Network Device Onboarding for Cisco DNA Center Deployment Guide

Prescriptive Deployment Guide

June, 2020

Contents

Introduction

Audience

The audience for this document is network administrators who wish to deploy a Catalyst 9000 series switch at a branch or campus using Cisco DNA Center.

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. You may apply this procedure to any Catalyst 9000 series switch but in this guide, we will only focus on Catalyst 9300 switch.

Reader tip

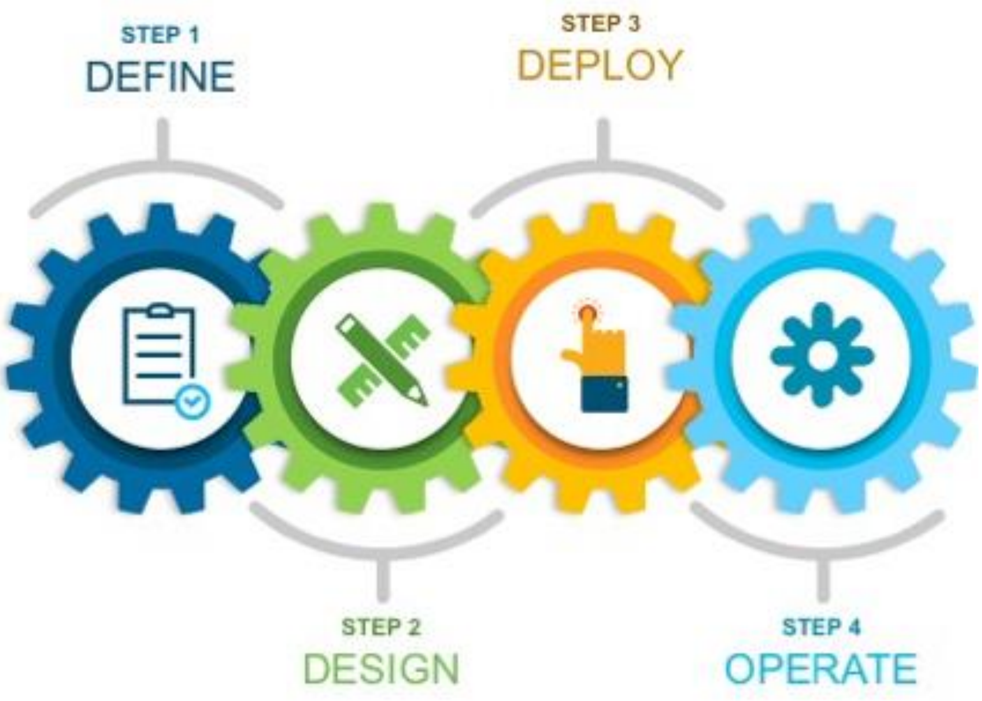
For more information on Cisco DNA Center supported devices please refer to the compatibility matrix information https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-device-support-tables-list.html

Use Cases

Following are the two use cases covered within this guide:

- Automate day-zero onboarding of a switch with Plug and Play (PnP).
- Simplified process for Return Material Authorization (RMA).

Figure 1.
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 and Return Material Authorization (RMA).
- The **Operate** section briefly discusses the known caveats of device onboarding using PnP and RMA.

Define

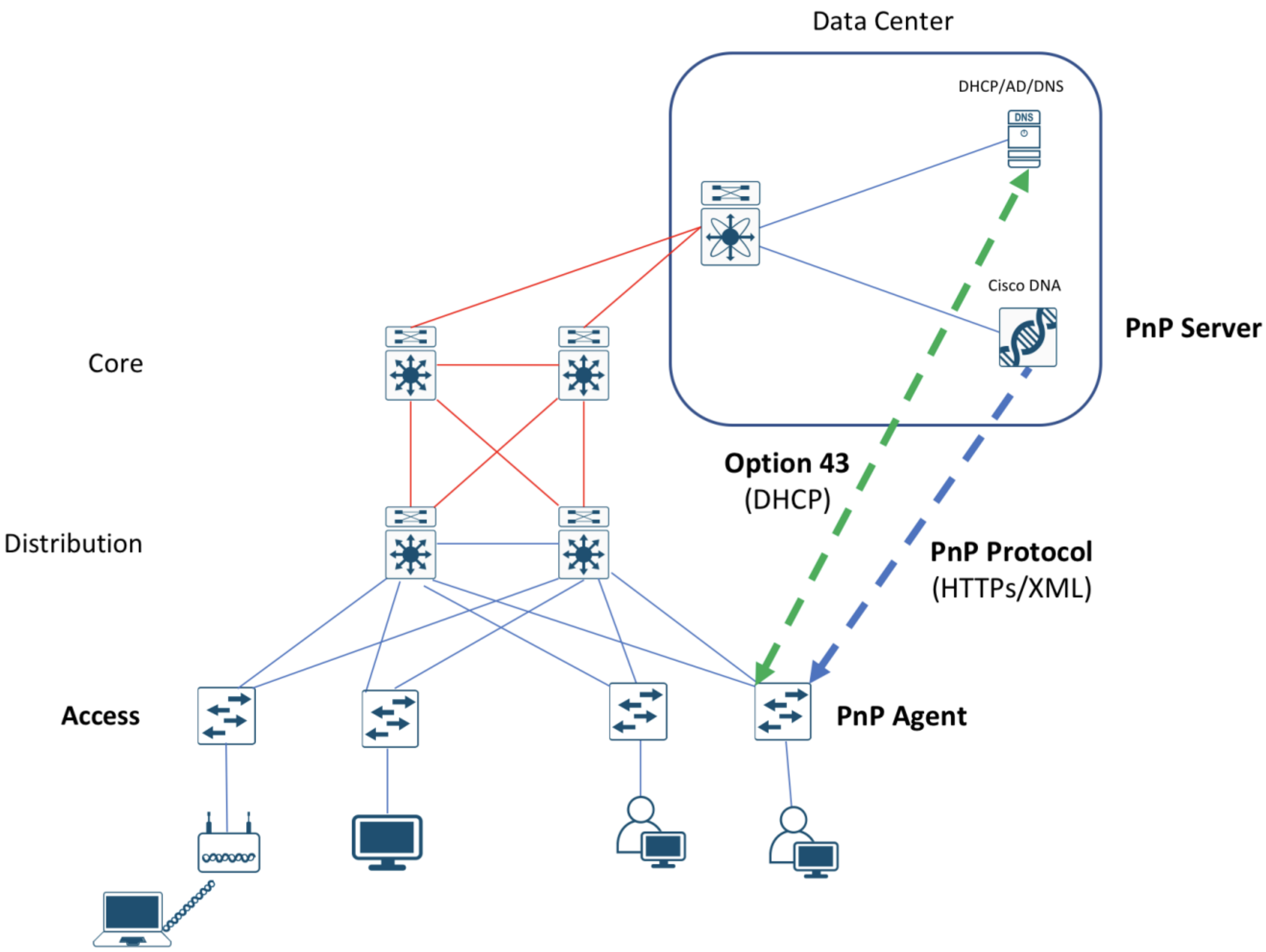
Solution overview

Cisco DNA Center can help with the non-fabric wired deployments in various different ways such as – network discovery, network inventory, management of software revisions, Return Material Authorization, etc.

Reader tip

This guide only covers day-zero onboarding of a switch with Plug and Play (PnP) and Return Material Authorization (RMA). For software image management (SWIM) refer to Campus Software Image Management Using Cisco DNA Center Deployment Guide.

Figure 2.
Campus Topology highlighting device onboarding in Access layer.



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.

Reader tip

For more information on how to install Cisco DNA Center, refer to Software-Defined Access Management Infrastructure Prescriptive Deployment Guide.

Cisco ISE is not required for the use cases covered in this guide.

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

Procedure 1. Create an area

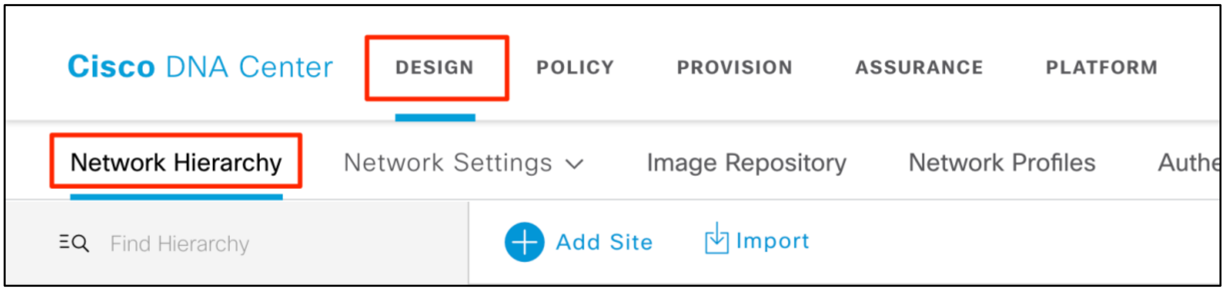
Step 1. Login to the Cisco DNA Center. (For example: dnac.company.com)

Tech tip

If SSL is not configured a warning indicating the connection is not secure will appear. For setup purpose you can continue by clicking on Advanced button and click the link to proceed to Cisco DNA Center webpage.

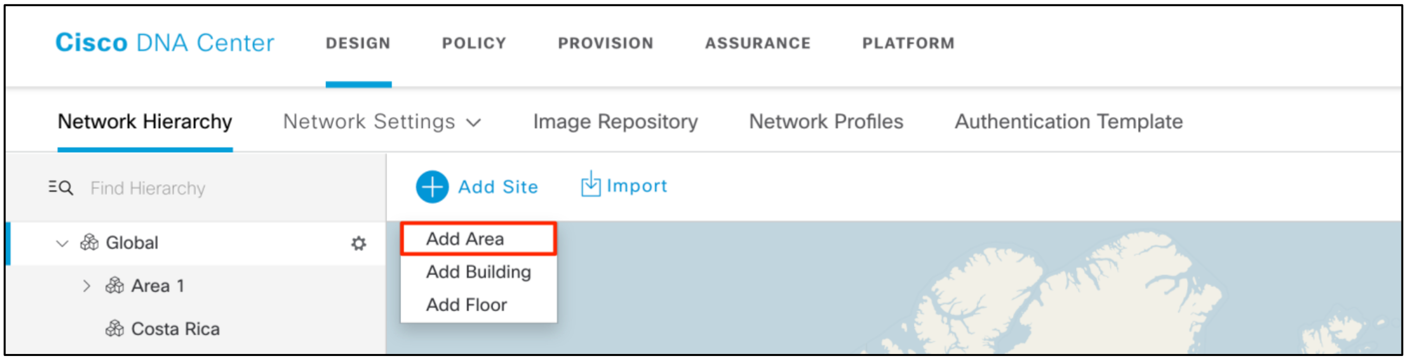
Also, the credentials (userid and password) you enter must have SUPER-ADMIN-ROLE OR NETWORK-ADMIN-ROLE privileges.

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

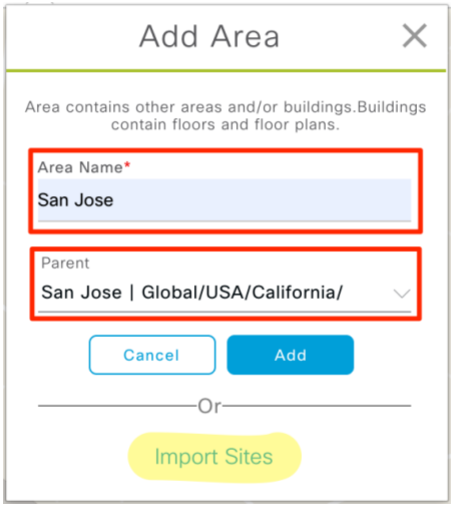


Step 3. Click **Add Site**

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



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



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

Area Name* San Jose

Parent San Jose | Global/USA/California/

Tech tip

For single area enter the **Area Name** as the City (example: San Jose) and leave **Parent** as Global. For multi-level areas create parent and child areas in the appropriate order.

For example: Country > State > City (USA > California > San Jose).

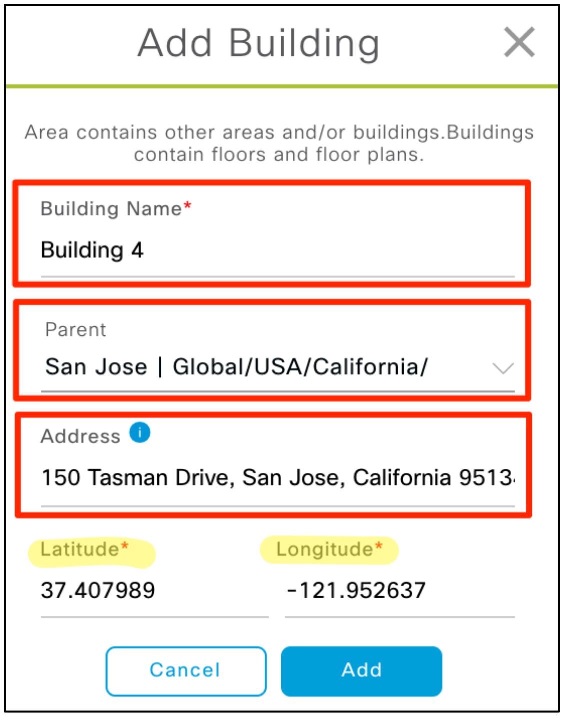
To import large number of sites, choose **Import Sites** as highlighted in the above screenshot.

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

Procedure 2. Create building within the area

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

Step 2. From the 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

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** (example: Building 4).

Step 4. Select the **Parent** area. (example: San Jose | Global/USA/California/)

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. For more details refer to Catalyst 9800 Non-Fabric Deployment using Cisco DNA Center Guide.

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.

Procedure 1. Add network services

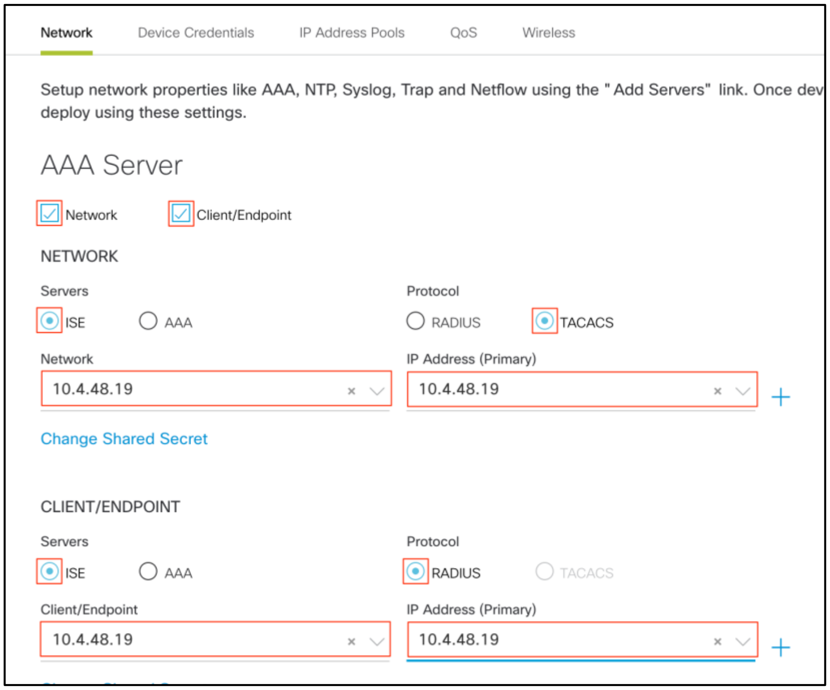
Step 1. Login to Cisco DNA Center and navigate to Design > Network Settings > Network.

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.



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: 10.4.48.19

IP Address (Primary): 10.4.48.19

CLIENT/ENDPOINT

Servers: ● ISE ○ AAA

Protocol: ● RADIUS ○ TACACS

Client/Endpoint: 10.4.48.19

IP Address (Primary): 10.4.48.19

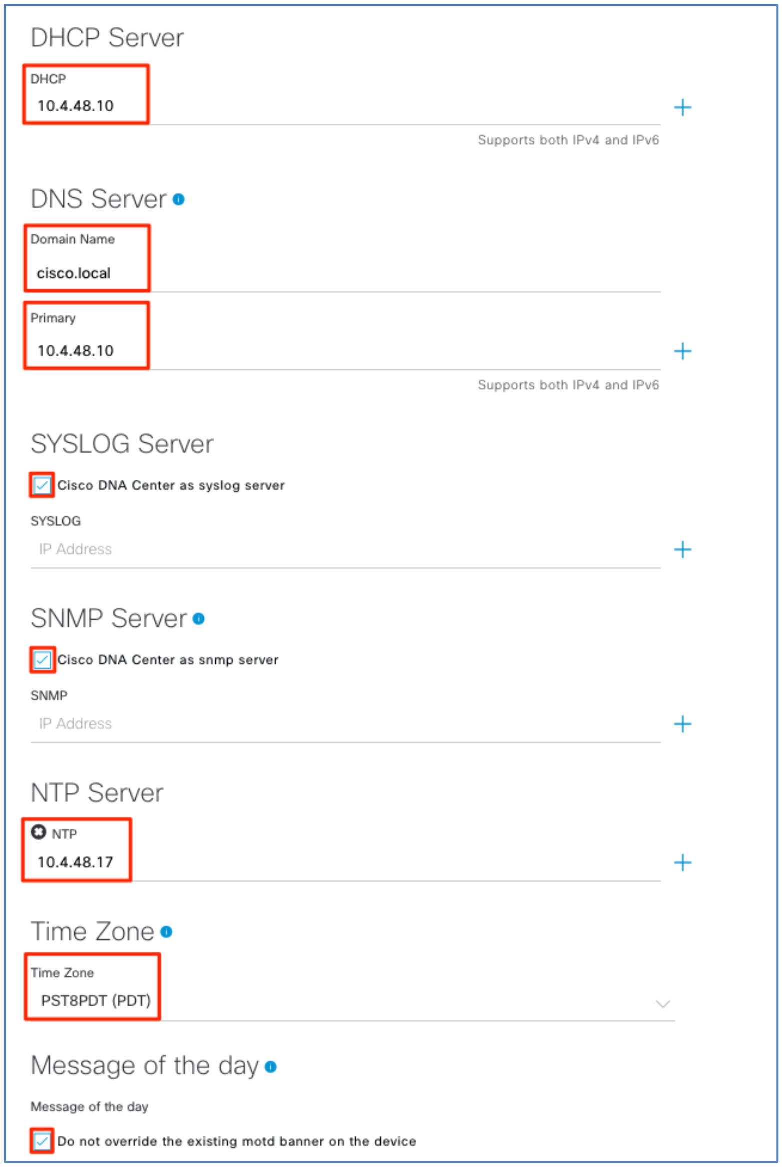
Tech tip

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



DHCP Server

DHCP: 10.4.48.10

Supports both IPv4 and IPv6

DNS Server

Domain Name: cisco.local

Primary: 10.4.48.10

Supports both IPv4 and IPv6

SYSLOG Server

☑ Cisco DNA Center as syslog server

SYSLOG: IP Address

SNMP Server

☑ Cisco DNA Center as snmp server

SNMP: IP Address

NTP Server

NTP: 10.4.48.17

Time Zone

Time Zone: PST8PDT (PDT)

Message of the day

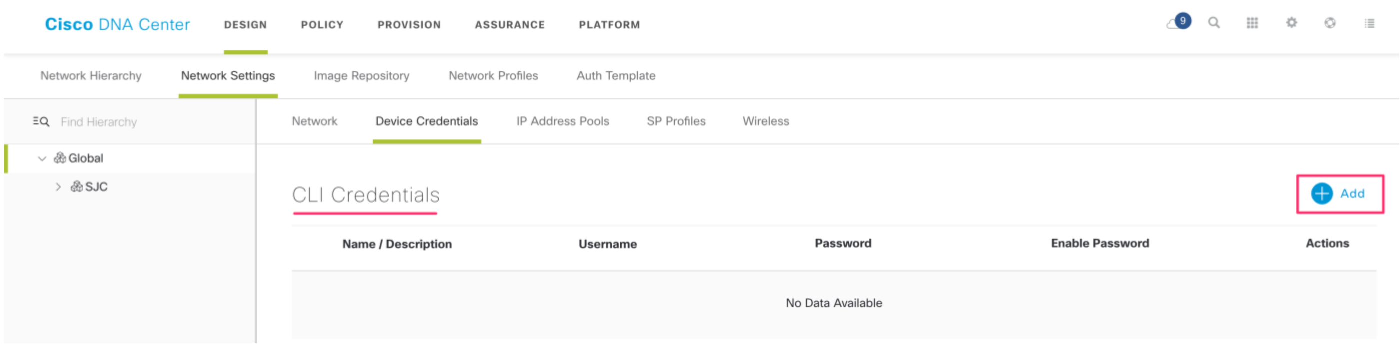
Message of the day

☑ Do not override the existing motd banner on the device

Procedure 2. Add device credentials to manage.

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

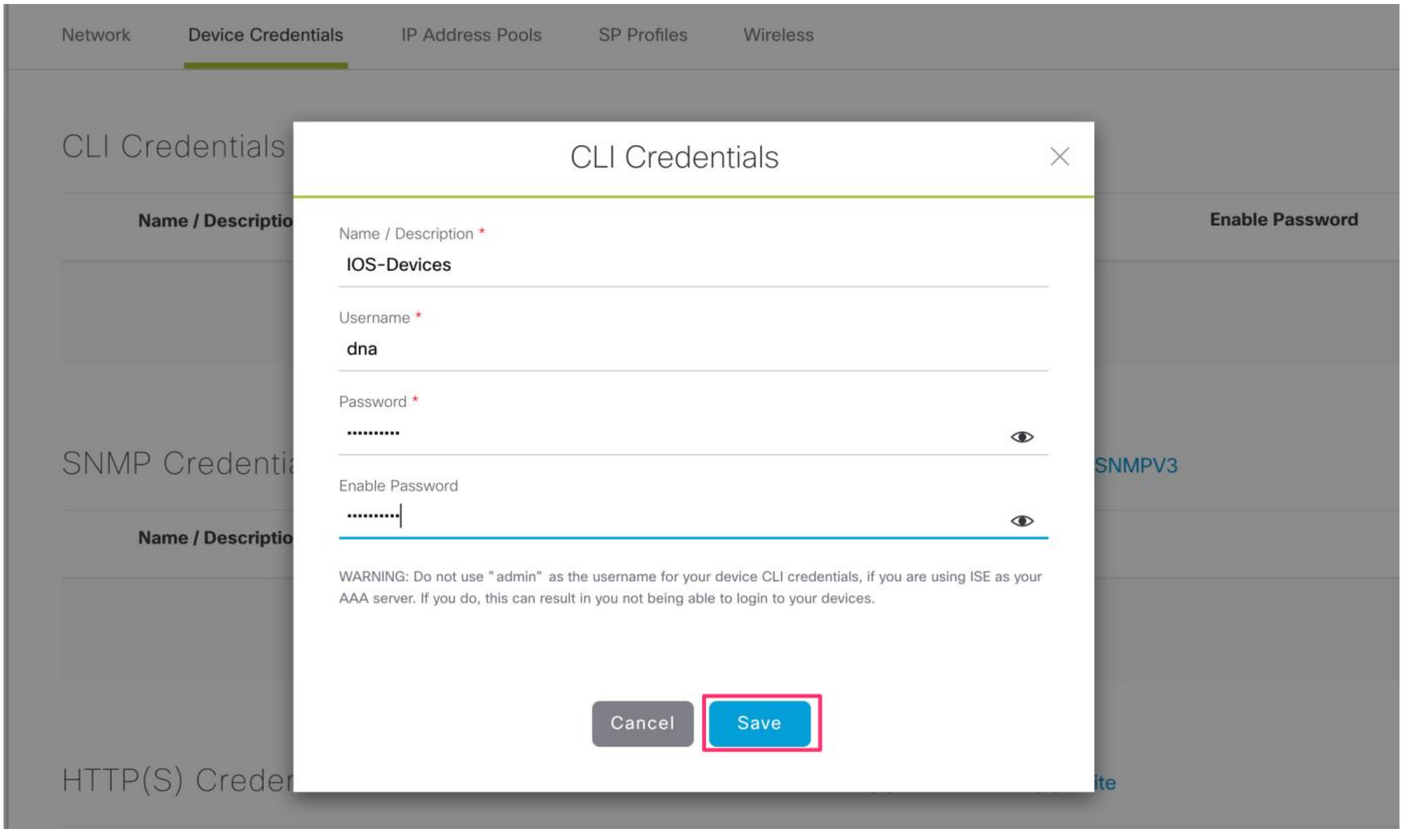
Step 1. Navigate to **Design > Network Settings > Device Credentials**, select an appropriate level of the site hierarchy in the left pane (example: Global for common credentials across the hierarchy).



CLI Credentials

Name / Description	Username	Password	Enable Password	Actions
No Data Available				

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.



CLI Credentials

Name / Description *
IOS-Devices

Username *
dna

Password *
••••••••••

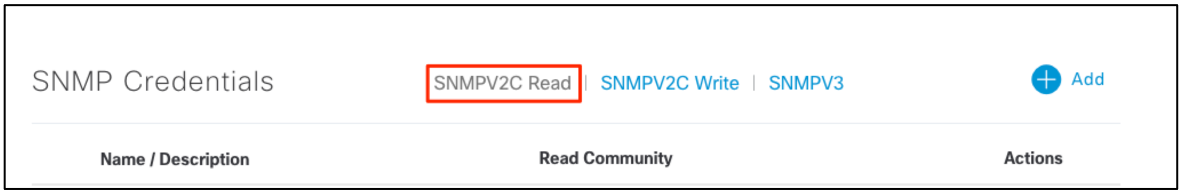
Enable Password
••••••••••

WARNING: Do not use "admin" as the username for your device CLI credentials, if you are using ISE as your AAA server. If you do, this can result in you not being able to login to your devices.

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.**

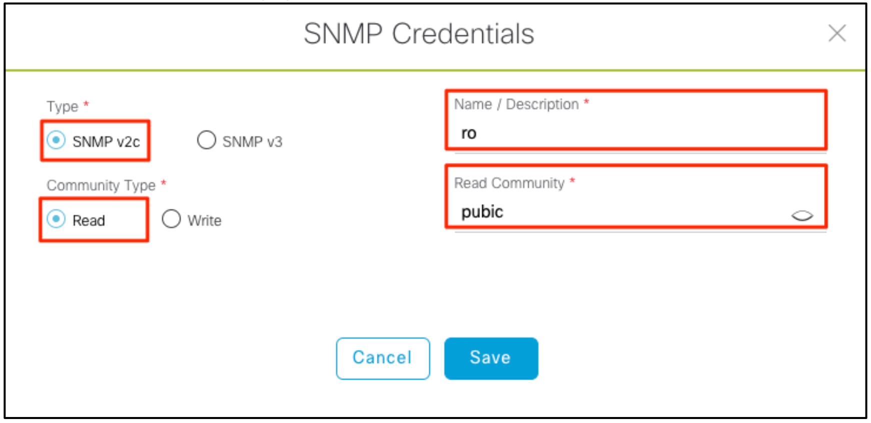


SNMP Credentials

Name / Description	Read Community	Actions

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

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



SNMP Credentials

Type *: ● SNMP v2c ○ SNMP v3

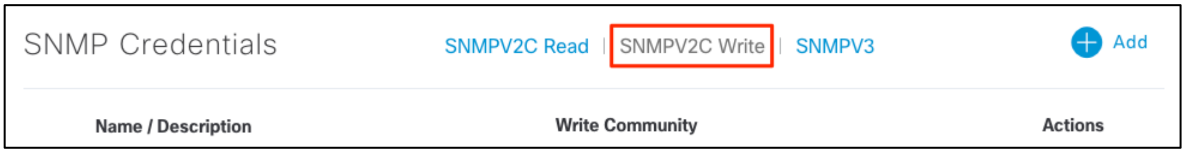
Community Type *: ● Read ○ Write

Name / Description *: ro

Read Community *: pubic

Step 5. Click Save

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

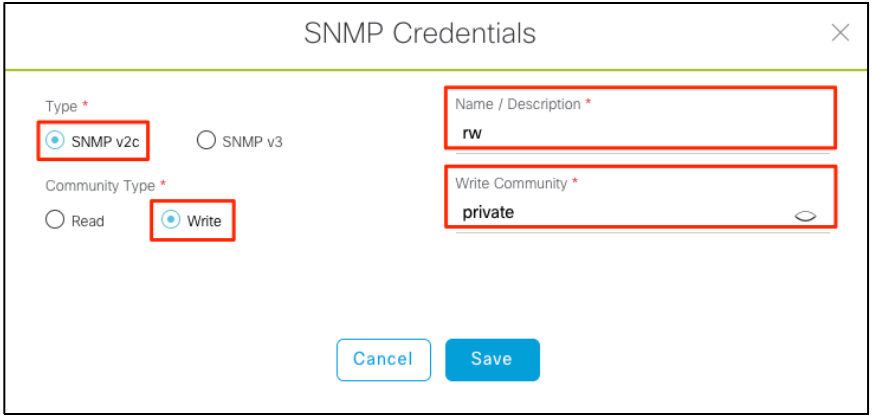


SNMP Credentials

Name / Description	Write Community	Actions

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

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



SNMP Credentials

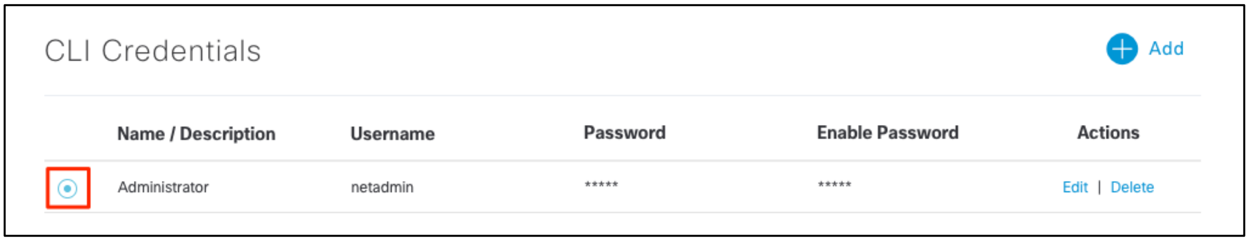
Type *: ● SNMP v2c ○ SNMP v3

Community Type *: ○ Read ● Write

Name / Description *: rw

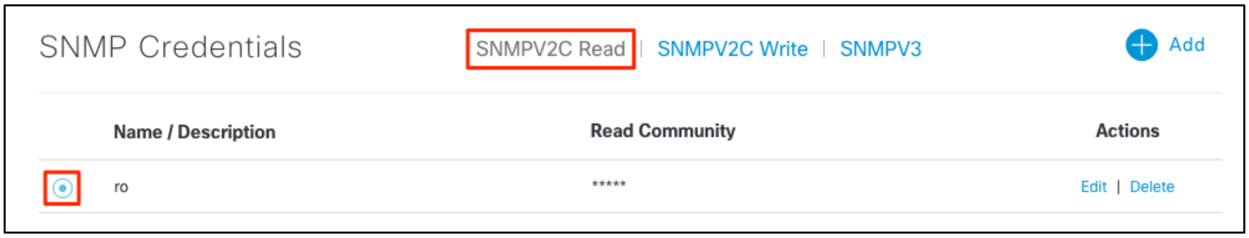
Write Community *: private

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.



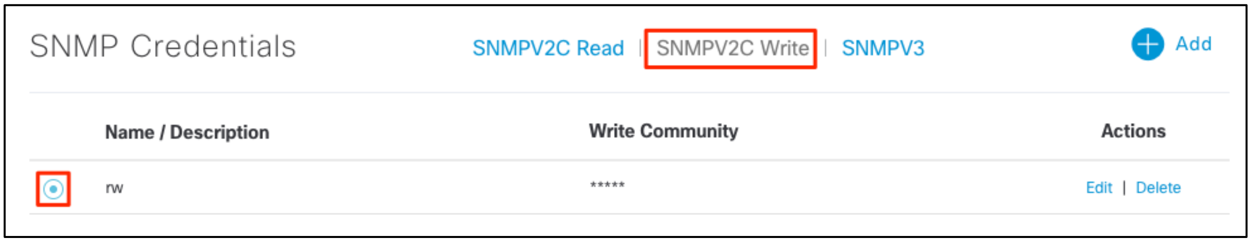
CLI Credentials

	Name / Description	Username	Password	Enable Password	Actions
◉	Administrator	netadmin	*****	*****	Edit | Delete



SNMP Credentials

	Name / Description	Read Community	Actions
◉	ro	*****	Edit | Delete



SNMP Credentials

	Name / Description	Write Community	Actions
◉	rw	*****	Edit | Delete

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.

Process 3: Automate onboarding of a Switch with Plug and Play (PnP)

For LAN Automation deployments, CLI and SNMP credentials is supplied to access and prepare one or more supported PnP seed devices, such as 9300 Series Switches for access. 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.

Procedure 1. Define Golden image for devices in inventory

The software image management capability built into Cisco DNA Center is used to upgrade any devices that are not running a recommended image version.

Tech tip

In this example switch is upgraded from the default image to 16.9.1.

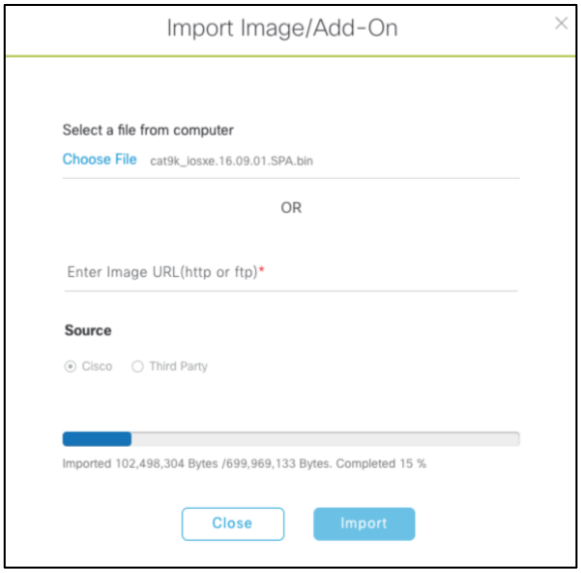
Use the following steps to apply software updates of images and software maintenance updates (SMUs) to the devices, by importing the required images, marking images as golden, and applying images to devices.

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

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

Step 3. Click **+Import**

Step 4. From the **Import Image/Add-On** dialog, choose a file location, and then click **Import**.



Import Image/Add-On

Select a file from computer

Choose File cat9k_iosxe.16.09.01.SPA.bin

OR

Enter Image URL(http or ftp)*

Source

● Cisco ○ Third Party

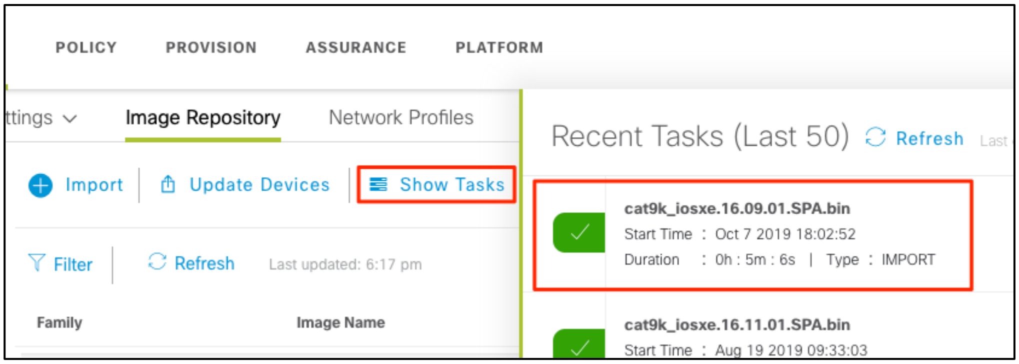
Imported 102,498,304 Bytes /699,969,133 Bytes. Completed 15 %

Step 5. Repeat this step for all images that you wish to deploy using Cisco DNA Center.

Tech tip

Images to be used for device families not yet available in Cisco DNA Center will be listed under the **Unassigned** category.

Step 6. Under **Image Repository**, click **Show Tasks** to verify if the import was successful.



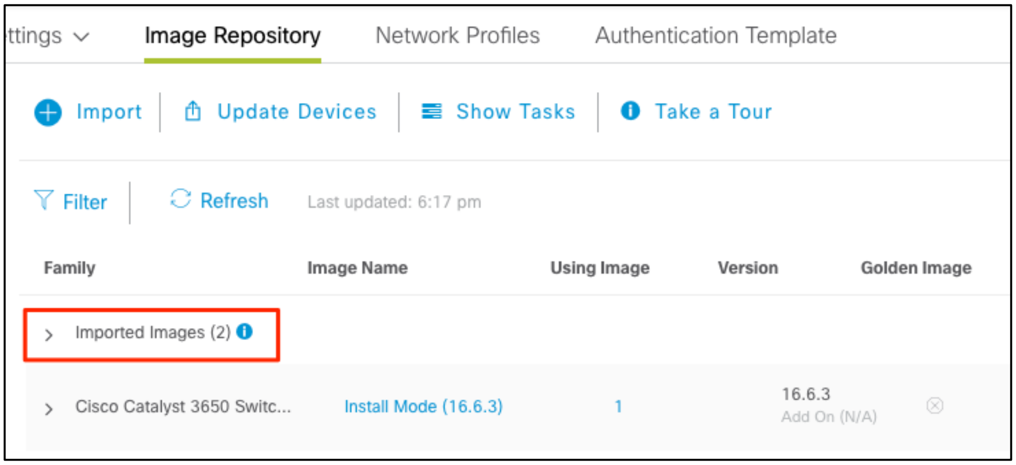
```
cat9k_iosxe.16.09.01.SPA.bin
Start Time  :  Oct 7 2019 18:02:52
Duration    :  0h : 5m : 6s  |  Type  :  IMPORT

cat9k_iosxe.16.11.01.SPA.bin
Start Time  :  Aug 19 2019 09:33:03
```

Tech tip

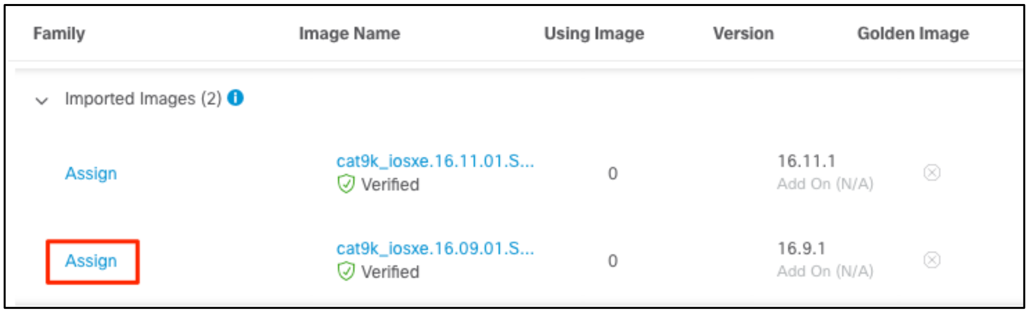
If image import fails, next to the failed image in the list click on **See why?** for more details.

Step 7. Under **Image Repository**, click **Imported Images** to expand the list of all the imported images that are pending to be assigned to a device family.



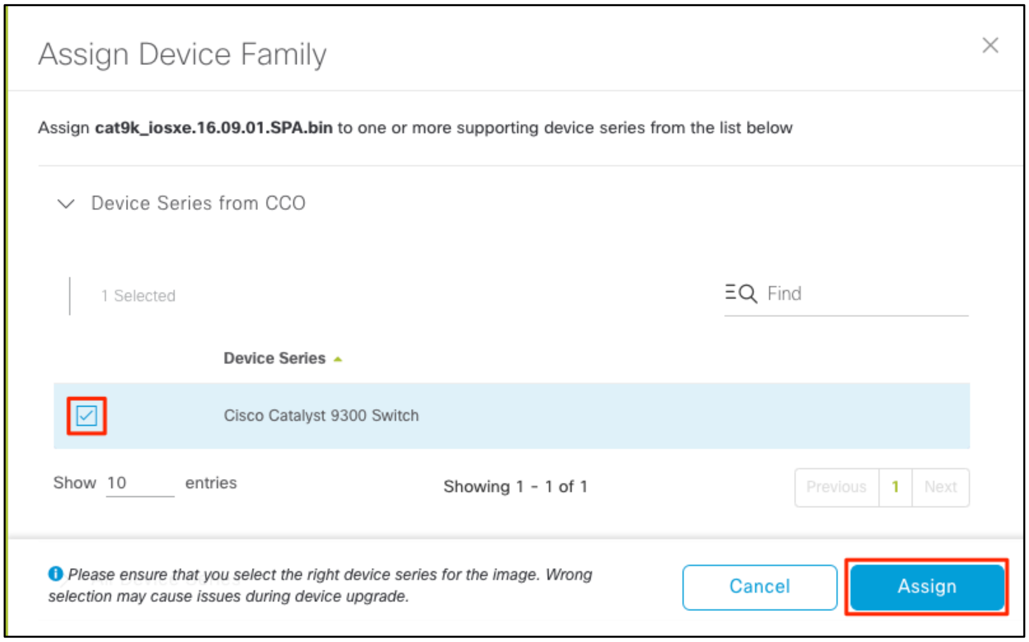
Family	Image Name	Using Image	Version	Golden Image
› Imported Images (2) ⓘ				
› Cisco Catalyst 3650 Switc...	Install Mode (16.6.3)	1	16.6.3 Add On (N/A)	⊗

Step 8. Click on **Assign** next to the image name need to be assigned.



Family	Image Name	Using Image	Version	Golden Image
⌄ Imported Images (2) ⓘ				
Assign	cat9k_iosxe.16.11.01.S... ✓ Verified	0	16.11.1 Add On (N/A)	⊗
Assign	cat9k_iosxe.16.09.01.S... ✓ Verified	0	16.9.1 Add On (N/A)	⊗

Step 9. The slide out panel will show the list of device type from CCO based on the image. Check the box next to the Device Series and click **Assign**.



Assign Device Family

Assign **cat9k_iosxe.16.09.01.SPA.bin** to one or more supporting device series from the list below

Device Series from CCO

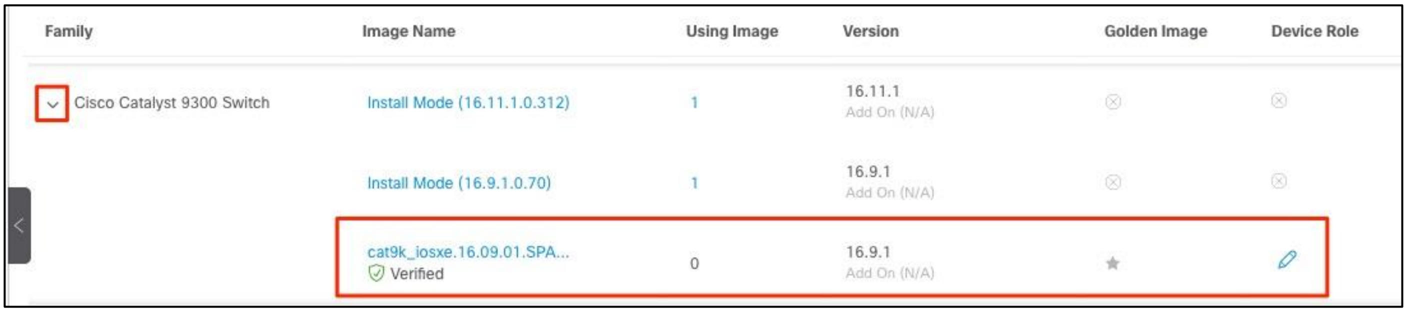
1 Selected

	Device Series
☑	Cisco Catalyst 9300 Switch

Show 10 entries   Showing 1 - 1 of 1

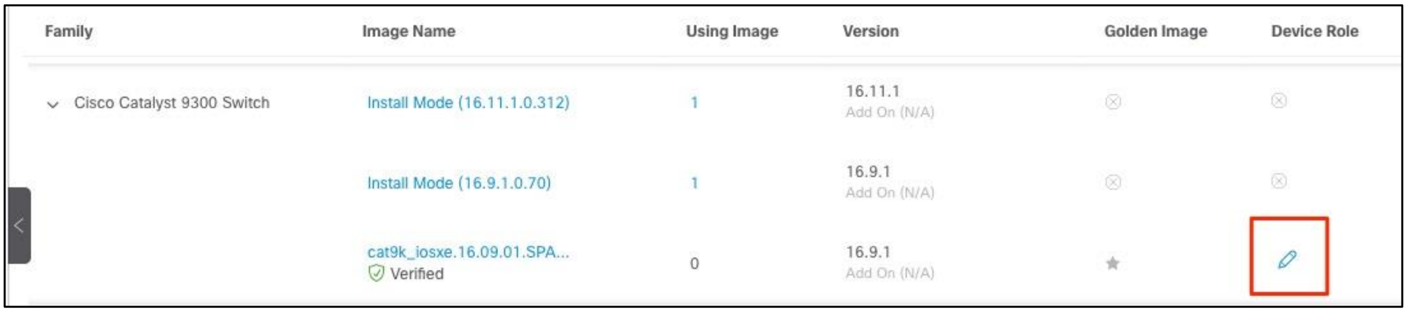
Please ensure that you select the right device series for the image. Wrong selection may cause issues during device upgrade.

Step 10. Go to the assigned **Device Family** and click the expand icon and verify the image imported is available to mark as golden.



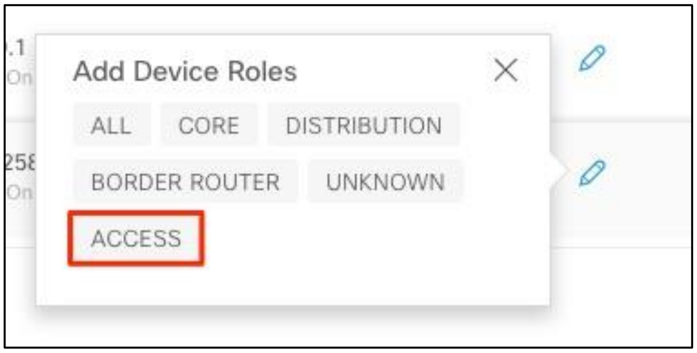
Family	Image Name	Using Image	Version	Golden Image	Device Role
Cisco Catalyst 9300 Switch	Install Mode (16.11.1.0.312)	1	16.11.1 Add On (N/A)	⊗	⊗
	Install Mode (16.9.1.0.70)	1	16.9.1 Add On (N/A)	⊗	⊗
	cat9k_iosxe.16.09.01.SPA... Verified	0	16.9.1 Add On (N/A)	★	✎

Step 11. Click the pencil icon and select the appropriate role, to mark a **Golden Image** for specific device role.

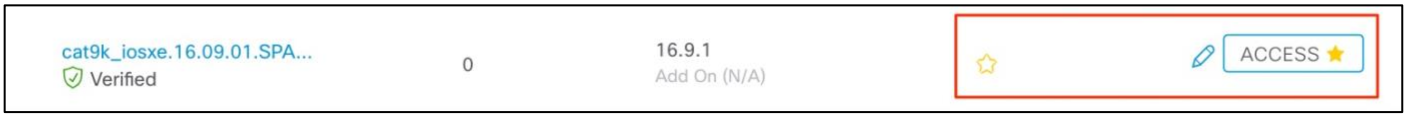


Family	Image Name	Using Image	Version	Golden Image	Device Role
Cisco Catalyst 9300 Switch	Install Mode (16.11.1.0.312)	1	16.11.1 Add On (N/A)	⊗	⊗
	Install Mode (16.9.1.0.70)	1	16.9.1 Add On (N/A)	⊗	⊗
	cat9k_iosxe.16.09.01.SPA... Verified	0	16.9.1 Add On (N/A)	★	✎

Step 12. Select **ACCESS** tag.



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



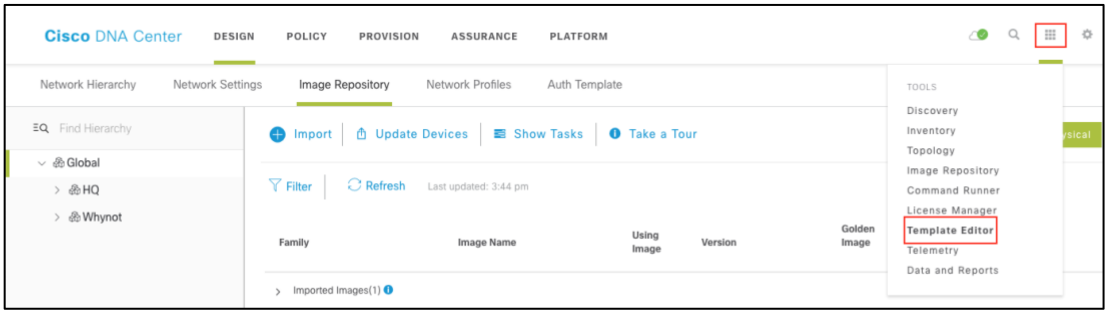
Procedure 2. Create Onboarding Templates

Golden Image → Onboard Template → Create Profile → Assign Profile → Discover Controller → Provision Devices

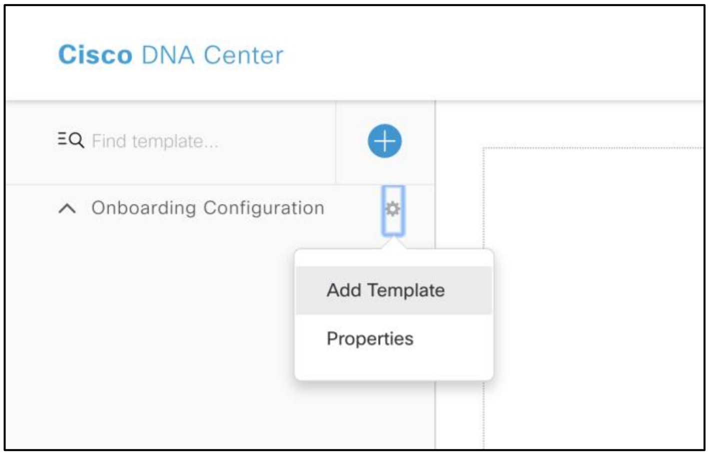
By default, the Onboarding Configuration project is available for creating day-0 templates. You can create your own custom projects. Templates created in custom projects are categorized as day-N templates.

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**.



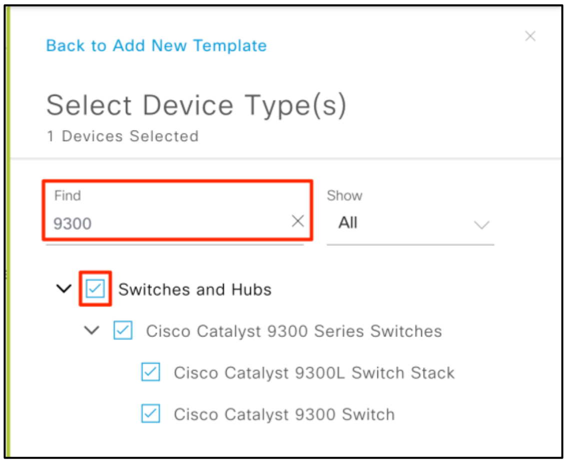
Step 4. In the Add New Template window, select **Regular Template** and fill in the following details:

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 (example: Cisco Catalyst 9300 Switch) name in **Find** field to narrow the devices and choose the device types that you want to apply to the template.


Back to Add New Template
×
Select Device Type(s)
1 Devices Selected
Find
9300
Show
All
☑ Switches and Hubs
☑ Cisco Catalyst 9300 Series Switches
☑ Cisco Catalyst 9300L Switch Stack
☑ Cisco Catalyst 9300 Switch

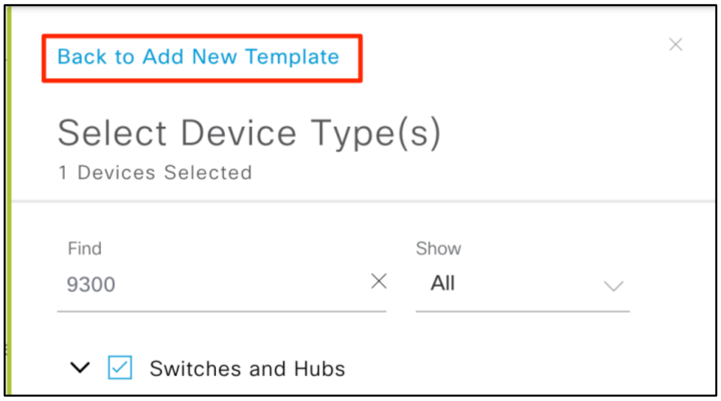
Tech tip

There are different granularity levels for choosing the device type from the hierarchical structure. The device type is used during deployment to ensure that templates deploy devices that match the specified device type criteria. This lets you create specialized templates for specific device models.

Tech tip

Template Editor does not show device product IDs (PIDs); instead, it shows the device series and model description. You can use cisco.com to look up the device data sheet based on the PID, find the device series and model description, and choose the device type appropriately.

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.

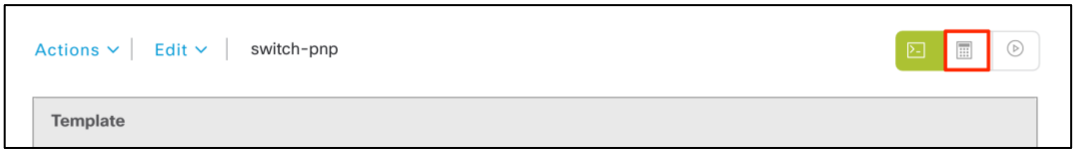
Tech tip
We have provided a sample configuration in **Appendix A**.

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**.

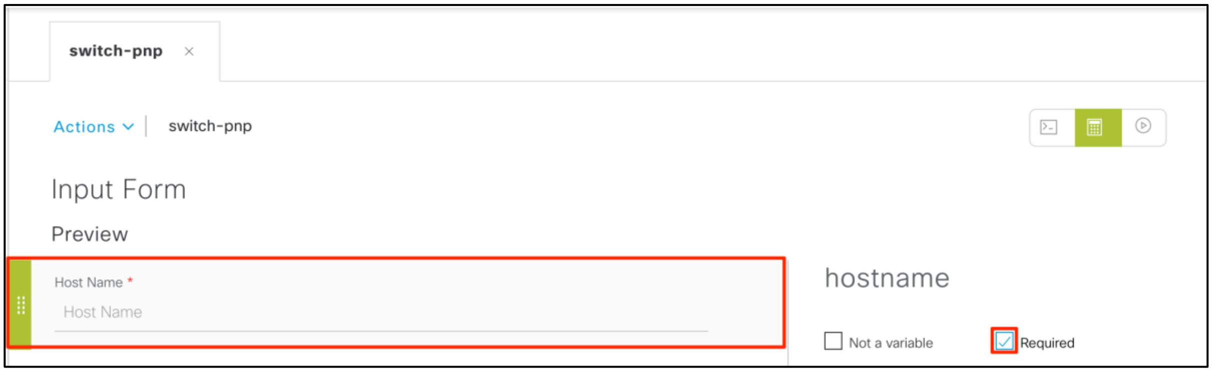
Tech tip
Only the committed templates cab be associated with a network profile and to use it for provisioning.

Step 12. From the top-right, click the calculator icon to go to the **Form Editor**.



Tech tip
All the form fields are drag and drop to rearrange the order.

Step 13. Select a form field (example: Host Name) and check the **Required** box:



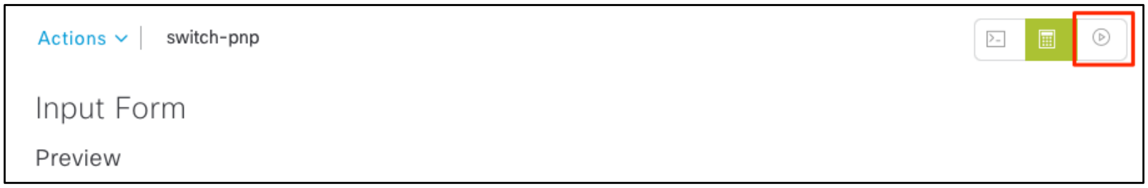
Step 14. Fill in the remaining details as following:

Field	Value
Field Name	Host Name
Tooltip Text	`Enter the switch name`
Default Value	-
Instructional Text	-
Maximum Characters	`10`
Definition of hostname: Data Type	`String`
Definition of hostname: Display Type	`Text Field`

Tech tip
Repeat the above step for all the fields to have friendly names (example: $vlan_mgmt will become Management VLAN). Based on the variable the data and display type changes. Example for VLAN the data type is integer.

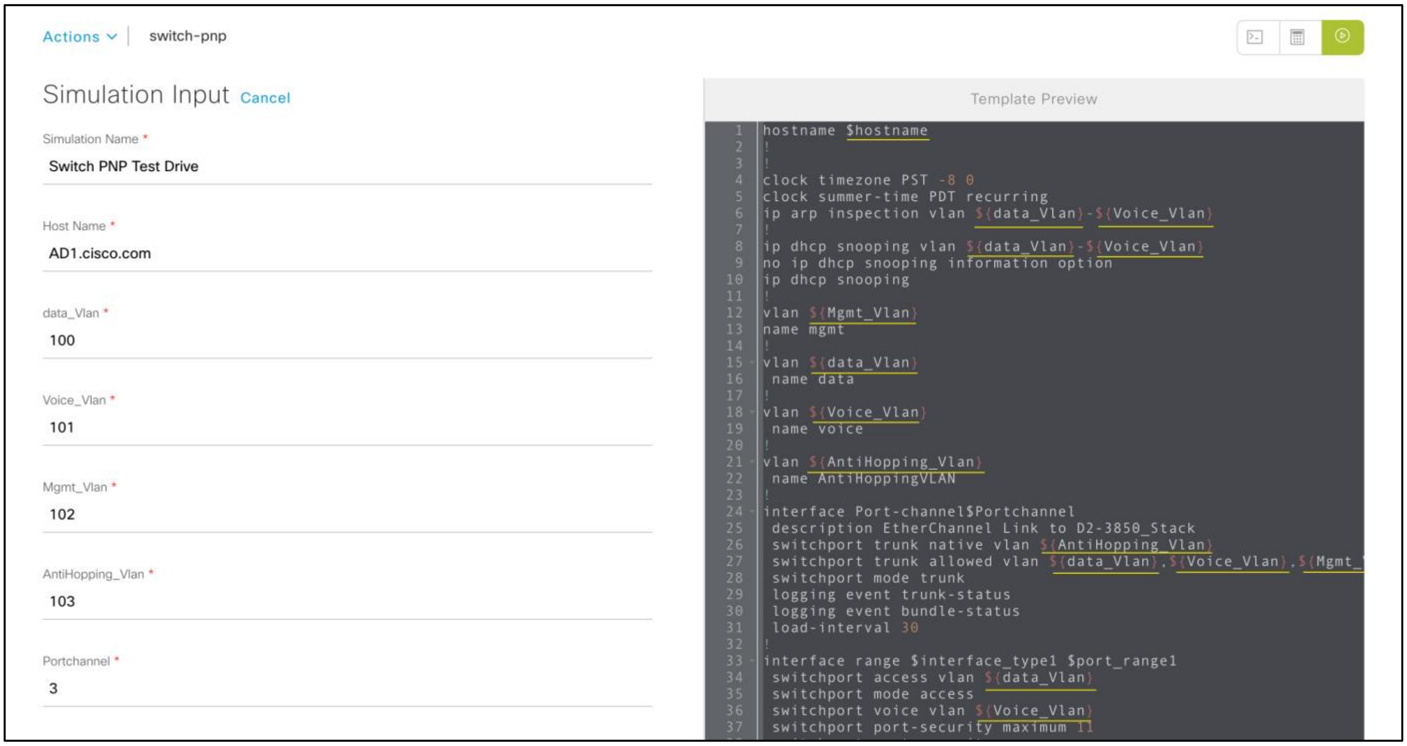
Tech tip
Bind to Source is not supported for **Day 0** template, it is only supported for **Day 1** template.

Step 15. To test the template, click the button to switch to **simulation editor**.



Step 16. Click **New Simulation**.

Step 17. Fill in the **Simulation input** form. (Only partial configuration is displayed in the screenshot below.)



Simulation Input Cancel

Simulation Name *
Switch PNP Test Drive

Host Name *
AD1.cisco.com

data_Vlan *
100

Voice_Vlan *
101

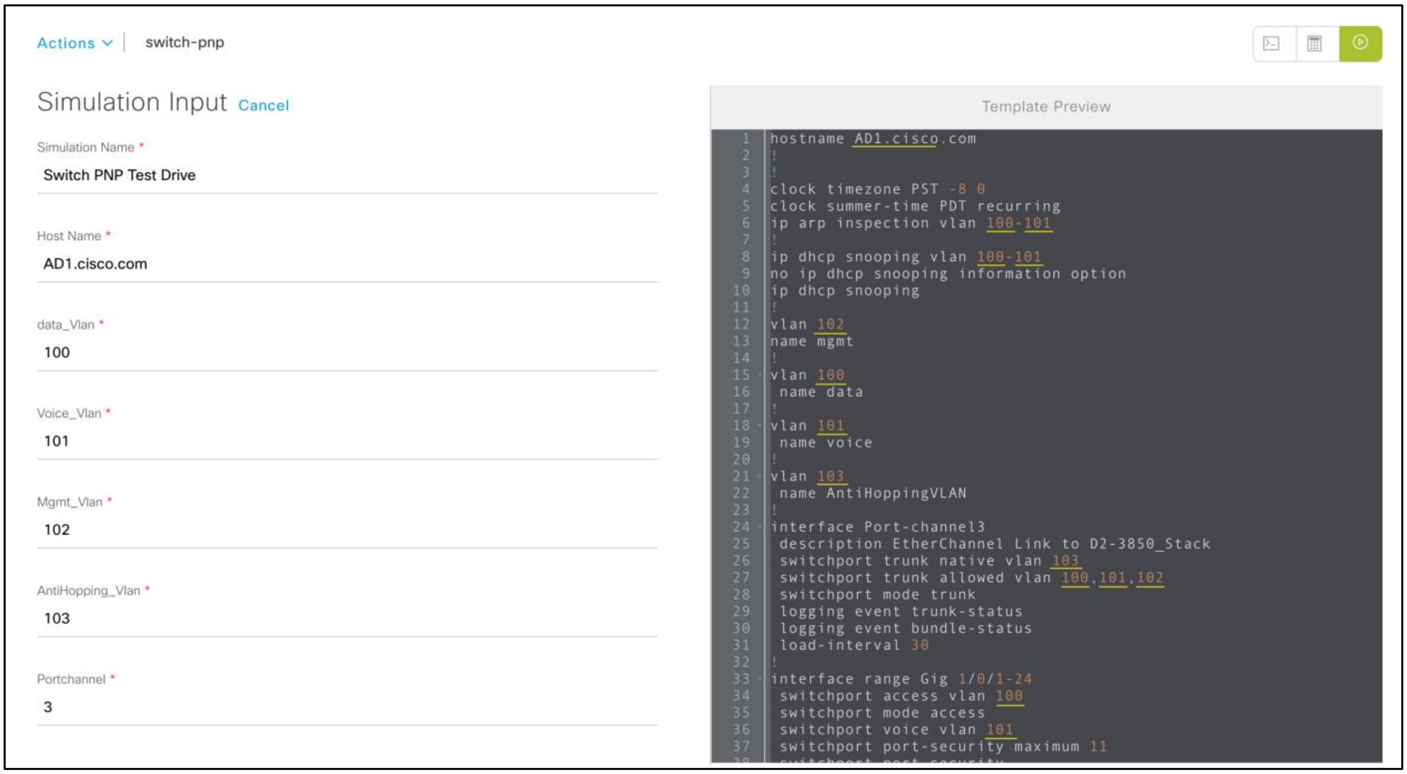
Mgmt_Vlan *
102

AntiHopping_Vlan *
103

Portchannel *
3

```
hostname $hostname
!
!
clock timezone PST -8 0
clock summer-time PDT recurring
ip arp inspection vlan ${data_Vlan}-${Voice_Vlan}
!
ip dhcp snooping vlan ${data_Vlan}-${Voice_Vlan}
no ip dhcp snooping information option
ip dhcp snooping
!
vlan ${Mgmt_Vlan}
name mgmt
!
vlan ${data_Vlan}
 name data
!
vlan ${Voice_Vlan}
 name voice
!
vlan ${AntiHopping_Vlan}
 name AntiHoppingVLAN
!
interface Port-channel$Portchannel
 description EtherChannel Link to D2-3850_Stack
 switchport trunk native vlan ${AntiHopping_Vlan}
 switchport trunk allowed vlan ${data_Vlan},${Voice_Vlan},${Mgmt_
 switchport mode trunk
 logging event trunk-status
 logging event bundle-status
 load-interval 30
!
interface range $interface_type1 $port_range1
 switchport access vlan ${data_Vlan}
 switchport mode access
 switchport voice vlan ${Voice_Vlan}
 switchport port-security maximum 11
```

Step 18. Click **Run**, and all the variables in the CLI will now displays the actual value entered in the form fields on the left.



Simulation Input Cancel

Simulation Name *
Switch PNP Test Drive

Host Name *
AD1.cisco.com

data_Vlan *
100

Voice_Vlan *
101

Mgmt_Vlan *
102

AntiHopping_Vlan *
103

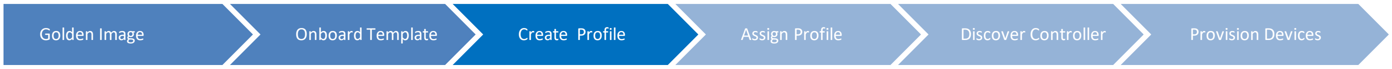
Portchannel *
3

```
hostname AD1.cisco.com
!
!
clock timezone PST -8 0
clock summer-time PDT recurring
ip arp inspection vlan 100-101
!
ip dhcp snooping vlan 100-101
no ip dhcp snooping information option
ip dhcp snooping
!
vlan 102
name mgmt
!
vlan 100
 name data
!
vlan 101
 name voice
!
vlan 103
 name AntiHoppingVLAN
!
interface Port-channel3
 description EtherChannel Link to D2-3850_Stack
 switchport trunk native vlan 103
 switchport trunk allowed vlan 100,101,102
 switchport mode trunk
 logging event trunk-status
 logging event bundle-status
 load-interval 30
!
interface range Gig 1/0/1-24
 switchport access vlan 100
 switchport mode access
 switchport voice vlan 101
 switchport port-security maximum 11
```

Tech tip

Make sure to **commit** the template before proceeding for the latest configuration to take affect during device provisioning.

Procedure 3. Create Network Profiles for Switching


Golden Image

Onboard Template

Create Profile

Assign Profile

Discover Controller

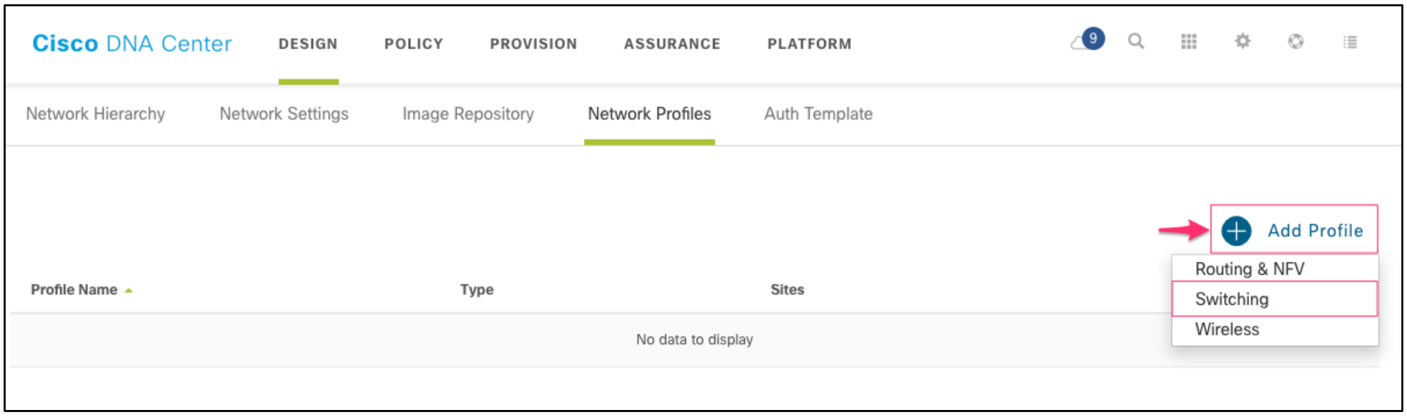
Provision Devices

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.

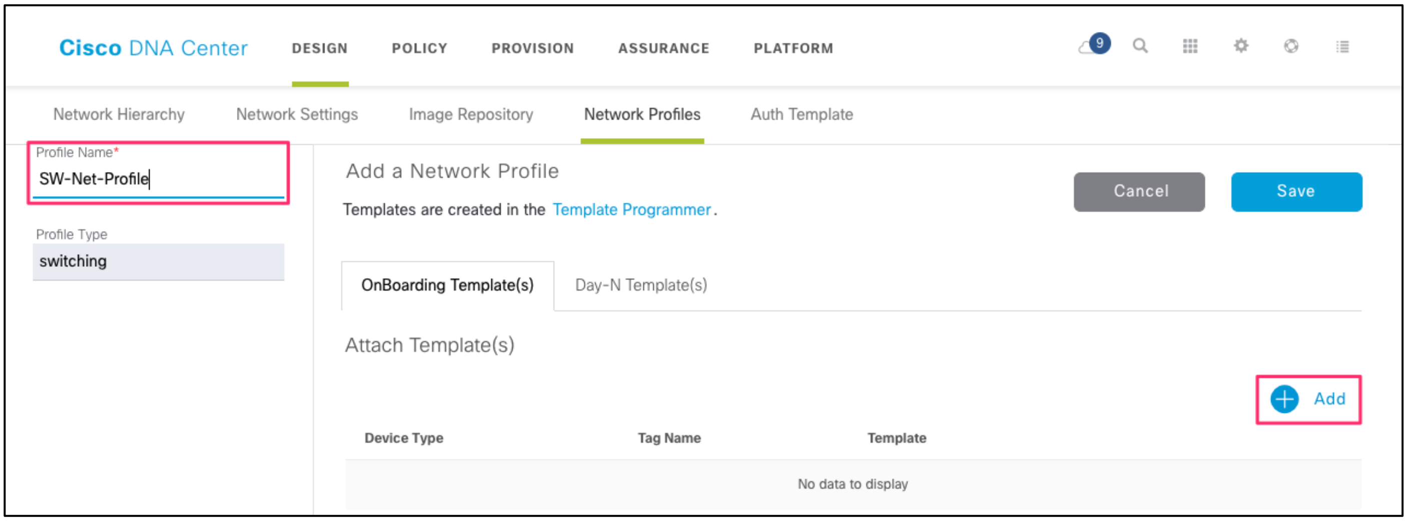
For this procedure, follow these steps:

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.



Profile Name* SW-Net-Profile

Profile Type switching

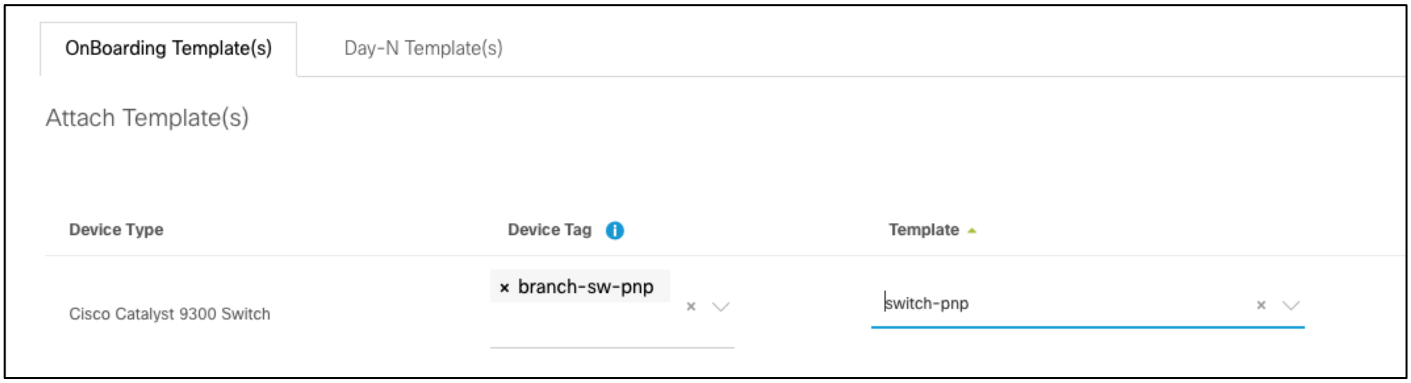
Add a Network Profile

Templates are created in the Template Programmer.

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	Template
Cisco Catalyst 9300 Switch	× branch-sw-pnp	switch-pnp

Step 7. Click **Save**.

Tech tip

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

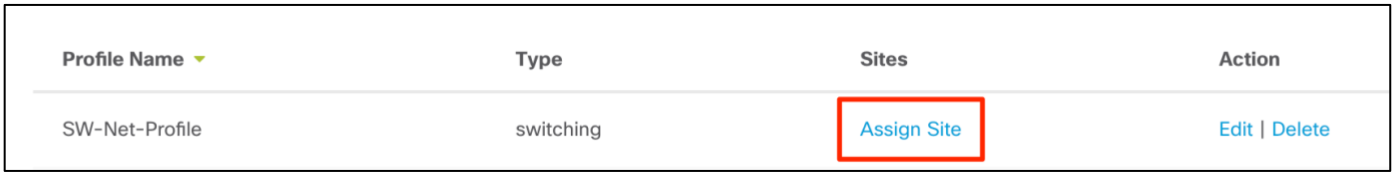
Procedure 4. Assign Network Profile to Site

Golden Image > Onboard Template > Create Profile > Assign Profile > Discover Controller > Provision Devices

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.

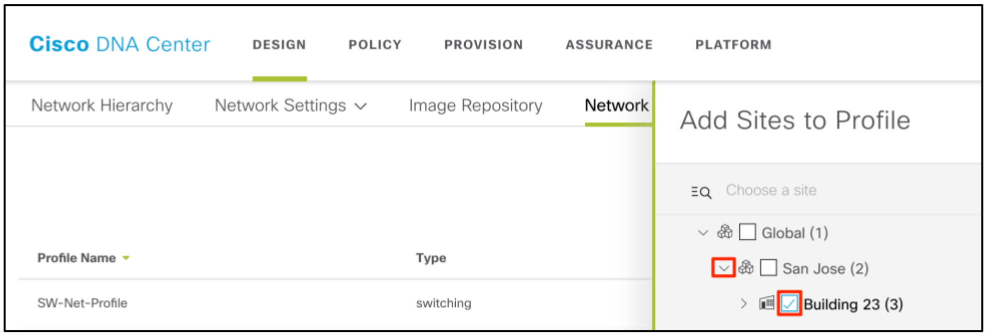
Step 1. Choose Design > **Network Profiles**.

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



Profile Name	Type	Sites	Action
SW-Net-Profile	switching	Assign Site	Edit | Delete

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



Profile Name	Type
SW-Net-Profile	switching

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)

Golden Image → Onboard Template → Create Profile → Assign Profile → Discover Controller → Provision Devices

For the device to connect with the controller (PnP Server), there are five options:

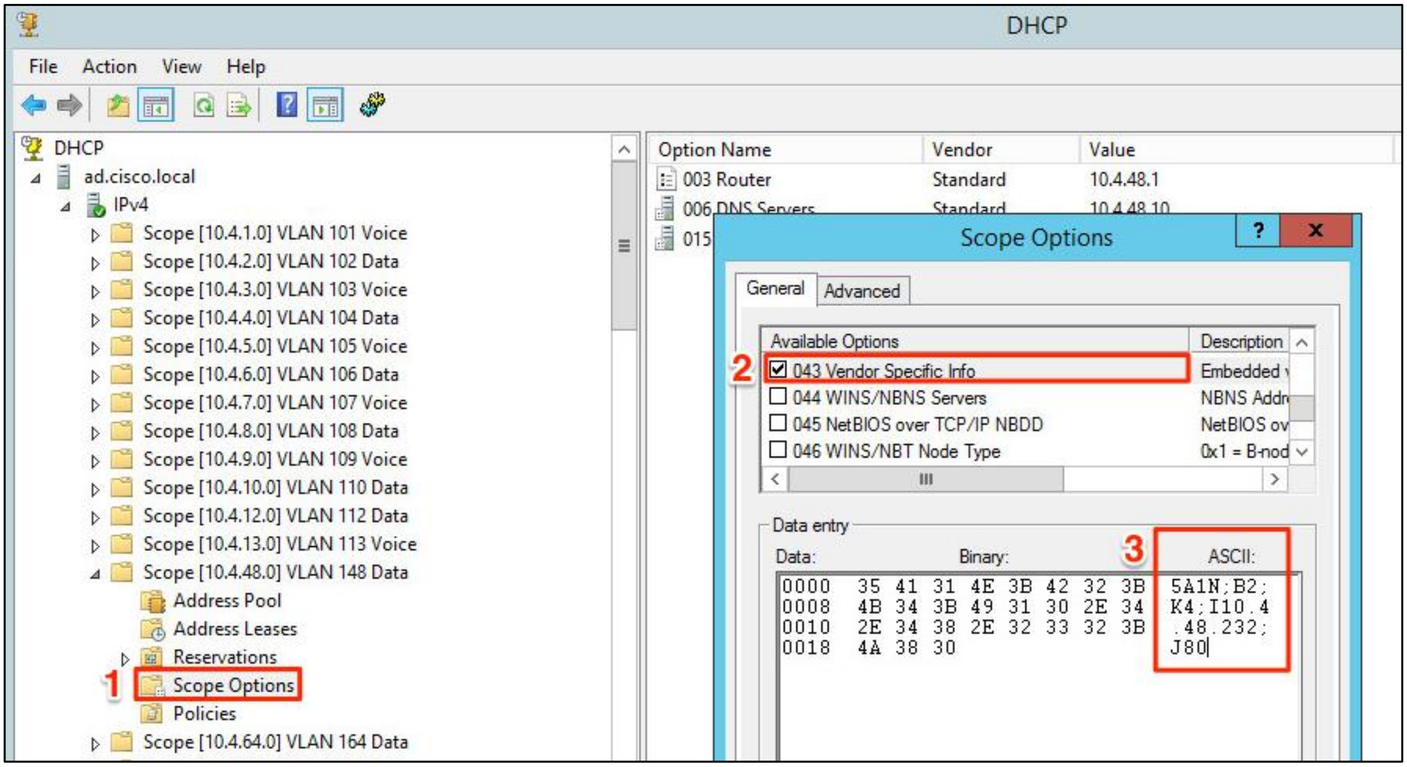
- DHCP server, using **option 43** (set the IP Address of the controller).
- DHCP server, using a DNS domain name (DNS lookup of pnphelper).
- Cisco Plug and Play Connect (cloud-based device discovery).
- USB key (bootstrap config file).
- Cisco Installer App (For iPhone/Android).

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. For more information on DHCP controller discovery, go here.

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



DHCP

- DHCP
  - ad.cisco.local
    - IPv4
      - Scope [10.4.1.0] VLAN 101 Voice
      - Scope [10.4.2.0] VLAN 102 Data
      - Scope [10.4.3.0] VLAN 103 Voice
      - Scope [10.4.4.0] VLAN 104 Data
      - Scope [10.4.5.0] VLAN 105 Voice
      - Scope [10.4.6.0] VLAN 106 Data
      - Scope [10.4.7.0] VLAN 107 Voice
      - Scope [10.4.8.0] VLAN 108 Data
      - Scope [10.4.9.0] VLAN 109 Voice
      - Scope [10.4.10.0] VLAN 110 Data
      - Scope [10.4.12.0] VLAN 112 Data
      - Scope [10.4.13.0] VLAN 113 Voice
      - Scope [10.4.48.0] VLAN 148 Data
        - Address Pool
        - Address Leases
        - Reservations
        - 1 Scope Options
        - Policies
      - Scope [10.4.64.0] VLAN 164 Data

Option Name	Vendor	Value
003 Router	Standard	10.4.48.1
006 DNS Servers	Standard	10.4.48.10
015		

Scope Options

General | Advanced

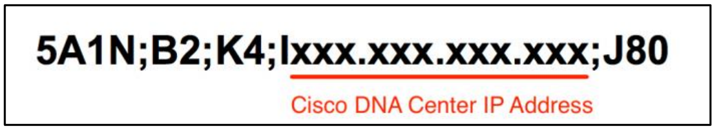
Available Options	Description
2 ☑ 043 Vendor Specific Info	Embedded v
☐ 044 WINS/NBNS Servers	NBNS Addr
☐ 045 NetBIOS over TCP/IP NBDD	NetBIOS ov
☐ 046 WINS/NBT Node Type	0x1 = B-nod

Data entry

```
Data:         Binary:                   3   ASCII:
0000   35 41 31 4E 3B 42 32 3B    5A1N;B2;
0008   4B 34 3B 49 31 30 2E 34    K4;I10.4
0010   2E 34 38 2E 32 33 32 3B    .48.232;
0018   4A 38 30                   J80
```

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

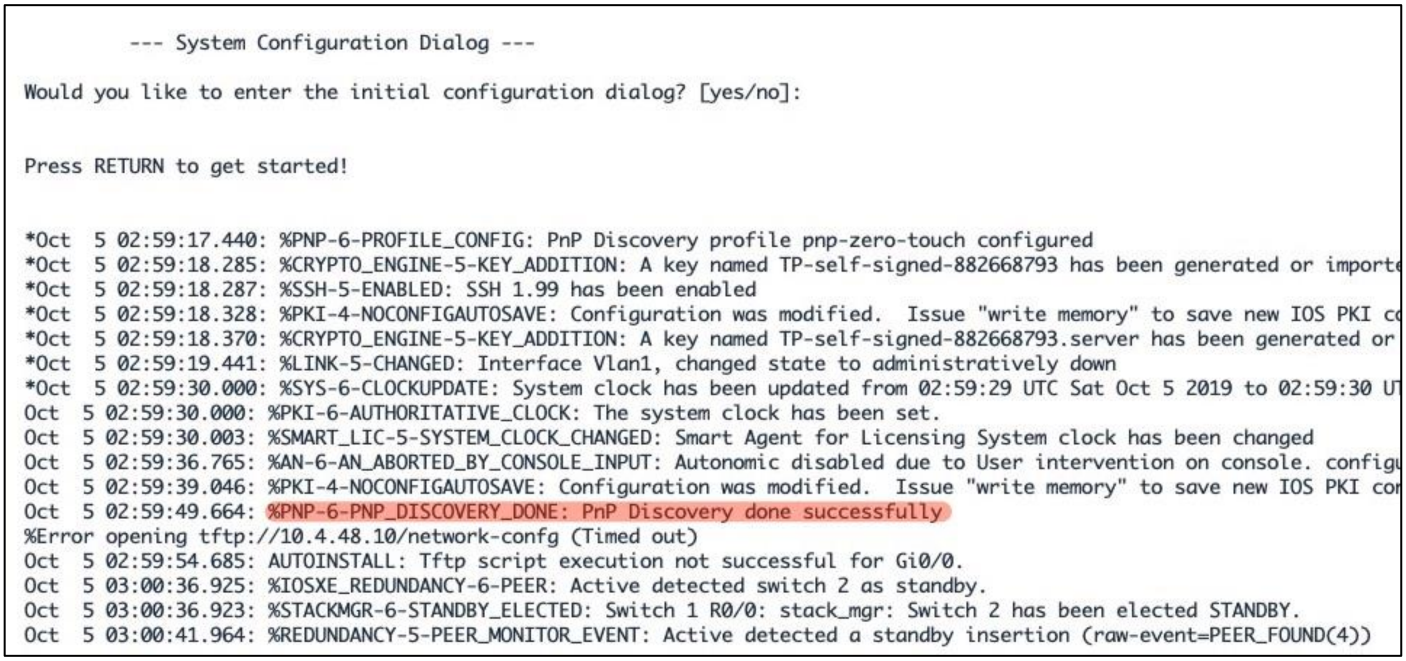
4. Copy and paste the ascii

```
option 43 ascii "5A1N;B2;K4;I10.4.48.232;J80"
```

5. Click **Apply** and OK.

Step 2. Connect a single switch (example: Catalyst 9300) to access layer that's getting onboarded.

Step 3. (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 importe
*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 co
*Oct  5 02:59:18.370: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named TP-self-signed-882668793.server has been generated or
*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 UT
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. configu
Oct  5 02:59:39.046: %PKI-4-NOCONFIGAUTOSAVE: Configuration was modified.  Issue "write memory" to save new IOS PKI cor
Oct  5 02:59:49.664: %PNP-6-PNP_DISCOVERY_DONE: PnP Discovery done successfully
%Error opening tftp://10.4.48.10/network-confg (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

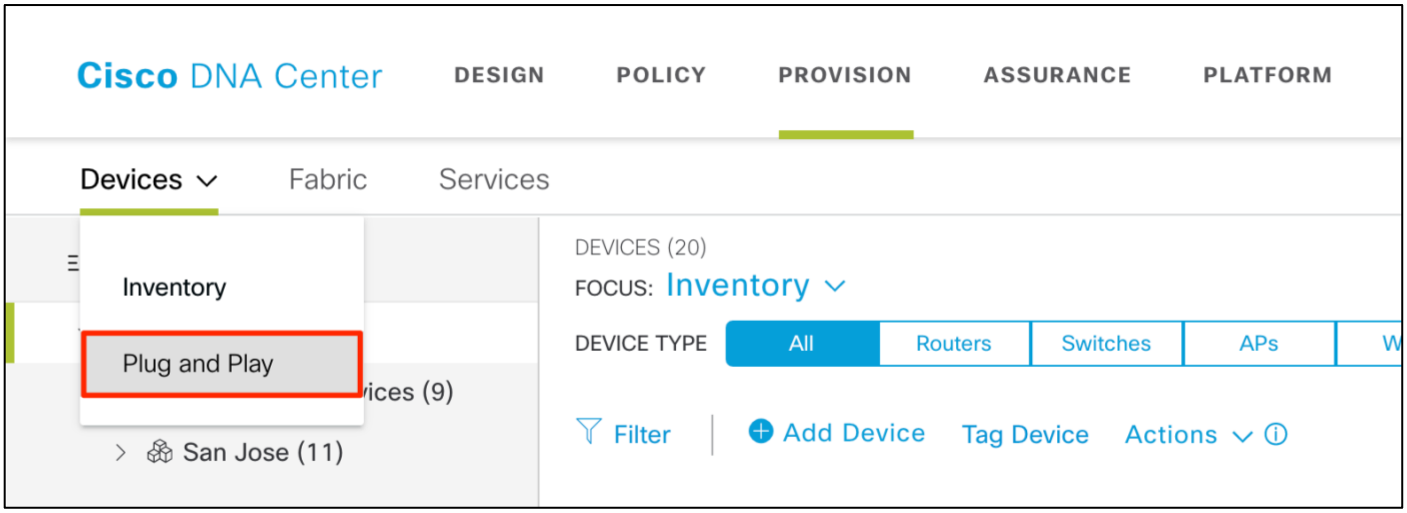
When the device is in process of PnP discovery do not touch the device as it will break the PnP process.

Procedure 6. Day-zero provisioning of switch onboarded with PnP

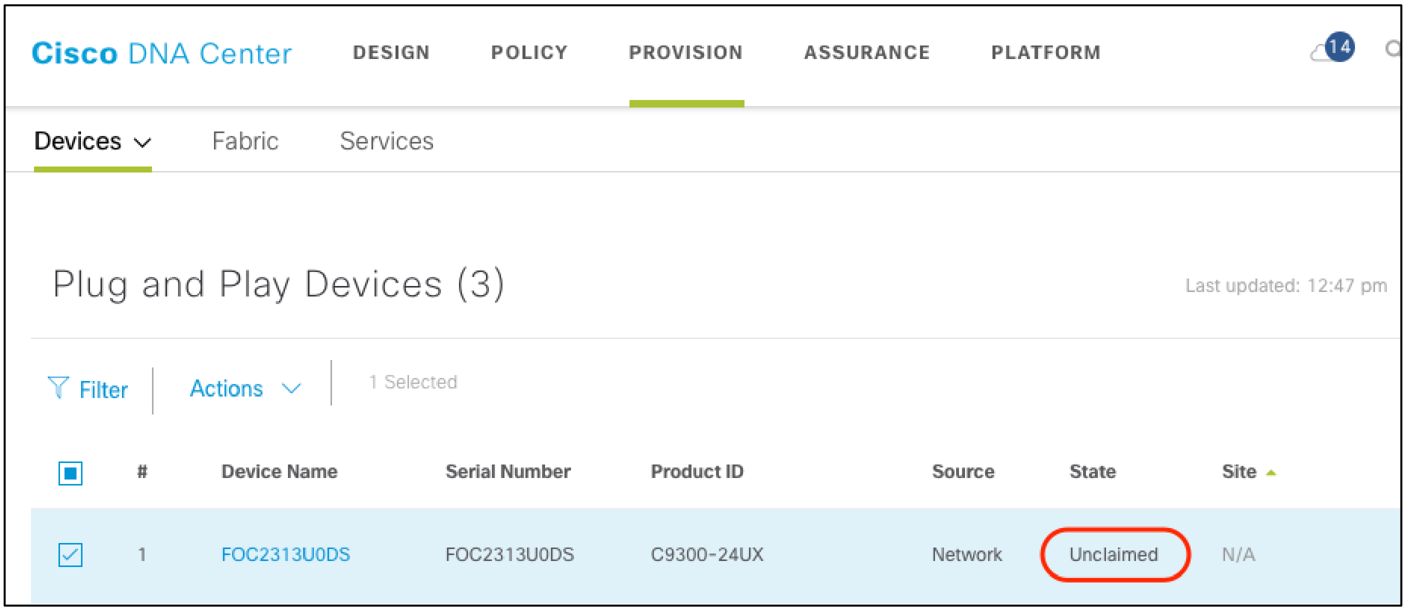
Golden Image
Onboard Template
Create Profile
Assign Profile
Discover Controller
Provision Device

Step 1. Login to Cisco DNA Center.

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



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



Plug and Play Devices (3)

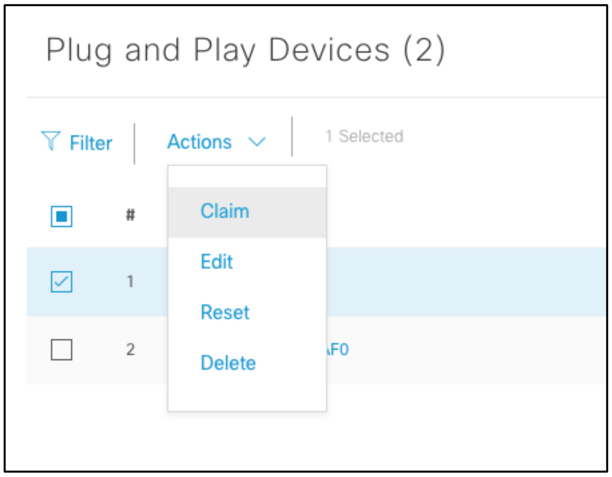
Last updated: 12:47 pm

■	#	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

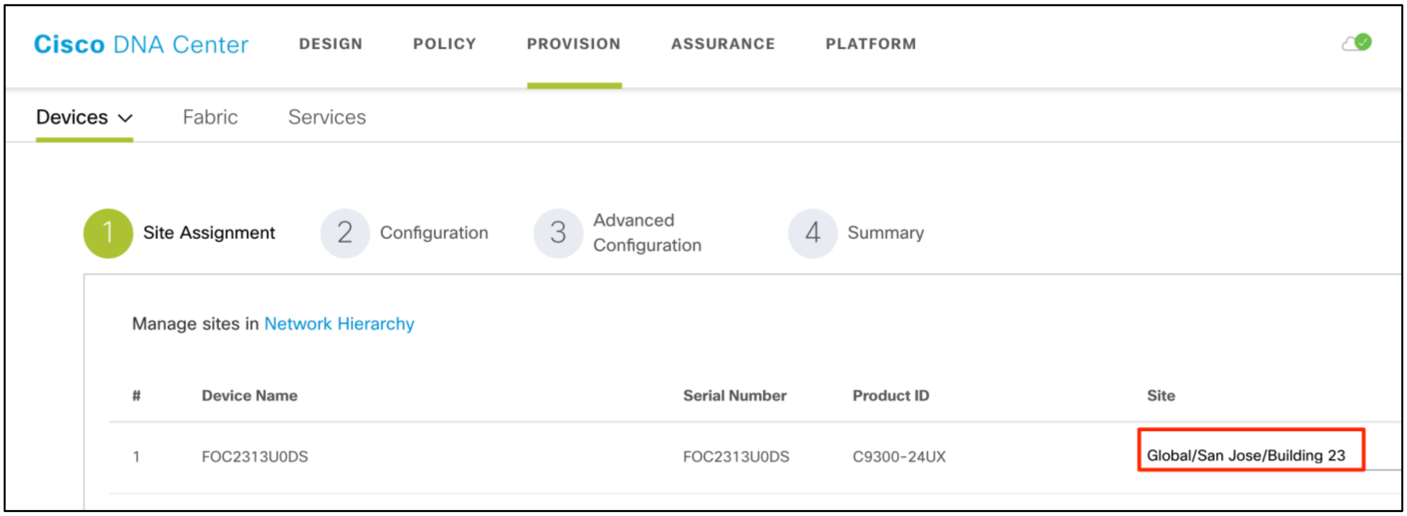
Before you claim a switch, if the access to the console is available, monitor the configuration in process by Cisco DNA Center. Copy and paste the following EEM script in the switch console:

```
event manager applet catchall
event cli pattern ".*" sync no skip no
action 1 syslog msg "$_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 according while processing the claim request.

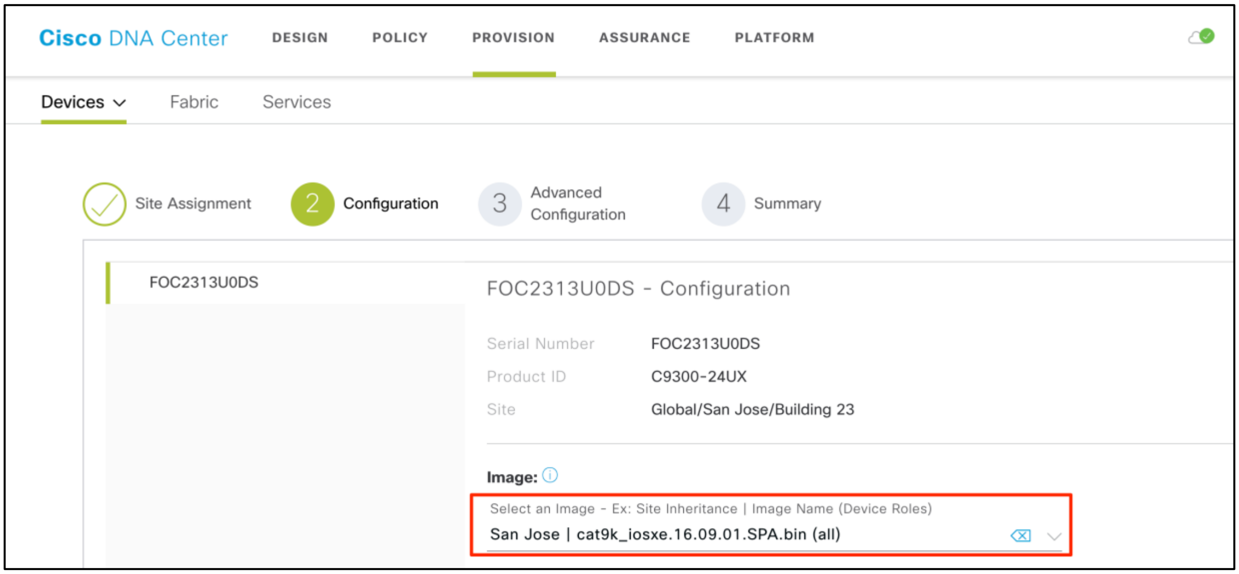


#	Device Name	Serial Number	Product ID	Site
1	FOC2313U0DS	FOC2313U0DS	C9300-24UX	Global/San Jose/Building 23

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.



FOC2313U0DS

FOC2313U0DS - Configuration

Serial Number FOC2313U0DS

Product ID C9300-24UX

Site Global/San Jose/Building 23

Image:

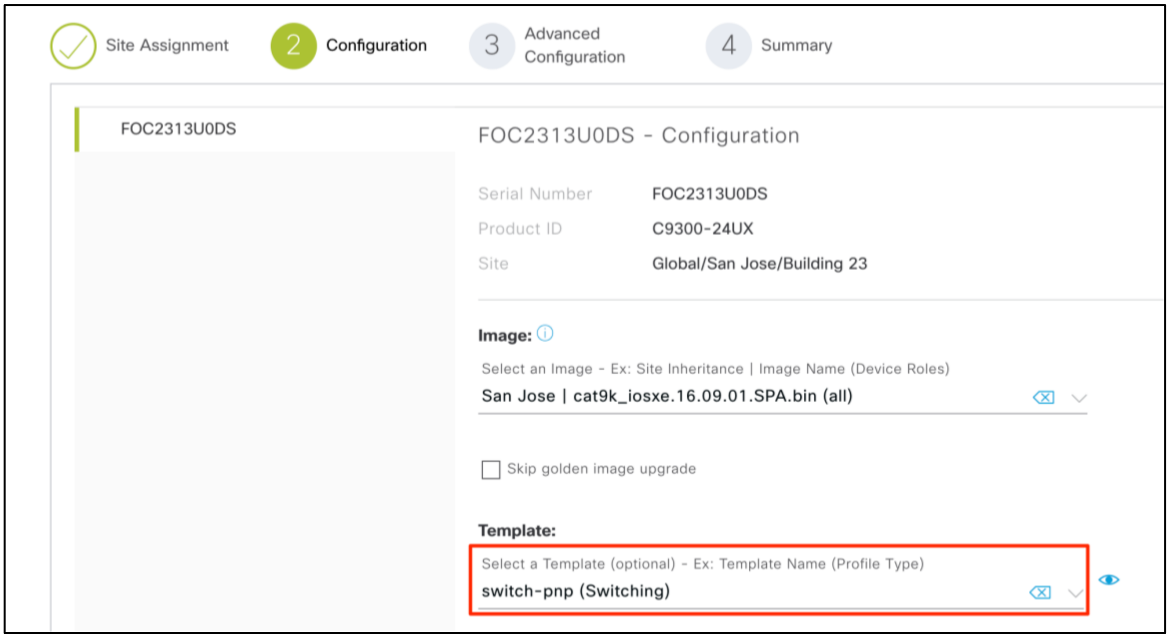
Select an Image - Ex: Site Inheritance | Image Name (Device Roles)

San Jose | cat9k_iosxe.16.09.01.SPA.bin (all)

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**.



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

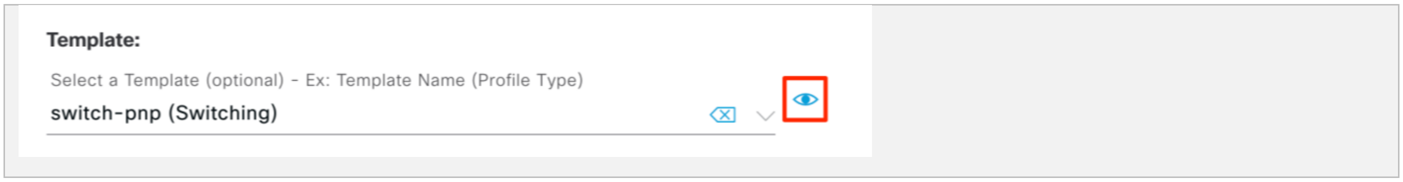
Template:

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.

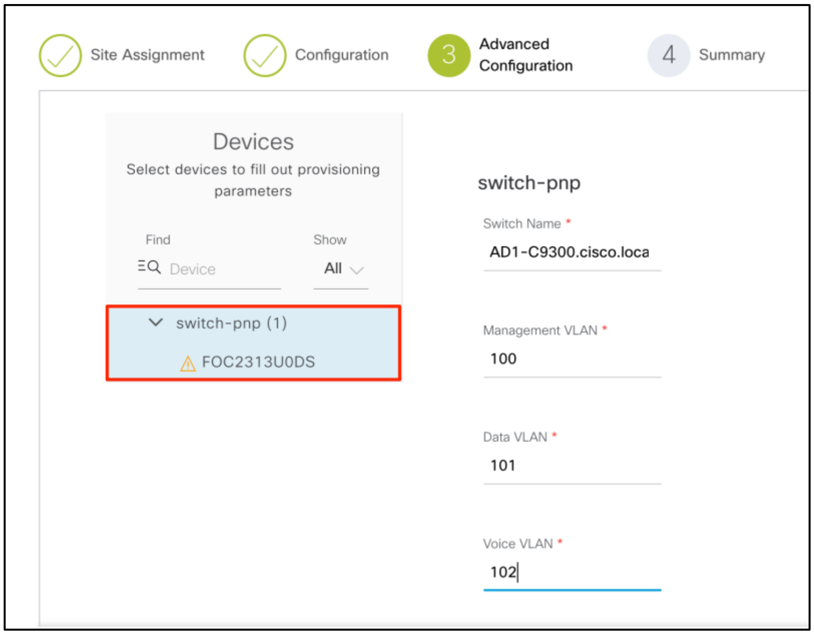


Template:

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**.



Devices

Select devices to fill out provisioning parameters

switch-pnp (1)

FOC2313U0DS

switch-pnp

Switch Name *: AD1-C9300.cisco.loca

Management VLAN *: 100

Data VLAN *: 101

Voice VLAN *: 102

Tech tip

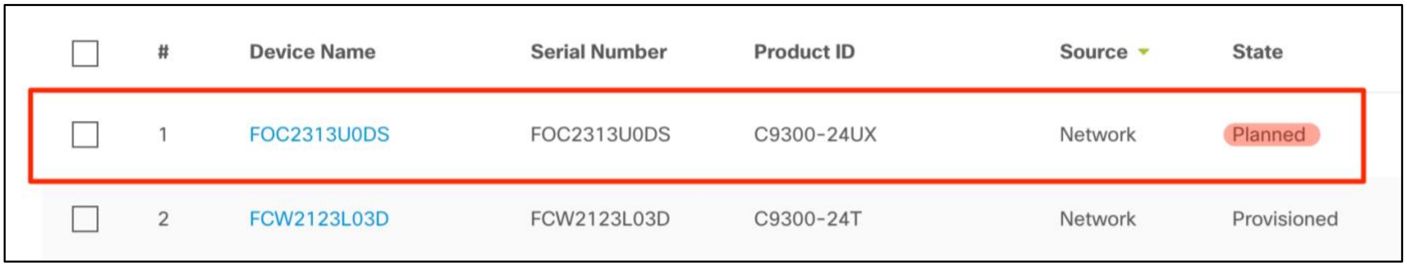
For large number of devices, bulk import using CSV format.

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.

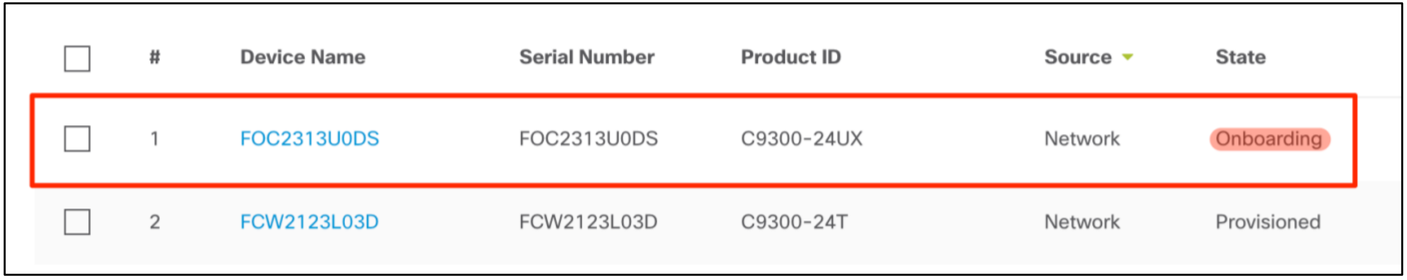
Step 11. Now watch the state of the switch change from **Unclaimed** to **Provisioned**

1. Unclaimed to Planned



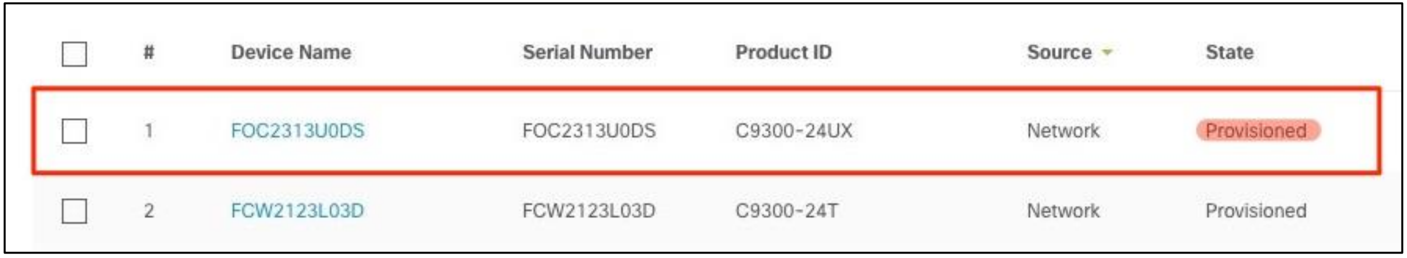
□	#	Device Name	Serial Number	Product ID	Source	State
□	1	FOC2313U0DS	FOC2313U0DS	C9300-24UX	Network	Planned
□	2	FCW2123L03D	FCW2123L03D	C9300-24T	Network	Provisioned

2. Planned to Onboarding



□	#	Device Name	Serial Number	Product ID	Source	State
□	1	FOC2313U0DS	FOC2313U0DS	C9300-24UX	Network	Onboarding
□	2	FCW2123L03D	FCW2123L03D	C9300-24T	Network	Provisioned

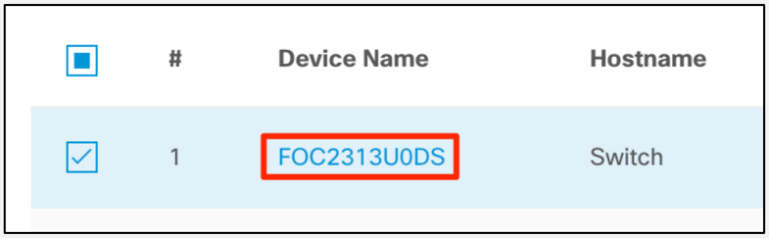
3. Onboarding to Provisioned



□	#	Device Name	Serial Number	Product ID	Source	State
□	1	FOC2313U0DS	FOC2313U0DS	C9300-24UX	Network	Provisioned
□	2	FCW2123L03D	FCW2123L03D	C9300-24T	Network	Provisioned

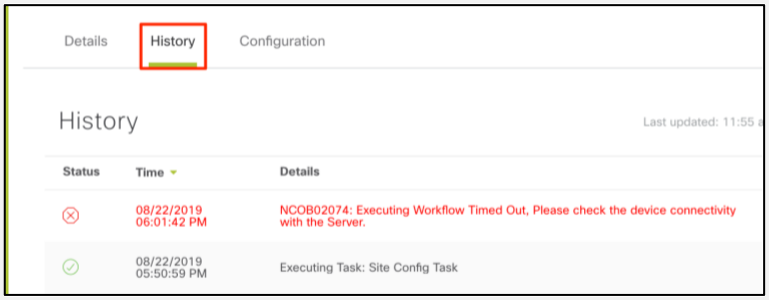
Tech tip

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.



■	#	Device Name	Hostname
☑	1	FOC2313U0DS	Switch

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

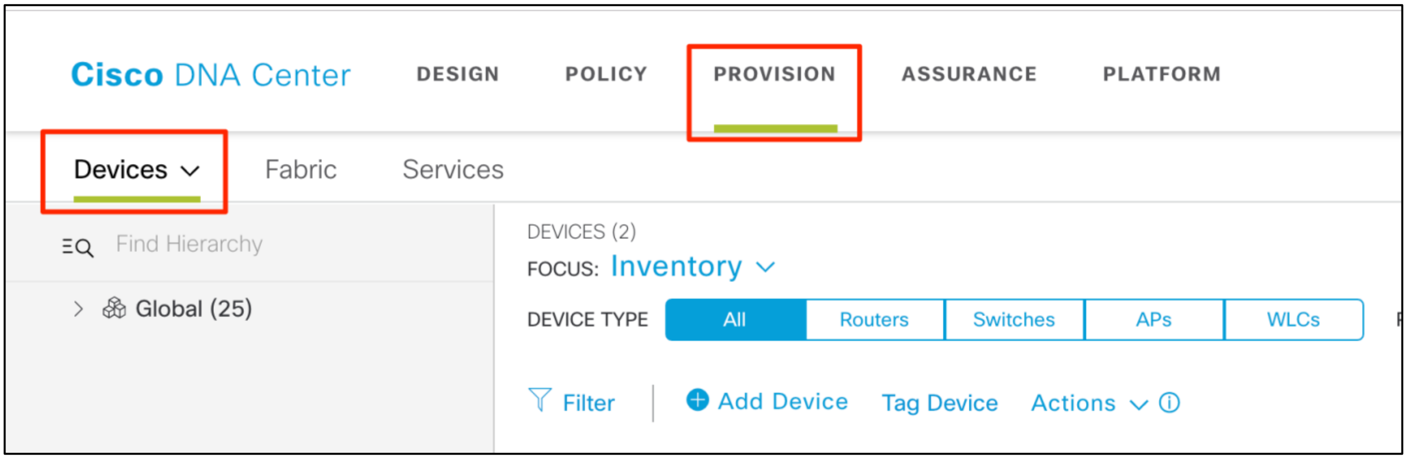


History

Last updated: 11:55 a

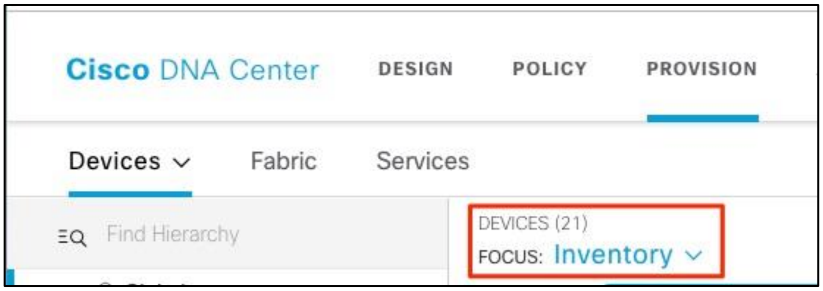
Status	Time	Details
⊗	08/22/2019 06:01:42 PM	NCOB02074: Executing Workflow Timed Out, Please check the device connectivity with the Server.
✓	08/22/2019 05:50:59 PM	Executing Task: Site Config Task

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

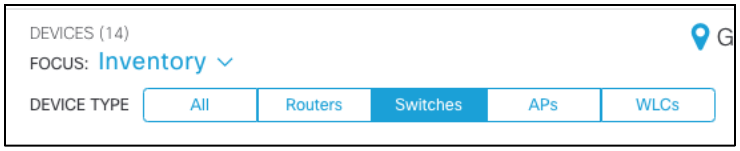


Step 13. Select the site hierarchy in the left pane.

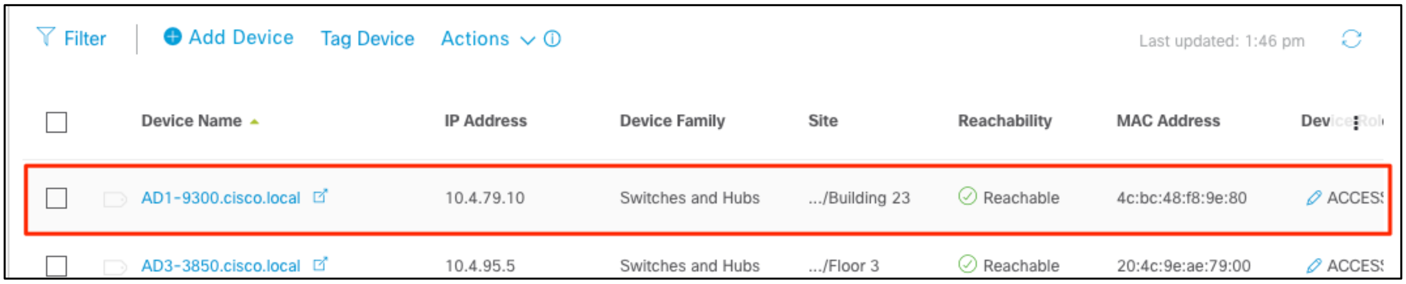
Step 14. Verify the devices focus is set to **Inventory**.



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



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



□	Device Name	IP Address	Device Family	Site	Reachability	MAC Address	Device Rol
□	AD1-9300.cisco.local	10.4.79.10	Switches and Hubs	.../Building 23	Reachable	4c:bc:48:f8:9e:80	ACCES
□	AD3-3850.cisco.local	10.4.95.5	Switches and Hubs	.../Floor 3	Reachable	20:4c:9e:ae:79:00	ACCES

Process 4: Simplified Return Material Authorization (RMA) process.

With hundreds and thousands of devices in an enterprise network, replacing older devices hardware becomes a complex process considering the steps involved such as identifying the replacement hardware with appropriate software version, configuration and copy paste errors involved in configuring the potential replacement and such. Cisco DNA Center offers a complete workflow to seamlessly identify, configure and replace the device hardware in the network.

Tech tip

RMA feature is available starting in Cisco DNA Center release 1.3.1.

Checklist before proceeding with RMA.

- Cisco DNA Center release 1.3.1 is installed.
- The replacement switch has the same exact SKU as the RMA device (faulty).
- Replacement switch is racked and powered up.
- All the connections are moved from the RMA device to the replacement switch.
- Replacement switch onboarded using PnP and is available as an unclaimed device in the PnP inventory.
- License on the replacement device should match the license on the faulty device to be replaced.
- Make sure the switch is in INSTALL MODE and not in BUNDLE MODE.
- Faulty switch that needs to be replaced must be in UNREACHABLE state.

Tech tip

For License Check

Run the following command on both the switches (faulty and replacement device) to verify the license:

```
show license right-to-use
```

Tech tip

For Mode Check

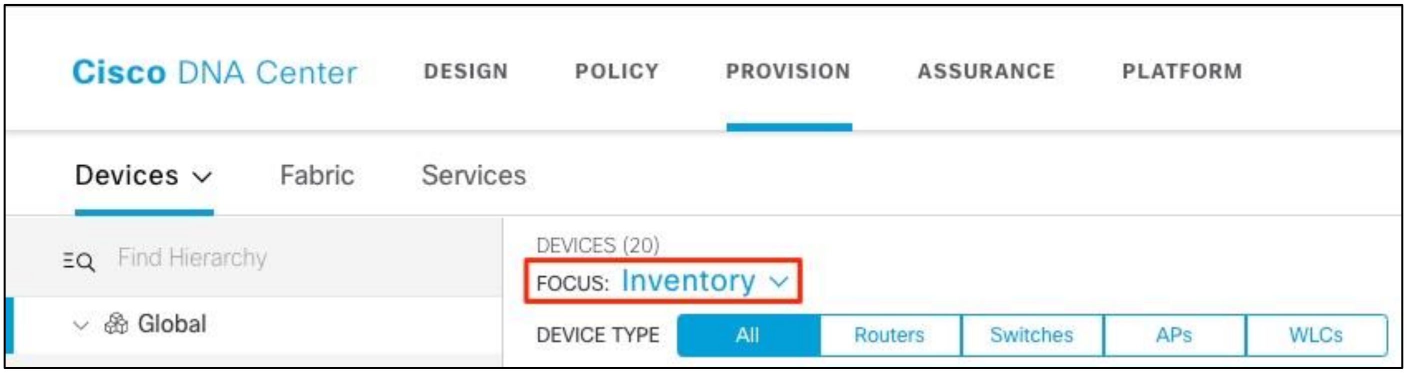
Run the following command on both the switches (faulty and replacement device) to verify the mode:

```
show version | begin Switch Ports
```

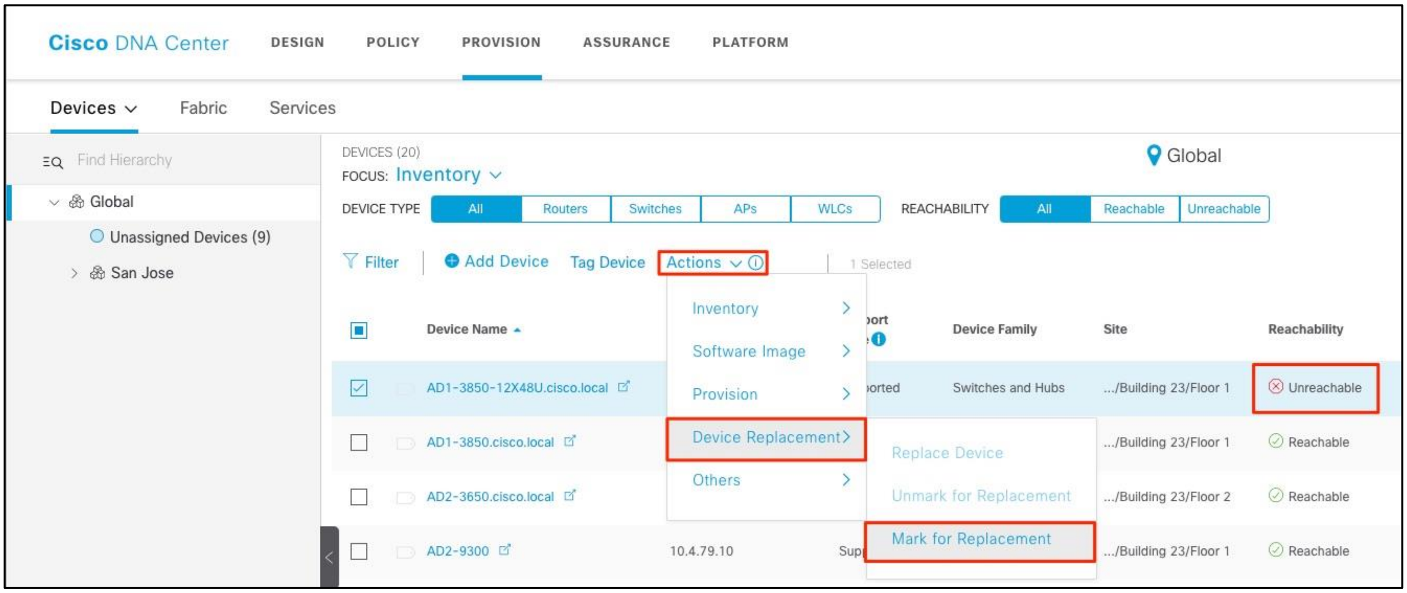
Follow the steps below to proceed with the RMA process:

Step 1. Login to Cisco DNA Center

Step 2. Navigate to **Provision > Devices** and make sure **Inventory** is selected as the **FOCUS**.



Step 3. Go to **Action** > **Device Replacement** and select **Mark for Replacement**.

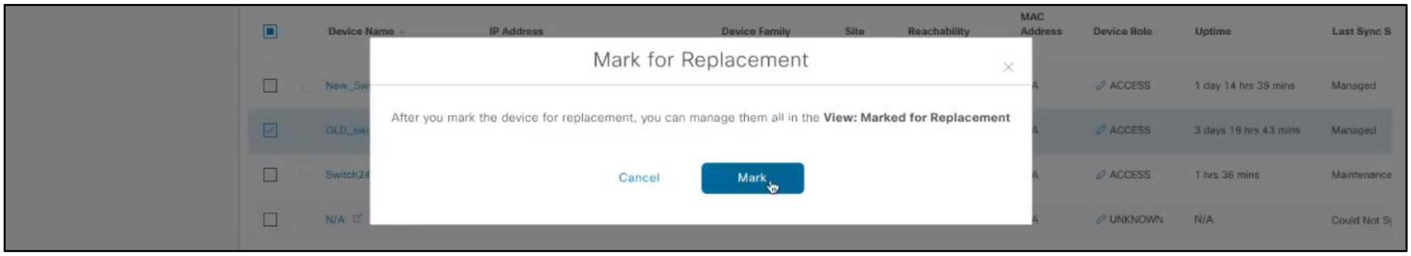


Device Name		ort	Device Family	Site	Reachability
☑ AD1-3850-12X48U.cisco.local		orted	Switches and Hubs	.../Building 23/Floor 1	Unreachable
□ AD1-3850.cisco.local				.../Building 23/Floor 1	Reachable
□ AD2-3650.cisco.local				.../Building 23/Floor 2	Reachable
□ AD2-9300	10.4.79.10	Sup		.../Building 23/Floor 1	Reachable

Tech tip

If the option to select **Mark Device for Replacement** in not available under the drop-down, then verify the current version of Cisco DNA Center is at least release 1.3.1. Also notice the selected device is in **Unreachable** state.

Step 4. Click **Mark**.

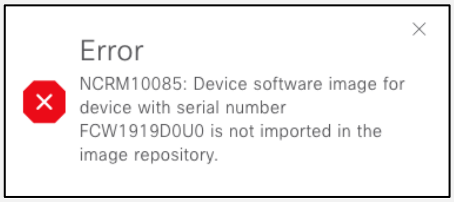


Mark for Replacement

After you mark the device for replacement, you can manage them all in the **View: Marked for Replacement**

Tech tip

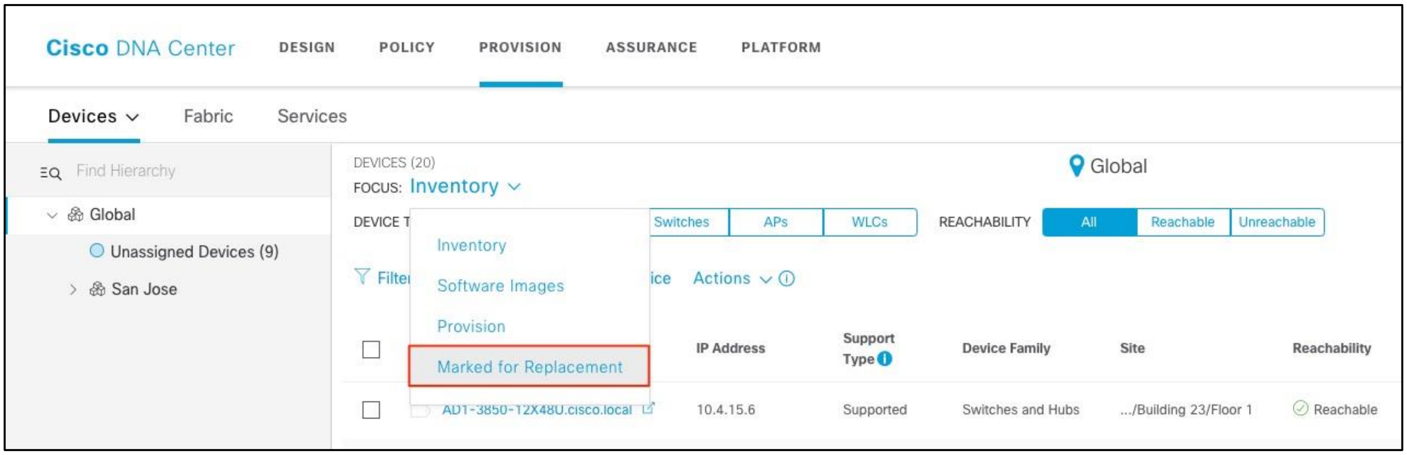
If there is an error **Error NCRM10085**, it means the software image version is not available in the image repository and needs to be uploaded and assigned to the switch family (example: Cisco Catalyst38xx switch)



Error

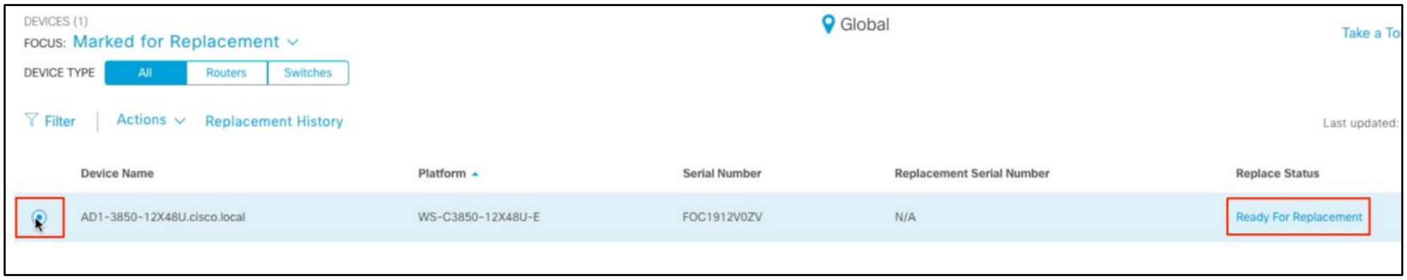
NCRM10085: Device software image for device with serial number FCW1919D0U0 is not imported in the image repository.

Step 5. From the **Inventory** drop-down, select **Marked for Replacement** to view all devices that have been marked for replacement,



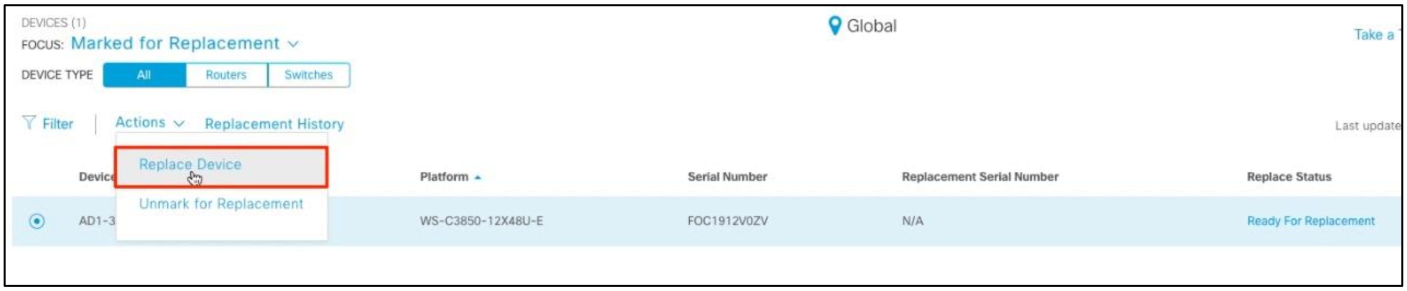
	IP Address	Support Type	Device Family	Site	Reachability
□ AD1-3850-12X48U.cisco.local	10.4.15.6	Supported	Switches and Hubs	.../Building 23/Floor 1	Reachable

Step 6. Select the radio button next the **Device Name** of the faulty device (example: AD1-3850-12X48U).



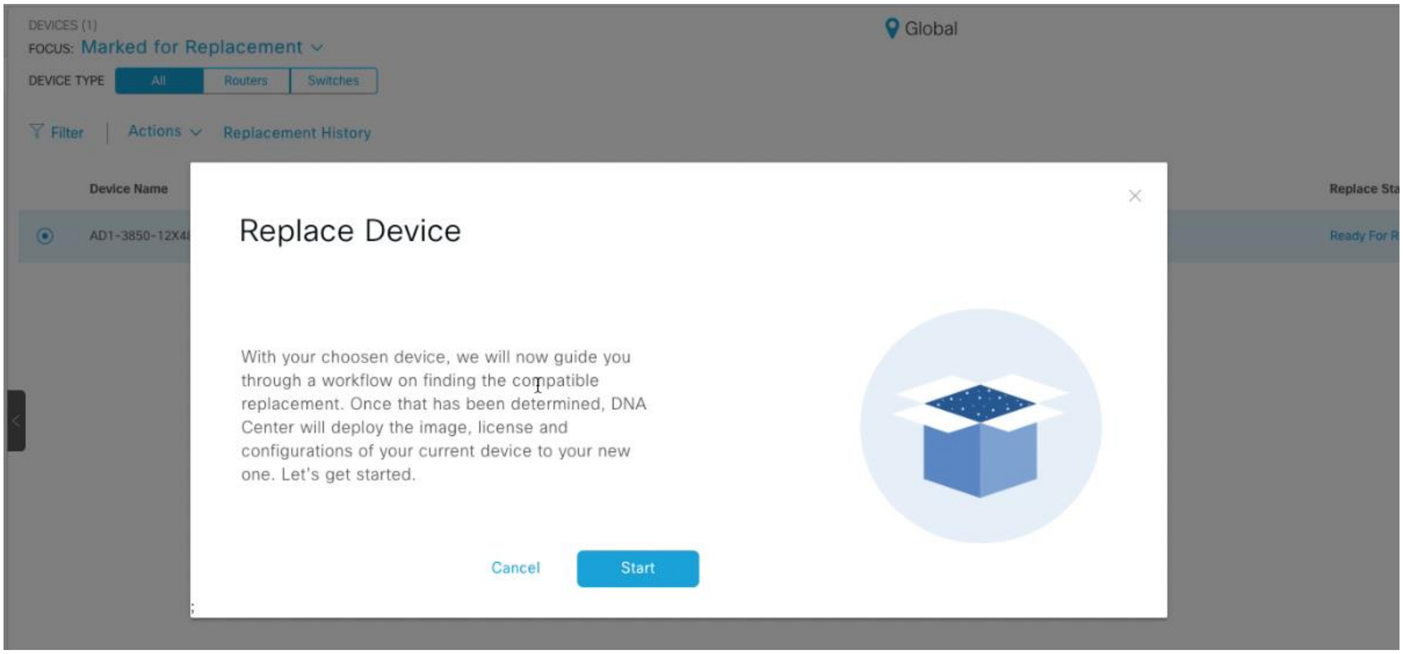
	Device Name	Platform	Serial Number	Replacement Serial Number	Replace Status
●	AD1-3850-12X48U.cisco.local	WS-C3850-12X48U-E	FOC1912V0ZV	N/A	Ready For Replacement

Step 7. Click **Replace Device** from **Actions** menu to start to RMA workflow.



	Devic	Platform	Serial Number	Replacement Serial Number	Replace Status
●	AD1-3	WS-C3850-12X48U-E	FOC1912V0ZV	N/A	Ready For Replacement

Step 8. Click **Start** to begin the workflow to help find a compatible replacement

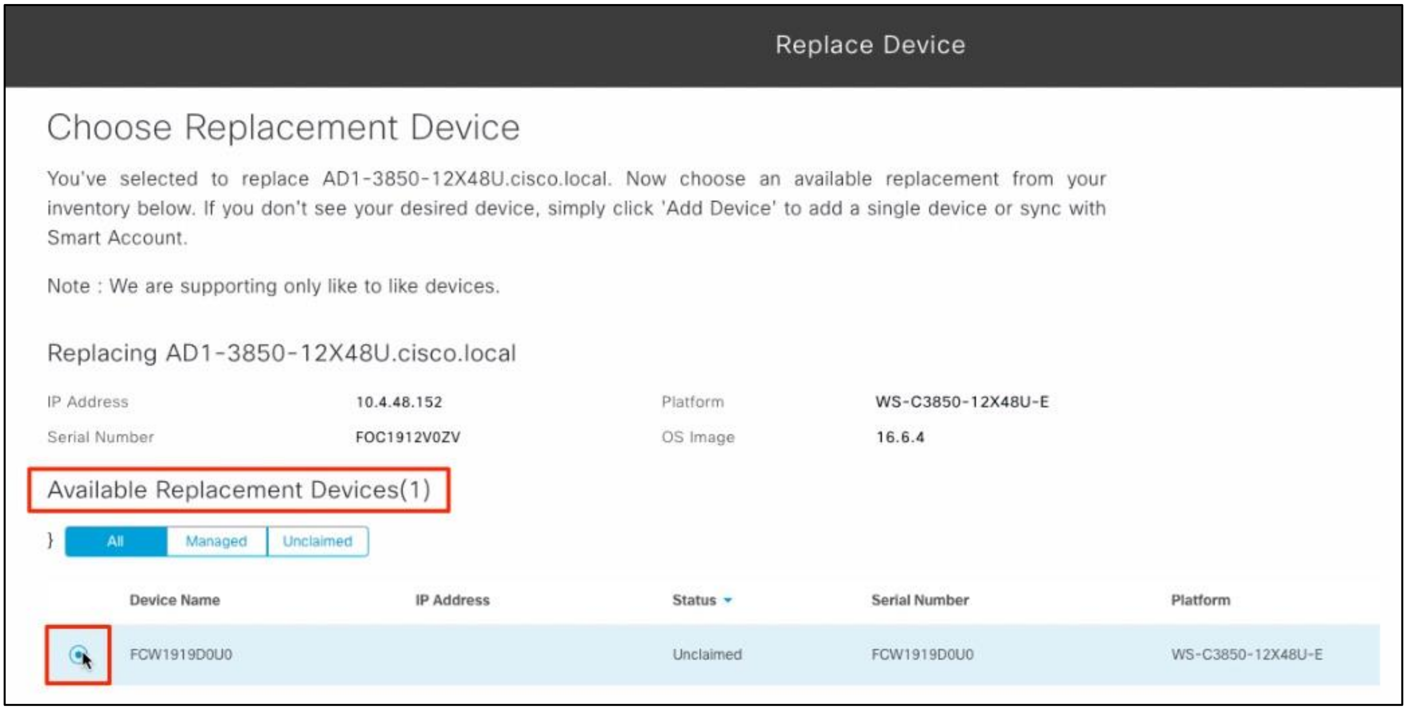


Replace Device

With your choosen device, we will now guide you through a workflow on finding the compatible replacement. Once that has been determined, DNA Center will deploy the image, license and configurations of your current device to your new one. Let's get started.

Tech tip
User can choose the replacement device from the list of managed devices or use the **Unclaimed** tab to add the replacement device to Cisco DNA Center using Cisco Plug and Play feature.

Step 9. Under **Available Replacement Devices**, select the **Unclaimed** device that will replace the faulty device and click **Next**.



Replace Device

Choose Replacement Device

You've selected to replace AD1-3850-12X48U.cisco.local. Now choose an available replacement from your inventory below. If you don't see your desired device, simply click 'Add Device' to add a single device or sync with Smart Account.

Note : We are supporting only like to like devices.

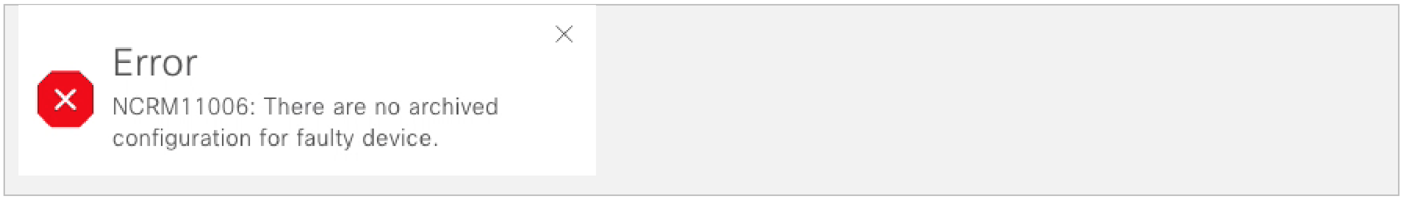
Replacing AD1-3850-12X48U.cisco.local

IP Address	10.4.48.152	Platform	WS-C3850-12X48U-E
Serial Number	FOC1912V0ZV	OS Image	16.6.4

Available Replacement Devices(1)

Device Name	IP Address	Status	Serial Number	Platform
FCW1919D0U0		Unclaimed	FCW1919D0U0	WS-C3850-12X48U-E

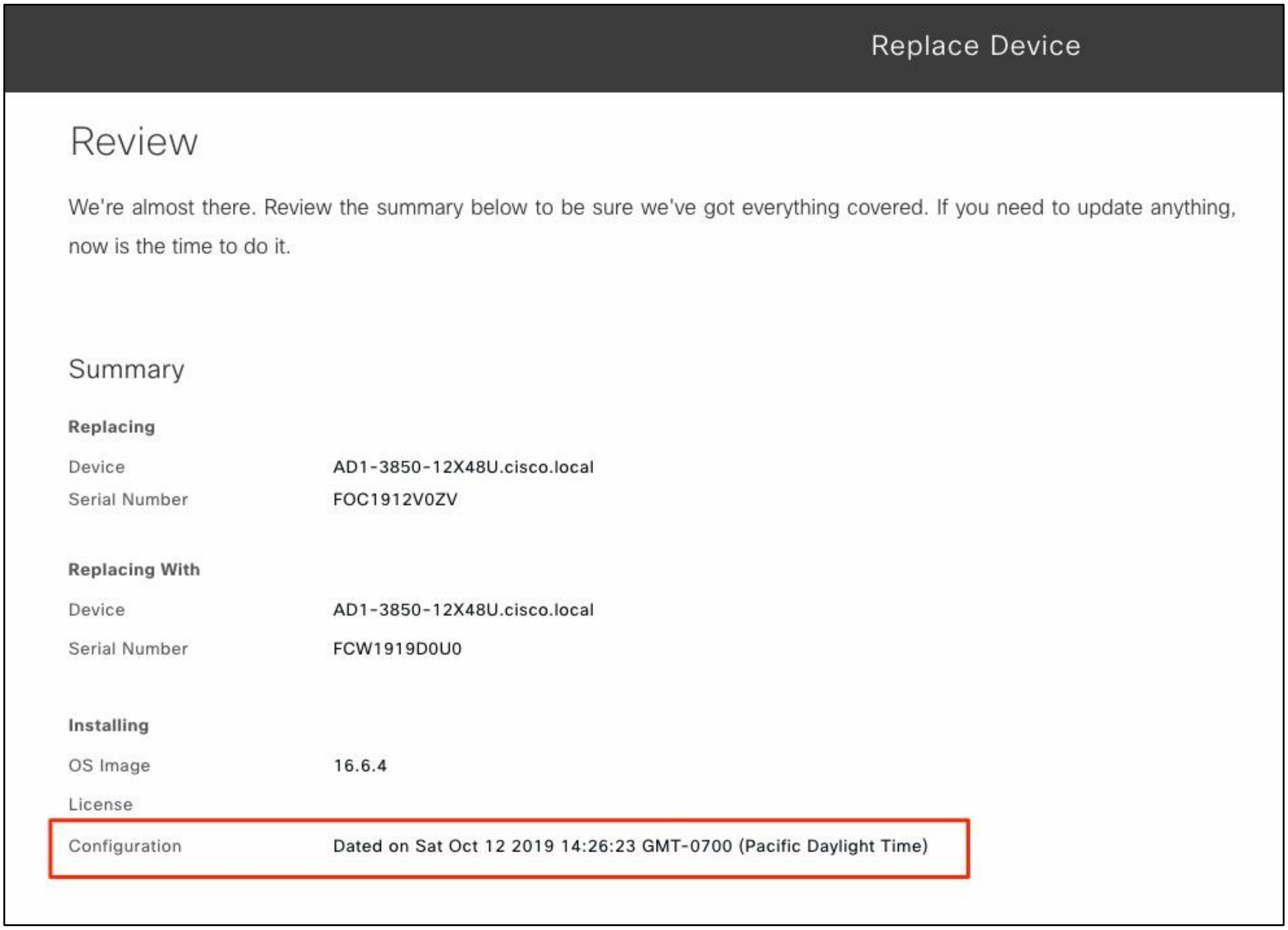
Tech tip
Error NCRM11006 indicates the RMA device has not been onboarded using the PnP function so the RMA process will not continue for that device.



Error

NCRM11006: There are no archived configuration for faulty device.

Step 10. Review **Summary** to make sure the faulty device is being replaced with the right new switch and click **Next**.



Review

We're almost there. Review the summary below to be sure we've got everything covered. If you need to update anything, now is the time to do it.

Summary

Replacing

Device	AD1-3850-12X48U.cisco.local
Serial Number	FOC1912V0ZV

Replacing With

Device	AD1-3850-12X48U.cisco.local
Serial Number	FCW1919D0U0

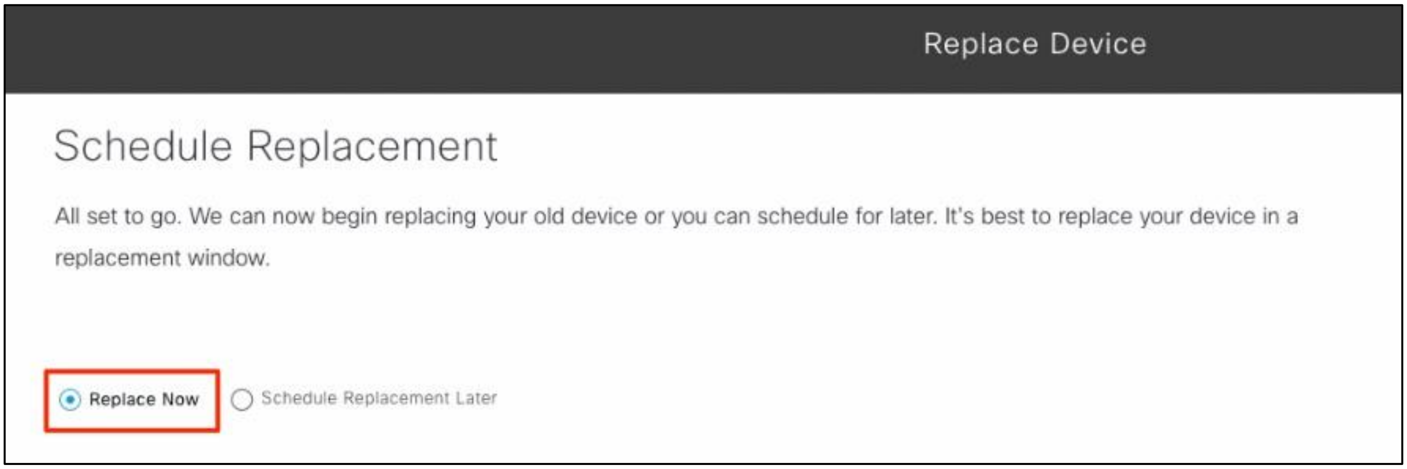
Installing

OS Image	16.6.4
License	
Configuration	Dated on Sat Oct 12 2019 14:26:23 GMT-0700 (Pacific Daylight Time)

Tech tip

As shown in the above summary, the **Configuration** for the RMA device was archived on the mentioned date and time stamp. This configuration will be applied to the new replacement device.

Step 11. Select **Replace Now** and click **Submit**.



Replace Device

Schedule Replacement

All set to go. We can now begin replacing your old device or you can schedule for later. It's best to replace your device in a replacement window.

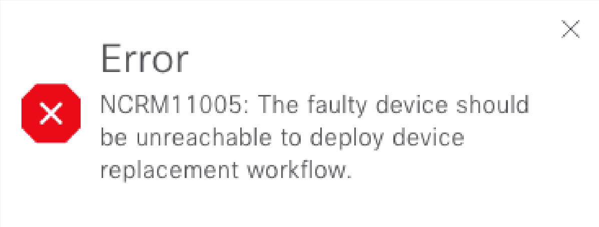
● Replace Now ○ Schedule Replacement Later

Tech tip

To schedule the RMA for later date and time select Schedule Replacement Later and select the appropriate parameter and click **Schedule**. Scheduling a software update was tested successfully.

Tech tip

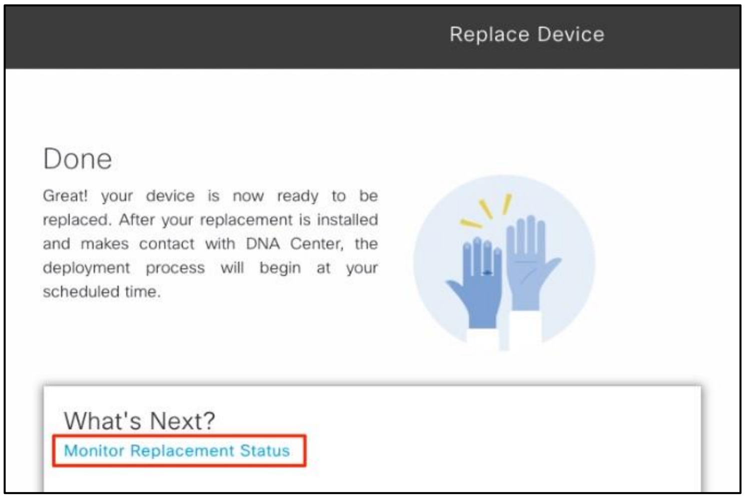
Error NCRM11005 indicates the RMA device is still in **REACHABLE** state and needs to be **UNREACHABLE**. Either have the RMA device physical unplugged or make changes in configurations to make in unreachable.



Error

NCRM11005: The faulty device should be unreachable to deploy device replacement workflow.

Step 12. Click **Monitor Replacement Status** once you are presented with the following screen.



Replace Device

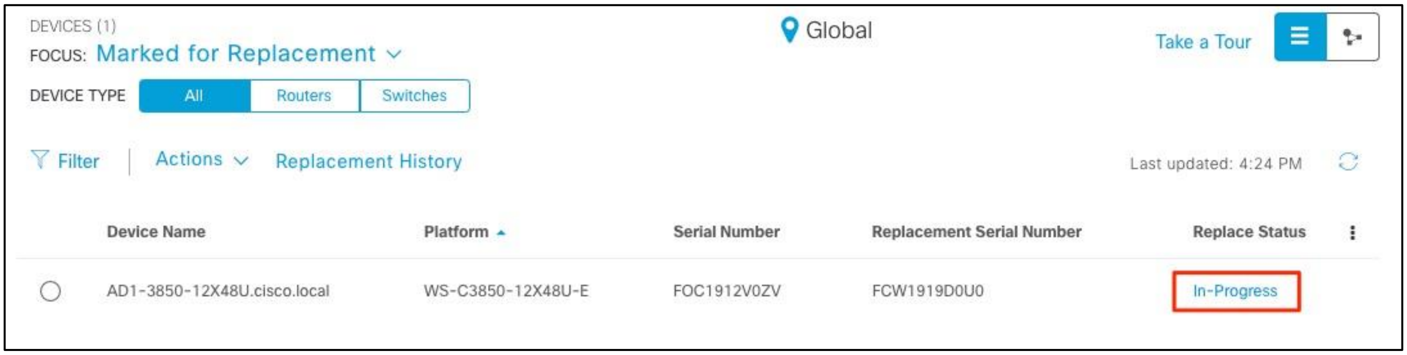
Done

Great! your device is now ready to be replaced. After your replacement is installed and makes contact with DNA Center, the deployment process will begin at your scheduled time.

What's Next?

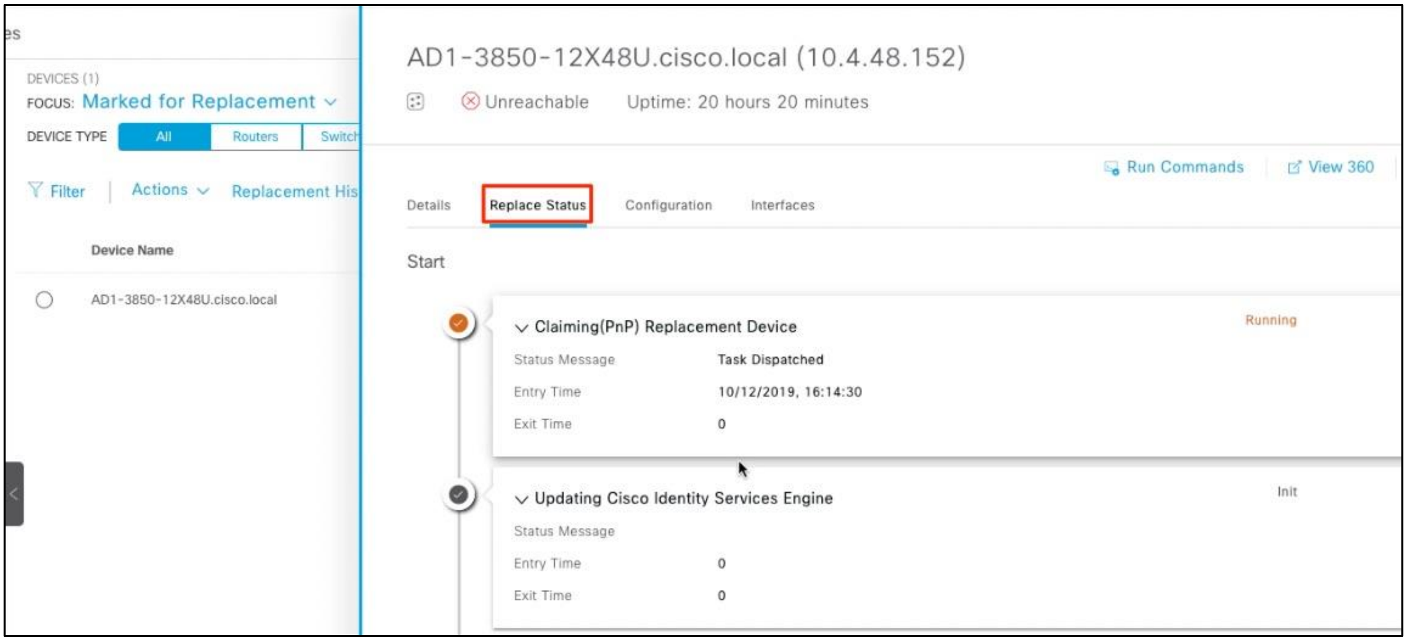
Monitor Replacement Status

Step 13. Click **In-Progress** under **Replace Status** for the RMA device.



Device Name	Platform	Serial Number	Replacement Serial Number	Replace Status
AD1-3850-12X48U.cisco.local	WS-C3850-12X48U-E	FOC1912V0ZV	FCW1919D0U0	In-Progress

Step 14. Select the **Replace Status** tab to monitor the progress of RMA process.



Claiming(PnP) Replacement Device — Running

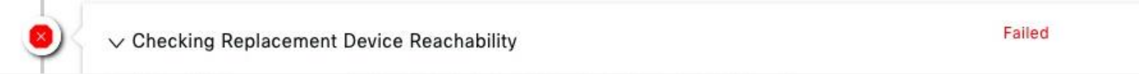
Status Message	Task Dispatched
Entry Time	10/12/2019, 16:14:30
Exit Time	0

Updating Cisco Identity Services Engine — Init

Status Message	
Entry Time	0
Exit Time	0

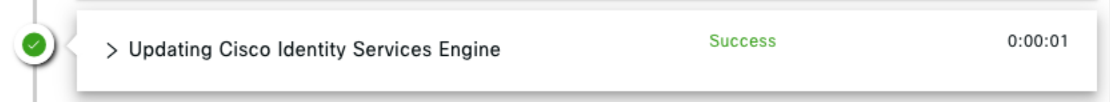
Tech tip

This process may take roughly 15-30 minutes if there are no errors. Hit the **Refresh** button to make sure the process has not failed due to an error.



Tech tip

As part of the RMA process Cisco ISE information is also applied to the device. But Cisco ISE is not a requirement for RMA use case.



After the RMA process is complete successfully, verify the configuration, image, and license on the new switch are exactly same.

Operate

Known Caveats

- The RMA process **does not** pull the configuration from the *Onboarding Configuration Template* or the *Cloud Day-N Template*. The configuration for the RMA devices is saved in the archive and applied to the new replacement device during RMA process.
- RMA supports replacement of similar devices only. For example, a Cisco Catalyst 3850 switch can be replaced only with another Cisco Catalyst 3850 switch. Also, the platform ID of the faulty and replacement devices must be the same.
- If the supervisor engine of the replacement device is different from that of the faulty device, the software image pushed to the replacement device may not be compatible, and the image activation in the replacement device goes to ROMMON mode.
- The RMA workflow supports device replacement only if:
  - Both faulty and replacement devices have the same extension cards.
  - The number of ports in both devices does not vary because of extension cards.
- Make sure that the replacement device is connected to the same port to which the faulty device was connected before.
- Cisco DNA Center does not support legacy license deployment. Also, the RMA workflow does not register the faulty device with CSSM, nor remove the faulty device license from CSSM.
- Cisco DNA Center provisions the replacement device with the running and VLAN configurations of the faulty device available in the archive. If any configuration changes were made to the old device after the latest archive, the replacement device may not have the latest configuration.
- If the replacement device onboards through PnP-DHCP functionality, make sure that the device gets the same IP address after every reload, and the lease timeout of DHCP is more than two hours.
- RMA workflow only supports enabling DNA licenses (DNA/Network Essentials and DNA/Network Advantage) on the replacement device. If the faulty device is running a legacy license (e.g. IP Base, IP Services and etc.), it requires users to enable the licensing on the replacement device outside RMA workflow, except when licenses on the faulty and replacement devices match.
- If users choose zero-touch RMA via PnP, RMA could fail if the replacement device gets the DHCP IP address from an IOS DHCP server initially and image upgrade is involved, since the replacement is very likely to get a new DHCP IP from IOS DHCP server after reboot.
- If the software image from the faulty device is not available in Cisco DNA Center Image repository, RMA workflow will fail since it cannot deploy the software image to the replacement device.

For more information you may also refer to Cisco DNA Center User Guide, Release 1.3.1.0.

Appendix A—Onboarding template example configuration

```
hostname $hostname
!
!
clock timezone PST -8 0
clock summer-time PDT recurring
ip arp inspection vlan ${data_Vlan}-${Voice_Vlan}
!
ip dhcp snooping vlan ${data_Vlan}-${Voice_Vlan}
no ip dhcp snooping information option
ip dhcp snooping
!
vlan ${Mgmt_Vlan}
name mgmt
!
vlan ${data_Vlan}
 name data
!
vlan ${Voice_Vlan}
 name voice
!
vlan ${AntiHopping_Vlan}
 name AntiHoppingVLAN
!
interface Port-channel$Portchannel
 description EtherChannel Link to D2-3850_Stack
 switchport trunk native vlan ${AntiHopping_Vlan}
 switchport trunk allowed vlan ${data_Vlan},${Voice_Vlan},${Mgmt_Vlan}
 switchport mode trunk
 logging event trunk-status
 logging event bundle-status
 load-interval 30
!
interface range $interface_type1 $port_range1
 switchport access vlan ${data_Vlan}
 switchport mode access
 switchport voice vlan ${Voice_Vlan}
 switchport port-security maximum 11
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 ip arp inspection limit rate 100
 load-interval 30
 spanning-tree portfast
 ip verify source
 ip dhcp snooping limit rate 100
!
interface TenGigabitEthernet1/1/7
 description Uplink D2-3850_Stack
 switchport trunk native ${AntiHopping_Vlan}
 switchport trunk allowed ${data_Vlan},${Voice_Vlan},${Mgmt_Vlan}
 switchport mode trunk
 logging event trunk-status
 logging event bundle-status
 load-interval 30
 channel-protocol lacp
 channel-group $Portchannel mode active
!
interface TenGigabitEthernet1/1/8
 description Uplink D2-3850_Stack
 switchport trunk native ${AntiHopping_Vlan}
 switchport trunk allowed ${data_Vlan},${Voice_Vlan},${Mgmt_Vlan}
 switchport mode trunk
 logging event trunk-status
 logging event bundle-status
 load-interval 30
 channel-protocol lacp
 channel-group $Portchannel mode active
!
interface Vlan${Mgmt_Vlan}
 ip address ${Mgmt_IPAdddr} 255.255.255.0
!
ip default-gateway ${Default_GW}
ip http server
ip http secure-server
ip http client source-interface Vlan${Mgmt_Vlan}
!
```

Appendix B— Hardware and software used for validation

Table 1. Hardware and software

Functional area	Product	Software version
Controller (PnP Server)	Cisco DNA Center	1.3.1.2
Device to Onboard (PnP Agent)	Catalyst 9300 Switch Series	16.09.01
RMA Device (faulty)	C3850-12X48U	16.06.04
Replacement Device (Good)	C3850-12X48U	16.06.04

Appendix C—Glossary

Cisco DNA Cisco Digital Network Architecture

Cisco PnP Cisco Plug and Play

RMA Return Material Authorization

SSL Secure Sockets Layer

VLAN Virtual Local Area Network

Feedback

For comments and suggestions about this guide and related guides, join the discussion on Cisco Community.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.