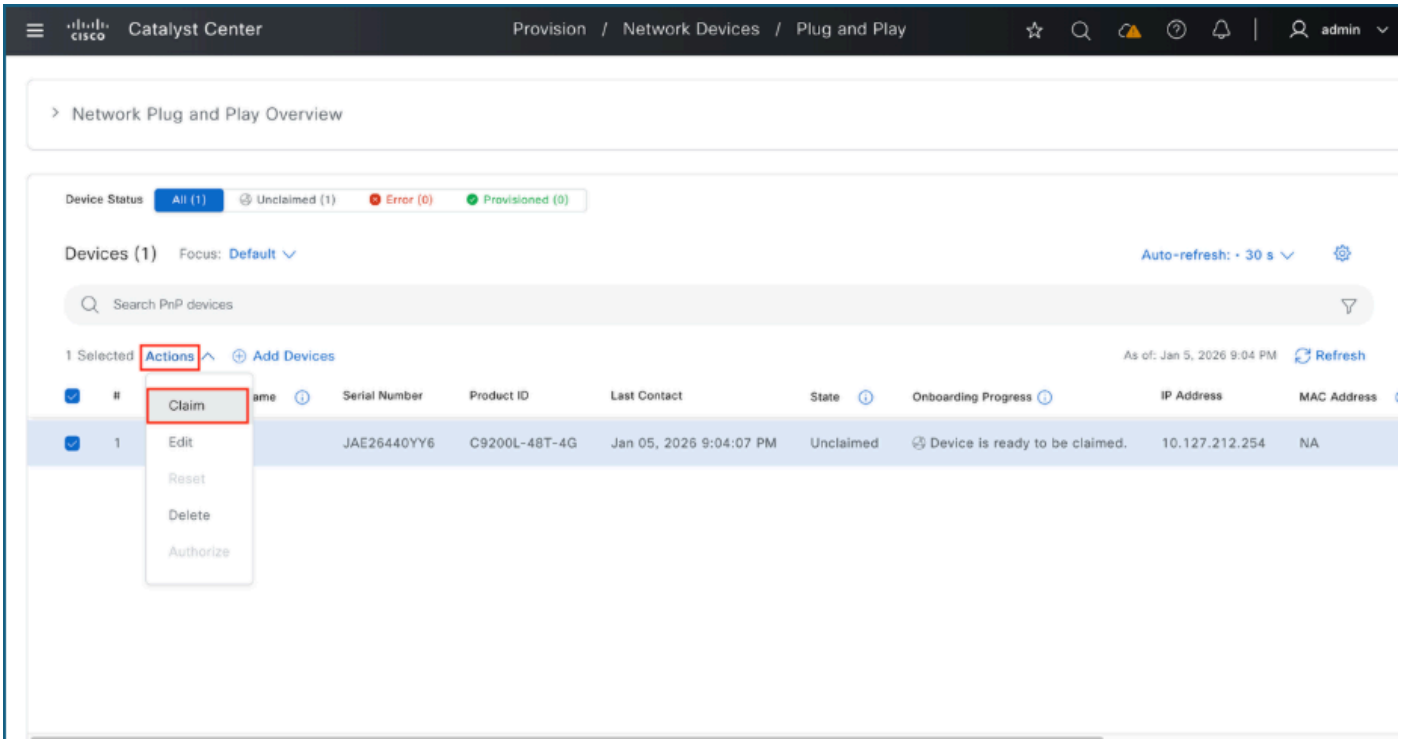
7. Assign network profile to the site where switch/switches are to be onboarded

- **Initiate Assignment:** Click the **Assign Site** option for the network profile that was just created.
- **Choose the Site:** Select the specific site where the switches are to be onboarded.
- **Confirm:** Click **Save** to finalize the assignment.



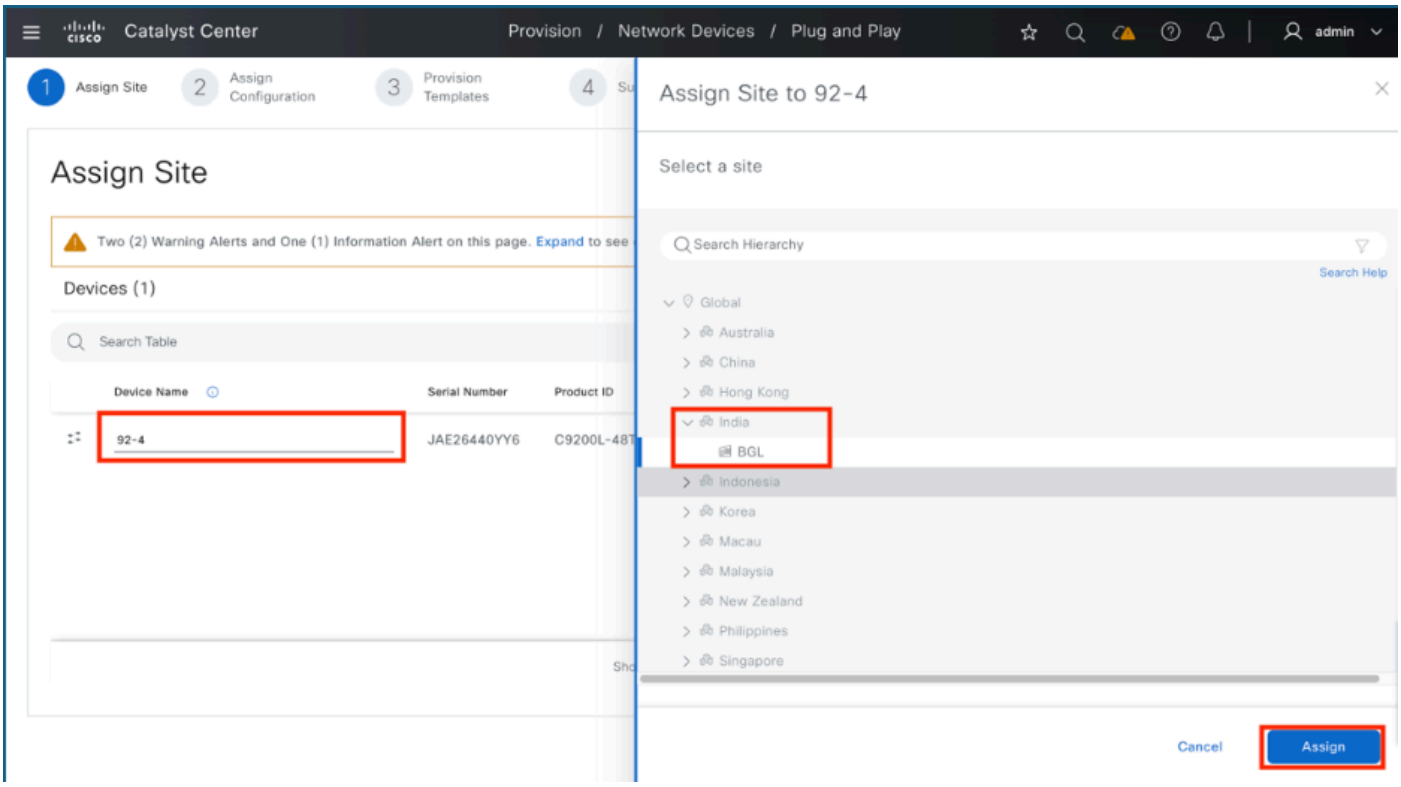
8. Claim Switches

- **Navigate to Plug and Play:** Go to **Provision** menu and select **Plug and Play.**
- **Select Devices:** Locate the switch or switches to be claimed and click the checkbox next to each switch's name.
- **Initiate Claim:** Navigate to the **Actions** menu and select **Claim.**



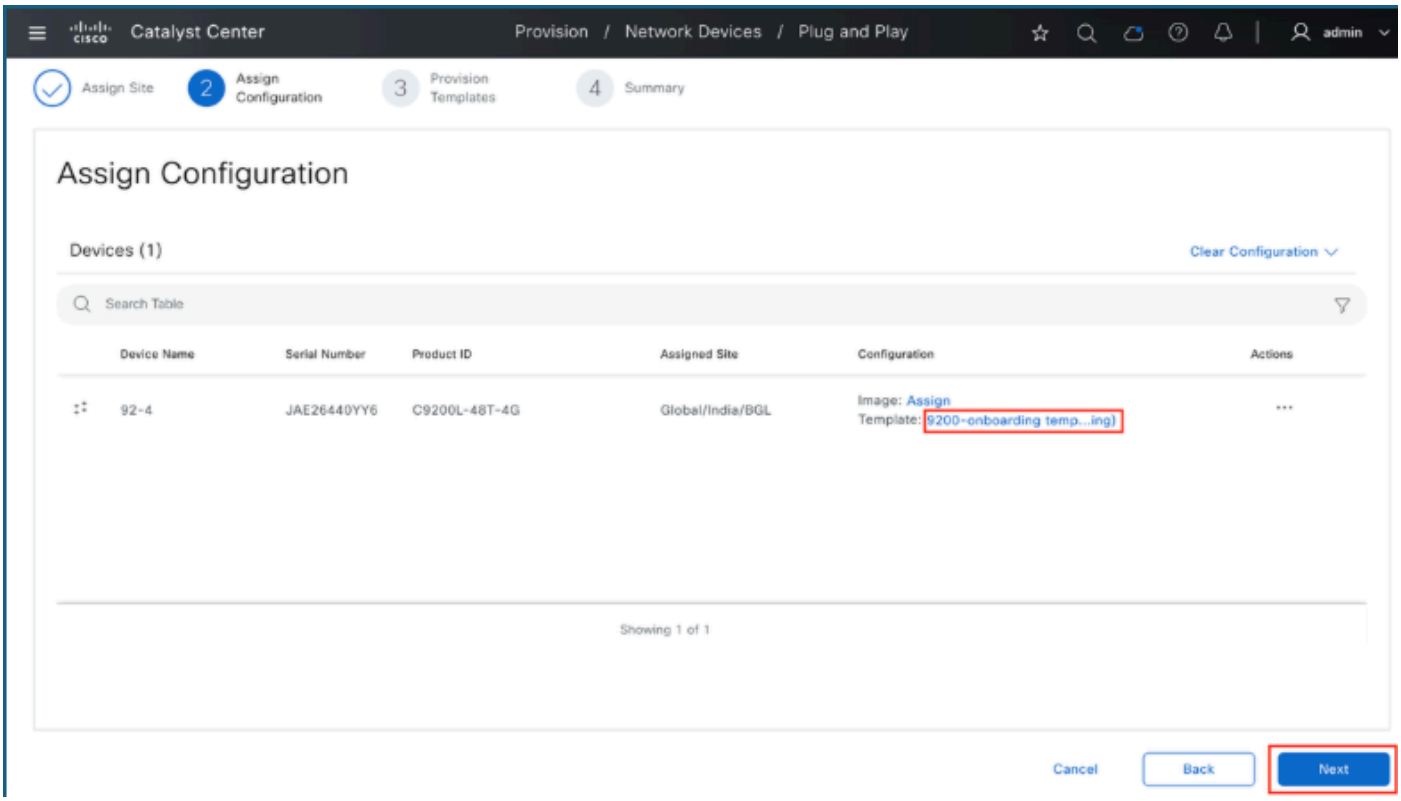
9. Assign a name for the switch and assign to a site

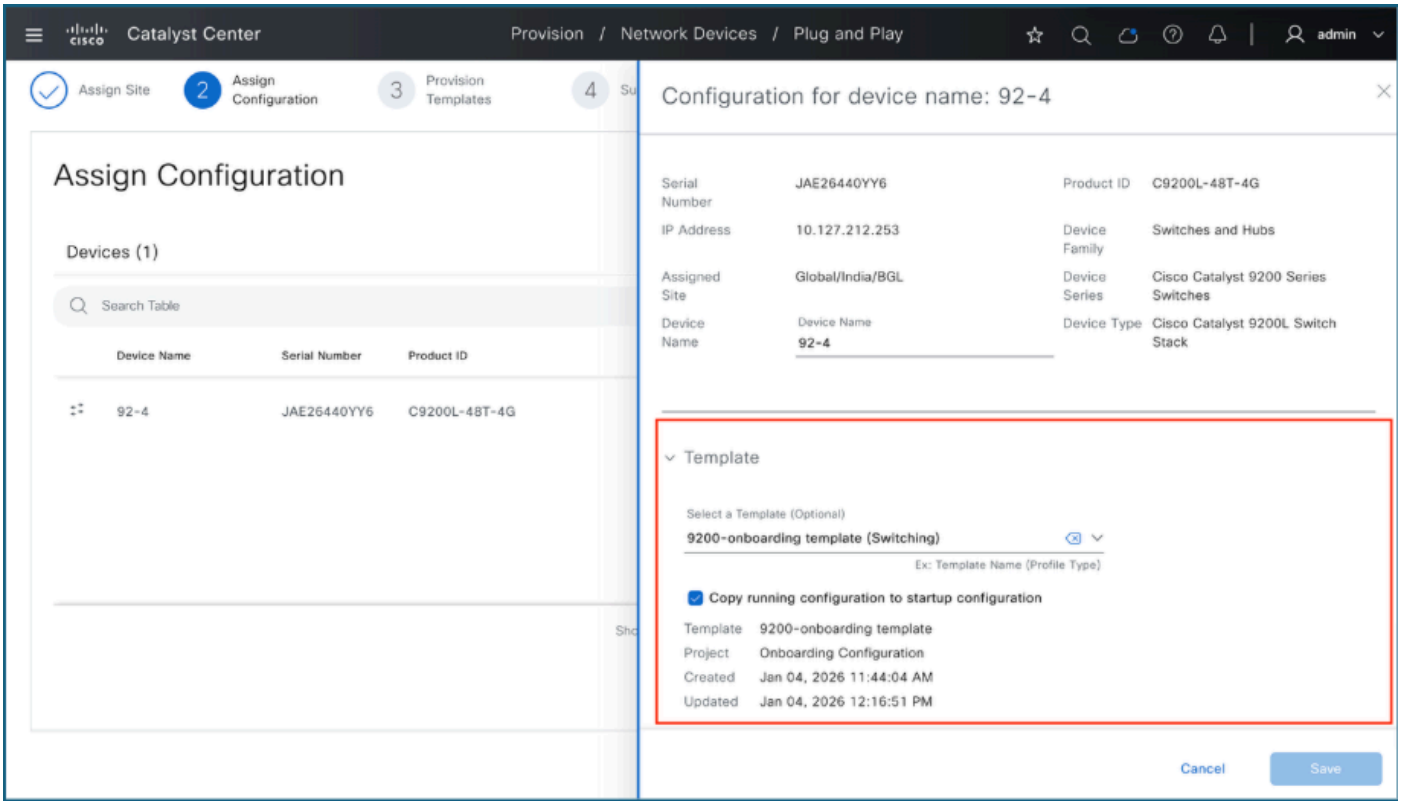
- **Name the Device:** Enter the desired name for the switch in the **Device Name** field.
- **Initiate Assignment:** Click the **Assign** button.
- **Select Location:** Choose the appropriate site or building, click **Assign** again, and then click **Next** to proceed.



10. Assign a Day-0 template

- **Select the Template:** Click on the template that has been automatically selected next to the **Template** option.
- **Review Details:** Carefully verify the configuration details of the assigned template.
- **Proceed:** Once you have confirmed the template assignment, click **Next.**



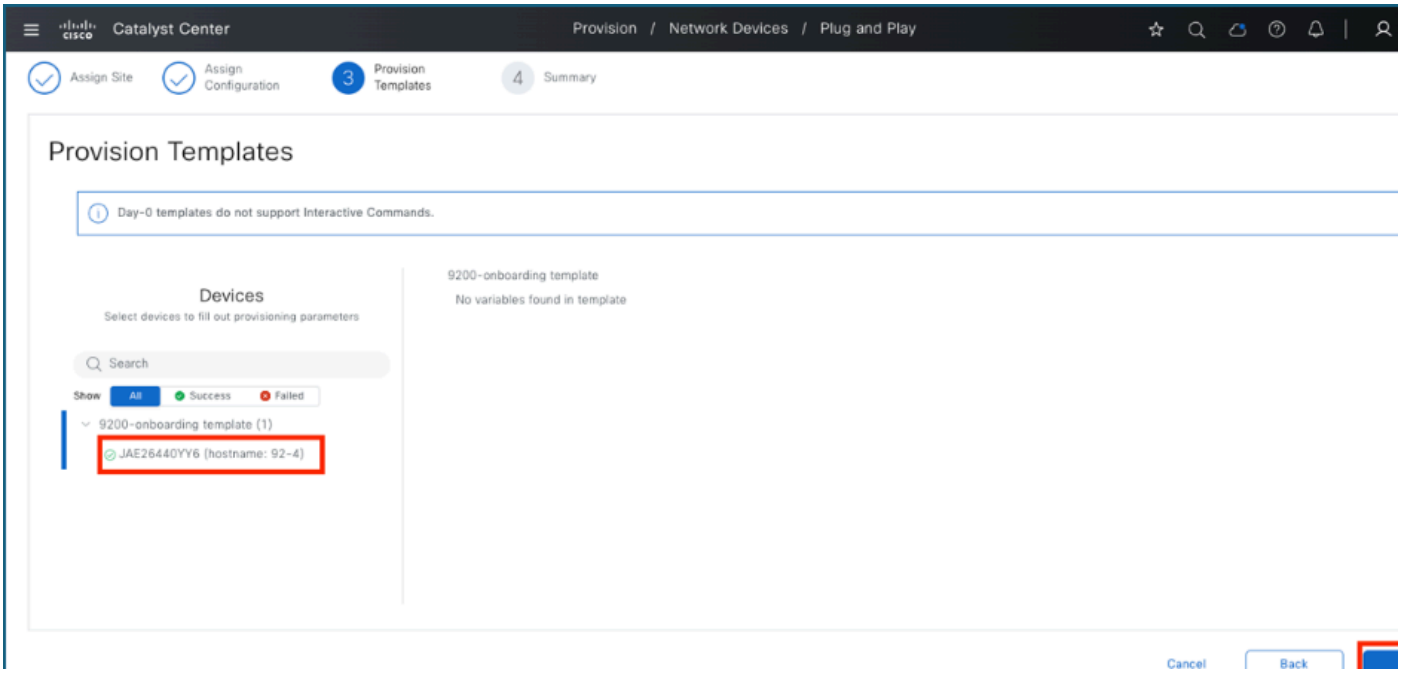


11. Provision templates

- **Select Device:** Under the template section, click on the specific device you are configuring.
- **Identify Variables:** Check for any required variable values associated with the template.

- **Enter Values:** If any variables are mandatory, fill in the necessary values.

- **Proceed:** Click **Next** to move to the next step.



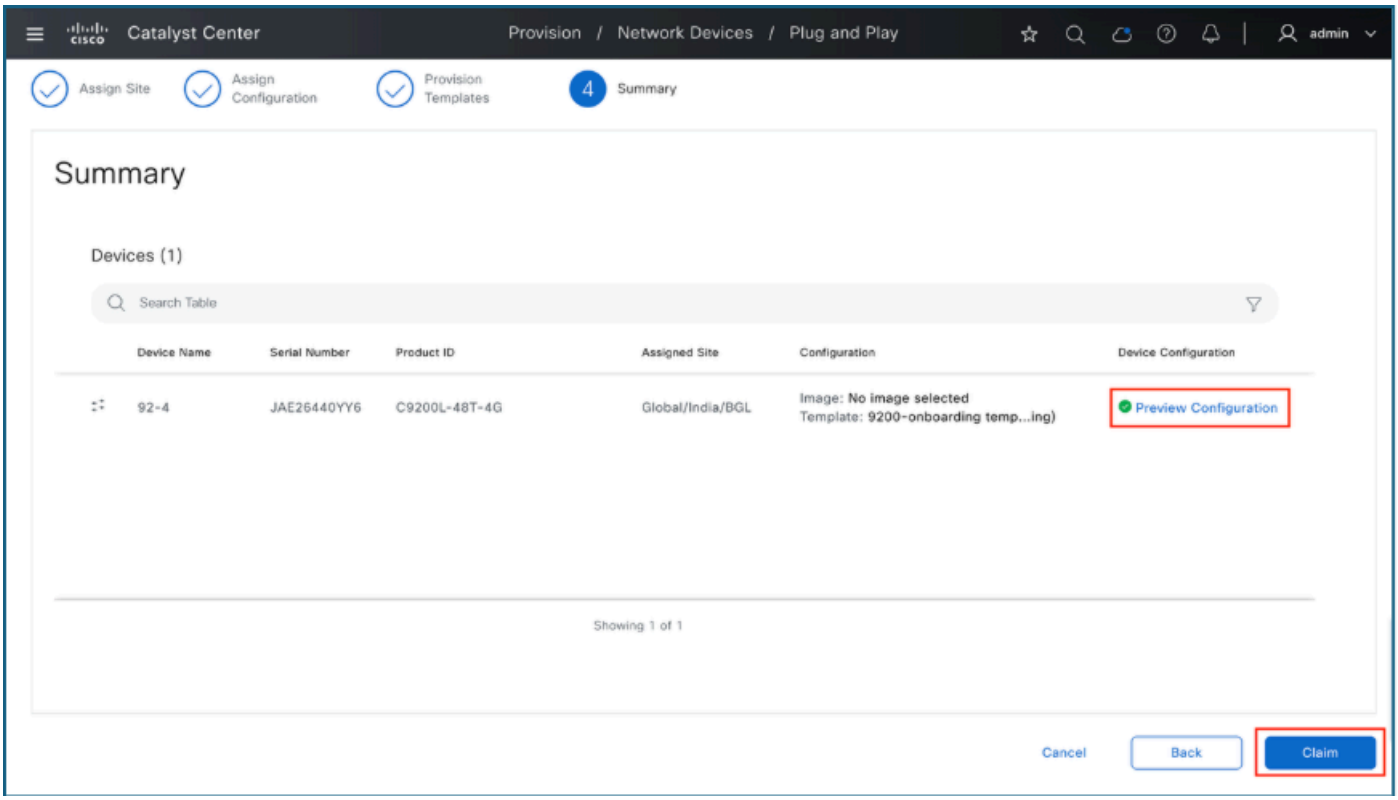
12. Summary

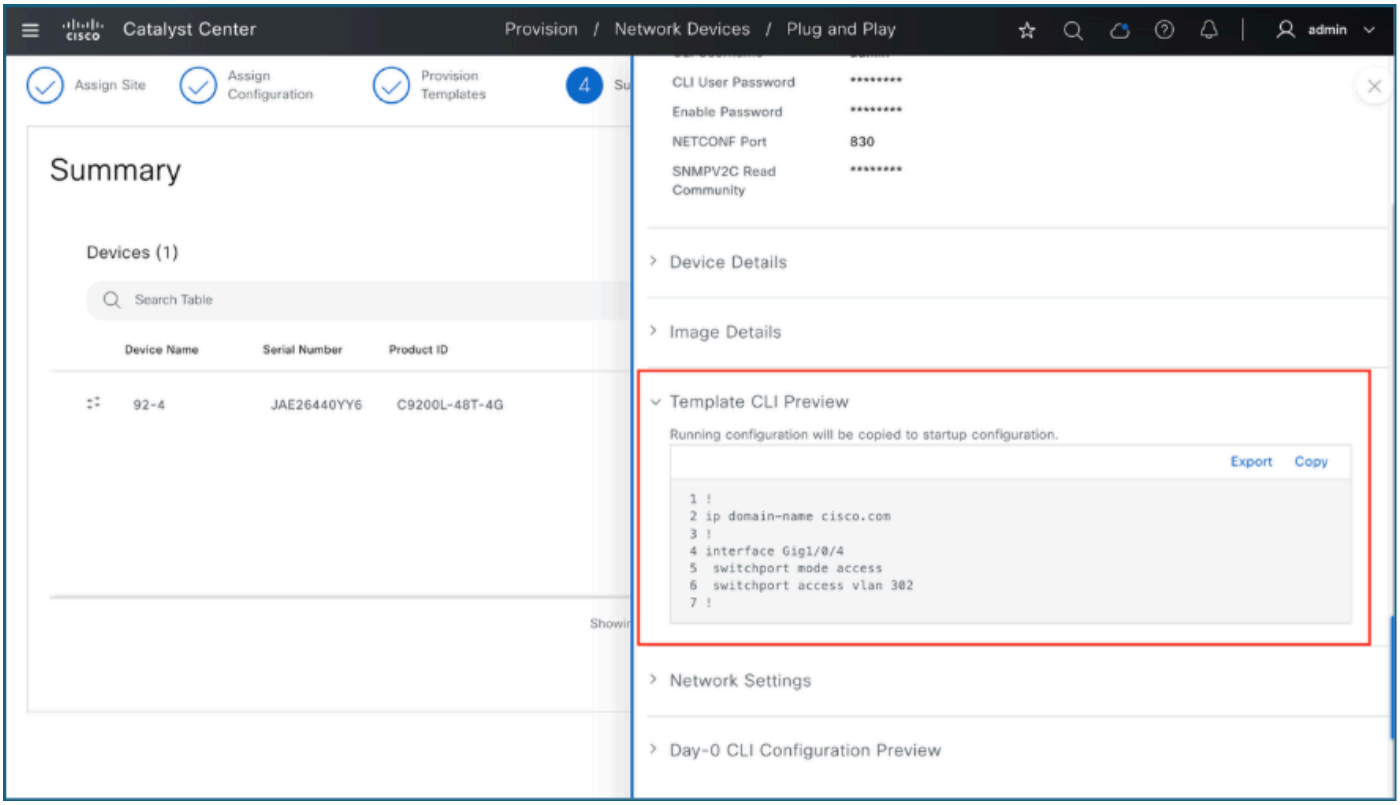
- **Review Configuration:** On the **Summary** page, audit the configuration settings prepared by Catalyst Center.

- **Preview Details:** Click on **Preview Configuration** to see the pending changes.

- **Verify Sections:** Expand each section to inspect the specific configuration details.

- **Finalize:** Once you have verified the settings, click **Claim** to proceed.



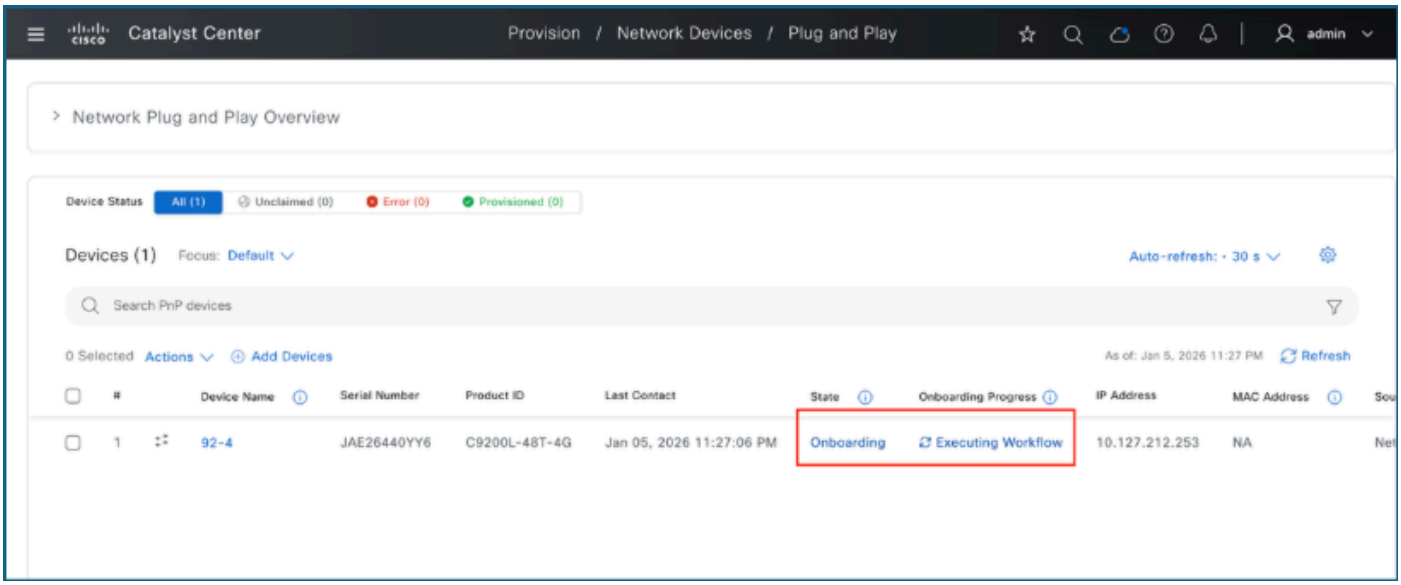


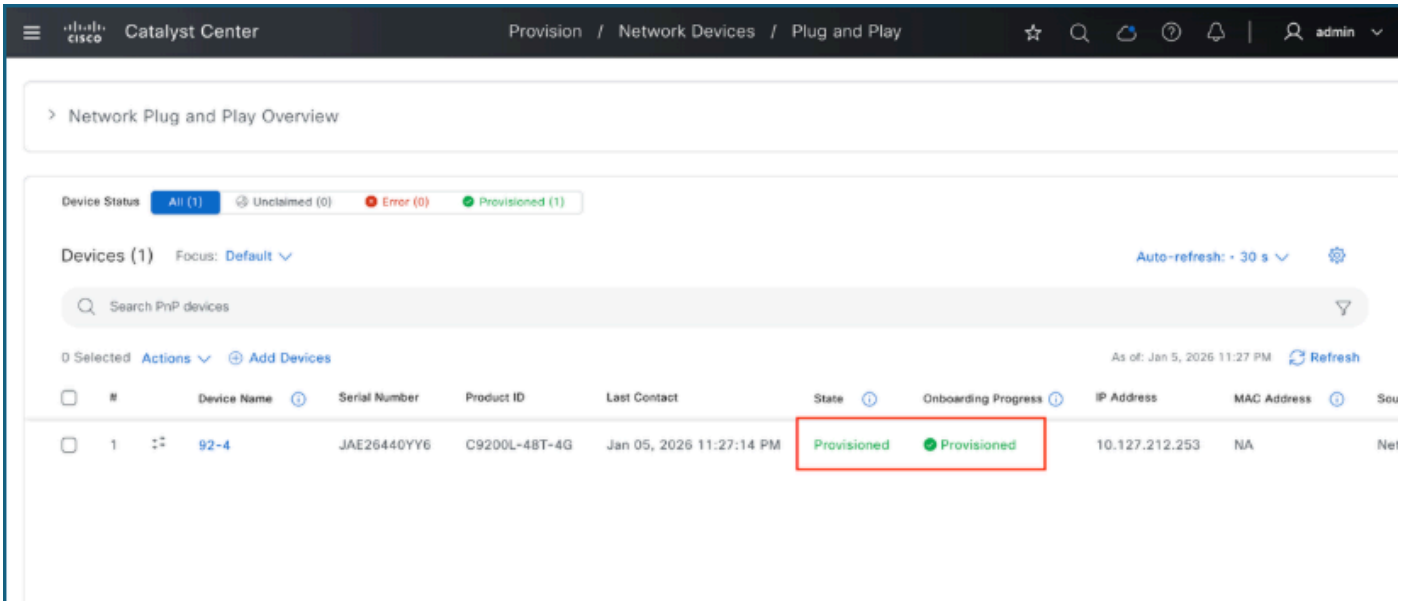
13. Monitor claim progress

You are redirected to the **Plug and Play** page to track the device progress.

- **Monitor Status:** Observe the device state as the claiming process proceeds.

- **Confirm Completion:** When the status updates to **Provisioned**, the switch has been successfully claimed and integrated into the Catalyst Center inventory.



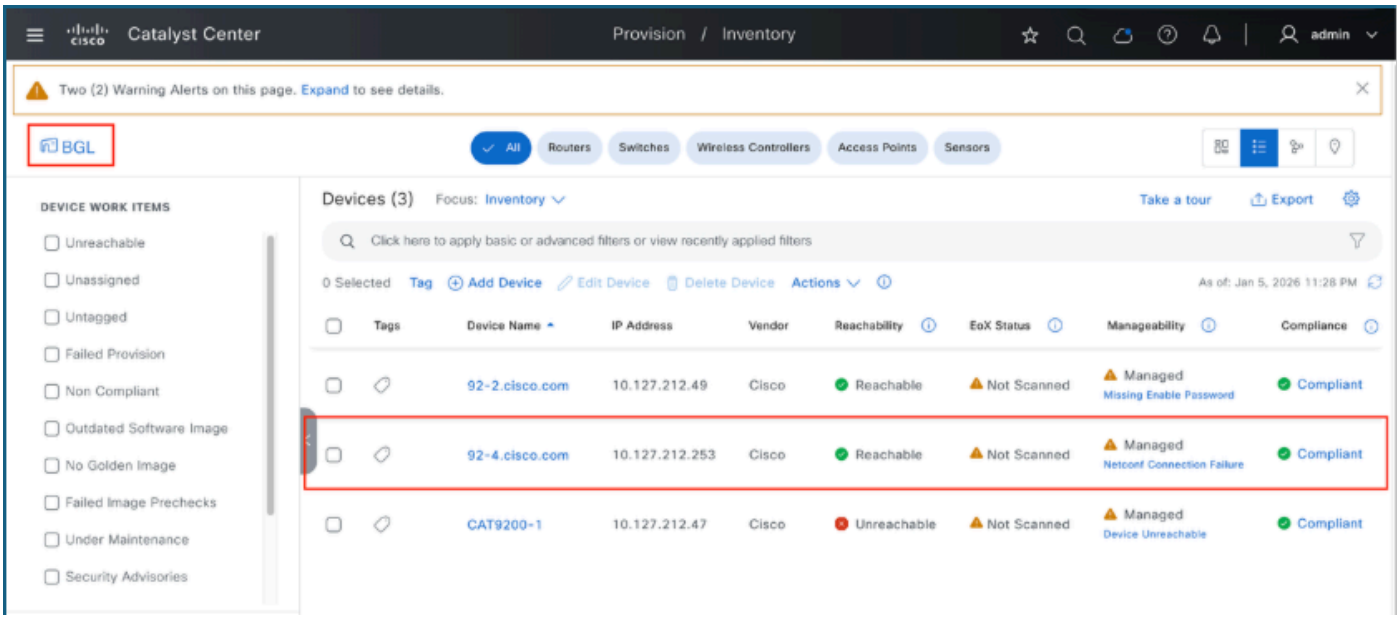


Verification

- **Access the Provision Menu:** Open the **Provision** tab in the main page.

- **View Inventory:** Select the **Inventory** option.

- **Verify Status:** Check the list to confirm that the switches have been successfully provisioned.



Bulk Import of Devices into Catalyst Center Plug and Play Inventory

To streamline large network rollouts, Catalyst Center supports a bulk import method for staging devices in advance. This process involves uploading device identifiers such as PIDs, serial numbers, and optional site or template data allowing the system to automatically onboard devices as soon as they are powered on and connected.

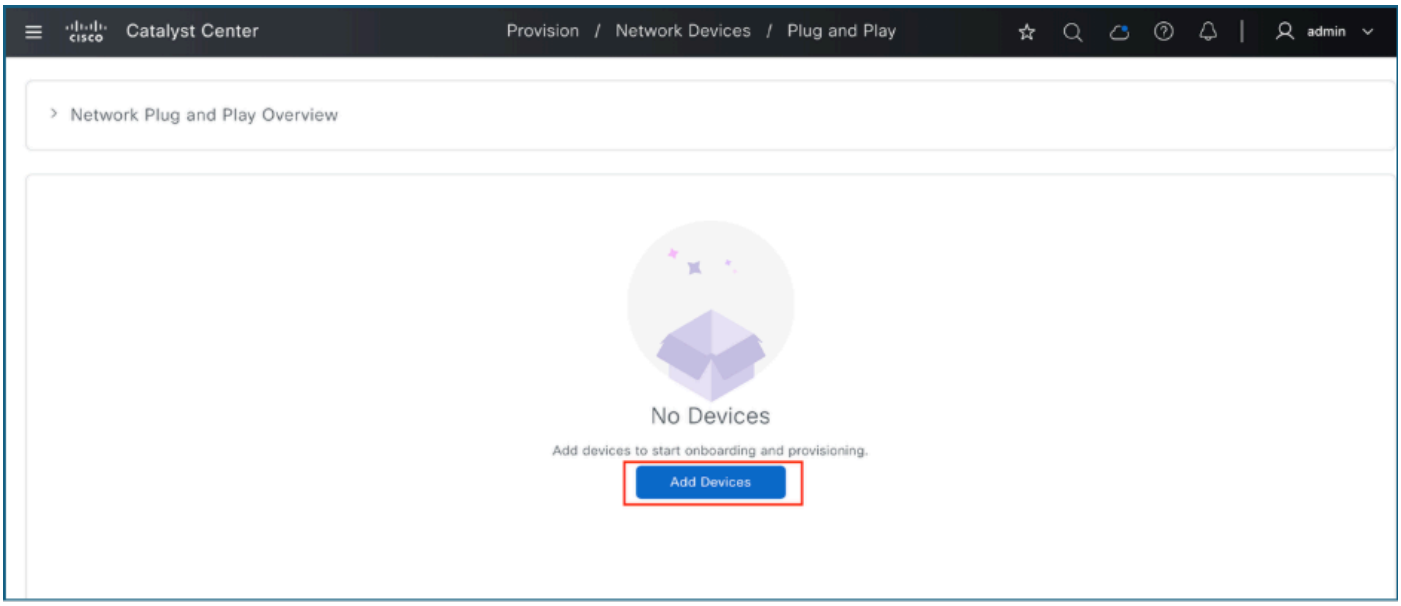
1. Prerequisites

To ensure a successful bulk import, these requirements must be met:

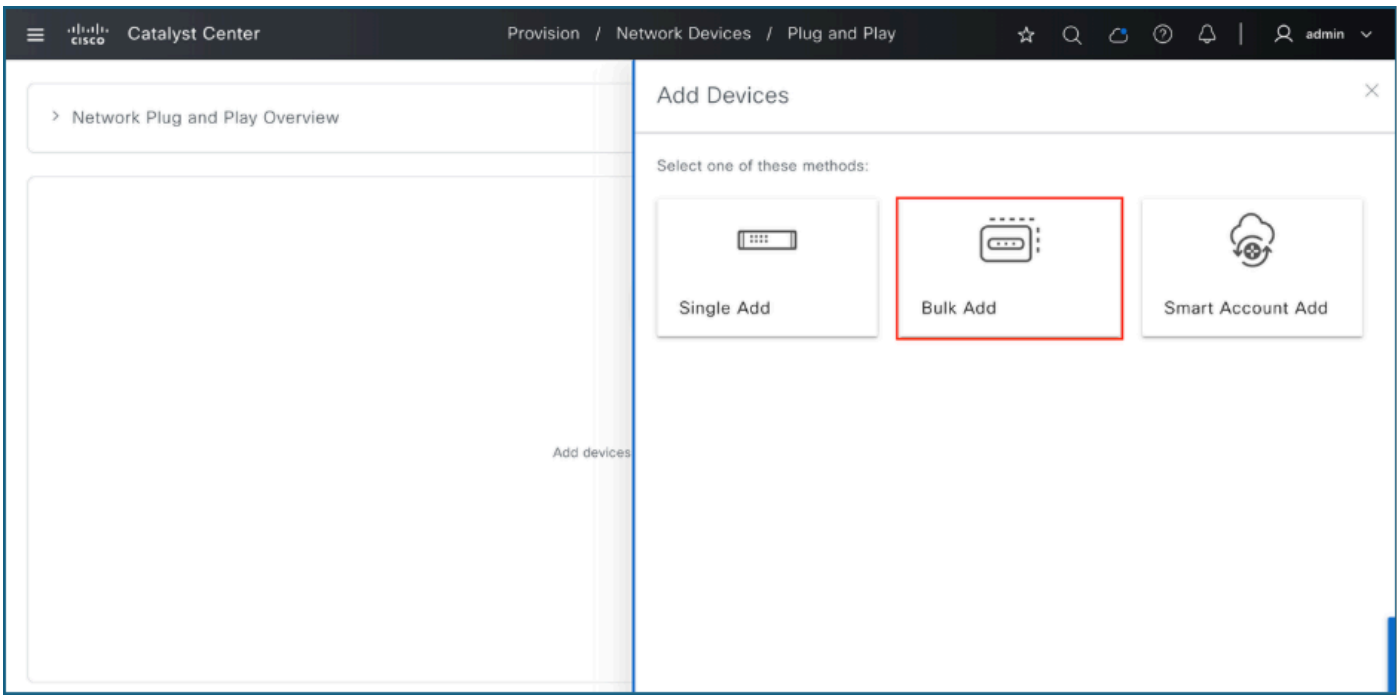
- The Catalyst Center instance must be reachable and operational.
- Hardware must be officially supported by the Cisco Plug and Play service.
- Device serial numbers and PIDs must be accessible.
- Target site hierarchies must be pre-configured in the Catalyst Center environment.

2. Bulk Import Procedure

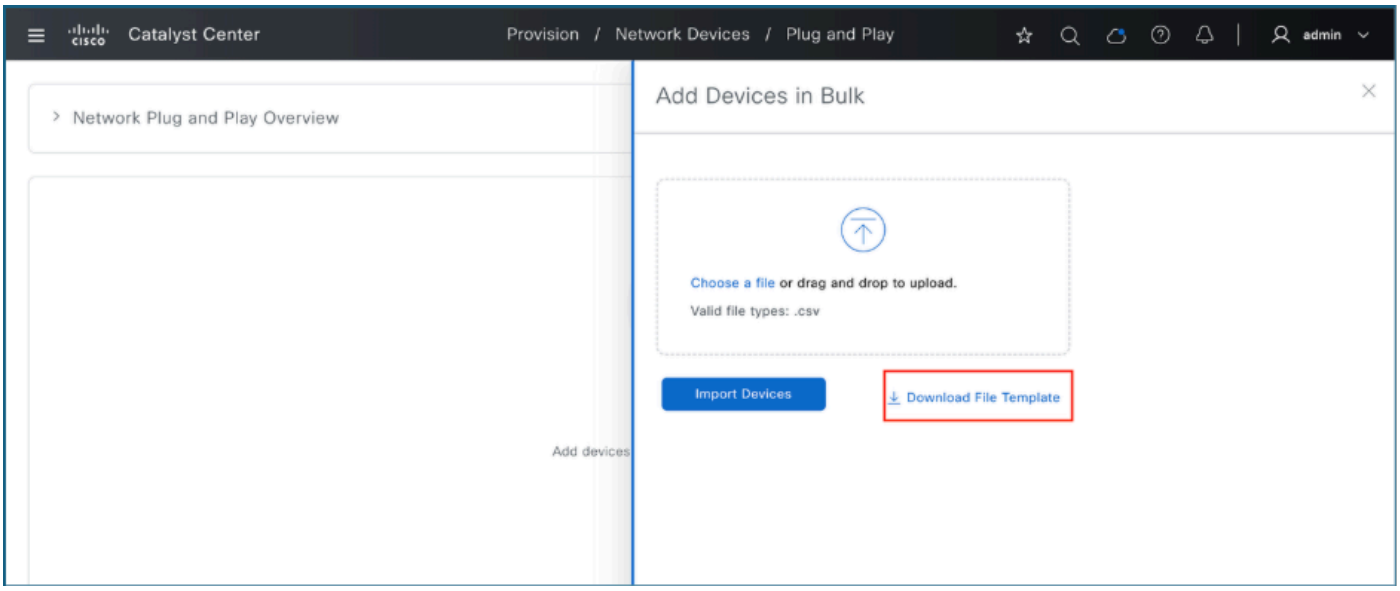
1. Log in to Catalyst Center
2. Navigate to **Provision > Plug and Play**
3. Click on **Add Devices**



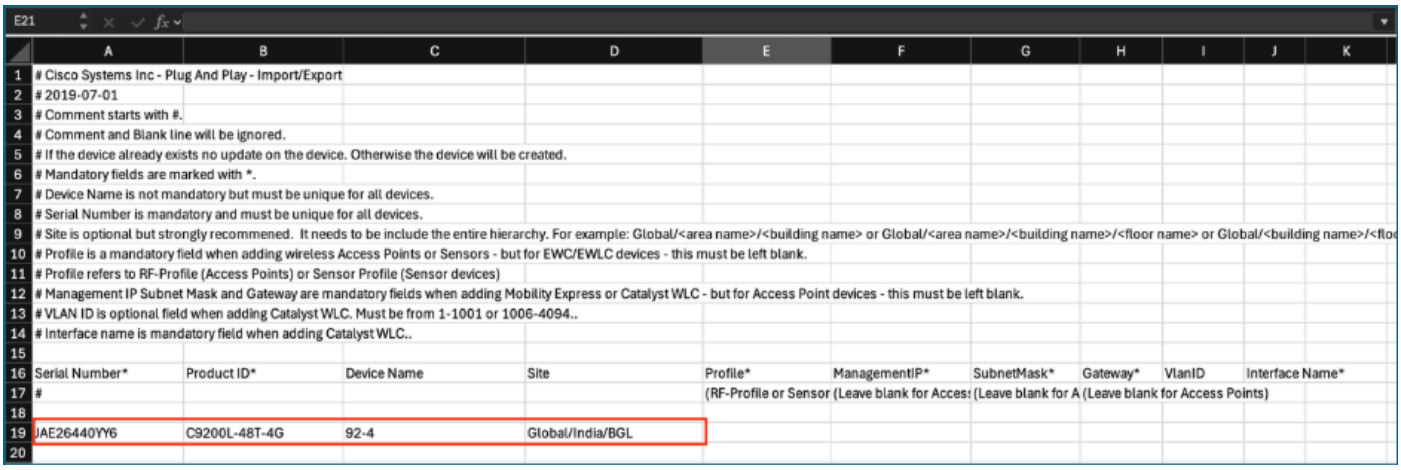
4. Click on **Bulk Add**



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

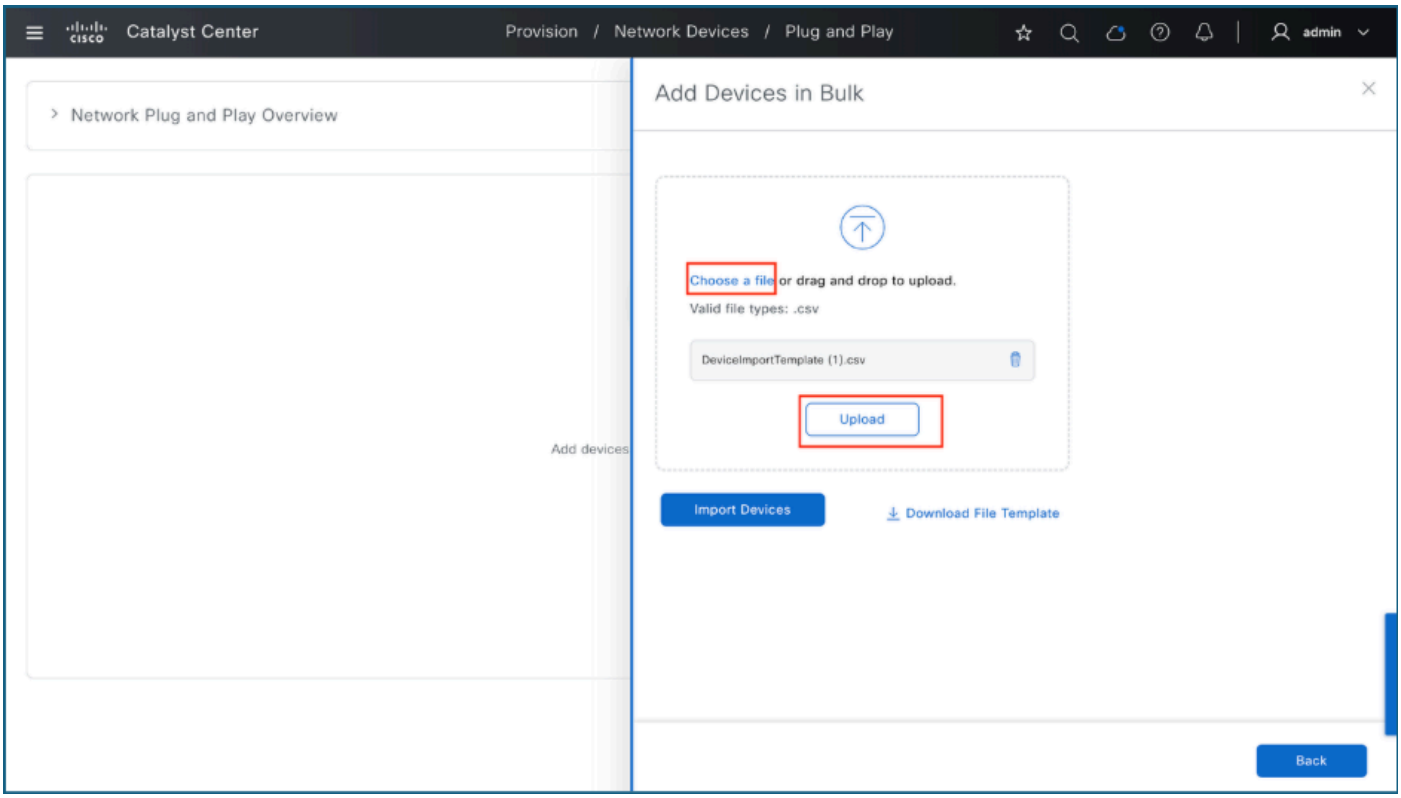


6. Populate the CSV file with the required device details.

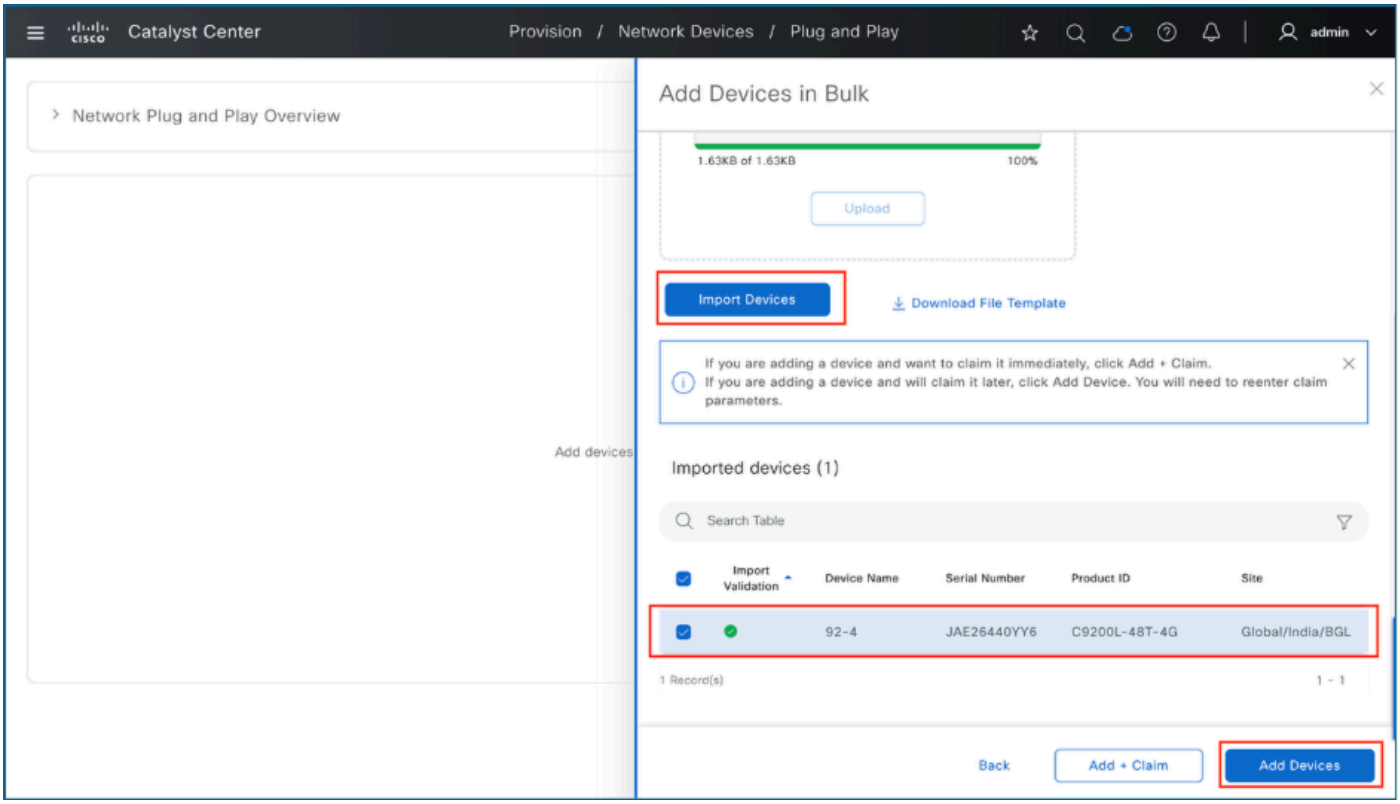


	A	B	C	D	E	F	G	H	I	J	K
1	# Cisco Systems Inc - Plug And Play - Import/Export										
2	# 2019-07-01										
3	# Comment starts with #.										
4	# Comment and Blank line will be ignored.										
5	# If the device already exists no update on the device. Otherwise the device will be created.										
6	# Mandatory fields are marked with *.										
7	# Device Name is not mandatory but must be unique for all devices.										
8	# Serial Number is mandatory and must be unique for all devices.										
9	# Site is optional but strongly recommened. It needs to be include the entire hierarchy. For example: Global/<area name>/<building name> or Global/<area name>/<building name>/<floor name> or Global/<building name>/<flo										
10	# Profile is a mandatory field when adding wireless Access Points or Sensors - but for EWC/EWLC devices - this must be left blank.										
11	# Profile refers to RF-Profile (Access Points) or Sensor Profile (Sensor devices)										
12	# Management IP Subnet Mask and Gateway are mandatory fields when adding Mobility Express or Catalyst WLC - but for Access Point devices - this must be left blank.										
13	# VLAN ID is optional field when adding Catalyst WLC. Must be from 1-1001 or 1006-4094..										
14	# Interface name is mandatory field when adding Catalyst WLC..										
15											
16	Serial Number*	Product ID*	Device Name	Site	Profile*	ManagementIP*	SubnetMask*	Gateway*	VlanID	Interface Name*	
17	#				(RF-Profile or Sensor	(Leave blank for Acces	(Leave blank for A	(Leave blank for Access Points)			
18											
19	JAE26440YY6	C9200L-48T-4G	92-4	Global/India/BGL							
20											

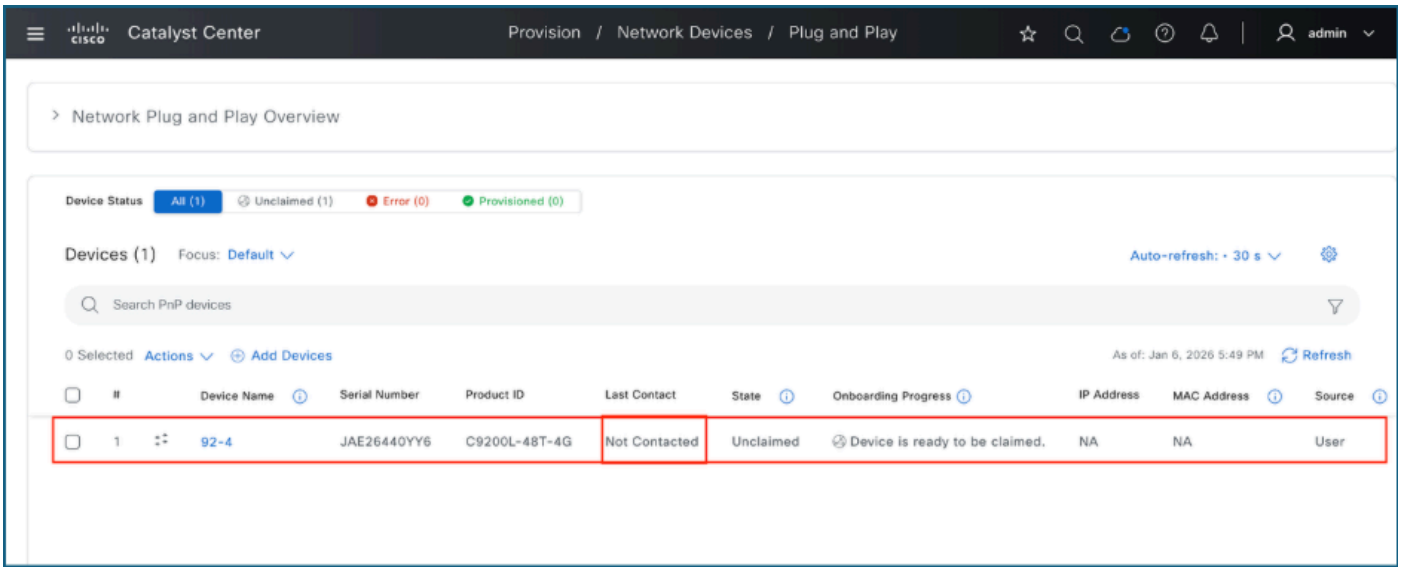
7. Upload the completed CSV file.



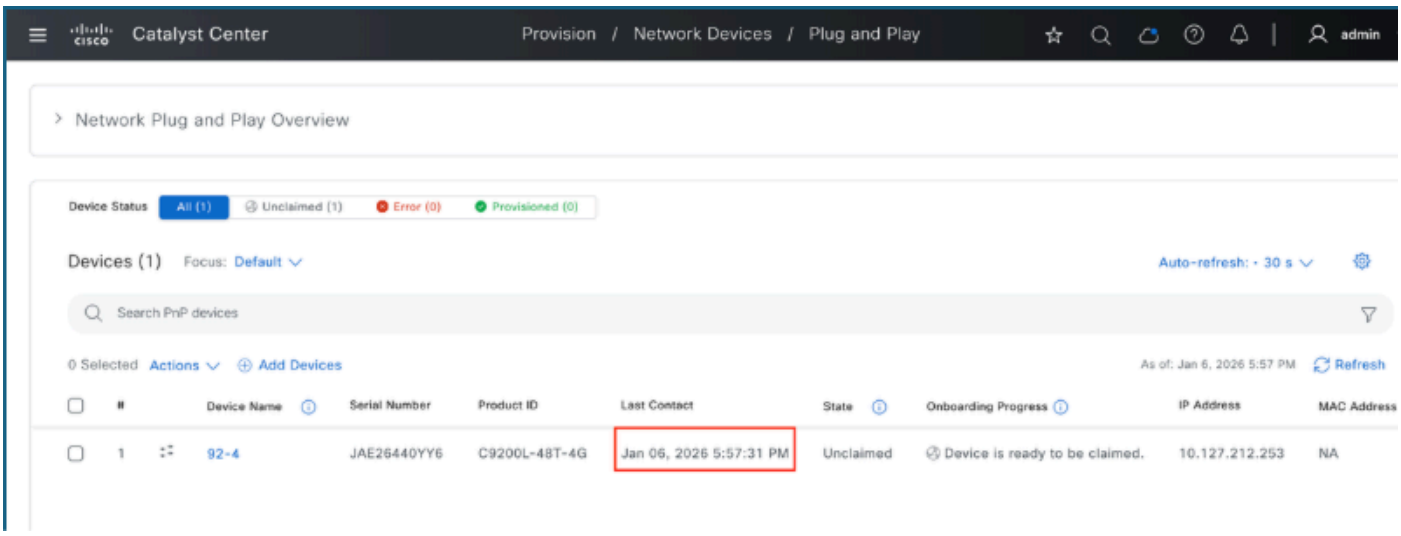
8. Import the devices from the CSV file and add them into the PnP inventory



9. The devices appear in the inventory as Not Contacted.



10. Once the device contacts Catalyst Center, it is ready to be claimed.



Troubleshooting

If the switch does not appear on Catalyst Center's Plug and Play page, these are the steps to identify and resolve the issue.

1. PnP Connectivity Validation

These commands validate PnP connectivity to Catalyst Center.

1.1. ICMP Reachability

Verify ICMP connectivity by pinging Catalyst Center's enterprise interface IP or Virtual IP (VIP) address.

Ensure that Catalyst Center is reachable via ping.

```
Switch#ping 10.127.212.43
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.127.212.43, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Switch#
```

1.2. HTTP HELLO validation

Plug and Play (PnP) fails if Catalyst Center does not respond to HELLO validation requests. To verify connectivity, run this command from a device terminal or command prompt: **curl -v http://<Catalyst Center IP>/pnp/HELLO**

Confirm that a "HELLO" response is received.

```
sitirkey@SITIRKEY-M-6PGJ netbox-docker % curl -v http://10.127.212.43/pnp/HE
*   Trying 10.127.212.43:80...
* Connected to 10.127.212.43 (10.127.212.43) port 80
> GET /pnp/HELLO HTTP/1.1
> Host: 10.127.212.43
> User-Agent: curl/8.7.1
> Accept: */*
>
* Request completely sent off
< HTTP/1.1 200 OK
< Date: Sun, 04 Jan 2026 07:51:20 GMT
< Content-Type: text/plain;charset=iso-8859-1
< Content-Length: 5
< Connection: keep-alive
<
* Connection #0 to host 10.127.212.43 left intact
```

1.3. HTTPS certificate retrieval

PnP functionality fails if the Catalyst Center server's certificate cannot be manually retrieved over HTTPS. To verify this, use this command: **copy https://<catc-ip-address>/ca/pem mypem2**

Confirm that the file transfer completes without errors.

```
92-4#copy https://10.127.212.43/ca/pem mypem2
Destination filename [mypem2]?
Accessing https://10.127.212.43/ca/pem...
Loading https://10.127.212.43/ca/pem
1472 bytes copied in 0.060 secs (24533 bytes/sec)
92-4#
```

1.4. PnP profile status

If a switch does not appear on Catalyst Center's PnP page, examine the PnP HTTP connectivity by executing the command**show pnp profile**

- Verify that PnP is using the correct Active-URL.

- Confirm that "Failed Counters" in the HTTP statistics is 0. A value greater than 0 indicates reachability issues between the switch and the Catalyst Center. This image illustrates a scenario involving reachability issues.

```
Switch#show pnp profile
PnP Profiles: Active:0, Created:0, Deleted:0, Hidden:0

Name            CBType Node     Primary-Path           Primary-Trans  Backup-Trans

-------------- show pnp http tracking ---------------

PNP-T3-Discovery: Active-Name=[PnP-Discovery-Proc], Last-Name=[PnP-Discovery-Proc]
        Active-URL=[http://10.127.212.43:80/pnp/HELLO], Last-URL=[http://10.127.212.43:80/pnp/HELLO]
        SID=7, Last-SID=6, TID=4294967295, last-TID=4294967295, Head-Date=[-], Status-Code=0, Get-Status=0, Get-Watch=7F6CDC0EF0
        HTTP-Register Stats: Total=3, OK=3, Failed=0, Ignored=0
        HTTP-Unregister Stats: Total=2, OK=2, Failed=0, Ignored=0
        HTTP-Resp-Data-Alloc Stats: Total=0, OK=0, Failed=0, Ignored=0
        HTTP-Resp-Data-Free Stats: Total=0, OK=0, Failed=0, Ignored=0
        HTTP-Resp-Data-Proc Stats: Total=6, OK=0, Failed=6, Ignored=0
        HTTP-Get-Watch-Init Stats: Total=6, OK=6, Failed=0, Ignored=0
        HTTP-Get-Wait-Complete Stats: Total=6, OK=6, Failed=0, Ignored=0
        HTTP-Send-Get Stats: Total=6, OK=0, Failed=6, Ignored=0
        HTTP-Send-Head Stats: Total=0, OK=0, Failed=0, Ignored=0
        HTTP-Send-Hello Stats: Total=0, OK=0, Failed=0, Ignored=0
        SSL-Handshake Stats: Total=0, OK=0, Failed=0, Ignored=0
        Server-ID-Check Stats: Total=0, OK=0, Failed=0, Ignored=0

PNP-HTTP-Tracker: Active-Name=[-], Last-Name=[-]
        Active-URL=[-], Last-URL=[-]
        SID=0, Last-SID=0, TID=0, last-TID=0, Head-Date=[-], Status-Code=0, Get-Status=0, Get-Watch=0
        HTTP-Register Stats: Total=0, OK=0, Failed=0, Ignored=0
        HTTP-Unregister Stats: Total=0, OK=0, Failed=0, Ignored=0
        HTTP-Resp-Data-Alloc Stats: Total=0, OK=0, Failed=0, Ignored=0
        HTTP-Resp-Data-Free Stats: Total=0, OK=0, Failed=0, Ignored=0
        HTTP-Resp-Data-Proc Stats: Total=0, OK=0, Failed=0, Ignored=0
        HTTP-Get-Watch-Init Stats: Total=0, OK=0, Failed=0, Ignored=0
        HTTP-Get-Wait-Complete Stats: Total=0, OK=0, Failed=0, Ignored=0
        HTTP-Send-Get Stats: Total=0, OK=0, Failed=0, Ignored=0
        HTTP-Send-Head Stats: Total=0, OK=0, Failed=0, Ignored=0
        HTTP-Send-Hello Stats: Total=0, OK=0, Failed=0, Ignored=0
        SSL-Handshake Stats: Total=0, OK=0, Failed=0, Ignored=0
        Server-ID-Check Stats: Total=0, OK=0, Failed=0, Ignored=0
Switch#
```

This example illustrates a scenario with no reachability issues.

```
PNP-T1-Discovery: Active-Name=[PnP-Discovery-Proc], Last-Name=[-]
        Active-URL=[http://catc1.cisco.com:80/pnp/HELLO], Last-URL=[-]
        SID=5, Last-SID=0, TID=1, last-TID=0, Head-Date=[Mon, 05 Jan 2026 15:28:17 GMT], Status-Code=200, Get-Status=8, Get-Watch=4B881114
        HTTP-Register Stats: Total=1, OK=1, Failed=0, Ignored=0
        HTTP-Unregister Stats: Total=0, OK=0, Failed=0, Ignored=0
        HTTP-Resp-Data-Alloc Stats: Total=1, OK=1, Failed=0, Ignored=0
        HTTP-Resp-Data-Free Stats: Total=1, OK=1, Failed=0, Ignored=0
        HTTP-Resp-Data-Proc Stats: Total=1, OK=1, Failed=0, Ignored=0
        HTTP-Get-Watch-Init Stats: Total=1, OK=1, Failed=0, Ignored=0
        HTTP-Get-Wait-Complete Stats: Total=1, OK=1, Failed=0, Ignored=0
        HTTP-Send-Get Stats: Total=1, OK=1, Failed=0, Ignored=0
        HTTP-Send-Head Stats: Total=0, OK=0, Failed=0, Ignored=0
        HTTP-Send-Hello Stats: Total=0, OK=0, Failed=0, Ignored=0
        SSL-Handshake Stats: Total=0, OK=0, Failed=0, Ignored=0
        Server-ID-Check Stats: Total=0, OK=0, Failed=0, Ignored=0

PNP-T1-pnp-zero-touch: Active-Name=[PnP-pnp-zero-touch], Last-Name=[-]
        Active-URL=[https://catc1.cisco.com:443/pnp/HELLO], Last-URL=[-]
        SID=8, Last-SID=0, TID=8, last-TID=0, Head-Date=[Mon, 05 Jan 2026 15:28:34 GMT], Status-Code=200, Get-Status=8, Get-Watch=4B881570
        HTTP-Register Stats: Total=1, OK=1, Failed=0, Ignored=0
        HTTP-Unregister Stats: Total=0, OK=0, Failed=0, Ignored=0
        HTTP-Resp-Data-Alloc Stats: Total=1, OK=1, Failed=0, Ignored=0
        HTTP-Resp-Data-Free Stats: Total=1, OK=1, Failed=0, Ignored=0
        HTTP-Resp-Data-Proc Stats: Total=1, OK=1, Failed=0, Ignored=0
        HTTP-Get-Watch-Init Stats: Total=1, OK=1, Failed=0, Ignored=0
        HTTP-Get-Wait-Complete Stats: Total=1, OK=1, Failed=0, Ignored=0
        HTTP-Send-Get Stats: Total=1, OK=1, Failed=0, Ignored=0
        HTTP-Send-Head Stats: Total=0, OK=0, Failed=0, Ignored=0
        HTTP-Send-Hello Stats: Total=1, OK=1, Failed=0, Ignored=0
        SSL-Handshake Stats: Total=0, OK=0, Failed=0, Ignored=0
        Server-ID-Check Stats: Total=0, OK=0, Failed=0, Ignored=0
```

2. DHCP Validation

These commands help validate DHCP configuration and connectivity.

2.1. Verify DHCP IP address assignment

Execute the command: show ip interface brief, to verify that the PnP VLAN SVI has successfully received an IP address from the DHCP server.

```
Switch#show ip int brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  unassigned      YES unset  administratively down down
Vlan302                10.127.212.254  YES DHCP   up                    up
GigabitEthernet0/0     unassigned      YES unset  up                    up
```

2.2. Confirm Lease Server

Execute the command **show dhcp lease**to verify the DHCP lease server information.

```
Switch#show dhcp lease
Temp IP addr: 10.127.212.254  for peer on Interface: Vlan302
Temp  sub net mask: 255.255.255.0
   DHCP Lease server: 10.127.212.49, state: 5 Bound
   DHCP transaction id: 23F1
   Lease: 86400 secs,  Renewal: 43200 secs,  Rebind: 75600 secs
Temp default-gateway addr: 10.127.212.49
   Next timer fires after: 11:52:27
   Retry count: 0   Client-ID: cisco-4464.3cb1.2bf7-Vl302
   Client-ID hex dump: 636973636F2D343436342E336362312E
                       326266372D566C333032
   Hostname: Switch
```

2.3. Validate Option 43 using debug logs

To validate Option 43, enable DHCP debugging with the command **debug dhcp detail.** After enabling the debug perform a shutdown and no shutdown on the interface to restart the DHCP process. In the logs, locate the section "DHCP: Scan: Vendor specific option 43:". Copy the hex string as shown on this section, convert it to text using a suitable hex-to-ASCII converter, and verify that the resulting string correctly points to Catalyst Center.

```
000344: Jan  4 08:55:39.247: DHCP Offer Message   Offered Address: 10.127.212.254
000345: Jan  4 08:55:39.247: DHCP: Lease Seconds: 86400    Renewal secs:  43200    Rebind secs:   75600
000346: Jan  4 08:55:39.247: DHCP: Server ID Option: 10.127.212.49
000347: Jan  4 08:55:39.247: DHCP: offer received from 10.127.212.49
000348: Jan  4 08:55:39.247: DHCP: SRequest attempt # 1 for entry:
000349: Jan  4 08:55:39.247: Temp IP addr: 10.127.212.254  for peer on Interface: Vlan302
000350: Jan  4 08:55:39.247: Temp  sub net mask: 255.255.255.0
000351: Jan  4 08:55:39.247:    DHCP Lease server: 10.127.212.49, state: 4 Requesting
000352: Jan  4 08:55:39.247:    DHCP transaction id: A62
000353: Jan  4 08:55:39.247:    Lease: 86400 secs,  Renewal: 0 secs,  Rebind: 0 secs
000354: Jan  4 08:55:39.247:    Next timer fires after: 00:00:03
000355: Jan  4 08:55:39.247:    Retry count: 1   Client-ID: cisco-4464.3cb1.2bf7-Vl302
000356: Jan  4 08:55:39.247:    Client-ID hex dump: 636973636F2D343436342E336362312E
000357: Jan  4 08:55:39.247:                        326266372D566C333032
000358: Jan  4 08:55:39.248:    Hostname: Switch
000359: Jan  4 08:55:39.248: DHCP: SRequest- Server ID option: 10.127.212.49
000360: Jan  4 08:55:39.248: DHCP: SRequest- Requested IP addr option: 10.127.212.254
000361: Jan  4 08:55:39.248: DHCP: SRequest placed lease len option: 86400
000362: Jan  4 08:55:39.248: DHCP: SRequest placed class-id option: 636973636F706E70
000363: Jan  4 08:55:39.248: DHCP: SRequest: 323 bytes
000364: Jan  4 08:55:39.248: DHCP: SRequest: 323 bytes
000365: Jan  4 08:55:39.248:             B'cast on Vlan302 interface from 0.0.0.0
000366: Jan  4 08:55:39.254: DHCP: Received a BOOTREP pkt
000367: Jan  4 08:55:39.254: DHCP: Scan: Message type: DHCP Ack
000368: Jan  4 08:55:39.254: DHCP: Scan: Client ID: cisco-4464.3cb1.2bf7-Vl302
000369: Jan  4 08:55:39.254: DHCP: Scan: Server ID Option: 10.127.212.49 = A7FD431
000370: Jan  4 08:55:39.254: DHCP: Scan: Lease Time: 86400
000371: Jan  4 08:55:39.254: DHCP: Scan: Renewal time: 43200
000372: Jan  4 08:55:39.254: DHCP: Scan: Rebind time: 75600
000373: Jan  4 08:55:39.254: DHCP: Scan: Subnet Address Option: 255.255.255.0
000374: Jan  4 08:55:39.254: DHCP: Scan: Vendor specific option 43: 3541314E3B42323B4B343B4931302E3132372E3231322E34333B4A38303B
000375: Jan  4 08:55:39.254: DHCP: Scan: Router Option: 10.127.212.49
000376: Jan  4 08:55:39.254: DHCP: rcvd pkt source: 10.127.212.49,  destination:  255.255.255.255
000377: Jan  4 08:55:39.254:    UDP  sport: 43,  dport: 44,  length: 349
000378: Jan  4 08:55:39.255:    DHCP op: 2, htype: 1, hlen: 6, hops: 0
000379: Jan  4 08:55:39.255:    DHCP server identifier: 10.127.212.49
000380: Jan  4 08:55:39.255:         xid: A62, secs: 0, flags: 8000
000381: Jan  4 08:55:39.255:         client: 0.0.0.0, your: 10.127.212.254
000382: Jan  4 08:55:39.255:         srvr:   0.0.0.0, gw: 0.0.0.0
000383: Jan  4 08:55:39.255:         options block length: 101

000384: Jan  4 08:55:39.255: DHCP Ack Message
000385: Jan  4 08:55:39.255: DHCP: Lease Seconds: 86400    Renewal secs:  43200    Rebind secs:   75600
000386: Jan  4 08:55:39.255: DHCP: Server ID Option: 10.127.212.49
000387: Jan  4 08:55:40.232: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan302, changed state to up
000388: Jan  4 08:55:42.256: DHCP: Offered Address has no conflicts
000389: Jan  4 08:55:42.259: DHCP: Releasing ipl options:
000390: Jan  4 08:55:42.259: DHCP: Applying DHCP options:
000391: Jan  4 08:55:42.259:   Setting default_gateway to 10.127.212.49
000392: Jan  4 08:55:42.260:   Adding default route 10.127.212.49
000393: Jan  4 08:55:43.259: DHCPC: Notifying other components about option 43
000394: Jan  4 08:55:43.259: DHCP: Sending notification of ASSIGNMENT:
000395: Jan  4 08:55:43.259:   Address 10.127.212.254 mask 255.255.255.0
```

Best Practices

- Ensure the switch is in its factory default state. If it was previously provisioned, use the **pnpa service reset** command to reset it.
- Avoid interrupting the PnP process through the console.

- Verify certificates and DNS resolution prior to deployment.