

---

# Network Device Onboarding with Plug and Play

**Submitted**

**By**

## Contents

.....	<b>Error! Bookmark not defined.</b>
<b>Introduction .....</b>	<b>3</b>
<b>Implementation Flow .....</b>	<b>4</b>
<b>Define .....</b>	<b>4</b>
<b>Design.....</b>	<b>5</b>
<b>Process 1: Configure the site hierarchy within Cisco DNA Center. ....</b>	<b>5</b>
Create an area .....	6
Create building within the area .....	7
<b>Process 2. Configure network services and device credentials for network operation.....</b>	<b>8</b>
Add Network Services.....	8
Add device credentials to manage.....	10
<b>Deploy .....</b>	<b>13</b>
<b>Automate onboarding of a switch with Plug and Play (PnP) .....</b>	<b>13</b>
Procedure 1. Define Golden image for devices in inventory .....	13
Procedure 2. Create Onboarding Templates .....	15
Procedure 3. Create Network Profiles for Switching .....	18
Procedure 4. Assign Network Profile to Site .....	19
Procedure 5. Discover the Controller (PnP Server).....	20
Procedure 6. Day-0 provisioning of switch onboarded with PnP .....	22

# Introduction

## About The Solution

Cisco DNA Center can help automate with built-in Plug-and-Play (PnP) functionality and allow switches, routers, and wireless access points to be on-boarded to the network. An agent in the device, call-home Cisco DNA center and downloads the required software and device configuration.

## About This Guide

This guide will only focus on how to deploy a single non-fabric switch using Cisco DNA Center to help reduce the cost, remove complexity, and maximize productivity resulting in an overall savings in operational expenses.

## Use Cases

Automate Day-Zero onboarding of a switch with Plug and Play (PnP).

## Reader tip

For more information on Cisco DNA Center supported devices please refer to the compatibility matrix information <https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-device-support-tables-list.html>

# Implementation Flow

This document contains four major sections:

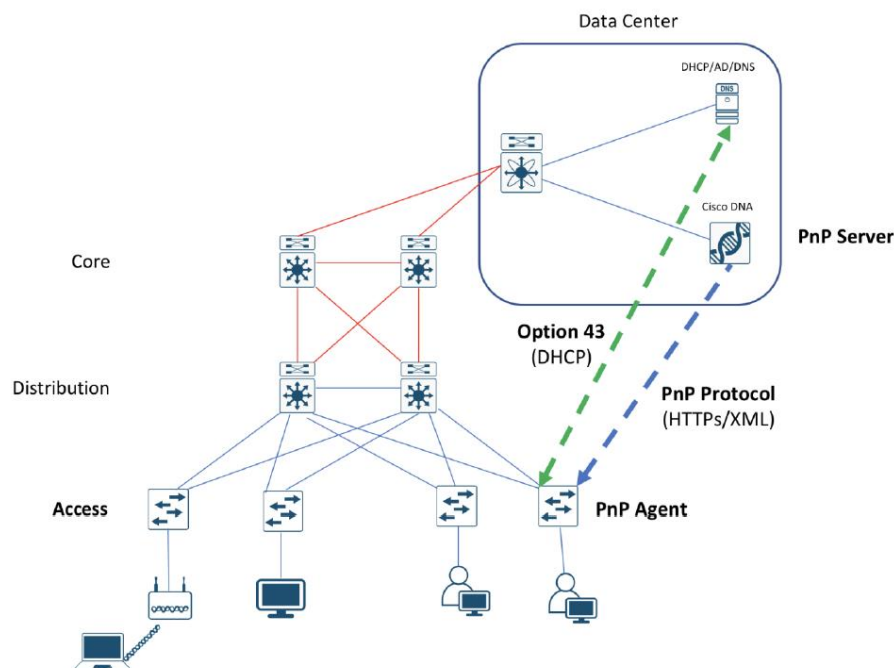
- The **Define** section presents a high-level overview of the campus LAN which will be designed and deployed through Cisco DNA Center.
- The **Design** section discusses the creation of the site hierarchy within Cisco DNA Center; configuration of various network services necessary for network operations.
- The **Deploy** section discusses discovery of the switch in a campus LAN; Define Golden image for a device in inventory, Create Onboarding Template, Create Network Profiles for Switching, Assign Network Profile to Site, Discover and manage network devices.
- The **Operate** section briefly discusses the known caveats of device onboarding using PnP.

## Define

### Solution overview

Cisco DNA Center can help with the non-fabric wired deployments in various different ways such as – network discovery, network inventory, return material authorization, software image management (SWIM), Plug and Play (PnP) etc.

This guide only covers day-zero onboarding of a switch with Plug and Play (PnP).



Cisco DNA Center is designed for intent-based networking (IBN). The solution breaks the process in to Day 0 and Day N. The solution provides a unified approach to provision enterprise networks comprised of Cisco routers, switches, and wireless devices with a near zero touch deployment experience.

When planning to provision any project, the PnP feature within Cisco DNA Center can help pre-provision and add devices to the project. This includes entering device information and setting up a bootstrap configuration, full configuration, and Cisco device image for each device to be installed. The bootstrap configuration enables the PnP Agent, specifies the device interface to be used, and configures a static IP address for it.

## Design

Before you proceed you must make sure you already have Cisco DNA Center installed on your network.

Complete the following prerequisites before proceeding:

- Configure the site hierarchy within Cisco DNA Center.
- Configure network services (ex. DNS, DHCP, etc.) necessary for network operation.

### Process 1: Configure the site hierarchy within Cisco DNA Center.

Configuring the site hierarchy involves defining the network sites for the deployment, and their hierarchical relationships. Network sites consist of areas, buildings, and floors. Their hierarchical relationship is important because child sites automatically inherit certain attributes from parent sites. However, these attributes may be overridden within the child site.

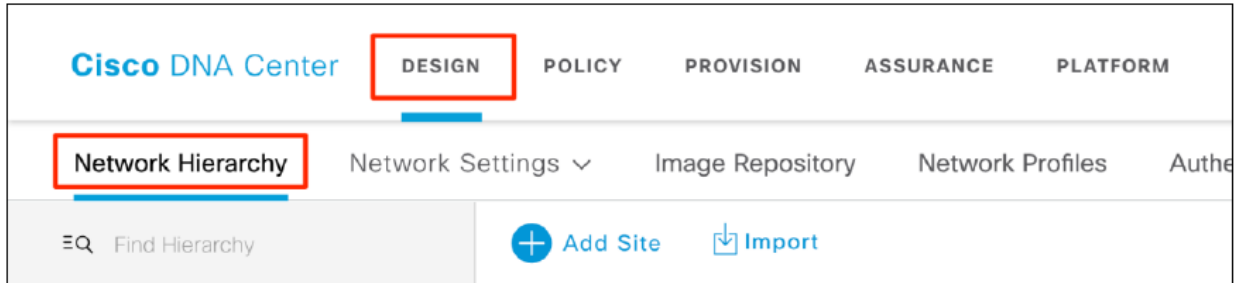
The following are the procedures for configuring the site hierarchy for this design and deployment guide:

- Create an area.
- Create buildings within the area.
- Create floors within each building and import floor maps

## Create an area

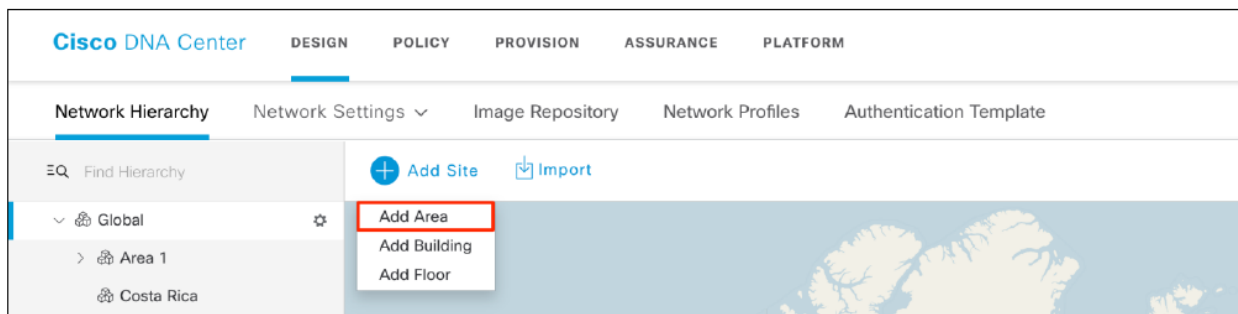
**Step 1.** Login to the Cisco DNA Center.

**Step 2.** Navigate to **Design > Network Hierarchy**.

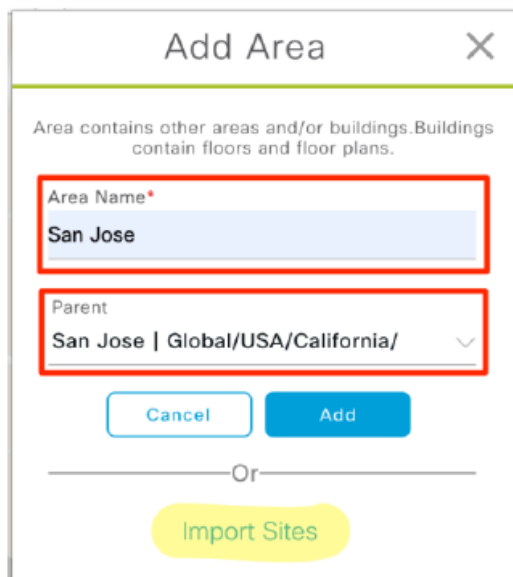


**Step 3.** Click **Add site**

**Step 4.** Select **Add Area** from drop-down menu.



**Step 5.** In **Add Area** pop-up window, type in the **Area Name** and select **Parent**.

The screenshot shows the 'Add Area' pop-up window. The 'Area Name' field is highlighted with a red box and contains the text 'San Jose'. The 'Parent' dropdown menu is also highlighted with a red box and shows the selected value 'San Jose | Global/USA/California/'. Below the fields are 'Cancel' and 'Add' buttons. At the bottom, there is an 'Import Sites' button and an 'Or' separator.

**Step 6.** Click **Add** button to add the area.

## Create building within the area

**Step 1.** Under **Network Hierarchy**, click **Add Site**.

**Step 2.** From drop-down menu select **Add Building**.

Add Building

Area contains other areas and/or buildings. Buildings contain floors and floor plans.

Building Name\*

Building 4

Parent

San Jose | Global/USA/California/

Address ⓘ

150 Tasman Drive, San Jose, California 9513

Latitude\*

37.407989

Longitude\*

-121.952637

Cancel Add

### Tech tip

For Latitude and Longitude, enter an **Address** and select the suggested full address from the drop down and both the fields will be auto populated.

**Step 3.** In the **Add Building** pop-up window, type in the **Building Name**.

**Step 4.** Select the **Parent** area.

**Step 5.** Enter the building address in the text field under **Address**.

**Step 6.** Click the **Add** button to add the building.

### Tech tip

Adding floor is required for setting up wireless network.

## Process 2. Configure network services and device credentials for network operation

In the procedure below configure the following services that align to the site hierarchy in Cisco DNA Center:

- AAA
- DHCP
- DNS
- Syslog
- SNMP

If the services use the same servers across the entire site hierarchy, you can configure them globally. The inheritance properties of the site hierarchy makes global settings available to all sites. Differences for individual sites can then be applied on a site-by-site basis. Then add device credentials to manage scopes of the site hierarchy created in the design.

### Add Network Services

**Step 1.** Login to Cisco DNA Center and navigate to **Design > Network Settings > Network**.

**Step 2.** Select **Global** in the navigation panel on the left side of the screen.

**Step 3.** Click on the **+Add Servers** button.

**Step 4.** From the **Add Servers** popup screen check the boxes next to **AAA** and **NTP** and click the **OK** button.

**Step 5.** Locate the **AAA Servers** section and fill in the necessary information.

Network    Device Credentials    IP Address Pools    QoS    Wireless

Setup network properties like AAA, NTP, Syslog, Trap and Netflow using the "Add Servers" link. Once dev deploy using these settings.

### AAA Server

Network     Client/Endpoint

#### NETWORK

Servers:  ISE     AAA    Protocol:  RADIUS     TACACS

Network:     IP Address (Primary):  +

[Change Shared Secret](#)

#### CLIENT/ENDPOINT

Servers:  ISE     AAA    Protocol:  RADIUS     TACACS

Client/Endpoint:     IP Address (Primary):  +



**Tech tip**

Cisco ISE is not required for the use cases covered in this guide but if already have Cisco ISE you may fill in the Cisco ISE info as the AAA services.

**Step 6.** Fill in the information for the remain network properties:

- DHCP
- DNS
- SYSLOG
- SNMP
- NTP
- Time Zone

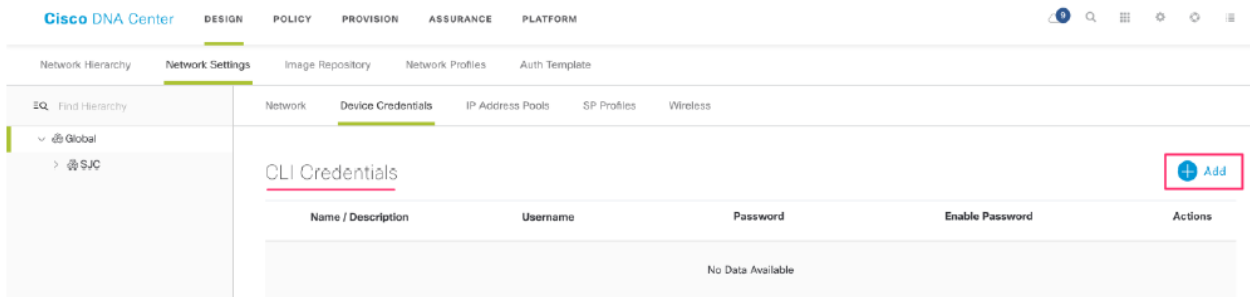
The screenshot displays a configuration page for network services. The following table summarizes the visible settings:

Service	Field	Value
DHCP Server	DHCP	10.4.48.10
	Supports both IPv4 and IPv6	Yes
DNS Server	Domain Name	cisco.local
	Primary	10.4.48.10
SYSLOG Server	Enabled	<input checked="" type="checkbox"/> Cisco DNA Center as syslog server
	IP Address	
SNMP Server	Enabled	<input checked="" type="checkbox"/> Cisco DNA Center as snmp server
	IP Address	
NTP Server	NTP	10.4.48.17
Time Zone	Time Zone	PST8PDT (PDT)
Message of the day	Do not override the existing motd banner on the device	<input checked="" type="checkbox"/>

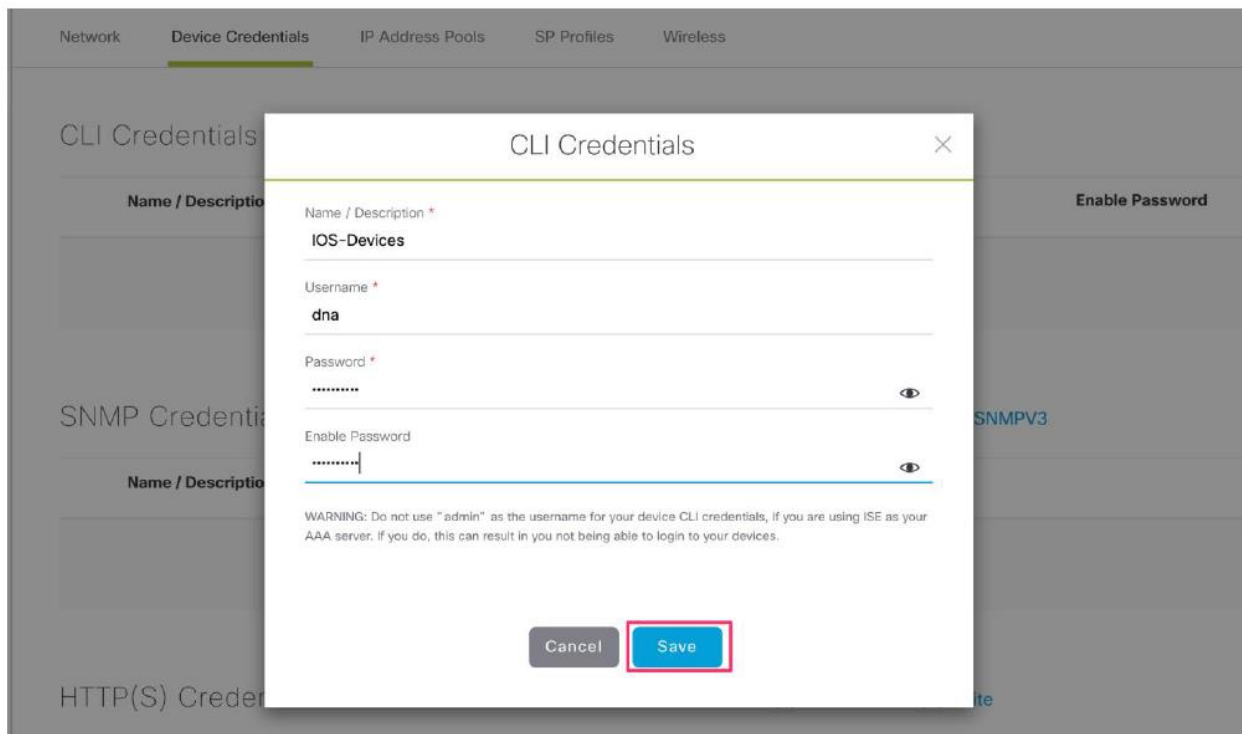
## Add device credentials to manage

These device credentials enable discovery and management for the network. For this procedure, follow these steps:

**Step 1.** Navigate to **Design > Network Settings > Device Credentials**, select an appropriate level of the site hierarchy in the left pane (example: Global for common credentials across the hierarchy).



**Step 2.** At the top of the CLI Credentials section, click Add, complete the Name / Description (example: IOS Devices), Username, Password, and Enable Password fields, and click Save.



**Tech tip**

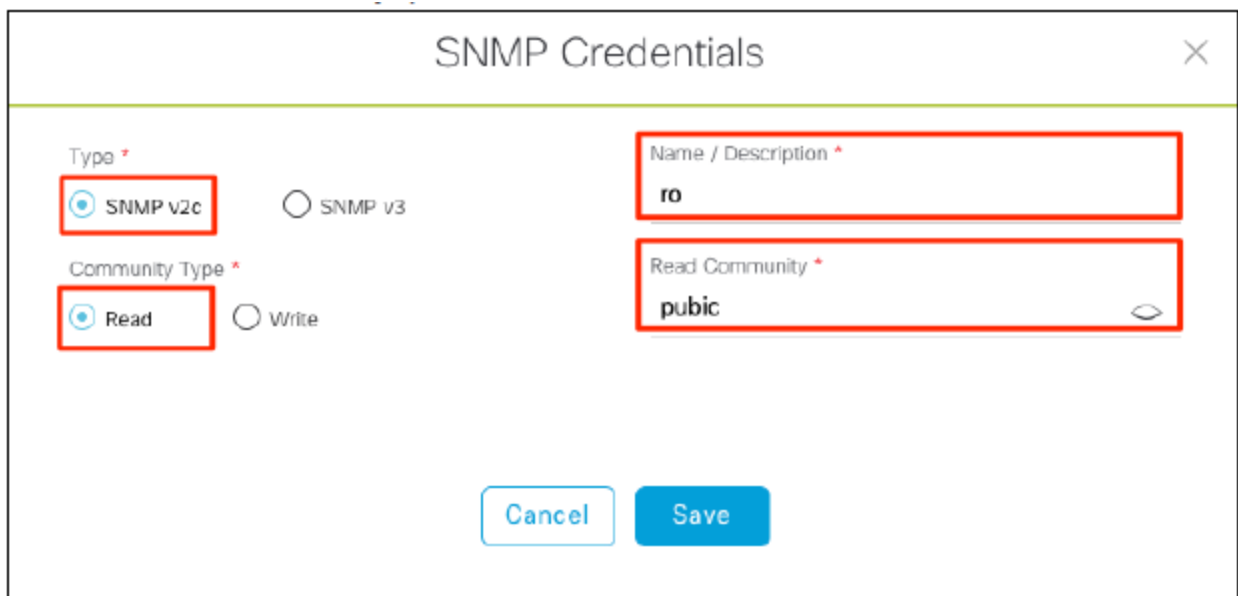
If you are using ISE as your AAA server, you should avoid using **admin** as the username for device CLI credentials, which can lead to username conflicts with the ISE administrator login, resulting in the inability to log in to devices.

**Step 3.** Select an SNMP credential type **SNMPv2c Read**.



**Step 4.** Click +Add and enter the following info:

- Name / Description: ro
- **Read Community:** public



**Step 5.** Click **Save**

**Step 6.** Select an SNMP credential type **SNMPv2c Write**.



**Step 7.** Click +Add and enter the following info:

- Name /Description: rw
- **Read Community:** private

### SNMP Credentials ✕

---

Type \*

SNMP v2c     SNMP v3

Community Type \*

Read     Write

Name / Description \*

rw

---

Write Community \*

private 👁

Cancel
Save

**Step 8.** For each of the CLI and SNMP credentials assigned, click all radio buttons next to each assignment created, make sure to toggle to **SNMPV2C Write** and select Write.

#### CLI Credentials + Add

	Name / Description	Username	Password	Enable Password	Actions
<input checked="" type="radio"/>	Administrator	netadmin	*****	*****	<a href="#">Edit</a>   <a href="#">Delete</a>

#### SNMP Credentials + Add

SNMPV2C Read | 
 [SNMPV2C Write](#) | 
 [SNMPV3](#)

	Name / Description	Read Community	Actions
<input checked="" type="radio"/>	ro	*****	<a href="#">Edit</a>   <a href="#">Delete</a>

#### SNMP Credentials + Add

[SNMPV2C Read](#) | 
 SNMPV2C Write | 
 [SNMPV3](#)

	Name / Description	Write Community	Actions
<input checked="" type="radio"/>	rw	*****	<a href="#">Edit</a>   <a href="#">Delete</a>

**Step 9.** Click Save and a **setting successfully** acknowledgment is displayed.

The device credentials to be used for network discovery and management should now be available in Cisco DNA Center.

## Deploy

This section of the guide implements the two use cases mentioned in the Solution Overview section of this document. Cisco DNA Center is used to automate the deployment of the wired profile created in the Design section of this document.

### Automate onboarding of a switch with Plug and Play (PnP)

For PnP Automation deployments, CLI and SNMP credentials is supplied to access and prepare one or more supported PnP seed devices. Plug-and-Play auto discovers switches directly connected to chosen seed device interfaces and their immediate neighbor switches using Cisco Discovery Protocol, all of which must be running the PnP agent and have no previous configuration. The credentials supplied allow Cisco DNA Center and seed devices to work together to configure the discovered devices and add them into managed inventory.

By default, PnP uses VLAN 1 as a management VLAN. If management VLAN is other than VLAN 1, needs to add “**pnp startup-vlan x**” command on upstream switch, any PnP switch will have VLAN X created and the uplink converted to a trunk with VLAN X enabled.

### Procedure 1. Define Golden image for devices in inventory

Cisco DNA Center displays the suggested and latest image list for each of the discovered device families.

Use the following steps to apply software updates of images and software maintenance updates (SMUs) to the devices, by importing the required images, marking images as golden, and applying images to devices.

It's highly recommended to mark a software image as golden from the list provided by Cisco-recommended images.

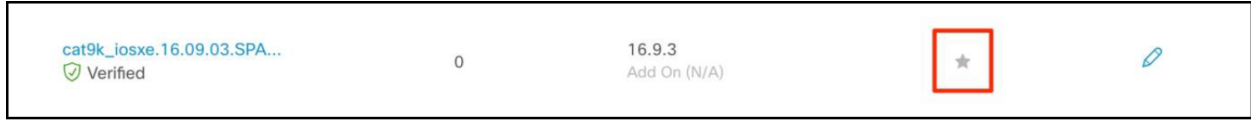
**Step 1.** Login to Cisco DNA Center.

**Step 2.** Go to **Design > Image Repository**

**Step 3.** Click to expand to view the full list available Cisco-recommended images.

Family	Image Name	Using Image	Version	Golden Image	Device Role
<input checked="" type="checkbox"/> Cisco Catalyst 9300 Switch	cat9k_iosxe.16.09.01.S... Verified	0	16.9.1 Add On (N/A)	★	ACCESS ★
	Install Mode (16.9.1.0.70)	1	16.9.1 Add On (N/A)	⊗	⊗

**Step 4.** Mark the Cisco-recommended image as golden.



After you mark the Cisco-recommended image as golden, Cisco DNA Center automatically downloads the image from cisco.com.

**Step 5.** (Optional) Click the pencil icon and select the appropriate role, to mark a **Golden Image** for specific device role.

Family	Image Name	Using Image	Version	Golden Image	Device Role
<input checked="" type="checkbox"/> Cisco Catalyst 9300 Switch	cat9k_iosxe.16.09.01.S... Verified	0	16.9.1 Add On (N/A)	★	ACCESS ★
	Install Mode (16.9.1.0.70)	1	16.9.1 Add On (N/A)	⊗	⊗
	cat9k_iosxe.16.09.03.S... Verified	0	16.9.3 Add On (N/A)	★	

**Step 6.** (Optional) Select **ACCESS** tag.



**Step 13.** Verify image is **marked as golden** and **ACCESS** tag is selected.

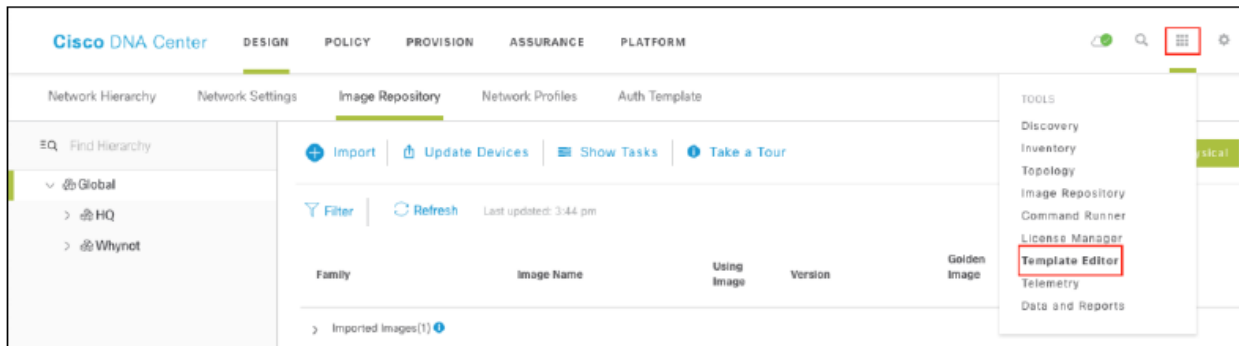
Family	Image Name	Using Image	Version	Golden Image	Device Role
> Cisco Catalyst 9300 Switch	cat9k_iosxe.16.09.03.S... Verified	0	16.9.3 Add On (N/A)	★	ACCESS ★

## Procedure 2. Create Onboarding Templates

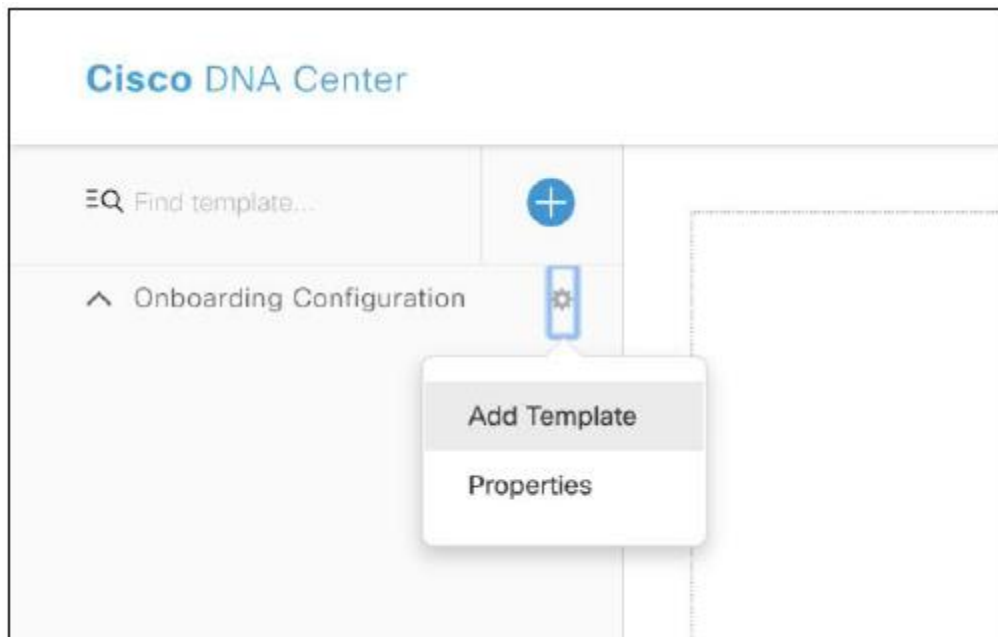
By default, the Onboarding Configuration project is available for creating Day-0 templates. You can create your own custom projects. Templates created in custom projects are categorized as Day-N templates.

Step 1. Login to Cisco DNA Center

Step 2. From the home page, choose **Tools > Template Editor**



Step 3. From the left pane, next to **Onboarding Configuration**, click the gear icon and select **Add Templates**.



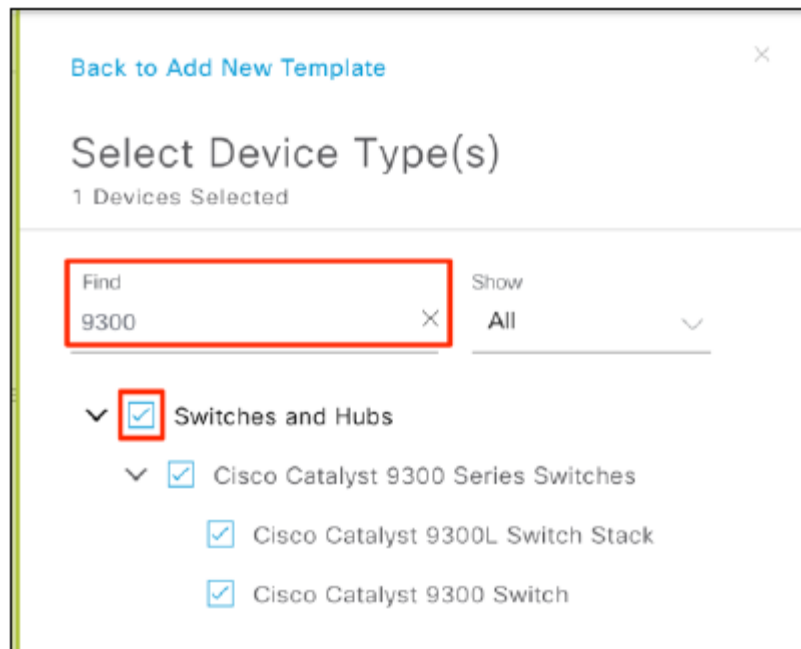
**Step 4.** In the Add New Template window, select **Regular Template** and fill in the following details:

Field	Value
Name	switch-pnp
Project Name	Onboarding Configuration (default)
Tags	branch-sw-pnp
Device Type(s)	Switches and Hubs > Cisco Cat 9300 Series
Software Type	IOS-XE
Software Version	(Optional)

**Tech tip**

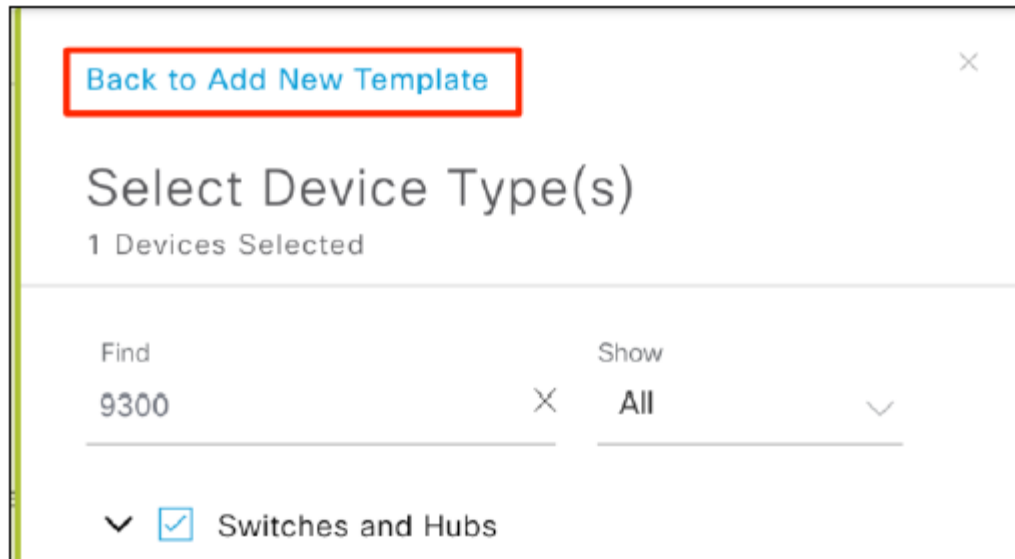
Tagging a configuration template helps you to search a template using the tag name in the search field. Use the tagged template as a reference to configure more devices.

**Step 5.** Under **Device Types**, click **Edit** to view the selected device types. Enter the device name in **Find** field to narrow the devices and choose the device types that you want to apply to the template.





**Step 6.** After choosing the device types, click **Back to Add New Template**.



**Step 7.** From the **Software Type** drop-down list, choose the software type **IOS-XE**.

**Tech tip**

If you select IOS as the software type, the commands apply to all software types, including IOS-XE. This value is used during provisioning to check whether the selected device conforms to the selection in the template.

**Step 8.** (Optional) For **Software Version**, enter the software version (example: 16.9.1) and Click **Add**.

**Tech tip**

During provisioning, Cisco DNA Center checks to see if the selected device has the software version listed in the template. If there is a mismatch, the provision skips the template.

**Step 9.** Select the recently created template from left pane, and in the Template Editor window on the right, enter the configuration for the template.

**Step 10.** To save the template content, from the **Actions** drop-down list, choose **Save**.

**Step 11.** To commit the template, from the **Actions** drop-down list, choose **Commit**.

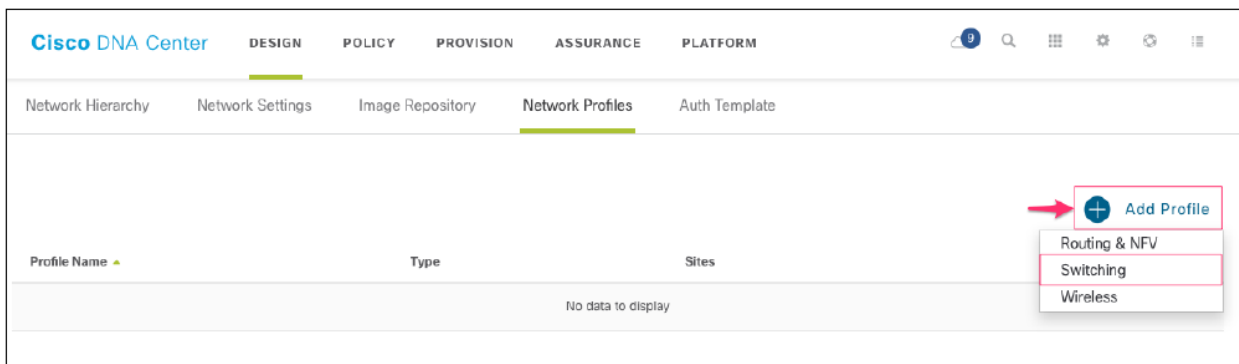
### Procedure 3. Create Network Profiles for Switching

Define the **Onboarding Configuration** template that you want to apply to the devices. Such templates contain basic network configuration commands to onboard a device so that it can be managed on the network.

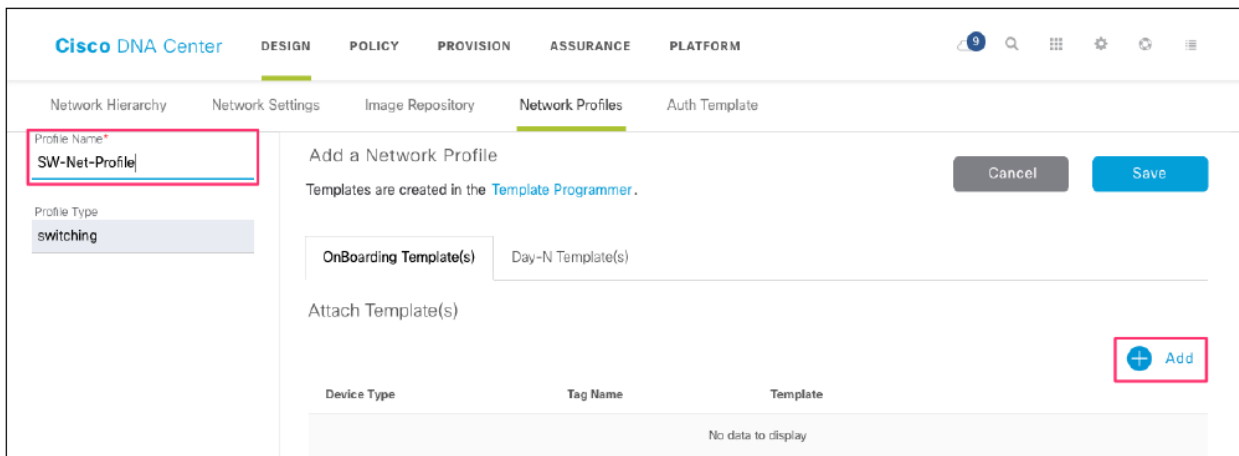
For this procedure, follow these steps:

**Step 1.** Navigate to **Design > Network Profiles**.

**Step 2.** Click **+Add Profiles** and choose **Switching**.



**Step 3.** Give a **Profile Name**, and Click **+Add**, under **OnBoarding Template(s)** tab.



**Step 4.** Select **Cisco Catalyst 9300 Switch** from the **Device Type** drop-down list.

**Step 5.** Select the **Tag Name** (example: branch-sw-pnp) from the drop-down list.

**Step 6.** Select an onboarding configuration **template** (example: switch-pnp) from the drop-down list.

OnBoarding Template(s)	Day-N Template(s)	
Attach Template(s)		
Device Type	Device Tag <span>!</span>	Template <span>▲</span>
Cisco Catalyst 9300 Switch	x branch-sw-pnp x ▼	switch-pnp x ▼

**Step 7.** Click **Save**.

**Tech tip**

The profile that is thus configured on the switch is applied when the switch is provisioned.

**Procedure 4. Assign Network Profile to Site**

Each network profile can have multiple device types and sites assigned. But multiple network profiles cannot share the same site, even though two different network profile can be assigned different floors from the same site.

**Step 1.** Choose Design > **Network Profiles**.

**Step 2.** Click on **Assign Site**.

Profile Name ▼	Type	Sites	Action
SW-Net-Profile	switching	<a href="#">Assign Site</a>	<a href="#">Edit</a>   <a href="#">Delete</a>

**Step 3.** On the side panel for **Add Sites to Profile**, expand **Site** (example: **San Jose**) and select **Building** (example: Building 23).

Cisco DNA Center | DESIGN | POLICY | PROVISION | ASSURANCE | PLATFORM

Network Hierarchy | Network Settings ▼ | Image Repository | **Network**

Add Sites to Profile

Choose a site

- Global (1)
- San Jose (2)
  - Building 23 (3)

**Step 4.** Click **Save** to complete all required steps for the design phase.

## Procedure 5. Discover the Controller (PnP Server)

For the device to connect with the controller (PnP Server), there are five options:  
DHCP server, using **option 43** (set the IP Address of the controller).

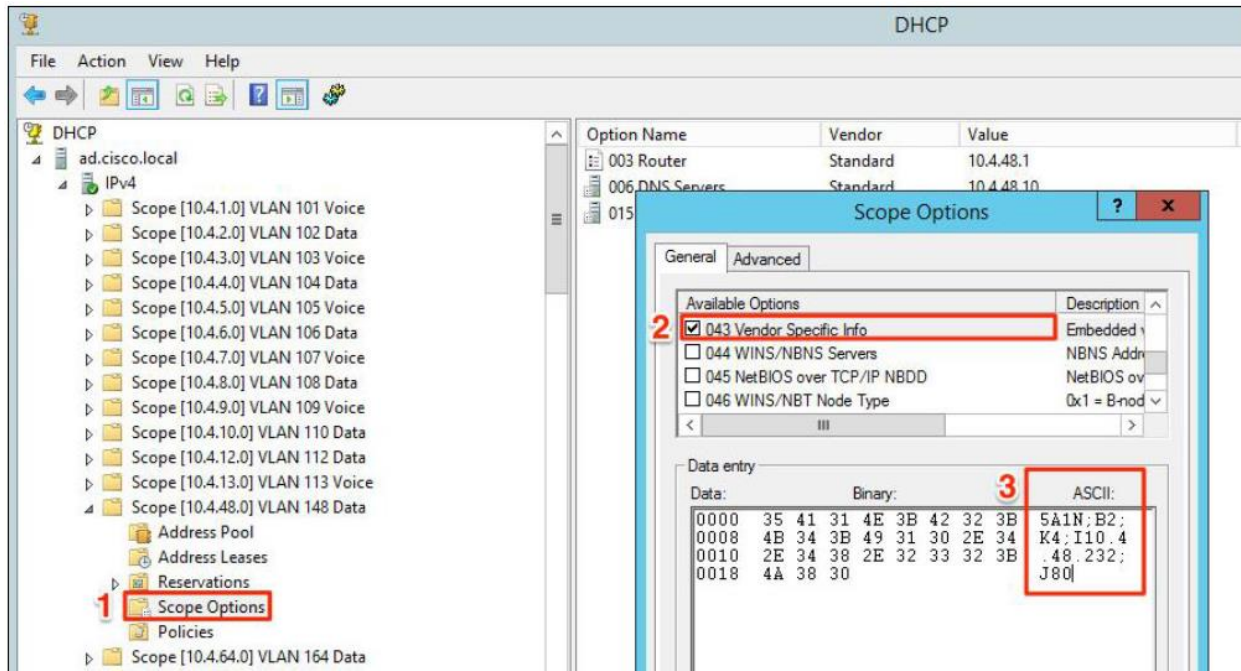
- DHCP server, using a DNS domain name (DNS lookup of pnhelper).
- Cisco Plug and Play Connect (cloud-based device discovery).
- USB key (bootstrap config file).
- Cisco Installer App (For iPhone/Android).

In order for devices to call home to plug and play server in Cisco DNA Center, this guide will cover only the first option, DHCP server, using **option 43** for PnP discovery.

### Tech tip

For this guide the **Option 43** is configured using a Microsoft DHCP server but it can be done using any other DHCP server such as Infoblox or on a router.

**Step 1.** Go to Microsoft DHCP server to configure using **option 43**.



1. Go to the Scope Options for the specific VLAN.
2. Under General tab, check 043 Vendor Specific Info.
3. Replace the IP address with the correct IP address of the Cisco DNA Center (PnP Server).

**5A1N;B2;K4;Ixxx.xxx.xxx.xxx;J80**

Cisco DNA Center IP Address

4. Copy and paste the ascii option 43 ascii "5A1N;B2;K4;I10.4.48.232;J80"
5. Click **Apply** and OK.

Step 2. Configure uplink switch interface as a trunk port

```
interface TenGigabitEthernet1/1/3
switchport trunk native vlan 999
switchport mode trunk
```

Step 3. (Optional) Configure PnP startup VLAN if you are using Management VLAN other than VLAN 1.

```
INNDA2-CS9500-01-DTC#sh run | in pnp
pnp startup-vlan 2
INNDA2-CS9500-01-DTC#
```

**Step 4.** Connect a single switch (example: Catalyst 9300) to access layer that's getting onboarded.

**Step 5.** (Optional) Connect the console to a new switch and power it on. Once the device boots up, it will get IP address of the Cisco DNA Center using the option 43 and will do a PnP discovery as below.

```

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

Press RETURN to get started!

*Oct 5 02:59:17.440: %PNP-6-PROFILE_CONFIG: PnP Discovery profile pnp-zero-touch configured
*Oct 5 02:59:18.285: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named TP-self-signed-882668793 has been generated or imported
*Oct 5 02:59:18.287: %SSH-5-ENABLED: SSH 1.99 has been enabled
*Oct 5 02:59:18.328: %PKI-4-NOCONFIGAUTOSAVE: Configuration was modified. Issue "write memory" to save new IOS PKI configuration
*Oct 5 02:59:18.370: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named TP-self-signed-882668793.server has been generated or imported
*Oct 5 02:59:19.441: %LINK-5-CHANGED: Interface Vlan1, changed state to administratively down
*Oct 5 02:59:30.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 02:59:29 UTC Sat Oct 5 2019 to 02:59:30 UTC Sat Oct 5 2019
Oct 5 02:59:30.000: %PKI-6-AUTHORITATIVE_CLOCK: The system clock has been set.
Oct 5 02:59:30.003: %SMART_LIC-5-SYSTEM_CLOCK_CHANGED: Smart Agent for Licensing System clock has been changed
Oct 5 02:59:36.765: %AN-6-AN_ABORTED_BY_CONSOLE_INPUT: Autonomic disabled due to User intervention on console. configuration
Oct 5 02:59:39.046: %PKI-4-NOCONFIGAUTOSAVE: Configuration was modified. Issue "write memory" to save new IOS PKI configuration
Oct 5 02:59:49.664: %PNP-6-PNP_DISCOVERY_DONE: PnP Discovery done successfully
%Error opening tftp://10.4.48.10/network-config (Timed out)
Oct 5 02:59:54.685: AUTOINSTALL: Tftp script execution not successful for Gi0/0.
Oct 5 03:00:36.925: %IOSXE_REDUNDANCY-6-PEER: Active detected switch 2 as standby.
Oct 5 03:00:36.923: %STACKMGR-6-STANDBY_ELECTED: Switch 1 R0/0: stack_mgr: Switch 2 has been elected STANDBY.
Oct 5 03:00:41.964: %REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a standby insertion (raw-event=PEER_FOUND(4))

```

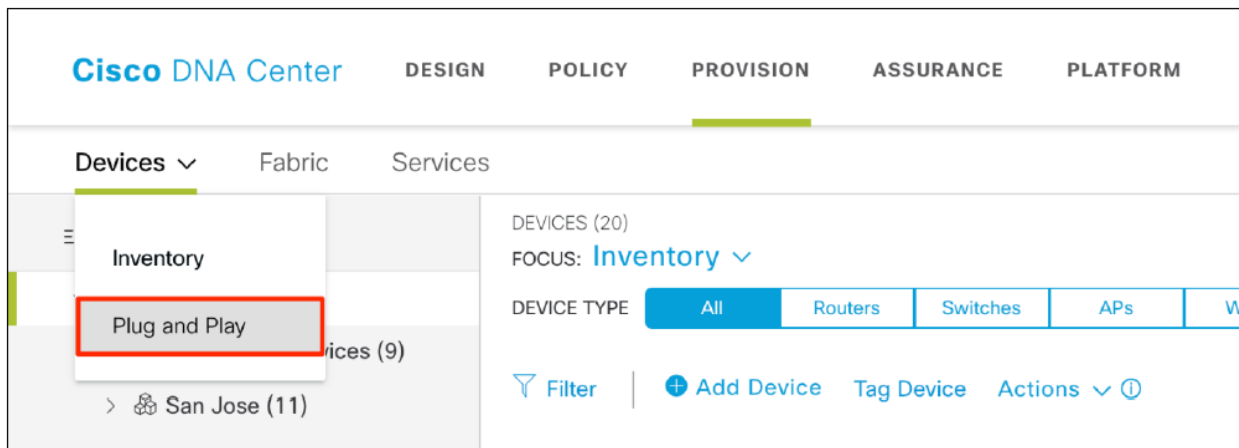
**Tech tip**

When the device is in process of PnP discovery do not touch the device as it will break the PnP process.

## Procedure 6. Day-0 provisioning of switch onboarded with PnP

**Step 1.** Login to Cisco DNA Center.

**Step 2.** Go to **Provision > Devices** drop-down and select **Plug and Play**



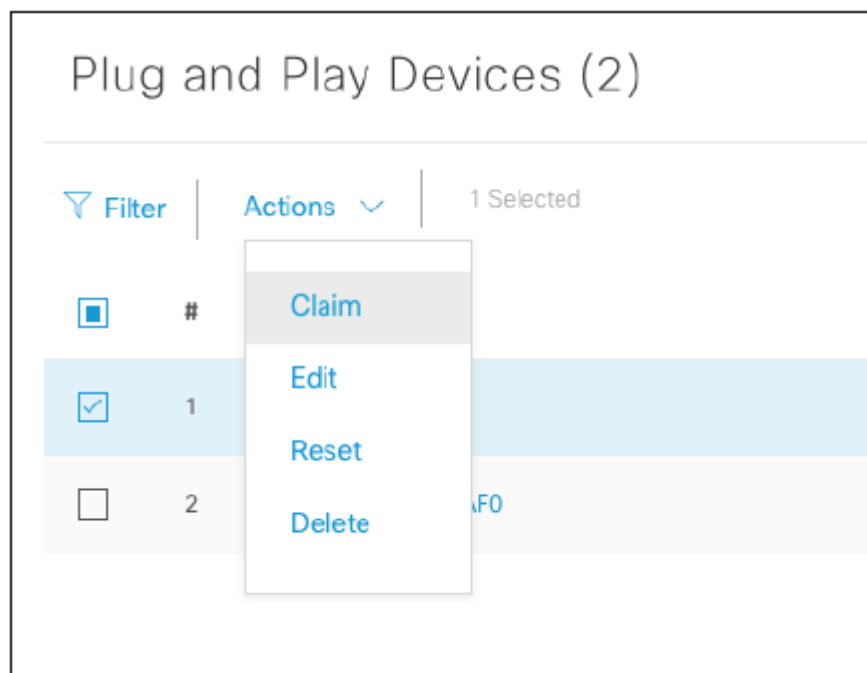
**Step 3.** Check the status of the switch to make sure it's **Unclaimed** before proceeding.

#	Device Name	Serial Number	Product ID	Source	State	Site
1	FOC2313U0DS	FOC2313U0DS	C9300-24UX	Network	Unclaimed	N/A

**Tech tip**

Devices can also be added and claimed using **Serial Number** and **Product ID**. On **Plug and Play Devices** page click on **Add** and select **Single Device**, **Bulk Devices** or **Smart Account Devices** and provide information respectively.

**Step 4.** Select the switch and click on **Actions** drop-down and select **Claim** to start the claim wizard.



**Tech tip**

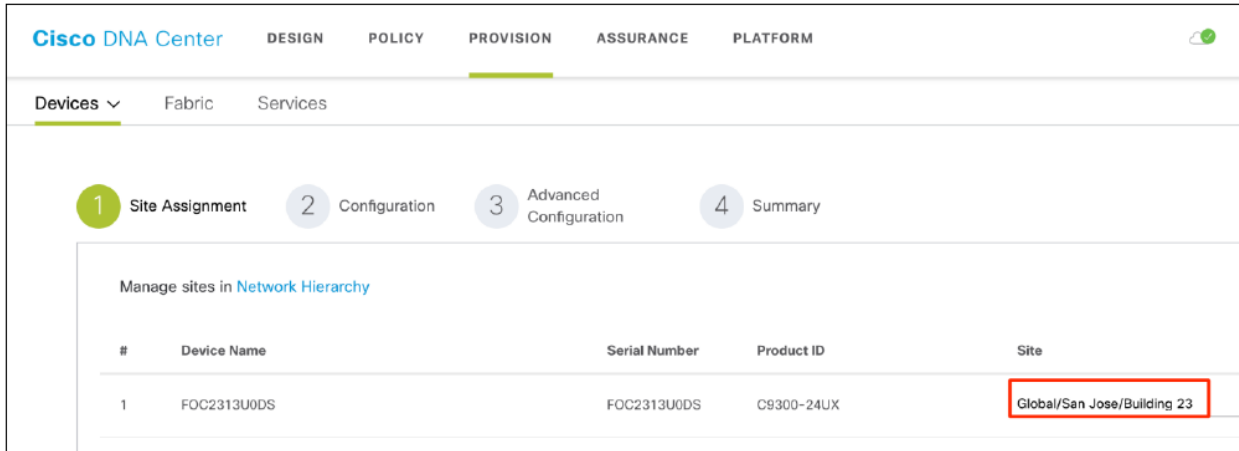
Before you claim a switch, if the access to the console is available, monitor the configuration in process by Cisco DNA Center. Copy and paste the following EEM script in the switch console:

```
event manager applet catchall
event cli pattern ".*" sync no skip no
action 1 syslogmsg "$_cli_msg"
```

**Step 5.** Assign a site to the device (example: Building 23) and click **Next**.

**Tech tip**

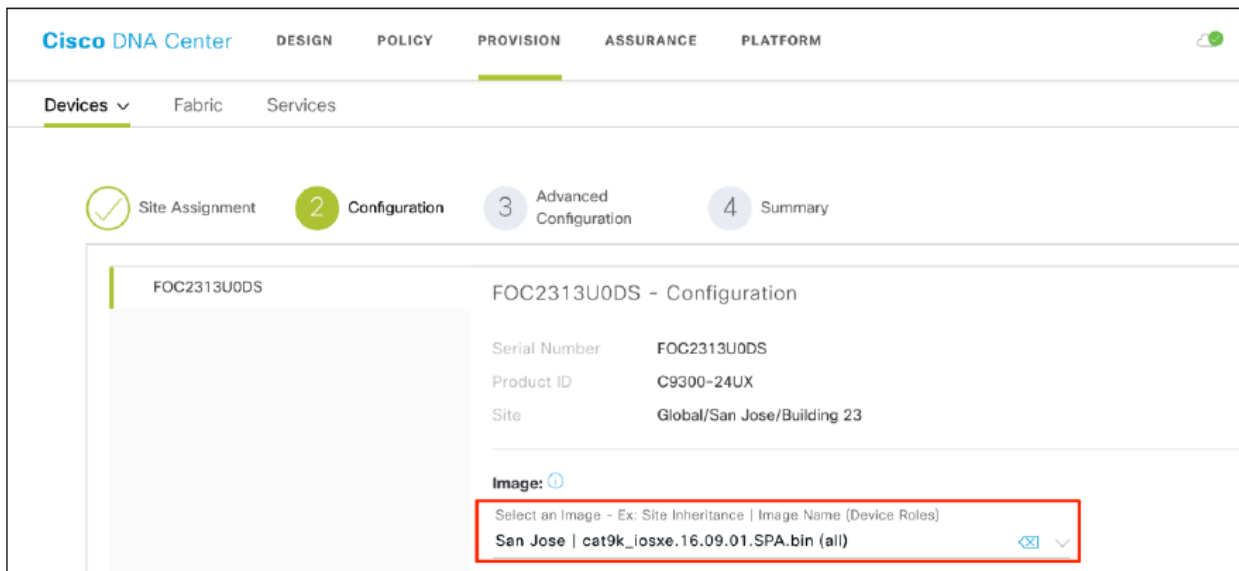
This tech tip is only applicable to a scenario where the floor is added to the building. If the network services and credentials are only applied to a floor and only the building is selected then an error will occur while processing the claim request.



**Step 6.** Select the golden image (example: cat9k\_iosxe.16.09.01.SPA.bin) and click **Next**.

**Tech tip**

If an image was marked as golden as shown in **Process 3** and **Procedure 1**, it will be auto assigned in this step.





**Tech tip**

Before proceeding with upgrade make sure the switch is in **INSTALL MODE** and not in BUNDLE MODE.

**Step 7.** Select the **OnBoarding template** (example: switch-pnp) that was created in **Procedure 2**, and click **Next**.

Site Assignment 2 Configuration 3 Advanced Configuration 4 Summary

FOC2313U0DS FOC2313U0DS - Configuration

Serial Number FOC2313U0DS  
Product ID C9300-24UX  
Site Global/San Jose/Building 23

**Image:** ⓘ  
Select an Image - Ex: Site Inheritance | Image Name (Device Roles)  
San Jose | cat9k\_iosxe.16.09.01.SPA.bin (all) ⓘ ▾

Skip golden image upgrade

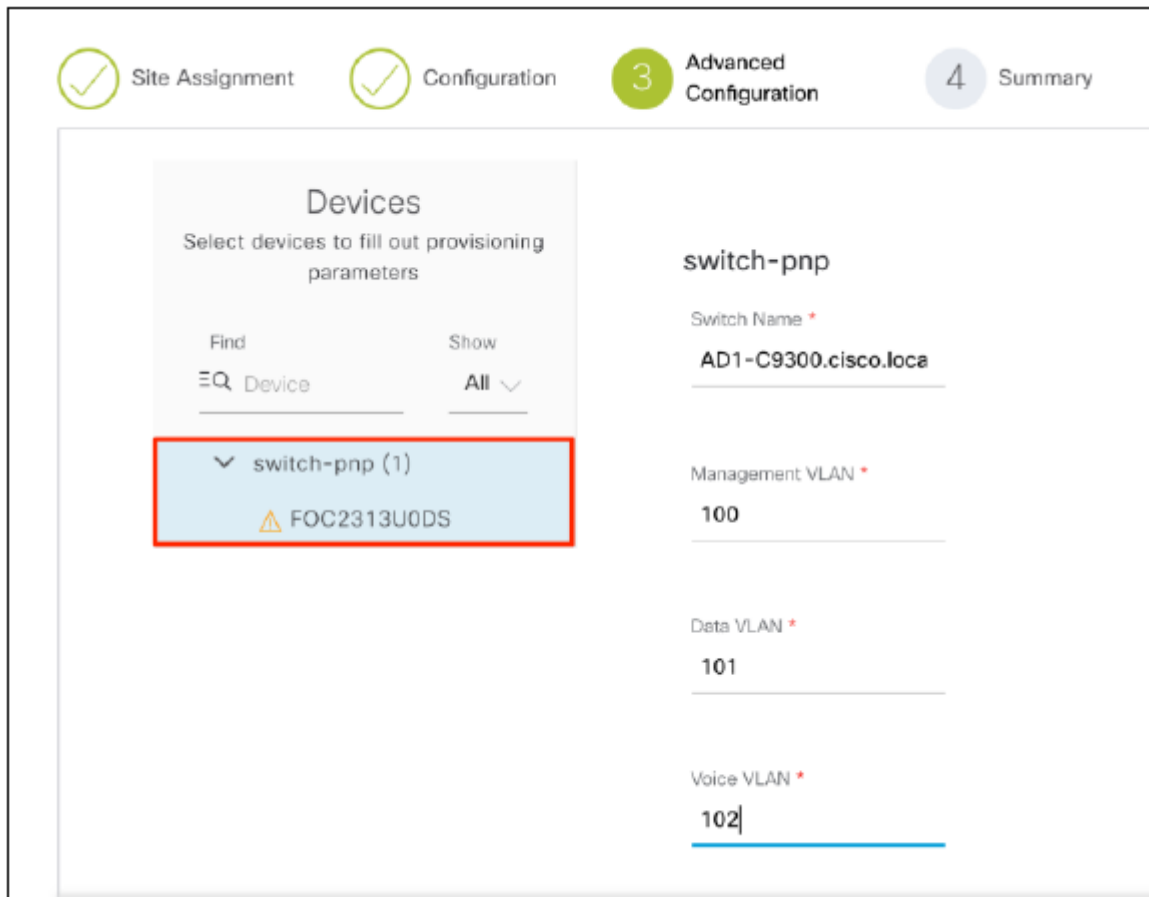
**Template:**  
Select a Template (optional) - Ex: Template Name (Profile Type)  
switch-pnp (Switching) ⓘ ▾ ⓘ

**Tech tip**

To give a quick glance at the onboarding template click the eye icon.

**Template:**  
Select a Template (optional) - Ex: Template Name (Profile Type)  
switch-pnp (Switching) ⓘ ▾ ⓘ

**Step 8.** Select a switch and enter the provisioning parameters, and click **Next**.



The screenshot shows the 'Advanced Configuration' step of a provisioning process. At the top, there are four progress indicators: 'Site Assignment' (checked), 'Configuration' (checked), 'Advanced Configuration' (active, highlighted in green), and 'Summary' (disabled, highlighted in grey). Below the progress indicators, the 'Devices' section on the left allows selecting devices to fill out provisioning parameters. A search bar is present, and a list of devices is shown, with 'switch-pnp (1)' and 'FOC2313U0DS' highlighted in a red box. The right side of the interface shows the configuration for 'switch-pnp', including Switch Name (AD1-C9300.cisco.loc), Management VLAN (100), Data VLAN (101), and Voice VLAN (102).

**Tech tip**

For large number of devices, bulk import using CSV format.

**Step 9.** Carefully review the summary by expanding each tab, and click **Claim**.

**Step 10.** Select **Yes** to confirm to proceed with the claim request.

**Step 11.** Now watch the state of the switch change from **Unclaimed** to **Provisioned**

1. Unclaimed to Planned

<input type="checkbox"/>	#	Device Name	Serial Number	Product ID	Source	State
<input type="checkbox"/>	1	FOC2313U0DS	FOC2313U0DS	C9300-24UX	Network	Planned
<input type="checkbox"/>	2	FCW2123L03D	FCW2123L03D	C9300-24T	Network	Provisioned

## 2. Planned to Onboarding

<input type="checkbox"/>	#	Device Name	Serial Number	Product ID	Source	State
<input type="checkbox"/>	1	FOC2313U0DS	FOC2313U0DS	C9300-24UX	Network	Onboarding
<input type="checkbox"/>	2	FCW2123L03D	FCW2123L03D	C9300-24T	Network	Provisioned

## 3. Onboarding to Provisioned

<input type="checkbox"/>	#	Device Name	Serial Number	Product ID	Source	State
<input type="checkbox"/>	1	FOC2313U0DS	FOC2313U0DS	C9300-24UX	Network	Provisioned
<input type="checkbox"/>	2	FCW2123L03D	FCW2123L03D	C9300-24T	Network	Provisioned

### Tech tip

Hit the refresh if it doesn't change. Now the device will be available under inventory. In case the status changes to **Error**, click on the device name.

<input type="checkbox"/>	#	Device Name	Hostname
<input checked="" type="checkbox"/>	1	FOC2313U0DS	Switch

An options panel will slide out from right. Now select the **History** tab to further investigate the error.

Details **History** Configuration

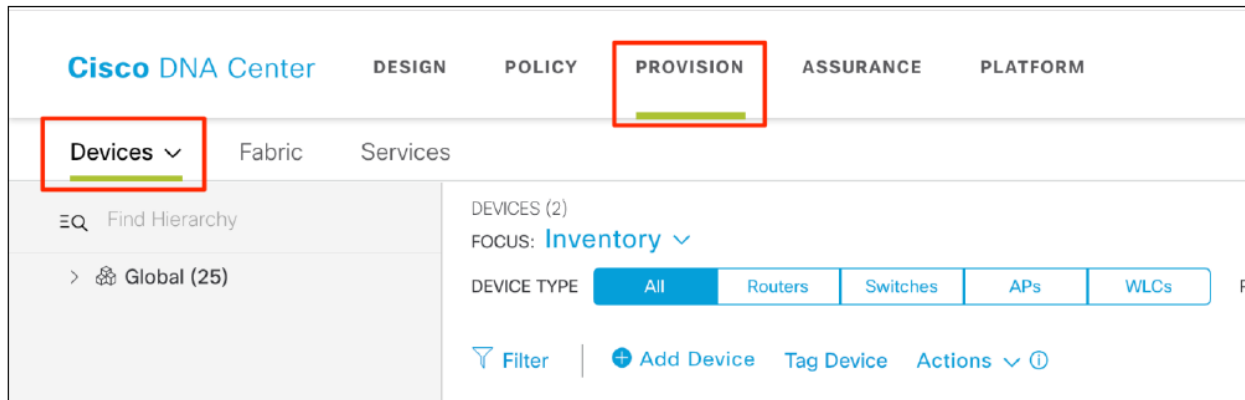
---

### History

Last updated: 11:55 a

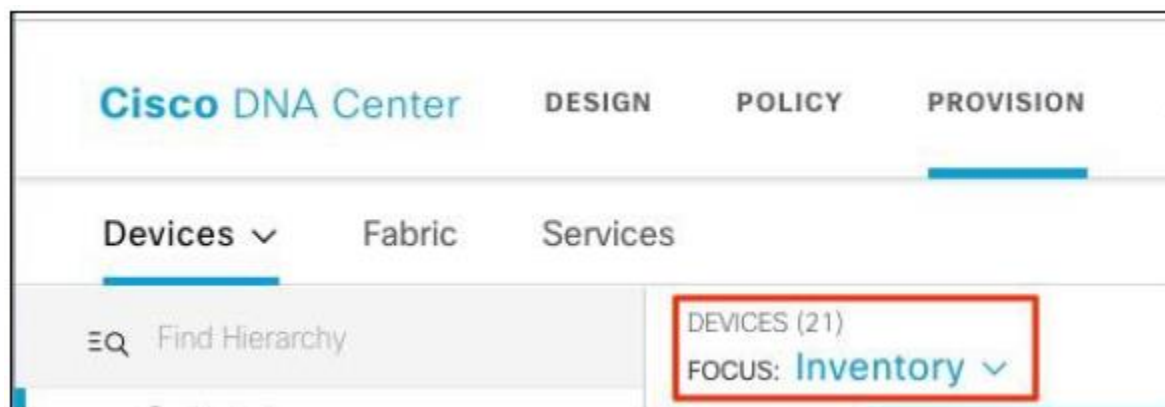
Status	Time	Details
	08/22/2019 06:01:42 PM	NCOB02074: Executing Workflow Timed Out, Please check the device connectivity with the Server.
	08/22/2019 05:50:59 PM	Executing Task: Site Config Task

**Step 12.** Go to **Provision > Devices**

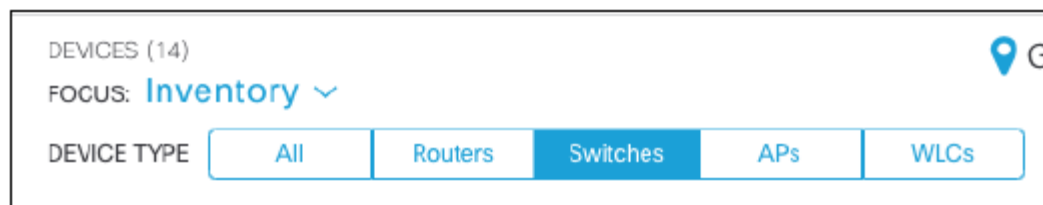


**Step 13.** Select the site hierarchy in the left pane.









**Step 14.** Verify the devices focus is set to **Inventory**.



**Step 15.** Select **Switches** as the **Device Type** to narrow down the devices.



**Step 16.** Verify the newly onboarded switch is in the **Inventory**.

<input type="checkbox"/>	Device Name	IP Address	Device Family	Site	Reachability	MAC Address	Device Model
<input type="checkbox"/>	 AD1-9300.cisco.local 	10.4.79.10	Switches and Hubs	.../Building 23	 Reachable	4c:bc:48:f8:9e:80	 ACCESS
<input type="checkbox"/>	 AD3-3850.cisco.local 	10.4.95.5	Switches and Hubs	.../Floor 3	 Reachable	20:4c:9e:ae:79:00	 ACCESS