

Unlocking the Automation Power in Catalyst Center for wired and wireless networks

cisco Live !

Adam Radford
Distinguished Solutions Engineer
@adamradford123

Cisco Webex App

Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until 14 November 2025.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKOPS2697>

Agenda

- 01 Intent Based Automation Framework
Templates
AAA**
- 02 Per-Device / Config at Scale**
- 03 Automation beyond the UI: API's**

Evolution of Automation



Intent Based Automation Framework Templates AAA

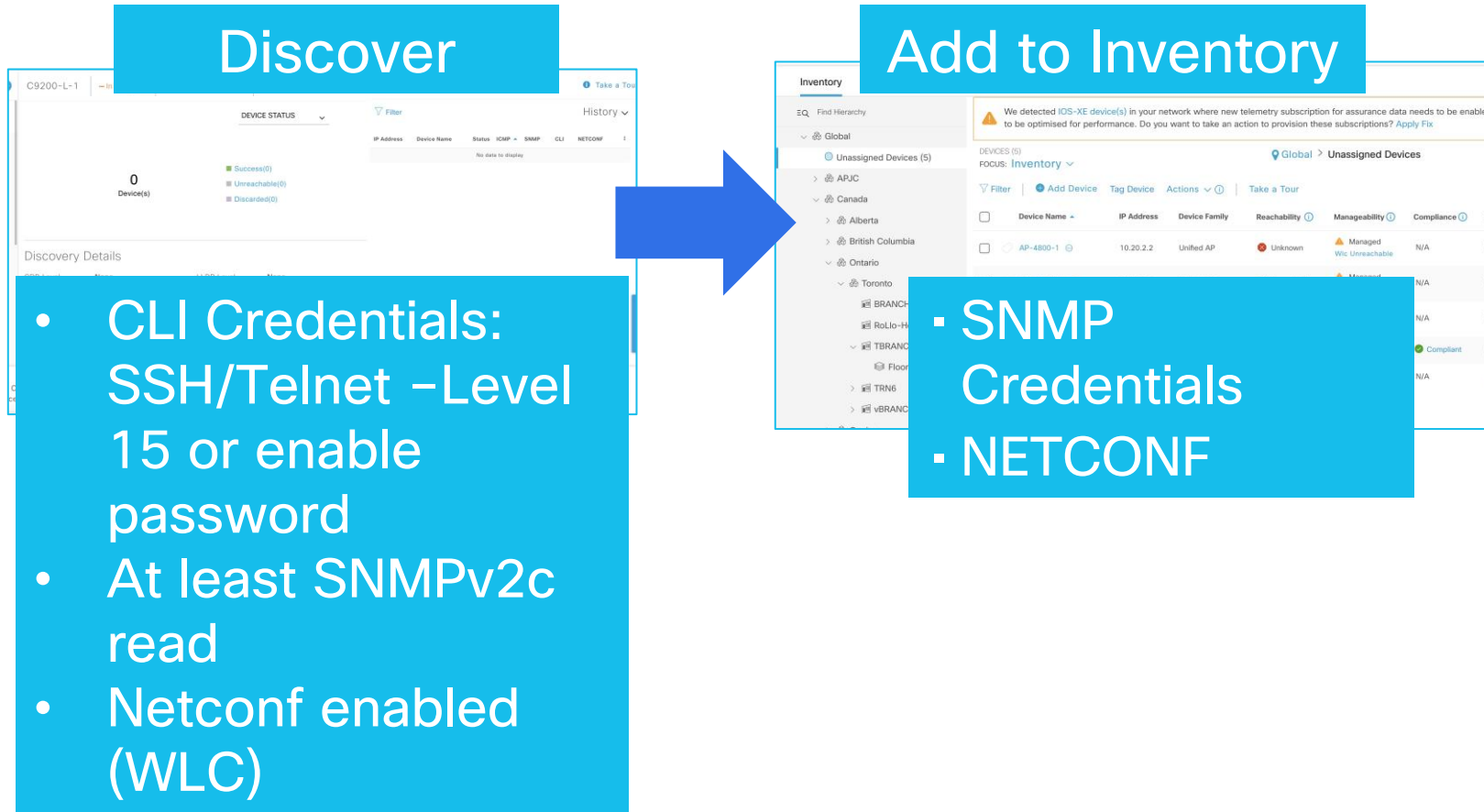
Steps for Device Provisioning using Intent Based Automation

- 01** Onboard Devices to Catalyst Center
- 02** Assign Devices to Sites
- 03** Populate Network Settings (Servers/Wireless)
- 04** Create Network Profiles
- 05** Provision Devices

Steps for Device Provisioning using Intent Based Automation

- 01** Onboard Devices to Catalyst Center
- 02** Assign Devices to Sites
- 03** Populate Network Settings (Servers/Wireless)
- 04** Create Network Profiles
- 05** Provision Devices

Brownfield device onboarding



Note: Devices can be onboarded through other methods like PnP, PDMT and others

Steps for Device Provisioning using Intent Based Automation

- 01 Onboard Devices to Catalyst Center
- 02 Assign Devices to Sites
- 03 Populate Network Settings (Servers/Wireless)
- 04 Create Network Profiles
- 05 Provision Devices

Brownfield device onboarding

Discover

- CLI Credentials: SSH/Telnet –Level 15 or enable password
- At least SNMPv2c read
- Netconf enabled (WLC)

Add to Inventory

- SNMP Credentials
- NETCONF

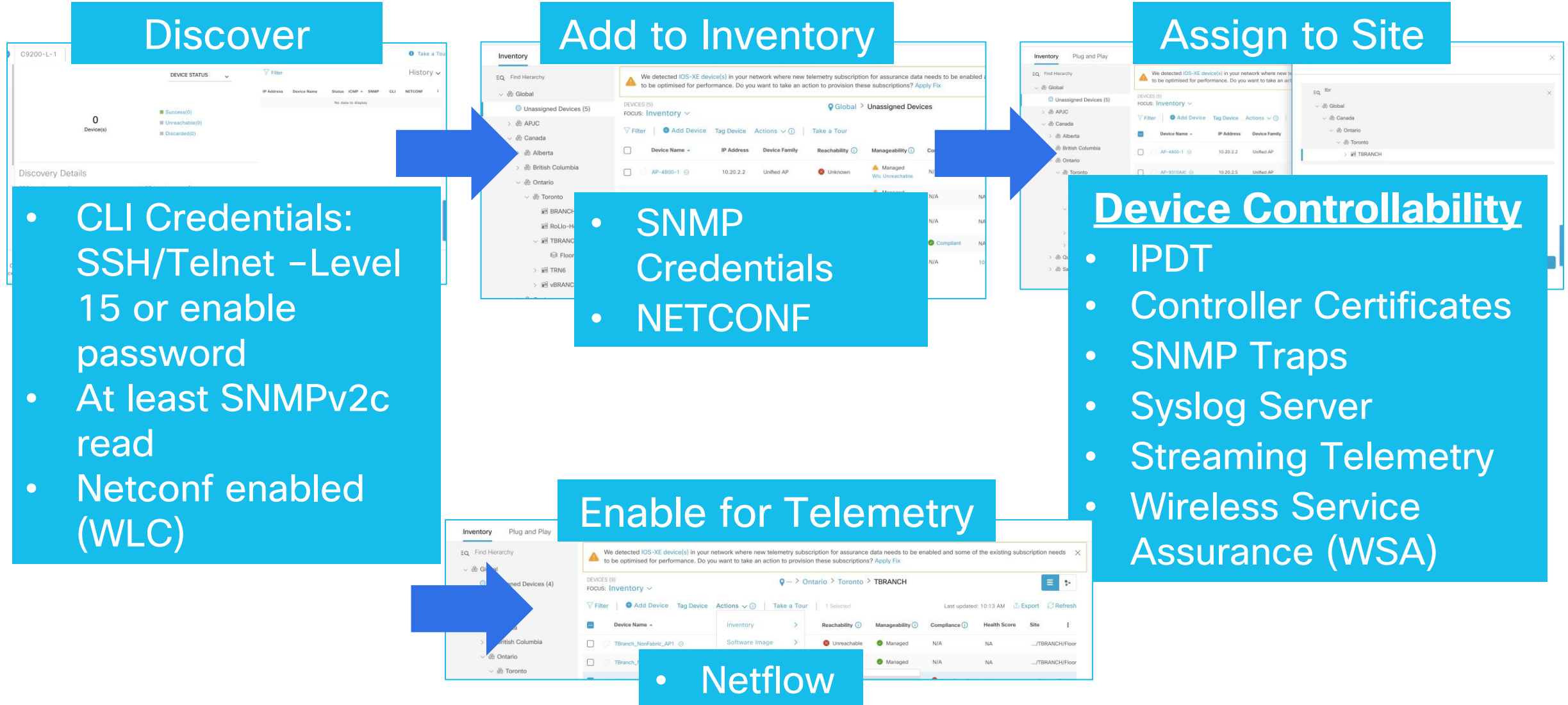
Assign to Site

Device Controllability

- IPDT
- Controller Certificates
- SNMP Traps
- Syslog Server
- Streaming Telemetry
- Wireless Service Assurance (WSA)

Enable for Telemetry

- Netflow

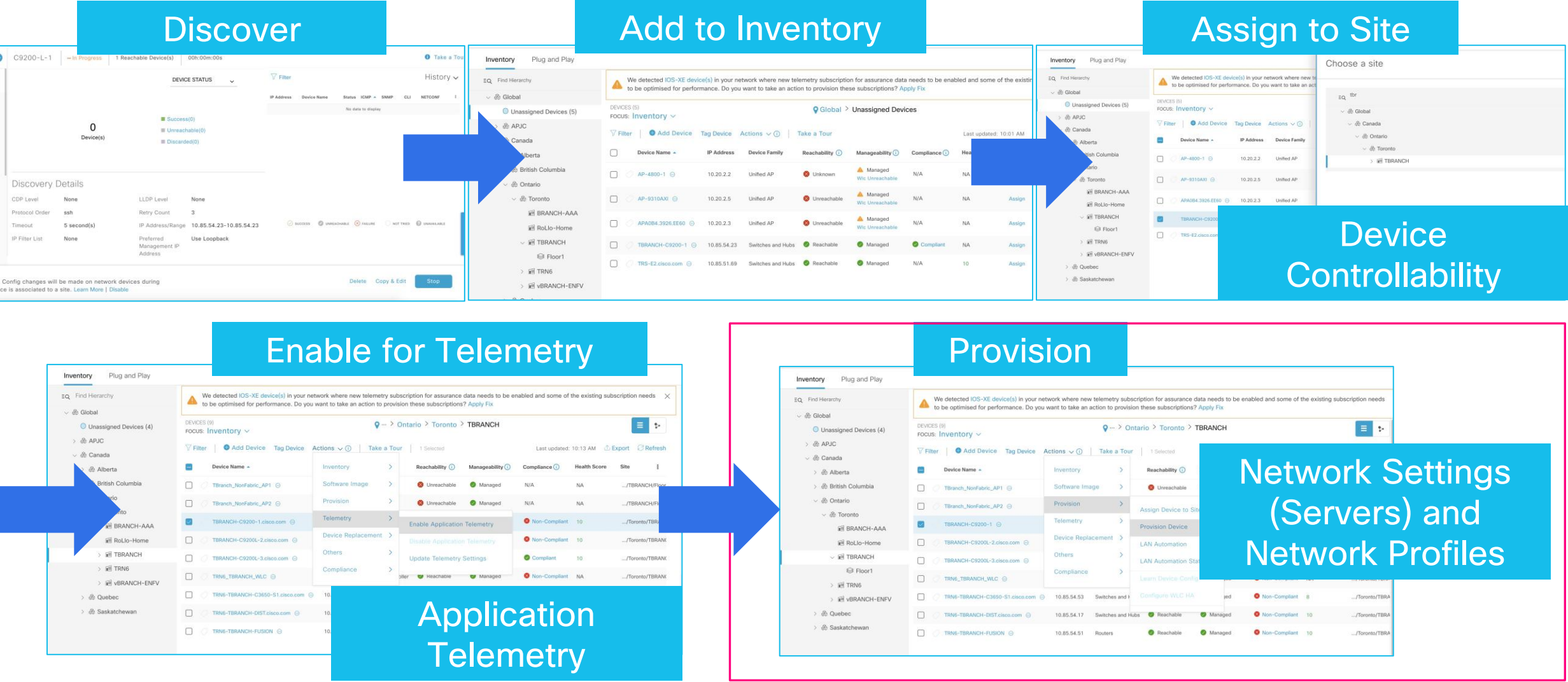


Steps for Device Provisioning using Intent Based Automation

- 01 Onboard Devices to Catalyst Center
- 02 Assign Devices to Sites
- 03 Populate Network Settings (Servers/Wireless)
- 04 Create Network Profiles
- 05 Provision Devices

Associated to Site

Brownfield device automation



Network Settings - Servers

- AAA (Network Client/Endpoint)
- DHCP
- DNS and Domain
- Stealthwatch Flow Destination
- Image Distribution
- NTP
- Time Zone
- Message of the Day

Configure external network servers, assign time zones to sites, and customize device CLI login banner messages. The system will deploy these settings when devices are provisioned.

✓ AAA ✓

Select AAA or Cisco Identity Services Engine (ISE) servers for network, client, and endpoint authentication.

Network Client/Endpoint

☐ Add AAA servers

✓ DHCP 🔍 ✓

Specify one or more dedicated DHCP servers for managing client device networking configuration.

☒ Add DHCP servers

IP Address*
10.85.54.175 +

✓ DNS 🔍 ✓

Configure your network's domain name and specify DNS servers for hostname resolution.

☒ Set a domain name

☒ Add DNS servers

Domain Name*
cirrus.cloud

IP Address* 64.102.6.247 IP Address* 10.85.54.175

Network Settings - Servers

Hierarchy facilitates the consistency of network settings in portions of the network

The screenshot displays the Cisco DNA Center configuration interface for Network Settings - Servers. The left sidebar shows a hierarchy of locations, with 'BRANCH-AAA' selected under 'Toronto'. The main content area is divided into two sections: 'AAA Server' and 'NTP Server'.

AAA Server Configuration:

- Network Tab:** Shows a table of servers with columns for 'Servers' and 'Protocol'. The 'Servers' column contains '10.85.54.185' and the 'Protocol' column contains 'RADIUS'.
- Client/Endpoint Tab:** Shows a table of servers with columns for 'Client/Endpoint' and 'Protocol'. The 'Client/Endpoint' column contains '10.85.54.185' and the 'Protocol' column contains 'RADIUS'.

NTP Server Configuration:

- NTP Tab:** Shows a table of NTP servers with columns for 'NTP' and 'Additional NTP'. The 'NTP' column contains '10.81.254.131' and the 'Additional NTP' column contains '10.81.254.202' and '171.68.38.65'.
- Additional NTP Tab:** Shows a table of additional NTP servers with columns for 'Additional NTP' and 'Protocol'. The 'Additional NTP' column contains '10.85.54.175' and the 'Protocol' column contains 'RADIUS'.

Time Zone: Set to 'US/Eastern (EDT)'.

Message of the day: 'Welcome to C9200L-1 - Managed by Cisco DNA Center.'

Steps for Device Provisioning using Intent Based Automation

- 01 Onboard Devices to Catalyst Center
- 02 Assign Devices to Sites
- 03 Populate Network Settings (Servers/Wireless)
- 04 Create Network Profiles
- 05 Provision Devices

Associated to Site

Network Profiles

- CLI Templates (Wired & Wireless)
- SSID's (Wireless)
- AP Zones (Wireless)
- Model Configs (Wireless)
- Advances Settings (Wireless)

SSID

GUHOA

WLAN Profile Name

GUHOA_6c12b73c94_profile

Policy Profile Name

GUHOA_6c12b73c94_profile

Fabric

☐ Yes ☒ No

802.11be Profile Name

☐ Enable SSID Scheduler

TRAFFIC SWITCHING

☒ Interface ☐ VLAN Group

Interface Name*

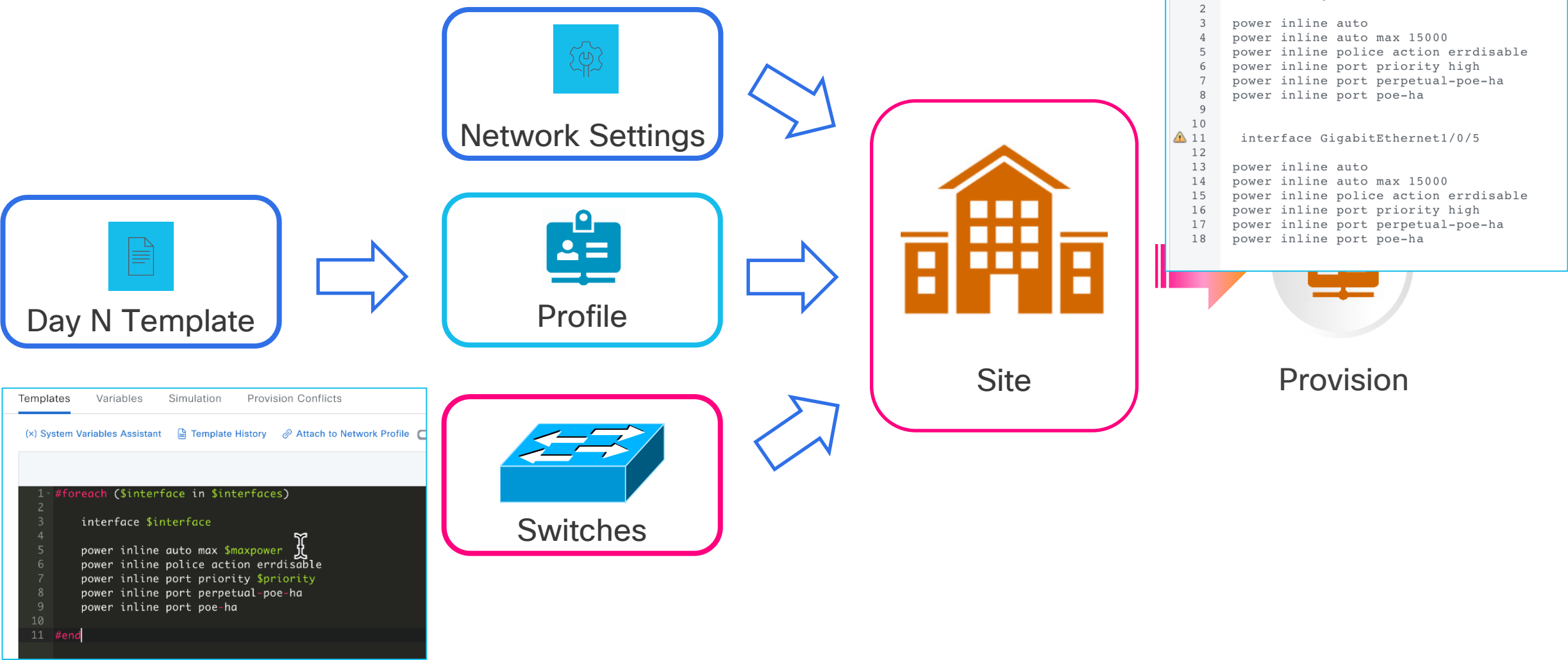
data

Do you need Anchor for this SSID?

☐ Yes ☒ No

☐ Flex Connect Local Switching

Catalyst Center - Intent Based Configuration Switches

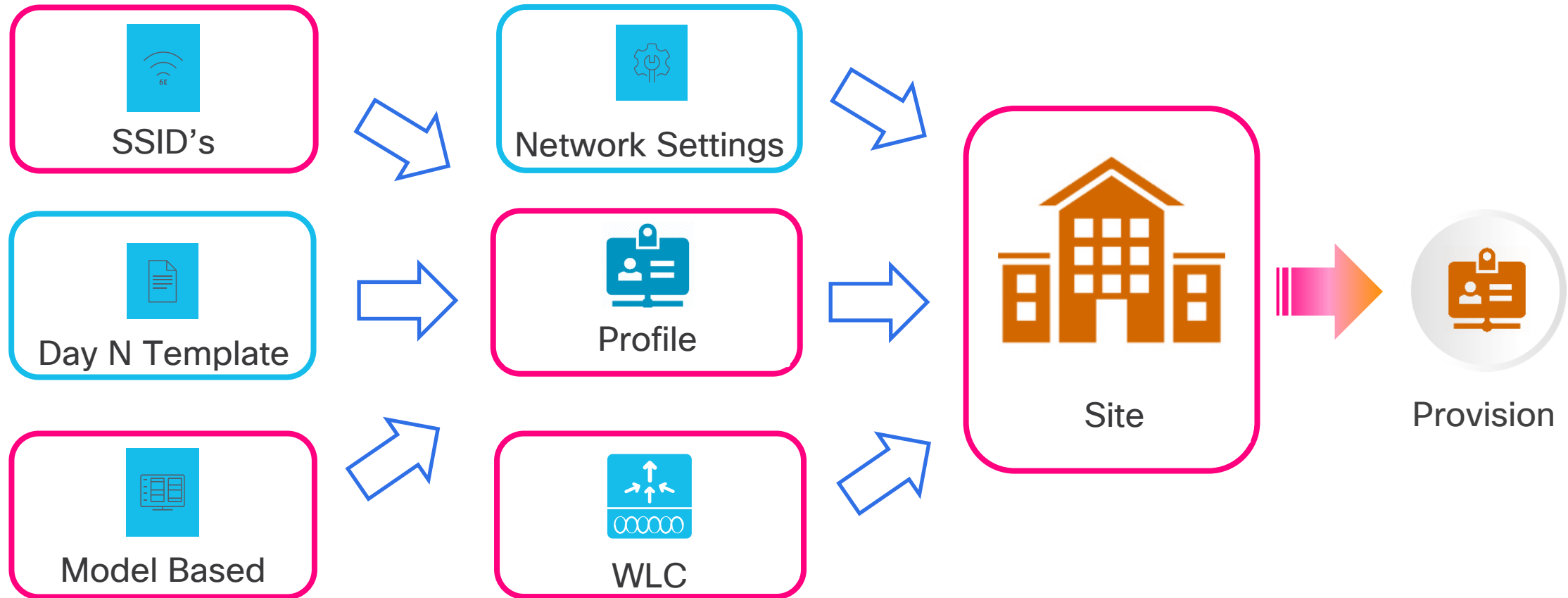


Templates Variables Simulation Provision Conflicts

(x) System Variables Assistant Template History Attach to Network Profile

```
1- #foreach ($interface in $interfaces)
2
3 interface $interface
4
5 power inline auto max $maxpower
6 power inline police action errdisable
7 power inline port priority $priority
8 power inline port perpetual-poe-ha
9 power inline port poe-ha
10
11 #end
```

Wireless Provisioning – intent based



A site can only be mapped to one profile
A profile can contain many sites

Step 1 : SSID Configuration

Design->Network Settings->Wireless



Cisco DNA Center

Wireless SSID

Basic Settings

Fill the information like name, wireless options, state and network to complete the basic setup of SSID

1

Except L2 Security, AAA Configuration, Mac Filtering, NAS-ID and Client Rate Limit, all other parameters will be inherited to overridden S

Wireless Network Name (SSID)

SSID1

WLAN Profile Name*

SSID1_profile

Policy Profile Name

SSID1_profile

Wireless Option

Multi band operation (2.4GHz, 5GHz, 6GHz)

Multi band operation with Band Select

5GHz only

2.4GHz only

6GHz Only

Primary Traffic Type

VoIP (Platinum)

SSID STATE

Admin Status

Broadcast SSID

Cisco DNA Center

Wireless SSID

Security Settings

Configure the security level and authentication, authorization, & accounting for SSID

1

One (1) Warning Alert and One (1) Information Alert on this page. Collapse to hide.

1

One (1) Warning Alert

For 2.4GHz+ 5GHz only, enable WPA2 , WPA3 is optional. For 2.4GHz+ 5GHz+6GHz to be operational on IOS devices version 17.7 and above, enable WPA3 and disable WPA2.

1

One (1) Information Alert

Except L2 Security, AAA Configuration, Mac Filtering, NAS-ID and Client Rate Limit, all other parameters will be inherited to overridden Site(s).

SSID Name: SSID1 (Enterprise)

Level of Security

Enterprise

Personal

Open Secured

Open

WPA2

WPA3

Most secure

User Credentials are validated with 802.1x Radius server to authenticate clients to the wireless network. WPA3 feature is supported for Wireless Controller version 8.10 & above, For Catalyst 9800 Controllers version 16.12 & above.

Authentication, Authorization, and Accounting Configuration

AAA Configured (1)

AAA Override

Fast Lane

Mac Filtering

Deny RCM Clients

Enable Posture

Cisco DNA Center

Wireless SSID

Advanced Settings

Configure the advanced fields to complete SSID setup.

1

Except L2 Security, AAA Configuration, Mac Filtering, NAS-ID and Client Rate Limit, all other parameters will be inherited to overridden Site(s).

SSID Name: SSID1 (Enterprise)

Fast Transition (802.11i)

Adaptive

Enable

Disable

Over the SS

MFP Client Protection

Optional

Required

Disabled

Protected Management Frame (802.11w)

Optional

Required

Disabled

11k

Neighbor List

Session Timeout

11v BSS Transition Support

BSS Max Idle Service

Client User Idle Timeout

Radius Client Profiling

NAS-ID

NAS-ID Op 1

Configure CCKM

Configure Client Rate Limit

Client Rate Limit (in bits per second)

Coverage Hole Detection



Step 2: Associate to wireless network profile



Associate SSID to Profile

Select a Profile on the left or Add Profile and click 'Associate' to associate the SSID to Profile.

+

Add Profile

Search

9800

BrownfieldProfile_7

Coles Secure

Flex

flex profile

fred

pnp2

pnp-DC-syd2

pnp-wireless

R1.0

R3.0

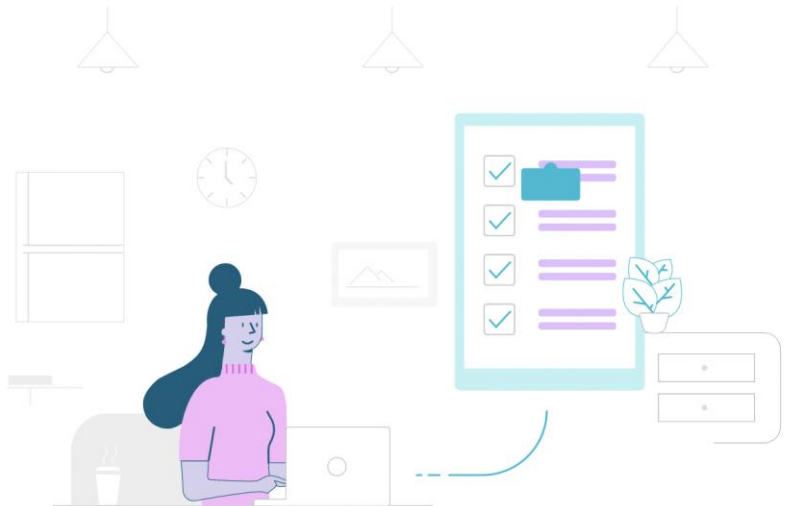
sda

thirdwheel

Voice Clients

wlc-config

2 profile(s) associated.



Can then assign a set of sites to the wireless network profile

© 2025 Cisco and/or its affiliates. All rights reserved.

BRKOPS-2697



Provision one WLC



Devices (2) Focus: Provision

deviceName: (9800-pnp)

1 Selected Add Device Tag Actions

Device Name	Inventory	Software Image	Device Family	Site
9800-pnp				
9800-pnp	Provision		Assign Device to Site	Global/DC - syd
9800-pnp2	Telemetry		Provision Device	Global/DC - syd
	Device Replacement		LAN Automation	

Inventory / Provision Devices

1 Assign Site

2 Configuration

3 Model Configuration

4 Advanced Configuration

5 Summary

Serial Number

9P015USKRB8

Devices

9800-pnp

Global/DC - syd

Select managed sites



Reference

Inventory / Provision Devices

1 Assign Site 2 Configuration 3 Model Configuration 4 Advanced Configuration 5 Summary

9800-pnp

Serial Number 9P015USKRB8

Devices 9800-pnp

WLC Role

☒ Active Main WLC ¹

☐ Anchor

Managed AP location(s)

[Select Primary Managed AP Locations](#)

[Select Secondary Managed AP Locations](#)

☐ Skip AP Provision ¹

- The sites WLC manages determines the relevant wireless network profiles (WNP)
- Secondary sites are for N+1 config
- AP are assigned to a site -> configuration pushed to AP
- Some commands are disruptive, so option to skip AP provisioning until later

Inventory / Provision Devices

1 Assign Site 2 Configuration 3 Model Configuration 4 Advanced Configuration 5 Summary

9800-pnp

Serial Number 9P015USKRB8

Devices 9800-pnp

☐ Skip AP Provision ¹

Rolling AP Upgrade

☐ Enable

AP Reboot Percentage 25 ¹

Managed AP Location

Search Hierarchy

- ☐ Global
- > ☐ AUS
- > ☐ brownfield
- > ☐ C
- ☐ DC - syd
- ☐ deak
- > ☐ EK
- > ☒ HongKong

SSID interfaces



L3 configuration is not best practice

Network Devices / Provision Devices

1 Assign Site

2 Configuration

3 Model Configuration

4 Advanced Configuration

5 Summary

pnp-9800

Serial Number
9P015USKRB8

Devices
pnp-9800

WLC Role
☒ Active Main WLC [?](#)
☐ Anchor

Managed AP location(s) [?](#)
[Managing 3 Primary location\(s\)](#)
[Select Secondary Managed AP Locations](#)

☐ Skip AP Provision [?](#)

Assign Interface

Interface Name	Interface Group Name	VLAN ID	IP Address	Gateway IP Address	Subnet Mask(in bits)
hk_ssid	-	14	IP Address	Gateway IP Address	Subnet Mask

1 Records

Show Records: 25

1 - 1

Rolling AP Upgrade

☐ Enable

AP Reboot Percentage
25

CancelNext

Template



Reference

Inventory / Provision Devices

1 Assign Site

2 Configuration

3 Model Configuration

4 Advanced Configuration

5 Summary

Devices

Select devices to fill out provisioning parameters

Find

≡Q Device

Show

All

▼

▼ pnp1-config (1)

✓ 9800-pnp

☐ Provision these templates even if they have been deployed before

☒ Copy running config to startup config

pnp1-config

No variables found in template

```
# add the OBM management interface.  L3
int g1
no switchport
#ip address 10.66.104.98 255.255.255.192
ip address 10.66.104.86 255.255.255.192

ip route 0.0.0.0 0.0.0.0 10.66.104.65
ip route 10.10.0.0 255.254.0.0 Vlan10
ip route 192.168.0.0 255.255.0.0 Vlan10

# add vlan 14 for the client connections
int g2
switchport trunk allowed vlan 1,10,14

# make sure serial active console port
platform console serial
```

Wireless Provisioning - Summary

1Assign Site

2Configuration

3Model Configuration

4Advanced Configuration

5Summary

pnnp-9800

Default AP Profile (Default_AP_Profile_Aireos/default-ap-profile) will be applied to all Cisco DNA Center generated AP Groups/Site Tags

Device Details

Device Name:

pnnp-9800

Platform Id:

C9800-CL-K9

Device IP:

10.10.10.146

Device Location:

Global/DC - syd

Device Role:

Active Main WLC

Associated Anchor device(s)

None

Device Details

Network Setting

NTP Server:

10.10.10.151

AAA Network ISE Server

10.66.104.67

AAA Network Primary Server:

10.10.10.127 (RADIUS)

AAA Client Server:

AAA client/endpoint settings are pushed as per the configuration added for each Managed AP location per WLAN.

WARNING: Do not use "admin" as the username for your device CLI credentials, if you are using ISE as your AAA server, you will not be able to login to your devices.

Network Settings

Syslog Server

Cisco DNA Center

Netflow Collector

Cisco DNA Center

Cisco TrustSec (CTS) Credentials

Yes

Wireless Streaming Telemetry

Yes

SNMP Trap Receiver

Cisco DNA Center

DNS Server

(Not configured)

DTLS Ciphersuite

Skipped

AP Impersonation

Enabled

Syslog Level

6 - Information Messages

Controller Certificates

Yes

Device Controllability

Wireless Intent

SSID (wlc-config)

SSID (thirdwheel)

Managed Sites

As Primary WLC:

3 Managed Sites

Rolling AP Upgrade

Rolling AP Upgrade

Disabled

AP Reboot Percentage

25

Interfaces

Name:

hk_ssid

VLAN ID:

14

Remote Teleworker Settings

Day N Templates

Advanced Configuration

Template Name:

pnnp1-config

Model based config

Model Configs

Capability

Design Name

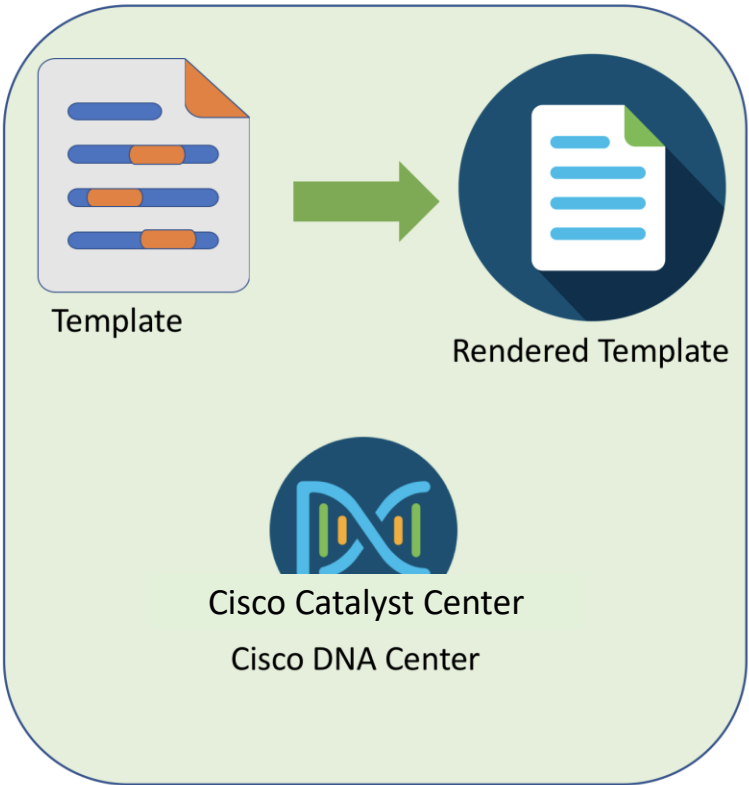
No data to display

Templates

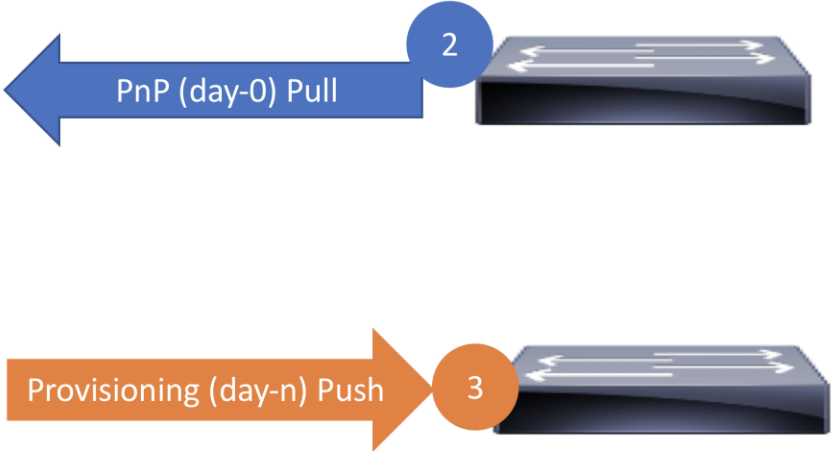
Day0 vs Day-N



Reference



1 Template Rendered on Catalyst Center



Implications	
Day0 - pull	DayN - push
change IP address or interface	Interactive commands
one-shot (rollback on failure)	line-by-line (no rollback)
no composite templates	composite templates supported
	only re-push on change

Velocity vs Jinja

	velocity	jinja
variable reference	<code>\$loopback</code>	<code>{{loopback}}</code>
assignment	<code>#set (\$loopback = "10.10.10.1")</code>	<code>{% set loopback = "10.10.10.1" %}</code>
conditional	<code>#if (\$hostname == "border01") foo #end</code>	<code>{% if hostname == "border01" %} foo {% endif %}</code>
loop	<code>#foreach (\$number in [0..3]) int gig1/\${number}/24 shutdown #end</code>	<code>{% for number in range(3) %} int gig1/{{ number }}/24 shutdown {% endfor %}</code>
implicit variables	<code>#foreach (\$interface in \$__interfaces)</code>	<code>{% for interface in __interface %}</code>
interactive mode	yes	yes
ENABLE and MULTLINE	yes	yes
filters	no	yes

Introduction to variables

The screenshot shows the 'Variables' configuration page in the Cisco Catalyst Center CLI Templates interface. The variable is named 'adam' and is a 'String' type. It is marked as a 'Required Variable'. The 'Variable Data Source' is set to 'User Defined'. The 'Data Entry Type' is 'Text Field'. The 'Default Variable Value' is empty. The 'Maximum Characters' is set to 20. The 'Sensitive Value' checkbox is unchecked. The 'Variable Notes' section contains the hint text 'no instructions required' and the additional info 'a var for adam'. The 'Review Form' button is at the bottom right.

CLI Templates / variable (2) Properties

Templates Variables Simulation Provision Conflicts

Search

VARIABLES

loopback

loopback

Variable

Field Name

adam

Required Variable

Variable Data Value

Variable Data Source

User Defined Bound to source

Variable Type

String

Data Entry Type

Text Field

Default Variable Value

Default Variable Value

Maximum Characters

Maximum Characters

Sensitive Value

Variable Notes

Hint Text

no instructions required

Additional Info

a var for adam

Review Form

Velocity variables are \$var
Sometimes need to ignore "\$"

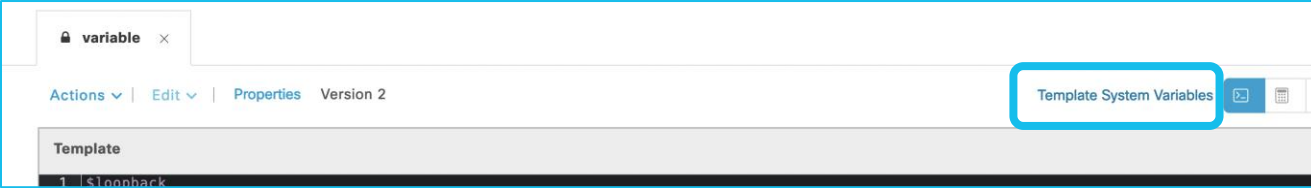
Human readable name of variable

Data type important:
- integer vs string

Hides the input (secret) 2.3.7

Shows under variable/fieldname

System Variables



- "introspect" data Catalyst Center has about the device
- Applied at runtime
- Only for day-N, not day-0 (catch-22)
- Lots of use cases:
- Interfaces on a device.
 - Model Number of device
 - Custom config for WLAN site/policy tags

Template System Variables			
Search Table			
Filter			
Source	Entity	Variable Name	Attribute Name
NetworkProfile	SSID	__ssid	
NetworkProfile	SSID	__ssid[index].wlanId	wlanId
NetworkProfile	SSID	__ssid[index].wlanProfileName	wlanProfileName
NetworkProfile	Policy Profile	__policyprofile	
NetworkProfile	AP Group	__apgroup	
NetworkProfile	Flex Group	__flexgroup	
NetworkProfile	Flex Profile	__flexprofile	
NetworkProfile	Site Tag	__sitetag	
NetworkProfile	Policy Tag	__policytag	
CommonSettings	dhcp.server	__dhcpserver	-
CommonSettings	syslog.server	__syslogserver	

Inventory	Device	> __device
Inventory	Interface	> __interface
Inventory	AP Group	__apgroup
Inventory	Flex Group	__flexgroup
Inventory	Wlan	> __wlan
Inventory	Policy Profile	__policyprofile
Inventory	Flex Profile	__flexprofile
Inventory	Webauth Parameter Map	__webauthparametermap
Inventory	Site Tag	__sitetag
Inventory	Policy Tag	__policytag
Inventory	RF Profile	__rfprofile

Bound Variables



Reference

Take a system variable and map to a variable inside the template.

- e.g. template to shut a list of interfaces
- Inventory -> interface -> portName

interfaces_bound * ×

Actions ▼ | Edit ▼ | Properties

Template

```
1 #foreach ($interface in $interfaces)
2 interface $interface
3 shutdown
4 #end
5
6
```

CLI Templates / interfaces_bound (1) Properties

Templates Variables Simulation Provision Conflicts

VARIABLES

interfaces ✓

☒ Variable

Field Name Field Name ☒ Required Variable

Variable Data Value

Variable Data Source

☐ User Defined ☒ Bound to source

Data Entry Type Multi Select ▼

Entity Interface ▼

Filter By ▼

Source Inventory ▼

Attribute portName ▲

pid

portMode

portName

portType portName

poweroverethernet

Variable Notes

Hint Text Hint Text

Simulation

CLI Templates / interfaces_bound (1) Properties

Templates Variables **Simulation** Provision Conflicts

(x) System Variables Assistant  Template History  Attach to Network Profile ☐

```
1 #foreach ($interface in $interfaces)
2 interface $interface
3 shutdown
4 #end
5
6 |
```

- Select "Simulation" on far right
- Create Simulation

Simulation - #2

CLI Templates / interfaces_bound (1) Properties

Templates Variables **Simulation** Provision Conflicts

Simulations (3) [+ Add Simulation](#)

Search Table

0 Selected [Edit](#) [More Actions](#) As of: Feb 3, 2024 9:52 PM

☐	Simulation Name	Date	Variables Simulated	Status	Report
☐	adam	28 November 2022	1	● SUCCESS	View

Create Simulation

Simulation Name*
adamnew1 [Import Template Parameters](#) [Export Template Parameters](#)

BIND TO SOURCE
This template has binding or system variables. Select the device for simulation.

Device*
9k-13 (10.10.3.122)

Search Device

- 9k-13 (10.10.3.122)
- 2960x-auckland (192.168.14.16)
- encs-9k (192.168.200.232)
- perth-9k (10.10.100.120)
- perth-9k-edge (10.10.9.128)

Create Simulation

Simulation Name*
adamnew1 [Import Template Parameters](#) [Export Template Parameters](#)

BIND TO SOURCE
This template has binding or system variables. Select the device for simulation.

Device*
9k-13 (10.10.3.122)

Search Device

interfaces

Search Table

0 Selected As of: Feb 3, 2024 9:55 PM

- ☐ interfaces
- ☐ AppGigabitEthernet1/0/1
- ☐ FortyGigabitEthernet1/1/1
- ☐ FortyGigabitEthernet1/1/2
- ☐ GigabitEthernet0/0
- ☐ GigabitEthernet1/0/1

- Click link to select device
- Choose device from list
- Interfaces will be assigned to a list (multi-select)

Simulation #3

Cisco

Catalyst Center

Design / CLI Templates

☆

🔍

🟢

?

🔔

Adam

▼

CLI Templates / interfaces_bound (1) Properties

TemplatesVariablesSimulationProvision Conflicts

Simulations (4)

+ Add Simulation

🔍 Search Table

🏠

0 Selected

Edit

More Actions ▼

As of: Feb 3, 2024 9:56 PM

🔄

☐	Simulation Name ▲	Date	Variables Simulated	Status	Report
☐	adam	28 November 2022	1	🟢 SUCCESS	View
☐	adam2	05 December 2023	1	🟢 SUCCESS	View
☐	adamnew1	03 February 2024	1	🟢 SUCCESS	View
☐	ams	07 February 2023	1	🟢 SUCCESS	View

Simulation - adamnew1

Variables Simulated: 1Status: SUCCESS

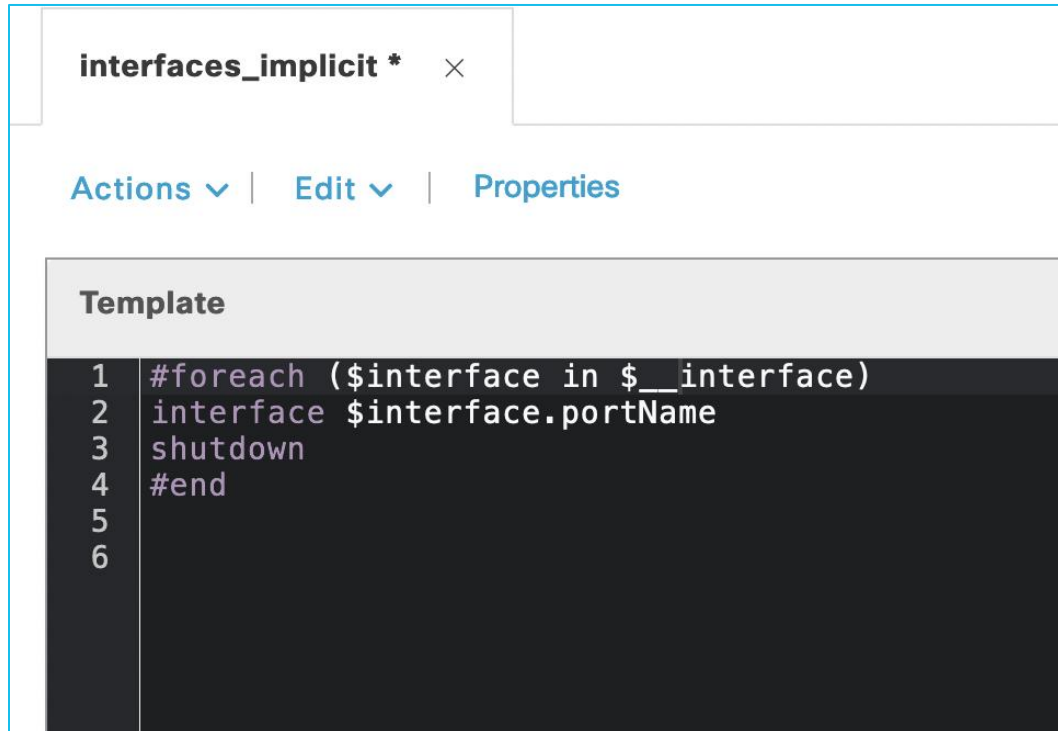
```
1 interface GigabitEthernet1/0/1
2 shutdown
3 interface GigabitEthernet1/0/10
4 shutdown
5 interface GigabitEthernet1/0/11
6 shutdown
7
8
```

- Shows configuration pushed to device
- Lots of options for more intelligent templates
- Can send all interface attributes and pick those needed

Implicit Variables

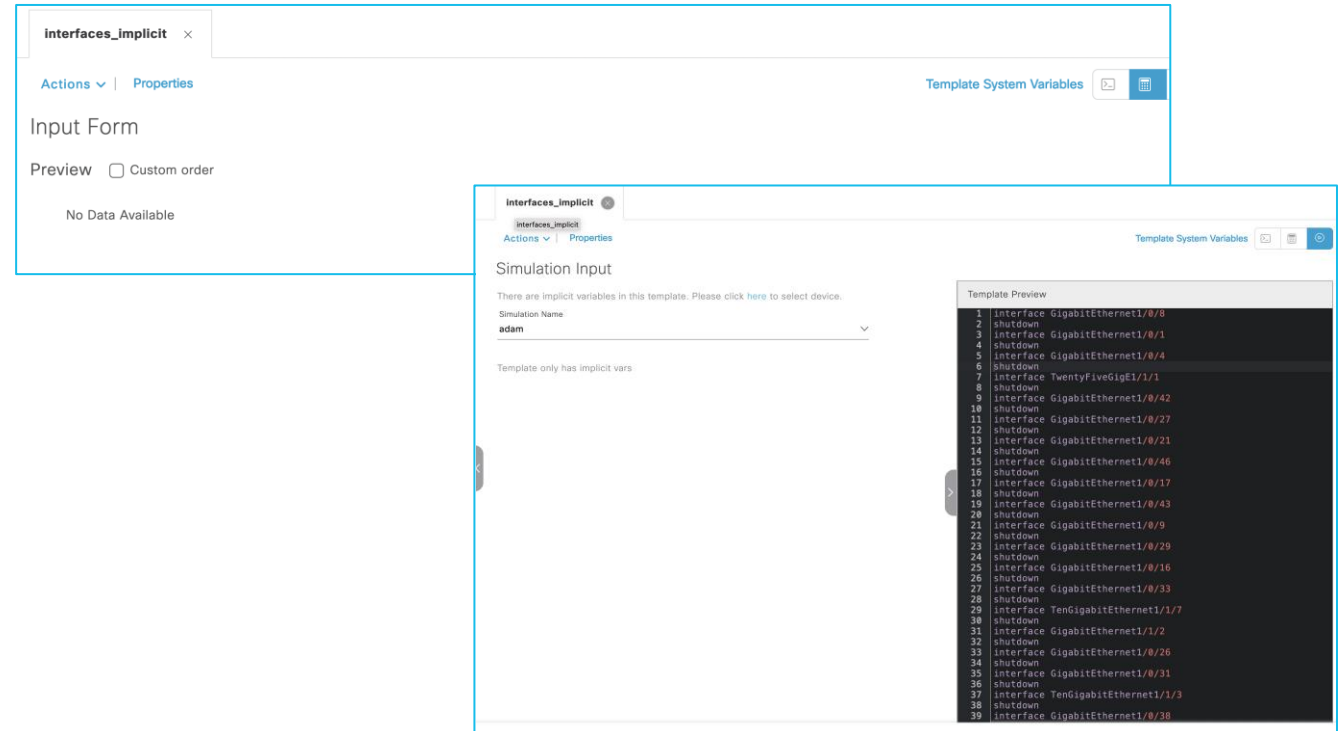
- Picking interface names from UI can be tedious. Possible to "implicitly" access all interfaces/SSID etc
- No longer any variable as the binding is implicit
- Need to use ".portName" to get interface name

Simulation shows this shuts down every interface.... Be careful!



The screenshot shows the 'interfaces_implicit' template editor. The 'Template' tab is active, displaying the following code:

```
1 #foreach ($interface in $__interface)
2   interface $interface.portName
3   shutdown
4 #end
```



The screenshot shows the 'interfaces_implicit' template editor with the 'Simulation Input' and 'Template Preview' tabs. The 'Simulation Input' tab shows the 'Simulation Name' set to 'adam'. The 'Template Preview' tab shows the resulting configuration:

```
1 interface GigabitEthernet1/0/0
2 shutdown
3 interface GigabitEthernet1/0/1
4 shutdown
5 interface GigabitEthernet1/0/4
6 shutdown
7 interface TwentyFiveGigE1/1/1
8 shutdown
9 interface GigabitEthernet1/0/42
10 shutdown
11 interface GigabitEthernet1/0/27
12 shutdown
13 interface GigabitEthernet1/0/21
14 shutdown
15 interface GigabitEthernet1/0/46
16 shutdown
17 interface GigabitEthernet1/0/17
18 shutdown
19 interface GigabitEthernet1/0/43
20 shutdown
21 interface GigabitEthernet1/0/9
22 shutdown
23 interface GigabitEthernet1/0/29
24 shutdown
25 interface GigabitEthernet1/0/16
26 shutdown
27 interface GigabitEthernet1/0/33
28 shutdown
29 interface TenGigabitEthernet1/1/7
30 shutdown
31 interface GigabitEthernet1/1/2
32 shutdown
33 interface GigabitEthernet1/0/26
34 shutdown
35 interface GigabitEthernet1/0/31
36 shutdown
37 interface TenGigabitEthernet1/1/3
38 shutdown
39 interface GigabitEthernet1/0/38
```

Real Example

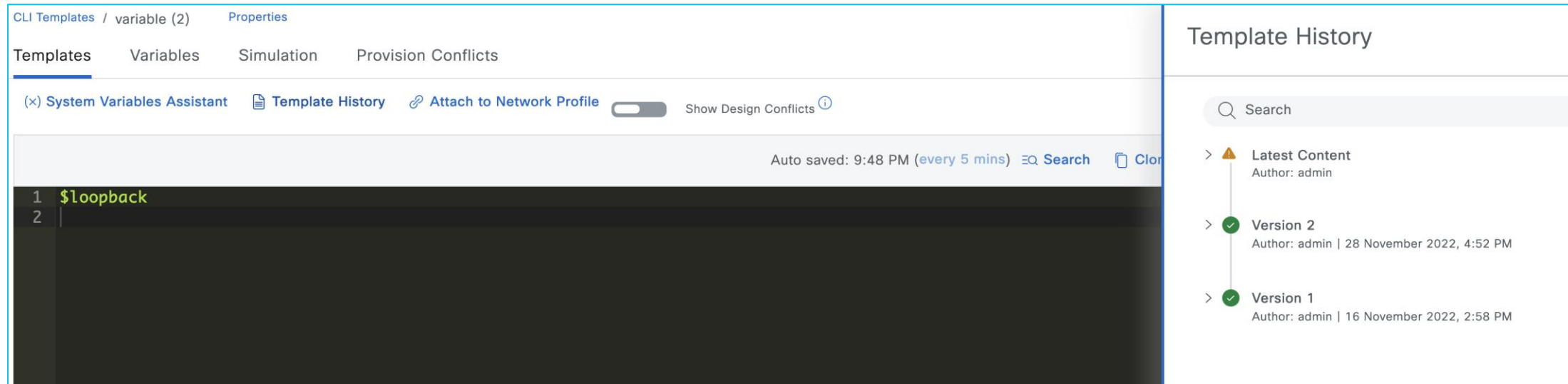
appX_implicit ×

Actions ▾ | Edit ▾ | Properties

Template

```
1 #foreach ($interface in $__interface)
2 #if ($interface.interfaceType == "Physical" && $interface.portMode == "access")
3 #if ($interface.description.matches(".* lan"))
4 int $interface.portName
5 desc $interface.description
6 #else
7 int $interface.portName
8 desc $interface.description lan
9 #end
10 #end
11 #end
```

Templates need to be committed and have versioning history



The screenshot displays the Cisco CLI Templates interface. The main area shows a template editor with a dark background and a light-colored text area. The text area contains the following content:

```
1 $loopback
2
```

The interface includes a top navigation bar with tabs for Templates, Variables, Simulation, and Provision Conflicts. Below the navigation bar, there are links for System Variables Assistant, Template History, and Attach to Network Profile. A status bar at the bottom indicates "Auto saved: 9:48 PM (every 5 mins)" and includes a search icon and a "Close" button. On the right side, the "Template History" panel is visible, showing a list of versions:

- > Latest Content
Author: admin
- > Version 2
Author: admin | 28 November 2022, 4:52 PM
- > Version 1
Author: admin | 16 November 2022, 2:58 PM

- Saving without committing will use the last committed version
- Design conflicts: attempts to show commands that clash with SDA push config.

INTERACTIVE JINJA



Reference

Template Hub / jinja-interactive (1)Properties

TemplatesVariablesSimulationProvision Conflicts

(x) System Variables AssistantTemplate HistoryAttach to Network Profile☐Show Design Conflicts ⓘ

1 #INTERACTIVE

2 no username bogus<IQ>confirm<R>y

3 #END_INTERACTIVE

Reboot switch



Reference

Template Hub / reload (1) Properties

Templates Variables Simulation Provision Conflicts

(x) System Variables Assistant Template History Attach to Network Profile ☐ Show Design Conflicts ⓘ

```
1 #MODE_ENABLE
2 ! save config first. then do not need to answer prompt for the message to save it
3 wr mem
4 #INTERACTIVE
5 reload in 1<IQ>confirm<R>y
6 #ENDS_INTERACTIVE
7 #MODE_END_ENABLE|
```

- With interactive, you are matching a regexp, not string. "[confirm]" <> "confirm"
- Reload in 1 as immediately will terminate connection, template fails

Filters Jinja

```
1  {# this was the original. Needed a throwaway var so the True command was suppressed #}  
2  {% set physicalInterfaces = __interface | selectattr("interfaceType", "equalto", "Physical") | list %}  
3  {% set interfaceNames = [] %}  
4  
5  {% for dict_item in physicalInterfaces %}  
6      {% for key, value in dict_item.items() %}  
7          {% if key == 'portName' %}  
8              {% set _ = interfaceNames.append(value) %}  
9          {% endif %}  
10     {% endfor %}  
11 {% endfor %}  
12  
13 {{ interfaceNames }}
```

```
15 {# the filter version #}  
16 {% set physicalInterfaces = __interface | selectattr("interfaceType", "equalto", "Physical") | list %}  
17 {% set interfaceNames = physicalInterfaces | map(attribute="portName") | list %}  
18  
19 {{ interfaceNames }}
```

"selectattr" and "map" are filters

- selectattr: if the attribute "interfaceType" == "Physical"
- map: just pick the attribute "portName" (vs all attributes)

Structured Data as input (vs strings)

The screenshot displays the Cisco DevNet CLI Templates interface. The top navigation bar shows 'CLI Templates / meta-data-json (2)' and 'Properties'. Below this, there are tabs for 'Templates', 'Variables', 'Simulation', and 'Provision Conflicts'. The 'Templates' tab is active, showing a list of templates. One template is selected, and its content is displayed in a code editor:

```
1 {% set data = json_var|fromjson %}  
2 {{{data.ip}}}
```

Below the code editor, there is a modal window titled 'Update Simulation'. This window contains fields for 'Simulation Name' (set to 'a') and 'Device'. Below these fields, there is a section titled 'CONFIGURE VARIABLE VALUES' with a field for 'json_var' containing the JSON object: `{"ip" : "1.2.3.4", "interface" : "g1/01/"}`. To the right of the 'Update Simulation' modal, there is a 'Simulation - a' window showing 'Variables Simulated: 1' and 'Status:'. Below this, a table displays the simulated variables:

Variable	Value
1	1.2.3.4

- Can do this via API.
- Also possible through UI (using a filter "fromjson")

Template Hub – 2.3.5.x+ – Ad Hoc template application



Reference

Tools / Template Hub

Templates (111)

1 Selected Export Import Delete | Provision Templates

	Name	Project	Type	Version	Commit State
☐	flexible_ep.json	Onboarding Configuration	Regular	1	02 Dec 2022 01:28 PM
☐	For-Loop-Jinja	Sample Jinja Templates	Regular	Not Committed	Not Committed
☐	For-Loop-Velocity	Sample Velocity Templates	Regular	Not Committed	Not Committed
☐	idempotent	adam	Regular	4	16 Jun 2020 07:06 PM
☐	If-Condition-Jinja	Sample Jinja Templates	Regular	Not Committed	Not Committed
☐	If-Condition-Velocity	Sample Velocity Templates	Regular	Not Committed	Not Committed
☐	If_loop	adam-jinja	Regular	1	16 Nov 2022 02:31 PM
☐	Implicit-Variables	Sample Jinja Templates	Regular	Not Committed	Not Committed
☐	Implicit_int_loop2	adam	Regular	1	27 May 2022 11:14 AM
☐	include	Sample Jinja Templates	Regular	Not Committed	Not Committed
☐	include2	Sample Jinja Templates	Regular	1	17 Mar 2022 08:52 AM
☒	int-desc	adam	Regular	10	08 Apr 2022 03:41 PM

Select Devices

You can select the applicable devices to provision the templates from the list below based on the device details defined by the template.

Devices (4)

Reachability **All** Reachable Unreachable

	Device Name	IP Address
☐	2960x-auckland	192.168.14.16
☐	encs-9k	192.168.200.232
☒	perth-9k	10.10.100.120
☐	perth-9k-edge	10.10.9.52

Configure Template Variables for Devices

Based on the device type and device tags defined when the templates was created. You can select the applicable devices from the list below to provision the templates.

☐ Provision these templates even if they have been deployed before

☒ Copy running config to startup config

[Export Template Parameters](#) [Import Template Parameters](#)

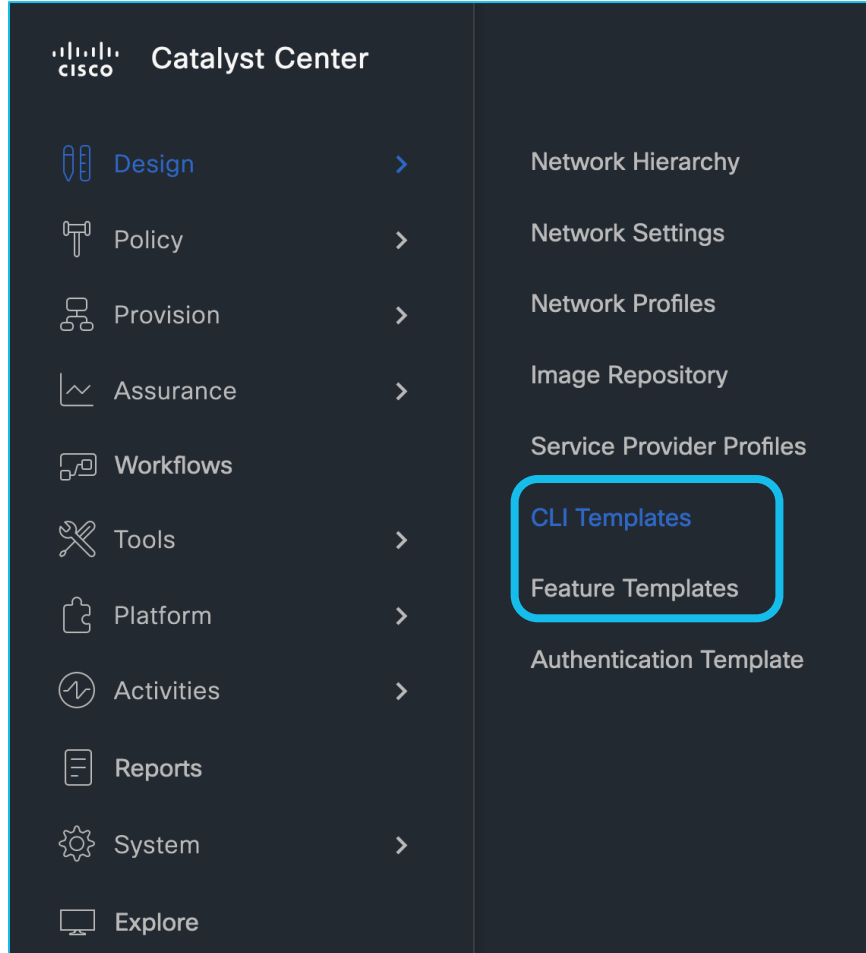
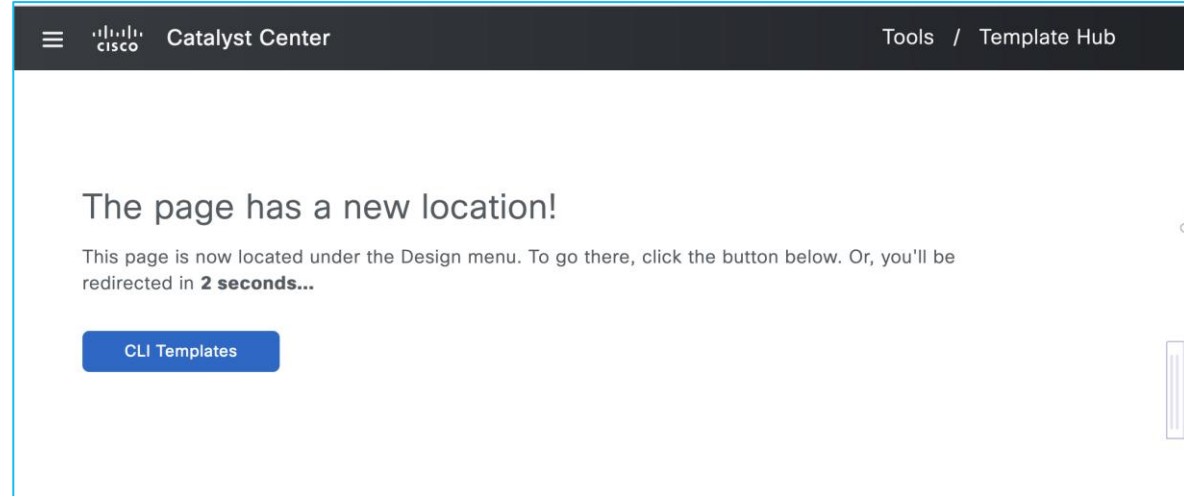
int-desc	
int*	<u>g1/0/10</u>
desc*	<u>template hub was here</u>

- Shows network profiles using templates
- Attach template to network profile
- Allows selective templates to be directly applied to devices – no need to do full provision (e.g. WLC)

New Location, Same functionality – 2.3.7.4



Reference



- Moved from tools to design. Old Menu gives a redirect
- "feature templates" also moved (was Model Config Editor)

AAA and Management of Credentials

Network Settings: AAA

▼ AAA ✓

Select AAA or Cisco Identity Services Engine (ISE)

Network Client/Endpoint

☒ Add AAA servers

Server Type

☒ ISE ☐ AAA

Protocol

☒ RADIUS ☐ TACACS

PAN*

10.85.54.185  ▼

- ISE or other AAA
- RADIUS or TACACS

▼ AAA ✓

Select AAA or Cisco Identity Services Engine

Network Client/Endpoint

☒ Add AAA servers

Server Type

☒ ISE ☐ AAA

Protocol

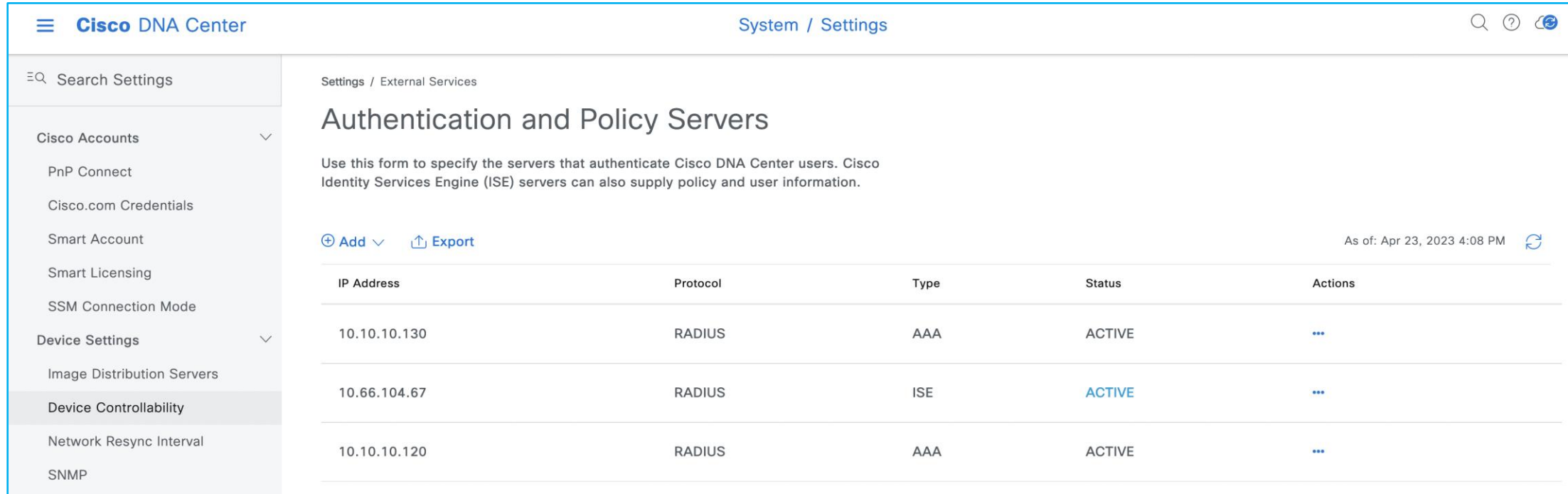
☒ RADIUS ☐ TACACS

PAN*

10.85.54.185  ▼

- ISE or other AAA
- RADIUS

ISE and Catalyst Center Integration

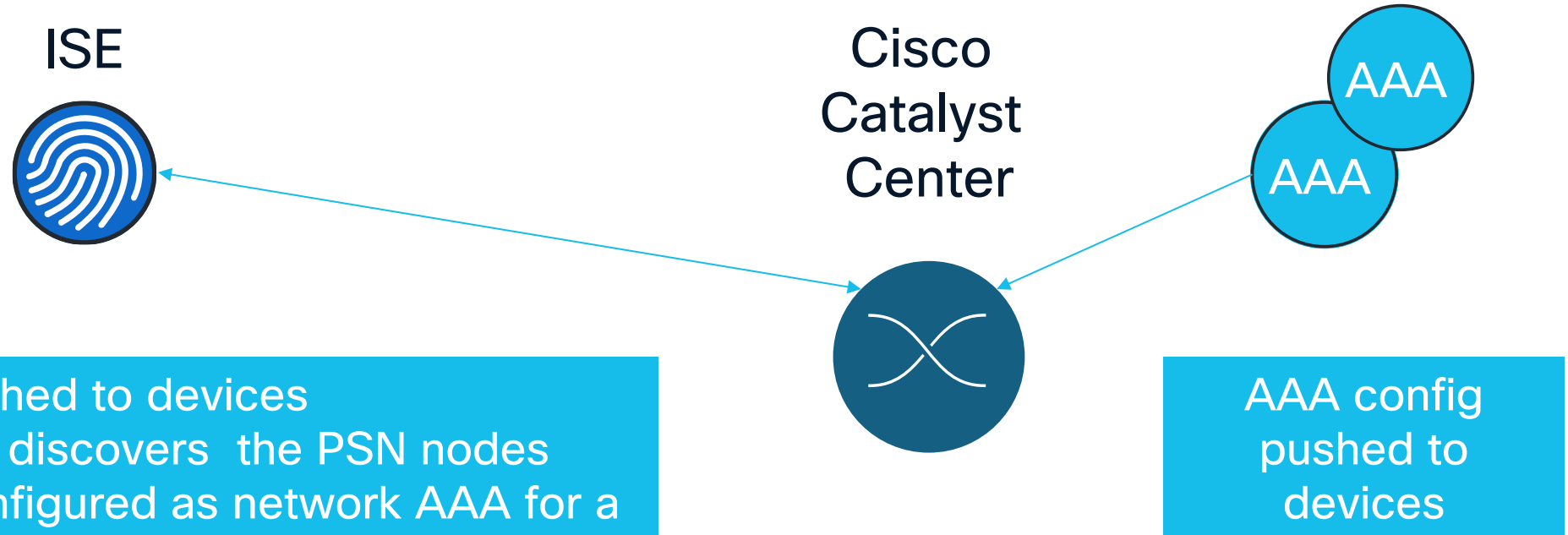


The screenshot shows the Cisco DNA Center interface. The top navigation bar includes the Cisco DNA Center logo, the path 'System / Settings', and search, help, and refresh icons. A left sidebar contains a 'Search Settings' field and a list of settings categories: Cisco Accounts (with sub-items: PnP Connect, Cisco.com Credentials, Smart Account, Smart Licensing, SSM Connection Mode), Device Settings (with sub-items: Image Distribution Servers, Device Controllability, Network Resync Interval, and SNMP). The main content area is titled 'Settings / External Services' and 'Authentication and Policy Servers'. It includes a description: 'Use this form to specify the servers that authenticate Cisco DNA Center users. Cisco Identity Services Engine (ISE) servers can also supply policy and user information.' Below this are 'Add' and 'Export' buttons. A table lists the configured servers, with a timestamp 'As of: Apr 23, 2023 4:08 PM' and a refresh icon. The table has columns for IP Address, Protocol, Type, Status, and Actions.

IP Address	Protocol	Type	Status	Actions
10.10.10.130	RADIUS	AAA	ACTIVE	...
10.66.104.67	RADIUS	ISE	ACTIVE	...
10.10.10.120	RADIUS	AAA	ACTIVE	...

- Only one ISE integration can be done per Catalyst Center.
- Other AAA servers can be added, but as an AAA server only (even if they are ISE servers)

Difference between ISE and AAA integration



- AAA config pushed to devices
- Catalyst Center discovers the PSN nodes
- When ISE is configured as network AAA for a site, devices in the site will automatically be added as NAD to ISE
- PxGrid:
 - Provides Username for wired devices
 - Device attributes for AI endpoint analytics
 - Micro-segmentation for SDA

Pre-requisites for ISE integration



Reference

- IP reachability required
- No proxy server between ISE and Catalyst Center
- ISE API needs to be enabled – ERS read write
- PxGrid needs to be enabled on ISE
- CLI credentials on ISE no longer used for integration. API only
- FQDN is required for the integration, not just an IP address (certificate)
- If using Enterprise issued Certificate, need VIP + real IP for Catalyst Center Cluster

Device AAA and Site AAA Interaction

Device has AAA configured	Site has AAA defined in Catalyst Center	Provisioning Workflow Success
		
		
		
		

Note: If just client/device AAA, then all will work.
Network AAA is the issue - due to lockout concerns (NAD entry in ISE)

Devices with AAA configured

Provision with Network AAA in Network Settings

```
C9200L-1#show run
Building configuration...
```

Device Configuration before Provision

```
Current configuration : 34587 bytes
!
! Last configuration change at 12:34:46 UTC Tue Mar 4 2025 by netadmin
! NVRAM config last updated at 15:10:21 UTC Tue Mar 4 2025 by netadmin
!
version 17.8
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service call-home
platform punt-keepalive disable-kernel-core
!
hostname C9200L-1
!
!
vrf definition Mgmt-vrf
!
 address-family ipv4
 exit-address-family
!
 address-family ipv6
 exit-address-family
!
!
!
!
aaa new-model
!
!
aaa group server radius dnac-network-radius-group
 server name dnac-radius_10.85.54.185
 ip radius source-interface Vlan419
!
aaa authentication login default local
aaa authentication login VTY_authn group dnac-network-radius-group local
aaa authorization exec default local
aaa authorization exec VTY_authn group dnac-network-radius-group local if-authn
aaa accounting update newinfo periodic 2880
aaa accounting exec default start-stop group dnac-network-radius-group
!
```

Network Settings

The screenshot shows the Cisco Catalyst Center interface for configuring AAA settings. The left sidebar displays a hierarchical tree with 'Global', 'Canada', 'Ontario', and 'Toronto' expanded, and 'BRANCH-AAA' selected. The main content area is titled 'Network Settings' and includes a description: 'Configure external network servers, assign time zones to sites, and customize device CLI login banner messages. The system will deploy these settings when devices are provisioned.' Below this, the 'AAA' section is expanded, showing a green status icon. The 'Add AAA servers' checkbox is checked. Under 'Server Type', 'ISE' is selected. Under 'Protocol', 'RADIUS' is selected. The 'PAN*' field is set to '10.85.54.185'. The 'Last PSN sync' is 'Mar 17, 2025 3:34 AM'. The 'Primary Server*' is also '10.85.54.185'.

Catalyst Center

Design / Network Settings

Servers Device Credentials IP Address Pools Wireless Telemetry Security and Trust

Q aaa X Search Help

Global Canada Ontario Toronto BRANCH-AAA

Configure external network servers, assign time zones to sites, and customize device CLI login banner messages. The system will deploy these settings when devices are provisioned.

AAA

Select AAA or Cisco Identity Services Engine (ISE) servers for network, client, and endpoint authentication.

Network Client/Endpoint

☒ Add AAA servers

Server Type

☒ ISE ☐ AAA

Protocol

☒ RADIUS ☐ TACACS

PAN*

10.85.54.185

Last PSN sync: Mar 17, 2025 3:34 AM

Primary Server*

10.85.54.185

Devices with AAA configured

Provision with Network AAA in Network Settings

Network Devices / Provision Devices

1 Assign Site 2 Advanced Configuration 3 Summary

C9200L-1.lila.com

Device Details

Device Name	C9200L-1.lila.com
Platform Id	C9200L-24T-4G
Device IP	10.85.54.23
Device Location	Global/Canada/Ontario/Toronto/BRANCH-AAA

Network

AAA Ne

AAA Ne

DNS Do

DNS Pri

DNS Se

Provision Device

Step 3 of 3: Preview Configuration

Review the device configuration provided below by clicking on each device. When you are done, a deferred review can be found in the [Tasks](#) menu.

Search by device name ⓘ

Device IP: 10.85.54.23 Site: Global/Canada/Ontario/Toronto/BRANCH-AAA

C9200L-1.lila.com ❌

Configuration to be Deployed

View by Configuration Source · All ▾

❌ Errors occurred during config generation. You can still opt to deploy the partial configuration (if any) that was generated successfully. [Collapse](#) to hide.

AAA CLI(s) are already present on the device C9200L-1.lila.com: aaa group server radius dnac-group, radius server groupName, aaa accounting settings. Remove the CLIs, resync the device and retry.

ⓘ No configuration was generated from current source

As of: 9:50:42 AM [Refresh](#)

Status: ❌ Failed

[← Back to workflow progress](#)

[📧](#) [📄](#)

Search configuration

Options:

#1 - Remove AAA (Network) from Device

#2 - Remove AAA (Network) from Network Settings

#3 - Optionally use Templates for AAA

Devices with no AAA configured

Provision with Network AAA in Network Settings

```

aaa new-model
!
!
aaa group server radius dnac-network-radius-group
 server name dnac-radius_10.85.54.185
 ip radius source-interface Vlan419
!
aaa authentication login default local
aaa authentication login VTY_authen group dnac-network-radius-group local
aaa authorization exec default local
aaa authorization exec VTY_author group dnac-network-radius-group local
authenticated
aaa accounting update newinfo periodic 2880
aaa accounting exec default start-stop group dnac-network-radius-group
!
!
aaa session-id common
!
!
!
ip radius source-interface Loopback0

```

```
radius-server attribute 6 on-for-login-auth
radius-server attribute 6 support-multiple
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server attribute 31 mac format ietf upper-case
radius-server attribute 31 send nas-port-detail mac-only
radius-server dead-criteria time 5 tries 3
```

Sample AAA config sent to device

Device added in ISE

```

!
line vty 0 4
  authorization exec VTY_auth
  login authentication VTY_auth

```

Cisco Identity Services Engine

- Home
- Context Visibility
- Operations
- Policy
- Administration
- Work Centers

Common

- System
- Identity Management
- Network Resources
 - Device Portal Management
 - pxGrid Services
 - Feed Service
 - Threat Centric NAC

Network Devices | Network Device Groups | Network Device Profiles | External RADIUS Servers | RADIUS Server Sequences | NAC Managers | External MDM | Location Services

Network Devices

Match the following rule:

Filter: Name Contains 9200 [Go] [Clear Filter]

Name	IP/Mask	Profile Name	Location	Type	Description
☐ C9200L-1.lila...	10.85.54.23/32	Cisco	All Locations	All Device Types	

Devices with local credentials

Changing local credential passwords

The screenshot shows the Cisco ISE GUI with the 'Device Credentials' tab selected. The left sidebar contains a search bar with 'scar' and a list of locations: Global, Canada, Ontario, and Toronto. The main content area has a heading 'Create and configure the credentials used to access devices.' and a link 'Manage Credentials'. Below this, it states: 'Assigned credentials aren't deployed automatically. To push a credential to your devices, click "Manage Credentials" and choose the credential's Apply action in the Manage Credentials table.' A table with one row 'CLI' is shown, with a checkbox 'Assign a CLI credential' checked and a dropdown menu set to 'Cisco Live'.

```
TBRANCH-C9200L-3#show run | i username
username netadmin privilege 15 password 7 04785A150C2E68602858
username ciscolive privilege 15 secret 8 $8$MHEMy60T0Qp.fk$eQBNEVYBCW7umuAarXnNbxDnyhZrk4o20RVYyQEFG.A
username lila privilege 15 secret 8 $8$YZ4SK4Hb4X9dmk$.Fi1.LkfwxF.YdjvLytRJ8R8V.jfN1aWuCaE9a0jTt6
```

Changing local credential passwords



Reference

Credentials

Manage Credentials

Credentials are applied locally to the site but changed globally

To view the assigned credentials' statuses and to apply them to only devices in the current site, choose "Focus: Current site."

To view, edit, or delete all available credentials and to apply them to all devices in all applicable sites, choose "Focus: System."

Focus:

Current site (TBRANCH-SCARBOROUGH) ^

Q

Current site (TBRANCH-SCARBOROUGH)

System

Add v

As of: Mar 4, 2025 12:25 PM

↺

Changing local credential passwords



Reference

Credentials

Manage Credentials

To view the assigned credentials' statuses and to apply them to only devices in the current site, choose "Focus: Current site."

To view, edit, or delete all available credentials and to apply them to all devices in all applicable sites, choose "Focus: System."

Focus: **System** ▾

Q

Search Table

Add ▾

As of: Mar 4, 2025 12:25 PM

Name ▴	Type	Actions
admin	CLI	...
Cisco Live	CLI	...
cli-canada	CLI	<div>Edit</div> <div>Delete</div> <div>Apply</div>
francis	CLI	...
lila	CLI	...

Credentials / Edit Credential

CLI

Name / Description*

Cisco Live

Username*

ciscolive

View Username Policy

Password*

.....

SHOW

View Password Policy

Enable Password

.....

SHOW

View Password Policy

Close

Back

Save

Credentials are applied locally but changed globally

New password applied at the site level, other sites not impacted until synched

Changing local credential passwords



Reference

← → ↺

Not Secure https://10.85.54.180/dna/design/networkSettings/deviceCredentials?selectedSite=f10009d3-3789-46a7-929f-64991323b24c

☆ 🔍 🗄️ 🌐

☰

Catalyst Center

Design / Network Settings

☆ 🔍 🗄️ 🌐 8 | 👤 Lila

Servers

Device Credentials

IP Address Pools

Wireless

Telemetry

Security and Tr

🔍 scar ✕ 🔍

Search Help

Global

Canada

Ontario

Toronto

TBRANCH-SCARBOR...

Create and configure the credentials used to access devices.

Assigned credentials aren't deployed automatically. To push a cred... choose the credential's Apply action in the Manage Credentials tab

CLI ✓

Assign a CLI credential

Credential* Cisco Live

SNMPv2c Read ✓

Assign an SNMPv2c Read credential

Credential* ro

SNMPv2c Write ✓

Assign an SNMPv2c Write credential

Credentials

Manage Credentials

To view the assigned credentials' statuses and to apply them to only devices in the current site, choose "Focus: Current site."

To view, edit, or delete all available credentials and to apply them to all devices in all applicable sites, choose "Focus: System."

Focus: System

🔍 Search Table

Add

As of: Mar 4, 2025 12:25 PM

Name	Type	Actions
admin	CLI	...
Cisco Live	CLI	...
cli-canada	CLI	...
francis	CLI	...
Lila	CLI	...

✓

Success

CLI credential **Cisco Live** has been updated.



Changing local credential passwords



Reference

New password applied at the site level, other sites not impacted until synched

Credentials

Manage Credentials

To view the assigned credentials' statuses and to apply them to only devices in the current site, choose "Focus: Current site."

To view, edit, or delete all available credentials and to apply them to all devices in all applicable sites, choose "Focus: System."

Focus: **Current site (TBRANCH-SCARBOROUGH)** ▾



Search Table

Add ▾

As of: Mar 4, 2025 12:26 PM



Name ▴	Type	Not Synced ⓘ 2 Devices	Actions
Cisco Live	CLI	ⓘ Not Synced (2)	...

Changing local credential passwords



Reference

Credentials

Manage Credentials

Local Credentials
updated in device

To view the assigned credentials' status, choose "Focus: Current site."

To view, edit, or delete all available credentials, choose "Focus: System."

Focus: [Current site \(TBRANCH-SC01\)](#)

```
C9K-STANDALONE-2> show run | i username
username netadmin privilege 15 password 0 xxxxxxxx
username httpuser privilege 15 password 0 xxxxxxxx
username ciscolive privilege 15 secret xxxxxx
C9K-STANDALONE-2>
```

Search Table

Add ▾

As of: Mar 4, 2025 12:26 PM

Name ▴	Type	Status	Actions
Cisco Live	CLI	Not Synced (2)	
NFVIS-HTTPS-RO	HTTP(S) Read	Not Synced (2)	

...

Apply

Changing local credential passwords

Catalyst Center pushes a temporary EEM script to validate the credentials

```
Apr  2 11:19:36.804: %SSH-5-SSH2_USERAUTH: User 'ciscolive' authentication for SSH
1) using crypto cipher 'aes128-ctr', hmac 'hmac-sha2-256-etm@openssh.com' Succeeded
Apr  2 11:19:36.830: %HA_EM-6-LOG: catchall: enable
Apr  2 11:19:36.848: %HA_EM-6-LOG: catchall: terminal length 0
Apr  2 11:19:36.875: %HA_EM-6-LOG: catchall: terminal width 0
Apr  2 11:19:36.907: %HA_EM-6-LOG: catchall: terminal width 0
Apr  2 11:19:36.933: %HA_EM-6-LOG: catchall: configure terminal
Apr  2 11:19:36.994: %HA_EM-6-LOG: catchall: event manager applet _NEW_CREDENTIAL
Apr  2 11:19:37.051: %HA_EM-6-LOG: catchall: event timer countdown time 1
Apr  2 11:19:37.116: %HA_EM-6-LOG: catchall: action 1.0 cli command "enable"
Apr  2 11:19:37.176: %HA_EM-6-LOG: catchall: action 1.1 cli command "config t"
Apr  2 11:19:37.342: %HA_EM-6-LOG: catchall: action 1.2 cli command "username ciscolive privilege 15 algorithm-type
sha256 secret XXX"
Apr  2 11:19:37.489: %HA_EM-6-LOG: catchall: action 1.3 cli command "enable algorithm-type sha256 secret XXX"
Apr  2 11:19:37.612: %HA_EM-6-LOG: catchall: action 1.4 cli command "no event manager applet _NEW_CREDENTIAL"
Apr  2 11:19:37.664: %HA_EM-6-LOG: catchall: action 1.5 cli command "end"
Apr  2 11:19:37.721: %HA_EM-6-LOG: catchall: action 1.6 cli command "exit"
Apr  2 11:19:37.738: %HA_EM-6-LOG: catchall: exit
Apr  2 11:19:37.752: %SYS-5-CONFIG_I: Configured from console by ciscolive on vty1 (10.85.54.180)
Apr  2 11:19:37.760: %HA_EM-6-LOG: catchall: exit
Apr  2 11:19:39.345: %HA_EM-6-LOG: catchall: show running-config yang brief
Apr  2 11:19:39.303: %DMI-5-SYNC_NEEDED: Switch 1 R0/0: dmiauthd: Configuration change requiring running
configuration sync detected - 'username *** privilege 15 algorithm-type sha256 secret ***'. The running
```

Changing credentials passwords for devices with AAA for Network Devices

Brownfield AAA, Template-Based AAA or AAA Configured via Network Settings

Servers

Device Credentials

IP Address Pools

Wireless

Telemetry

Security and Trust

AAA

×

⌵

Search Help

Create and configure the credentials used to access devices.

Assigned credentials aren't deployed automatically. To push a credential to your devices, click "Manage Credentials" to choose the credential's Apply action in the Manage Credentials table.

Credentials / Edit Credential

CLI

Name / Description*

Lila

Username*

lila

View Username Policy

Password*

.....

SHOW

View Password Policy

Enable Password

.....

SHOW

View Password Policy

C9200L-1#show run

Building configuration...

Current configuration : 34587 bytes

!

! Last configuration change at 12:34:46 UTC Tue Mar 4 2025 by netadmin

! NVRAM config last updated at 15:10:21 UTC Tue Mar 4 2025 by netadmin

!

!

!

aaa new-model

!

!

aaa group server radius dnac-network-radius-group

server name dnac-radius_10.85.54.185

ip radius source-interface Vlan419

!

aaa authentication login default local

aaa authentication login VTY_authen group dnac-network-radius-group local

aaa authorization exec default local

aaa authorization exec VTY_author group dnac-network-radius-group local if-authenticated

aaa accounting update newinfo periodic 2880

aaa accounting exec default start-stop group dnac-network-radius-group

!

Same workflow as local credentials

Same workflow as local credentials

Changing credentials passwords for devices with AAA for Network Devices

Brownfield AAA, Template-Based AAA or AAA Configured via Network Settings

Servers

Device Credentials

IP Address Pools

Wireless

Telemetry

Security and

AAA

Global

Canada

Ontario

Toronto

BRANCH-AAA

Create and configure the credentials used to access devices.

Assigned credentials aren't deployed automatically. To push a credential to devices, choose the credential's Apply action in the Manage Credentials table.

CLI

☒ Assign a CLI credential

Credential*

Lila

SNMPv2c Read

☒ Assign an SNMPv2c Read credential

Credential*

ro

Credentials

Manage Credentials

To view the assigned credentials' statuses and to apply them to only devices in the current site, choose "Focus: Current site."

To view, edit, or delete all available credentials and to apply them to all devices in all applicable sites, choose "Focus: System."

Focus: Current site (BRANCH-AAA)

Search Table

As of: Mar 17, 2025 10:46 AM

Name	Type	Status	Actions
Lila	CLI	Not Synced (1)	...
NFVIS-HTTPS-RO	HTTP(S) Read	Not Synced (1)	Apply

Credentials are updated in Catalyst Center only (not on device)

```
[C9200L-1#show run | i username
username netadmin privilege 15 password 7 15315A1F07250F0A0972
```

Changing credentials passwords for devices with AAA for Network Devices

Brownfield AAA, Template-Based AAA or AAA Configured via Network Settings

```
Mar 17 14:47:14.655: RADIUS: Message Authenticator encoded
Mar 17 14:47:14.655: RADIUS(00002D54): Send Access-Request to 10.85.54.185:1812 id 1645/84, len 317
RADIUS: authenticator 1B 33 24 4A 9E 2A 01 B8 - 2E 91 37 99 2A 22 AF DC
Mar 17 14:47:14.655: RADIUS: Vendor, Cisco [26] 211
Mar 17 14:47:14.656: RADIUS: Cisco AVpair [1] 205 "cts-pac-opaque="
Mar 17 14:47:14.656: RADIUS: User-Name [1] 6 "lila"
Mar 17 14:47:14.656: RADIUS: User-Password [2] 18 *
Mar 17 14:47:14.656: RADIUS: Calling-Station-Id [31] 14 "10.85.54.180"
Mar 17 14:47:14.656: RADIUS: NAS-Port [5] 6 6
Mar 17 14:47:14.656: RADIUS: NAS-Port-Id [87] 6 "tty6"
Mar 17 14:47:14.656: RADIUS: NAS-Port-Type [61] 6 Virtual [5]
C9200L-1#
Mar 17 14:47:14.656: RADIUS: Service-Type [6] 6 Login [1]
Mar 17 14:47:14.656: RADIUS: NAS-IP-Address [4] 6 10.85.54.23
Mar 17 14:47:14.656: RADIUS: Message-Authenticator[80] 18
RADIUS: 07 B2 AD 2E 41 9C A1 EB DD 91 84 37 AA 74 DC 37 [ .A7t7]
Mar 17 14:47:14.656: RADIUS(00002D54): Sending a IPv4 Radius Packet
Mar 17 14:47:14.656: RADIUS(00002D54): Started 2 sec timeout
Mar 17 14:47:14.678: RADIUS: Received from id 1645/84 10.85.54.185:1812, Access-Reject, len 38
RADIUS: authenticator 26 95 54 9F 4F 73 56 61 - CE B4 FA F9 53 84 7D 6D
Mar 17 14:47:14.678: RADIUS: Message-Authenticator[80] 18
C9200L-1#
RADIUS: C3 5E F8 D2 75 D6 14 59 06 B4 DC AF 9B 4E 4B 41 [ ^uYNKA]
Mar 17 14:47:14.678: RADIUS: PAC key found while sending request (rctx:0x46C7A3EC)
Mar 17 14:47:14.679: RADIUS(00002D54): Received from id 1645/84
C9200L-1#
```

Credentials are tested to see if they are valid

Changing credentials passwords for devices with AAA for Network Devices

Brownfield AAA, Template-Based AAA or AAA Configured via Network Settings

Servers

Device Credentials

IP Address Pools

AAA

Global

Canada

Ontario

Toronto

BRANCH-AAA

Create and configure

Assigned credentials

CLI

Assign a CLI credential

Credential*

Lila

SNMPv2c Read

Assign an SNMPv2c Read credential

Credential Status

Type	Name/Description	Status	Details	Actions
CLI	Lila	Failed	AAA server not updated with applied credential, please update and try again	
SNMP	rw	Success	Device credential in sync with credential assigned to site.	

Focus: Current site (BRANCH-AAA)

Search Table

Add

As of: Mar 17, 2025 10:47 AM

Name	Type	Status	Actions
Lila	CLI	Failed (1)	

Changing credentials passwords for devices with AAA for Network Devices

Brownfield AAA, Template-Based AAA or AAA Configured via Network Settings

Servers

Device Credentials

IP Address Pools

AAA

Global

Canada

Ontario

Toronto

BRANCH-AAA

Create and configure

Assigned credentials

CLI

Assign a CLI credential

Credential*

Lila

SNMPv2c Read

Assign an SNMPv2c Read

Credential Status

Type	Name/Description	Status	Details	Actions
CLI	Lila	Failed	AAA server not updated with applied credential, please update and try again	
SNMP	rw	Success	Device credential in sync with credential assigned to site.	

- If credentials are invalid, action will fail
- Change the password in ISE/AAA before applying new credential passwords
- If an AD/LDAP is integrated with ISE, perform the credential update in AD/LDAP

Netconf failure

- Netconf is mandatory for C9800 WLC and recommended for C9K switches

All Discoveries

C9200L-1

Date • Apr 3, 2025 12:31 PM (1) ▾

As of: Apr 3, 2025 12:36 PM ↺

✔ Completed

Type: Range Retry Count: 3 Protocol Order: SSH Total Time: 5 minutes 9 seconds [View all details](#) [Re-discover](#)

DEVICE SUMMARY

1

1

0

0

Discovered Successful Failed Discarded

Search Table

Export

IP Address ▴	Device Name	Status	ICMP	SNMP	CLI	HTTP(s)	NETCONF
10.85.54.23	C9200L-1.lila.com	✔	✔	✔	✔	⊖	<div>✖</div>

Netconf failure

```
C9200L-1#show ver
Cisco IOS XE Software, Version 17.08.01
```

```
C9200L-1#show run | section aaa
aaa new-model
aaa group server radius dnac-network-radius-group
  server name dnac-radius_10.85.54.185
  ip radius source-interface Vlan419
aaa authentication login VTY1_authen group dnac-network-radius-group local
aaa authorization exec VTY1_author group dnac-network-radius-group local if-authenticated
aaa accounting update newinfo periodic 2880
aaa accounting exec default start-stop group dnac-network-radius-group
aaa session-id common
```

```
C9200L-1#
Apr  3 16:31:21.440: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: netadmin] [Source: 10.85.54.180] [localport: 22] at 16:31:21 UTC Thu Apr 3 2025
Apr  3 16:31:21.535: %SYS-6-LOGOUT: User netadmin has exited tty session 4(10.85.54.180)
C9200L-1#
Apr  3 16:31:21.823: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: netadmin] [Source: 10.85.54.180] [localport: 22] at 16:31:21 UTC Thu Apr 3 2025
Apr  3 16:31:22.452: %DMI-5-AUTHORIZATION_FAILED: Switch 1 R0/0: dmiauthd: User 'netadmin' from 10.85.54.180:40254 was not authorized for netconf over ssh.
Apr  3 16:31:22.665: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: netadmin] [Source: 10.85.54.180] [localport: 22] at 16:31:22 UTC Thu Apr 3 2025
C9200L-1#
Apr  3 16:31:22.962: %SYS-5-CONFIG_I: Configured from console by netadmin on vty2 (10.85.54.180)
C9200L-1#
Apr  3 16:31:44.638: %DMI-5-AUTHORIZATION_FAILED: Switch 1 R0/0: dmiauthd: User 'netadmin' from 10.85.54.180:16298 was not authorized for netconf over ssh.
C9200L-1#
Apr  3 16:31:55.039: %SYS-6-LOGOUT: User netadmin has exited tty session 4(10.85.54.180)
C9200L-1#
Apr  3 16:32:04.917: %DMI-5-AUTHORIZATION_FAILED: Switch 1 R0/0: dmiauthd: User 'netadmin' from 10.85.54.180:1311 was not authorized for netconf over ssh.
C9200L-1#
Apr  3 16:32:19.483: %SYS-6-LOGOUT: User lila has exited tty session 3(10.85.54.180)
C9200L-1#
Apr  3 16:32:25.195: %DMI-5-AUTHORIZATION_FAILED: Switch 1 R0/0: dmiauthd: User 'netadmin' from 10.85.54.180:41401 was not authorized for netconf over ssh.
C9200L-1#
Apr  3 16:32:45.472: %DMI-5-AUTHORIZATION_FAILED: Switch 1 R0/0: dmiauthd: User 'netadmin' from 10.85.54.180:1438 was not authorized for netconf over ssh.
C9200L-1#
```

Netconf Requirements

- Discover C9800 WLC's and C9K switches with Netconf port enabled. Port 830 is recommended. Do not use standard ports like 22, 80, 8080
- Netconf uses SSH credentials and it has to be admin privilege
- If aaa new-model is enabled,
 - IOS XE < 17.9.x, default method needs to be specified for netconf
aaa authorization exec default <local or radius/tacacs group>
aaa authentication login default <local or radius/tacacs group>
 - IOS XE > 17.9.x, custom AAA method list can be specified for programmatic interfaces
yang-interfaces aaa authentication method-list <custom method list>
yang-interfaces aaa authorization method-list <custom method list>

Netconf failure solved

C9200L-1

Date • Apr 3, 2025 12:43 PM (1) ▾

As of: Apr 3, 2025 12:46 PM

Completed

Type: Range

Retry Count: 3

Protocol Order: SSH

Total Time: 0 minutes 4 seconds

[View all details](#)

[Re-discover](#)

DEVICE SUMMARY

1

1

0

0

Discovered

Successful

Failed

Discarded

Search Table

[Export](#)

Netconf failure solved

```
C9200L-1#show run | section aaa  
aaa new-model
```

```
aaa group server radius dnac-network-radius-group  
server name dnac-radius_10.85.54.185  
ip radius source-interface Vlan419
```

```
aaa authentication login default local
```

```
aaa authentication login VTY1 authen group dnac-network-radius-group local
```

```
aaa authorization exec default local
```

```
aaa authorization exec VTY1_author group dnac-network-radius-group local if-authenticated
```

```
aaa accounting update newinfo periodic 2880
```

```
aaa accounting exec default start-stop group dnac-network-radius-group
```

```
aaa session-id common
```

```
C9200L-1#show ver
```

```
Cisco IOS XE Software, Version 17.08.01
```

```
C9200L-1#
```

```
Apr 3 16:43:16.910: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: netadmin] [Source: 10.85.54.180] [localport: 22] at 16:43:16 UTC Thu Apr 3 2025
```

```
Apr 3 16:43:16.998: %SYS-6-LOGOUT: User netadmin has exited tty session 2(10.85.54.180)
```

```
C9200L-1#
```

```
Apr 3 16:43:17.286: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: netadmin] [Source: 10.85.54.180] [localport: 22] at 16:43:17 UTC Thu Apr 3 2025
```

```
C9200L-1#
```

```
Apr 3 16:43:17.902: %DMI-5-AUTH_PASSED: Switch 1 R0/0: dmiauthd: User 'netadmin' authenticated successfully from 10.85.54.180:50313 for netconf over ssh. External groups: PRIV15
```

```
Apr 3 16:43:18.832: %SYS-5-CONFIG_I: Configured from 10.85.54.180 by snmp
```

```
C9200L-1#
```

```
Apr 3 16:43:19.341: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: netadmin] [Source: 10.85.54.180] [localport: 22] at 16:43:19 UTC Thu Apr 3 2025
```

```
C9200L-1#
```

```
Apr 3 16:43:25.352: %DMI-5-AUTH_PASSED: Switch 1 R0/0: dmiauthd: User 'netadmin' authenticated successfully from 10.85.54.180:6246 for netconf over ssh. External groups: PRIV15
```

Netconf failure solved

Using custom AAA method list

```
aaa new-model
!  
!  
aaa group server radius dnac-network-radius-group  
  server name dnac-radius_10.85.54.185  
  ip radius source-interface Vlan419  
!  
aaa authentication login VTY1 authn group dnac-network-radius-group local  
aaa authentication login netconf-authn group dnac-network-radius-group local  
aaa authorization exec VTY1 authn group dnac-network-radius-group local if-authenticated  
aaa authorization exec netconf-authr group dnac-network-radius-group local if-authenticated  
aaa accounting update newinfo periodic 2880  
aaa accounting exec default start-stop group dnac-network-radius-group  
.  
netconf-yang  
yang-interfaces aaa authentication method-list netconf-authn  
yang-interfaces aaa authorization method-list netconf-authr
```

ISE Configuration

	C9800_NETCONF_	AND	 InternalUser-IdentityGroup EQUALS User Identity Groups:Employee	<input type="text" value="x Device_LVL15"/>		Employees	<input type="text" value="x"/>		0	
	_NETCONF	AND	 InternalUser-IdentityGroup EQUALS User Identity Groups:Employee	<input type="text" value="x Device_LVL15"/>		Employees	<input type="text" value="x"/>		0	
			 Network Access-NetworkDeviceName CONTAINS 9800							
			 NETCONF_9200							

Evolution to Per-Device Configuration/Campus Automation

Evolution of Automation



Simplified View and Edit of Switch Configuration

- Summary View of Configurations
- Actionable Switch Ports
- Instant Edit and Provisioning
- View/Edit of Detailed Configurations

All Devices / C9K-STANDALONE-2.cirrus.cloud

C9K-STANDALONE-2.cirrus.cloud

Run Commands

View 360

Reachable

Managed

IP Address: 10.85.54.26

Device Model: Cisco Catalyst 9300 Switch

Device Role: ACCESS

Site: Global/Canada/Ontario/Toronto/TBRANCH-SCARBOROUGH

CONFIGURATION

Layer 2

VLAN

Discovery Protocols

STP

VTP

DHCP Snooping

IGMP Snooping

MLD Snooping

Authentication

Cisco TrustSec

Logical Ports

Port Configuration

Discovery Protocols

CDP

Admin Status: Enabled (default)

Hold Time: 180 (default)

Timer: 60 (default)

Default Configurations

LLDP

Admin Status: Disabled (default)

Hold Time: 120 (default)

Timer: 30 (default)

Default Configurations

Catalyst Center- Per-Device Configuration - Switches

Phase 1: Layer 2 configurations

CONFIGURATION

Layer 2

VLAN

Discovery Protocols

STP

VTP

DHCP Snooping

IGMP Snooping

MLD Snooping

Authentication

Cisco TrustSec

Logical Ports

Port Configuration

Port Configuration

Ports (41)

Search Table

Port Name	Switchport Description
TenGigabitEthernet1/0/22	--
TenGigabitEthernet1/0/23	***** Uplink #1 to C3650 DISTRI **
TenGigabitEthernet1/0/24	***** Uplink #2 to C3650 DISTRI **
TenGigabitEthernet1/1/1	--

Simplified visualization

View Port

Port Name

TenGigabitEthernet1/0/23

Switchport

Description

***** Uplink #1 to C3650 DISTRI *****

Mode

Trunk

Access VLAN ID

1 (default)

Voice VLAN ID

--

Admin Status

Enabled (default)

Allowed VLANs

419,420

Default Configurations

VLAN Trunking

Dot1x

Authentication Mode

Closed (default)

Close

Catalyst Center- Per-Device Configuration - Switches

Phase 1: Layer 2 configurations

Edit 2 Port

2 Selected Ports >

Switchport

Switchport Description ⓘ

Switchport Mode ⓘ

Switchport Access VLAN ID ⓘ

Switchport Admin Status ⓘ

Campus Automation Description

Access ⓘ ▾

420 (VLAN0420) ⓘ ▾

Enabled ⓘ ▾

+ Add Configurations



Configuration to be Deployed ⓘ

10 Line(s)

```
1 interface GigabitEthernet1/1/2
2   description Campus Automation Description
3   switchport access vlan 420
4   switchport mode access
5   exit
6 interface GigabitEthernet1/1/3
7   description Campus Automation Description
8   switchport access vlan 420
9   switchport mode access
10  exit
```

Simplified Configuration

Catalyst Center- Per-Device Configuration - Switches



Reference

Pre-Requisites

- Catalyst 9000 Series Switches running Cisco IOS-XE 17.3 or later
- Cisco Catalyst Center version 2.3.7.9 or later
 - L2 Configurations available
- For devices provisioned using SDA, only Config Visibility is supported

9800 WLC - Per device configuration

All Devices / ar9800.adamlab.cisco.com

ar9800.adamlab.cisco.com

Manage 1 APs

Run Commands

View 360

Last Updated: 3 hours 12 minutes ago

Reachable

Managed

IP Address: 10.10.21.200

Device Model: Cisco Catalyst 9800-CL Wireless Controller for Cloud

Device Role: ACCESS

Uptime: 185 days 11 hrs 18 mins

Site: Global/SYD/north sydney

SECURITY

Advisories

FIELD NOTICES

Field Notices

Potential Field Notices

CONFIGURATION BETA

WLAN >

RF >

AP Join >

Flex Profiles

Tags >

Security >

Global Radio Configurations >

Global Wireless Configurations >

MDNS

EoGRE

Layer 2 >

Network Settings >

Hardware

Device Type

Wireless Controller

Series

Cisco Catalyst 9800 Wireless Controllers for Cloud

Platform

C9800-CL-K9

Serial Number

9MZF69DI31J

MAC Address

00:50:56:a0:66:8f

Vendor

Cisco

Software

Image

C9800-CL-universalk9.17.14.01.SPA.bin

Version

17.14.1

Operational Summary

Uptime

185 days 11 hrs 18 mins

Provision Status

Success

Last Provisioned

Jul 16, 2024 8:38 PM

Resync Interval

24 hours

Last Synced

3 hours ago

Cisco ISE Integration Status

Not Applicable

Private Beta: 2.3.7.6
Beta 2.3.7.9

IOS-XE 17.12+

Management choice: Site-Based or Per-device

All Devices / ar9800.adamlab.cisco.com

ar9800.adamlab.cisco.com

Manage 1 APs

Run Commands

View 360

Last Updated: 3 hours 12 minutes ago

Reachable

Managed

IP Address: 10.10.21.200

Device Model: Cisco Catalyst 9800-CL Wireless Controller for Cloud

Device Role: ACCESS

Uptime: 185 days 11 hrs 18 mins

Site: Global/SYD/north sydney

Search Features

DETAILS

Interfaces

System

Browse Configurations

User Defined Fields

Wireless Info

Mobility

SECURITY

Advisories

FIELD NOTICES

Field Notices

Potential Field Notices

WLAN Profiles

WLAN Profiles (2)

Search for WLAN Profile Name or SSID Name

0 Selected

	WLAN Profile Name	Status	WLAN ID	SSID Name	Policy Tags	AP Configuration Sets
☐	new_profile	✓	18	new	6	0
☐	test_profile	✓	17	test	3	1

2 Record(s)

Show Records: 25 1 - 2

Managed via Site-Based Network Profiles

This device is managed using site-based Network Profiles. All configurations are in **read-only** mode. Changes can only be made via the Network Profile.

2.3.7.9 – Convert to per-device mode

Catalyst Center

All Devices / pnp-9800

pnp-9800

Enable Per-Device Configuration

Run Commands

View 360

Reachable

Managed

IP Address: 10.10.10.146

Device Model: Cisco Catalyst 9800-CL Wireless Controller for Cloud

Device Role: ACCESS

Uptime: 63 d

DETAILS

Interfaces

System

Browse Configurations

User Defined Fields

Wireless Info

Hardware

Device Type

Wireless Controller

Series

Cisco Catalyst 9800 Wireless Co Cloud

Platform

C9800-CL-K9, C9800-CL-K9

Serial Number

9P015USKRB8, 93KOFYPUL17

MAC Address

00:1e:e5:a7:bf:ff

Vendor

Cisco

Software

Image

C9800-CL-universalk9.17.12.03.SPA.bin

Version

17.12.3

Operational Summary

Uptime

63 days 5 hrs 30 mins

Provision Status

Success

Last Provisioned

Dec 8, 2024 2:08 PM

Resync Interval

24 hours

Last Synced

4 hours ago

Cisco ISE Integration Status

Success

SECURITY

Advisories

FIELD NOTICES

Field Notices

Potential Field Notices

Device Mode	Per Device Config Support
Intent Mode config	read only
Greenfield	read-write
Assurance only	read-write



Per-Device configuration mode

All Devices / ar9800.adamlab.cisco.com

ar9800.adamlab.cisco.com

Manage 1 APs

Run commands

View 360

Last Updated: 3 hours 11 minutes ago

Reachable

Managed

IP Address: 10.10.21.200

Device Model: Cisco Catalyst 9800-CL Wireless Controller for Cloud

Device Role: ACCESS

Uptime: 27 days 27 mins

Site: Global/Sydney/RoseBay

DETAILS

Interfaces

System

Browse Configurations

User Defined Fields

Wireless Info

CONFIGURATION

WLAN

WLAN Profiles

Policy Profiles

Remote LAN Profiles

Remote LAN Policies

802.11be Profiles

WLAN Profiles ⓘ

Per-device configuration ⓘ ⚠

WLAN Profiles (3)

Search for WLAN Profile Name or SSID Name

0 Selected Actions

☐	WLAN Profile Name	Status	WLAN ID	SSID Name	Policy Tags	AP Configuration Sets
☐	new_profile	✓	18	new	6	0
☐	test_profile	✓	17	test	3	1
☐	sss_profile	✗	1	sss	0	0

3 Record(s)

Show Records: 25 1 - 3

Any configurations made outside Catalyst Center (e.g., via CLI or WebUI) will be detected and imported at the next inventory sync, which may cause conflicts. To ensure consistency and predictable outcomes, it's recommended always use Catalyst Center for all supported configurations.

Features supported



Reference

WLAN

- WLAN Profiles
- Policy Profiles
- Remote LAN Profiles
- Remote LAN Policies
- 802.11be Profiles

RF

- RF Profiles
- Radio Antenna Profiles
- Multi BSSID Profiles

AP Join

- AP Join Profiles
- AP Priming
- Mesh
- Power Profiles
- Calendar Profile

Flex Profiles

Tags

- Site Tags
- Policy Tags
- RF Tags
- Tag Mapping

Security

- AAA
- AAA Policy
- ACL
- EAP
- URL Filters
- Guest User
- Web Auth
- Trustsec
- Local Policy
- Wireless Protection Policies

Global Radio Configurations

- CleanAir
- High Throughput
- Media Parameters
- Network Parameters
- Global Parameters
- RRM

Global Wireless Configurations

- Airtime Fairness
 - Guest LAN
 - Media Stream
 - Advanced
 - Multicast
 - Location
 - Excluded Clients
 - QoS
 - Application Visibility
 - ~~Mobility**~~
 - Country
- mDNS
- EoGRE
- Layer 2
- VLAN
 - Interfaces
 - Discovery Protocols

Network Settings

- DHCP Pools
- HTTP/HTTPS
- SNMP
- NTP

Layer 3

- Routing

Administration

- Device
- User Administration
- DNS
- ~~Mobility**~~

in 2.3.7.9

New in 3.1.3

** removed in 3.1.5

Mobility is now part of inventory configuration (not per-device)

AllRoutersSwitchesWireless ControllersAccess PointsSensors

Devices (4)Focus: Software ImagesTake a tourExport

Click here to apply basic or advanced filters or view recently applied filters

1 SelectedTag + Add deviceSoftware Image ManagementActionsAs of: Oct 1, 2025 11:20 A

	Tags	Device Name	IP Address	Reachability	Image Version
☐		9k-tor-app-temp.adamlab.cisco.com	10.10.10.10		17.18.1
☐		APF4BD.9E9A.F1EC	10.10.10.10		17.15.3.28
☒		ar9800.adamlab.cisco.com	10.10.10.10		17.15.3
☐		perth-9k-edge	10.10.10.10		17.15.3

Inventory>Software Image>Provision>Telemetry>Device Replacement>Switch Refresh>Compliance>More>

Assign Device to SiteProvision DeviceConfigure WLC HAConfigure WLC MobilityManage LED Flash StatusFactory Reset

A Policy Profile contains a lot of attributes

Edit Policy Profile: adam

Search

General

Access Policies

QoS and AVC

Mobility

Advanced

WLAN Timeout

WLAN Flex Policy

AAA Policy

DHCP

DNS Layer Security

Miscellaneous

Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General

Configure WLAN switching policy , status and related configs

Policy Profile Name

adam

Description

Length: 0 to 64

Status

IP MAC Binding

Passive Client

Encrypted Traffic Analytics

WLAN Switching Policy

Central Switching

Central Authentication

Central DHCP

Flex NAT/PAT

© 2025 Cisco and/or its affiliates. All rights reserved.

BRKOPS-2697

Example: Turn off 2.4GHz

Search

General

Security

Layer 2

Layer 3

AAA

Advanced

11ax

11k

11v BSS

Device Analytics

Max Clients

Off Channel Scan

Miscellaneous

General

The General tab allows to define the basic WLAN profile properties such as the name, the SSID, the WLAN ID, radio policy and so on.

SSID State

Admin Status

Broadcast SSID

Radio Policy

Show Slot Configuration

6 GHz

5 GHz

2.4 GHz

Bg Policy*

802.11b/g

Band Select

6 GHz Client Steering

Search

General

Security

Layer 2

Layer 3

AAA

Advanced

11ax

11k

11v BSS

Device Analytics

Max Clients

Off Channel Scan

Miscellaneous

General

The General tab allows to define the basic WLAN profile properties such as the name, the SSID, the WLAN ID, radio policy and so on.

SSID State

Admin Status

Broadcast SSID

Radio Policy

Show Slot Configuration

6 GHz

5 GHz

2.4 GHz

Edit WLAN Profile: test_profile / Provision

Provision

Learn how the Visibility and Control of Configurations feature helps optimize your workflow.

This workflow supports enforcing network administrators and other users to preview configurations before deploying them on the network devices. To configure this setting, go to [System](#) → [Settings](#) → [Visibility and Control of Configurations](#).

Now

Preview and Deploy (Recommended)

Allows previewing device configurations and deploying them at any time. View status in [Tasks](#)

Task Name*

Edit WLAN Profile: test_profile-04_Dec_2024_

Now in VCR mode

Edit WLAN Profile: test_profile / Provision

Provision

Learn how the Visibility and Control of Configurations feature helps optimize your workflow.

This workflow supports enforcing network administrators and other users to preview configurations before deploying them on the network devices. To configure this setting, go to [System](#) → [Settings](#) → [Visibility and Control of Configurations](#).

Now

Preview

Allow

any time. View status in [Tasks](#)

Task Name

Edit WLAN

Warning

You are provisioning changes using the Per-Device Configuration. This feature is currently in **Beta** with no official Cisco technical support. Contact [Cisco](#) for more details.

Cancel

Ok

Cancel

Apply

Edit WLAN Profile: test_profile-04_Dec_2024_12_48_AM

As of: 12:51:58 AM

Step 1 of 3: Performing Initial Checks

Cisco Catalyst Center is now performing early validations to ensure a seamless provisioning operation.

✓ Pending Operations ⓘ

Success. No pending operations conflicting with the current operation found.

✓ Device Level Validations ⓘ

Success. No issues were found on a preliminary check of the devices involved in this operation. More checks will be performed as the workflow progresses. Currently, these preliminary checks are performed only on Switches and Routers. Wireless controllers, Access Points and other devices are not included.

Exit

Recheck

Back

Next

© 2025 Cisco and/or its affiliates. All rights reserved.

BRKOPS-2697

Visibility

Edit WLAN Profile: test_profile-04_Dec_2024_12_48_AM

As of: 12:52:58 AM [Refresh](#)

Step 3 of 3: Preview Configuration

Review the device configuration provided below by clicking on each device. When you are done reviewing, click Deploy. Click [Exit and Preview Later](#) to defer the review. The deferred review can be found in the [Tasks](#) menu.

Status: ✓ Ready

Search by device name

ar9800.adamlab.cisco.com ✓

Device IP: 10.10.21.200 Site: Global/Syd ⓘ

Configuration to be Deployed

View by Configuration Source • All ▾

Search configuration

YANG - All

17 Line(s)

```
1 <wlan-cfg-data xmlns= "http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-wlan-cfg" >
2   <wlan-cfg-entries >
3     <wlan-cfg-entry >
4       <profile-name>
5         <![CDATA[test_profile]]>
6       </profile-name>
7       <wlan-radio-policies >
8         <wlan-radio-policy >
9           <band>dot11-5-ghz-band</band>
10          <slot0>true</slot0>
11          <slot1>true</slot1>
12          <slot2>true</slot2>
13        </wlan-radio-policy>
14      </wlan-radio-policies>
15    </wlan-cfg-entry>
16  </wlan-cfg-entries>
17 </wlan-cfg-data>
```

[Generation Status Legend](#)

[Exit and Preview Later](#) [Discard](#) [Deploy](#)

Provisioning Task

Edit WLAN Profile: test_profile-04_Dec_2024_12_48_AM

Task

• PROVISION

Active

• In Progress

Start: Dec 4, 2024 12:53 AM

As of: 12:53:49 AM

Refresh

TASK PROGRESS

✓

⏹ Stop

1

1

0

0

0

0

Total

Success

Failed

Stopped

In Progress

Not Started

i

This task was created to deploy configuration that was previously previewed as a work item. [View Work Item Details](#)

Hostname

ar9800.adamlab.cisco.com

IP Address

10.10.21.200

Status

✓ Success

▼ Payload

```
{
  "featureName": "WlanConfigProfileGen_Configuration",
  "featureInstances": [
    {
      "@operator": "UPDATE",
      "connectedModelGraph": {
        "wlanDot11BeProfileName": "",
        "wlanRadioPolicyGen": {
          "@class": "com.cisco.dnac.wireless.model.WlanCfg.WlanRadioPolicyGen",
          "wlanRadioPolicySlot0": true,
          "wlanRadioPolicyBand": "DOT11_5_GHZ_BAND",
          "cd7c-42ca-961c-6be2f358a5f2",
          "wlanProfileName": "test_profile",
          "wlanRadioPolicySlot2": true,
          "wlanRadioPolicySlot1": true
        }
      }
    }
  ]
}
```



Success

Edit WLAN Profile: test_profile-04_Dec_2024_12_48_AM

Task

PROVISION

Completed

Success

Start: Dec 4, 2024 12:53 AM

End: Dec 4, 2024 12:53 AM

As of: 12:54:30 AM

Refresh

TASK PROGRESS

✓

Stop

1

1

0

0

0

0

Total

Success

Failed

Stopped

In Progress

Not Started

i

This task was created to deploy configuration that was previously previewed as a work item. [View Work Item Details](#)

Hostname

ar9800.adamlab.cisco.com

IP Address

10.10.21.200

Status

Success

> Payload

Updating/Adding Telemetry

Update Telemetry Settings Task

Step 3 of 3: Preview Configuration

Review the device configuration provided below by clicking on each device. When you are done reviewing, click Deploy. Click [Exit and Preview Later](#) to defer the review. The deferred review can be found in the [Tasks](#) menu.

As of: 3:48:56 PM [Refresh](#)

Status: Ready

Search by device name

ar9800.adamlab.cisco.com

3 snmp-server source-interface traps GigabitEthernet1

4 no crypto pki trustpoint DNAC-CA

5 crypto key ***** rsa DNAC-CA

6 ip http client source-interface GigabitEthernet1

7 ip ssh source-interface GigabitEthernet1

8 ip ssh version 2

9 ip domain lookup

10 crypto pki trustpoint DNAC-CA

11 source interface GigabitEthernet1

12 enrollment mode ra

13 enrollment terminal

14 usage ssl-client

15 revocation-check crl none

16 exit

17 crypto pki authenticate DNAC-CA

18 -----BEGIN CERTIFICATE-----

19 -----END CERTIFICATE-----

Generated CLI - All

8 Line(s)

Below is the "CLI preview" of the effective configuration change on the device after applying the YANG configuration payload. This CLI configuration should not be applied directly by logging onto the device.

1 crypto pki trustpoint sdn-network-infra-iwan

2 enrollment url http://10.10.21.124:80/ejbca/publicweb/apply/scep/sdnscep-PREVIEW

3 fqdn PREVIEW_FQDN.com

4 no revocation-check crl

5 no rsakeypair sdn-network-infra-iwan

6 subject-name CN=PREVIEW_sdn-network-infra-iwan

7 no subject-alt-name ar9800.adamlab.cisco.com

8 !

Is this feature helpful?

[Exit and Preview Later](#)

[Discard](#)

[Deploy](#)

This does not change from intent or assurance only.

Not part of the per device configuration

2.3.7.10 / 3.1.3 – clone profile from another device

All Devices / ar9800.adamlab.cisco.com

ar9800.adamlab.cisco.com

Manage 1 APs

Run commands

View 360

Last Updated: 31 minutes ago

Reachable

Managed

IP Address: 10.10.21.200

Device Model: Cisco Catalyst 9800-CL Wireless Controller for Cloud

Device Role: ACCESS

Uptime: 153 days 2 hrs 54 mins

Site: Global/Sydney/RoseBay

Search Features

DETAILS

Interfaces

System

Browse Configurations

User Defined Fields

Wireless Info

CONFIGURATION

WLAN

WLAN Profiles

Policy Profiles

Remote LAN Profiles

Remote LAN Policies

WLAN Profiles

Per-device configuration

Create WLAN Profile-30_Sep_2025_02_38_PM is completed successfully. View Task Details

WLAN Profiles (3)

Add

Clone from another WLC

Search for WLAN Profile Name or SSID Name

0 Selected Actions

	WLAN Profile Name	Status	WLAN ID	SSID Name	Policy Tags	AP Configuration Sets
☐	new_profile	✓	18	new	6	0
☐	test_profile	✓	17	test	3	1

© 2025 Cisco and/or its affiliates. All rights reserved.

BRKOPS-2697

AAA

All Devices / ar9800.adamlab.cisco.com

ar9800.adamlab.cisco.com

Manage 1 APs

Run commands

View 360

Last Updated: 16 hours 45 minutes ago

Reachable

Managed

IP Address: 10.10.21.200

Device Model: Cisco Catalyst 9800-CL Wireless Controller for Cloud

Device Role: ACCESS

Uptime: 34 days 18 hrs 27 mins

Site: Global/Sydney/RoseBay

User Defined Fields

Wireless Info

CONFIGURATION

WLAN

RF

AP Join

Flex Profiles

Tags

Security

AAA

AAA Policy

ACL

EAP

URL Filters

AAA

Per-device configuration

Servers/Groups

AAA Method List

AAA Advanced

AAA new-model is disabled, AAA Authorization Method List of Type EXEC & Group Type Local needs to be created to allow configuring AAA services.
Click here to create

RADIUS Servers (0)

Search for Server name, Server IP Address, Authentication Port or Accounting Port

0 Selected

Actions

Server Name

Server IP Address

Server IPv6 Address

Server FQDN

Authentication Port

Accounting Port

No data to display

```
ar9800#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ar9800(config)#aaa new
ar9800(config)#aaa new-model
ar9800(config)#end
ar9800#
```

Cisco Bug: CSCwm80901

Fixed in 3.2

Hulk P5: AAA PDC does not support adding aaa-new-model

Last Modified

Sep 17, 2025

Products (1)

Cisco DNA Center

Known Affected Release

CatC-2.3.7.9 Catc-2.3.7.10

Description (partial)

Symptom:

CactC Version:2.3.7.9-70163

eWLC : 17.14, 1712, 17.15

Description:

Issue: Per Device UI does not support adding AAA new model and without that all the provision tasks related to AAA config will fail

Steps:

Perform a couple of provision tasks on a large scale wlc to create AAA related config and make sure there is no aaa-new-model on the wlc

All the provision tasks will fail saying there is no aaa-new-model

Conditions:

CactC Version:2.3.7.9-70163

eWLC : 17.14, 1712, 17.15

Description:

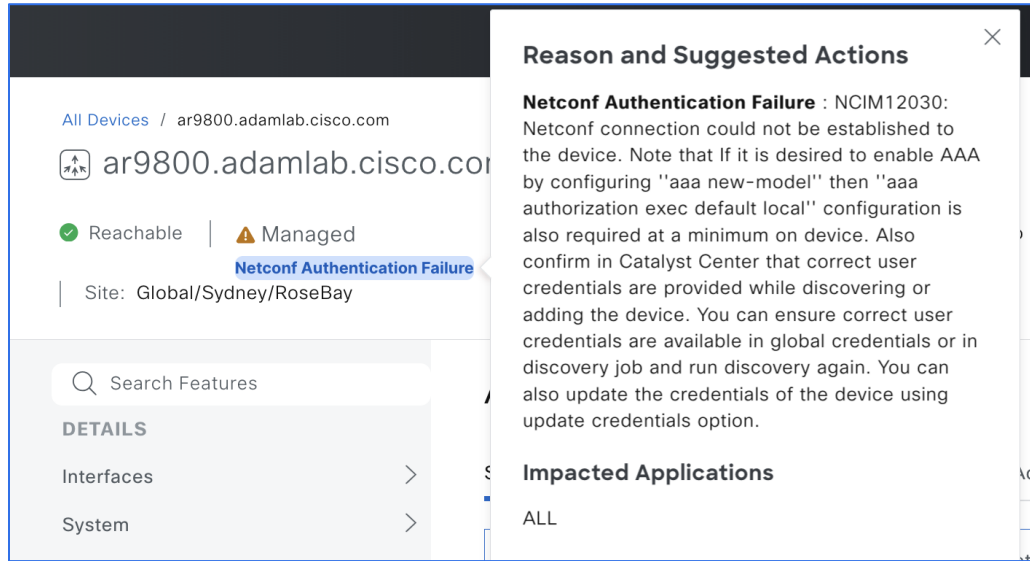
Issue: Per Device UI does not support adding AAA new model and without that all the provision tasks related to AAA config will fail

Steps:

Perform a couple of provision tasks on a large scale wlc to create AAA related config and make sure there is no aaa-new-model on the wlc

All the provision tasks will fail saying there is no aaa-new-model

new-model causes another issue



```
Nov 10 21:54:27.456: %DMI-5-AUTHORIZATION_FAILED: Chassis 1 R0/0: dmiauthd: User 'sdn' from 10.10.21.124:11797 was not authorized for netconf over ssh.
```

aaa new-model by itself breaks netconf

This command allow local authz for netconf

```
aaa authorization exec default local
```

AAA fixed – can now add servers

All Devices / ar9800.adamlab.cisco.com

ar9800.adamlab.cisco.com Manage 1 APs Run commands View 360

Last Updated: 8 minutes ago

Reachable Managed IP Address: 10.10.21.200 Device Model: Cisco Catalyst 9800-CL Wireless Controller for Cloud Device Role: ACCESS Uptime: 34 days 18 hrs 51 mins

Syncing...

Site: Global/Sydney/RoseBay

CONFIGURATION

WLAN >

RF >

AP Join >

Flex Profiles

Tags >

Security >

AAA

AAA Policy

ACL

EAP

URL Filters

AAA

Per-device configuration

Servers/Groups AAA Method List AAA Advanced

RADIUS Servers (0)

Search for Server name, Server IP Address, Authentication

0 Selected Actions

Server Name Server IP Address

Create RADIUS Server-11_Nov_2025_09_10_AM

Step 3 of 3: Preview Configuration

Review the device configuration provided below by clicking on each device. When you are done reviewing, click Deploy. Click [Exit and Preview Later](#) to defer the

Search by device name

ar9800.adamlab.cisco.com

Device IP: 10.10.21.200 Site: Global/Sydney/RoseBay

Configuration to be Deployed

View by Source • All

GENERATED CLI - ALL

4 Line(s)

Below is the "CLI preview" of the effective configuration change on the device after applying the YANG configuration payload

1 radius server ISE

2 address ipv4 10.10.10.127

3 key 0 PasswordPlaceholder

4 !

AAA server-groups

AAA ⓘ

Per-device configuration ⓘ ⚠

Servers/Groups ▾AAA Method List ▾AAA Advanced ▾

RADIUS

Servers

Server Groups

TACACS+

Servers

Server Groups

LDAP

Servers

Server Groups

Server name, Server IP Address, Authentication Port or Accounting Port

Server name

Server IP Address

Server IPv6 Address

Server FQDN

10.10.10.127

-

-

Create RADIUS Server Group

Server Group Name*
ise-radius-group ⓘ

MAC-Delimiter*
none ⓘ

Dead-Time (min)
5 ⓘ
Range: 0 to 1440

IPv4 Source Interface ⓘ

IPv4 VRF ⓘ

MAC-Filtering*
none ⓘ

☐ Load Balancing

IPv6 Source Interface ⓘ

IPv6 VRF ⓘ

Servers

Search

Add All

0 Unselected

Remove All

1 Selected

No Values Available

ISE

I always preview. I forgot to click add after selecting ISE (during testing)

Configuration to be Deployed

View by Source • All ▾

GENERATED CLI - ALL

5 Line(s)

Below is the "CLI preview" of the effective configuration change on the device

1aaa group server radius ise-radius-group

2server name ISE

3subscriber mac-filtering security-mode none

4mac-delimiter none

5!

© 2025 Cisco and/or its affiliates. All rights reserved.

BRKOPS-2697

What about the AP?

ar9800.adamlab.cisco.com **Manage 1 APs** Run commands View 360 Last Updated: 25 minutes ago

Reachable Managed IP Address: 10.10.21.200 Device Model: Cisco Catalyst 9800-CL Wireless Controller for Cloud Device Role: ACCESS Uptime: 34 days 19 hrs 52 mins Site: Global/Sydney/RoseBay

Search Features

DETAILS

Interfaces >

System >

Browse Configurations >

User Defined Fields

Wireless Info

Hardware

Device Type

Platform

MAC Address

Software

Image

Access Points

This Operational Access Points tab displays the state of the network only after the controller has been resynced. To configure other AP and Radio Parameters, launch the **Configure Access Points workflow**

Operational Access Points (1) Export

Click here to apply basic or advanced filters or view recently applied filters

0 Selected Edit AP Configuration Set Assign AP to Site As of: Nov 11, 2025

☐	AP Name	IP Address	AP Ethernet MAC Address	Connection Status	Policy Tag	Site Tag
☐	APF4BD.9E9A.F1EC	10.10.33.2	f4:bd:9e:9a:f1:ec	Reachable	PT_SYD_north_F1_407e5	ST_SYD_north

Access Points / Edit AP Configuration Set

Edit AP Configuration Set

AP Ethernet MAC Address f4:bd:9e:9a:f1:ec

Policy Tag* PT_SYD_north_F1_407e5

Site Tag* ST_SYD_northsyd_576e4_0

RF Tag* test

- Manage AP tags @ scale
- Bulk edit tags
- Use AP existing config workflows for other configuration
- Remember resync is important after any config push (it happens automatically – not instant)

Summary

Introduced in
CatC 2.3.7.9

Why Catalyst Center?

- ✓ Supports both **Brownfield** & **Greenfield** deployments
- ✓ C9800-like **intuitive UI** experience
- ✓ **Smart search**: find favorite “config” by name, description, or common terms – even with typo
- ✓ 95% **config parity** with Cisco Prime (for C9800 WLC)
- ✓ Config Cloning introduced in 2.3.7.10

CatC Platform offered capabilities

- ✓ **Visibility & Control**: change management with CLI preview
- ✓ **Config drift** detection: track what changed and when
- ✓ **Audit trail**: see who made changes and when
- ✓ **Assurance**: Visibility, Observability and Insights

How?

When 'Per-Device Configuration' is enabled, no configuration is pushed.

Catalyst Center only learns the device's existing configuration.

The image displays three screenshots of the Catalyst Center web interface, illustrating the process to enable per-device configuration for a Cisco Catalyst 9800 Wireless Controller (WLC).

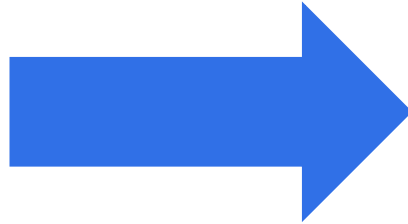
- Step 1: Inventory > View Device Details**: The first screenshot shows the 'Inventory' view with a list of devices. A callout points to the 'View Device Details' link for a specific device (C9800-IDT-13).
- Step 2: "Enable Per-Device Configuration"**: The second screenshot shows the 'View Device Details' page for the selected device. A callout points to the 'Enable Per-Device Configuration' toggle switch, which is currently turned on.
- Step 3: Resync WLC**: The third screenshot shows the 'WLAN Profiles' page. A callout points to the 'Resync WLC' button, which is used to synchronize the device's configuration with the Catalyst Center database.

* Capabilities mentioned are supported for Wired Infrastructure as well

What is next?

Per Device

Day-N
Wired + Wireless



**Config At
Scale**

Coverage/scale

3.1.5 Networks, and Device Groups - Beta

Networks

Learn more

Overview Unassigned devices 0

Q Search 1 results

Export Create Network

Network name	Device groups	Devices
Network 1	2	3

NOTE: Today this is switching only

← All networks

Network 1

Learn more Action

Device groups 2 Devices 3

Q Search 2 results

Export Create Device group

Device group name	Type	Devices
Device group 1	wired	2
Device group 2	wireless	1

- Networks are a logical grouping containing device groups
- Device groups are group of devices that have similar configuration
- Group profiles are configurations required in device groups
- Report on devices that don't have the configurations within the profile (config push in the future)

All networks > Network 1

Device group 1

Wired device group

Learn more

Devices

Q Search 2 results

Export Compare configuration Assign devices

Device name	IP address	Manageability	Platform	Uptime	Site
9k-tor-app-temp.adamlab.cisco.com	10.10.15.102	Managed	C9300-48U	7 days, 23:19:40.29	Global/S
perth-9k-edge	10.10.9.4	Managed	C9300-48U	111 days, 20:26:16.00	Global/S

3.1.5 Compare to profile – no provisioning (yet)

All networks > Network 1

Device group 1 Wired device group

Devices

Search

2 results

☐ Device name

☐ 9k-tor-app-temp

☐ perth-9k-edge

Compare configuration

All devices selected.

Compare the configurations of devices in a device group against a group profile.

Select profile type

Layer 2

Select profile

adam

Cancel

Compare

Compare configuration

All devices selected.

Compare the configurations of devices in a device group against a group profile.

Select profile type

Layer 2

Select profile

adam

Cancel

Compare

9k-tor-app-temp.adamlab.cisco.com

Compared with adam on Sep 30, 2025 03:47 PM

IP address

Platform

Device Role

Uptime

Site

Network

10.10.15.102

Cisco Catalyst 9300 Switch

ACCESS

7 days, 23 hrs

Global/Sydney/RoseBay

Network 1

Layer 2

VLAN

VLAN

Discovery Protocols

STP

VTP

DHCP Snooping

IGMP Snooping

MLD Snooping

UDLD

Authentication

VLANs (10)

Focus: Default View

Export

Search Table

VLAN ID

VLAN Name

Admin Status

15

Missing in profile

VLAN0015

Enabled

20

Missing in profile

VLAN0020

Enabled

80

Missing in profile

VLAN0080

Enabled

99

Missing in device

--

--

10 Record(s)

Show Records: 25

1 - 10

Automation beyond the UI: API's

API First 2.3.7.6 release notes

Table 6. New and Changed Features in Catalyst Center Platform, Release 2.3.7.7	
Feature	Description
New APIs	
Compliance API	<p>Catalyst Center platform supports the following Compliance API:</p> <ul style="list-style-type: none">POST <cluster-ip>/dna/intent/api/v1/compliance/networkDevices/\${id}/issues/remediation/provision Compliance Remediation. <p>To access the new Compliance API, click the menu icon and choose Platform > Developer Toolkit > APIs. Expand the Know Your Network drop-down list and choose Compliance.</p>
Issues APIs	<p>Catalyst Center platform supports the following Issues APIs:</p> <ul style="list-style-type: none">POST <cluster-ip>/dna/intent/api/v1/issues/resolve Resolve the given list of issues.POST <cluster-ip>/dna/intent/api/v1/issues/ignore Ignore the given list of issues.POST <cluster-ip>/dna/intent/api/v1/issues/\${id}/update Update the given issue by updating selected fields. <p>To access the new Compliance API, click the menu icon and choose Platform > Developer Toolkit > APIs. Expand the Know Your Network drop-down list and choose Issues.</p>
Licenses APIs	<p>Catalyst Center platform supports the following Licenses APIs:</p> <ul style="list-style-type: none">PUT <cluster-ip>/dna/intent/api/v1/licenseSetting Update license setting.GET <cluster-ip>/dna/intent/api/v1/licenseSetting Retrieve license setting. <p>To access the new Licenses APIs, click the menu icon and choose Platform > Developer Toolkit > APIs. Expand the Cisco DNA Center System drop-down list and choose Licenses.</p>
Network Settings APIs	<p>Catalyst Center platform supports the following Network Settings APIs:</p> <ul style="list-style-type: none">PUT <cluster-ip>/dna/intent/api/v1/sites/{id}/timeZoneSettings Set time zone for a site.PUT <cluster-ip>/dna/intent/api/v1/sites/{id}/bannerSettings Set banner settings for a site.PUT <cluster-ip>/dna/intent/api/v1/sites/{id}/telemetrySettings Set telemetry settings for a site. <p>To access the new Network Settings APIs, click the menu icon and choose Platform > Developer Toolkit > APIs. Expand the Site Management drop-down list and choose Network Settings.</p>
SDA APIs	<p>Catalyst Center platform supports the following SDA APIs:</p> <p>Multicast APIs</p> <ul style="list-style-type: none">GET <cluster-ip>/dna/intent/api/v1/sda/multicast/virtualNetworks Get multicast virtual networks.GET <cluster-ip>/dna/intent/api/v1/sda/multicast Get multicast.PUT <cluster-ip>/dna/intent/api/v1/sda/multicast/virtualNetworks Update multicast virtual networks.GET <cluster-ip>/dna/intent/api/v1/sda/multicast/virtualNetworks/count Get multicast virtual network count.DELETE <cluster-ip>/dna/intent/api/v1/sda/multicast/virtualNetworks/\${id} Delete multicast virtual network by ID.POST <cluster-ip>/dna/intent/api/v1/sda/multicast/virtualNetworks Add multicast virtual networks.

Site Design APIs	<p>Catalyst Center platform supports the following Site Design APIs:</p> <ul style="list-style-type: none">POST <cluster-ip>/dna/intent/api/v1/networkDevices/assignToSite/apply Assign network devices to a site.POST <cluster-ip>/dna/intent/api/v1/networkProfilesForSites/\${profileId}/siteAssignments Assign a network profile for sites to the given site <p>To access the new Site Design APIs, click the menu icon and choose Platform > Developer Toolkit > APIs. Expand the Site Management drop-down list and choose Site Design.</p>
SWIM APIs	<p>Catalyst Center platform supports the following SWIM APIs:</p> <ul style="list-style-type: none">GET <cluster-ip>/dna/intent/api/v1/images Get list of images available under the given site and product name.POST <cluster-ip>/dna/intent/api/v1/images/\${id}/download Download the software image from Cisco.com on the disk for the given 'id'.GET <cluster-ip>/dna/intent/api/v1/productNames Get the list of network device product names, their ordinal, and the support PIDs based on filter criteria.GET <cluster-ip>/dna/intent/api/v1/productNames/count Get count of product names based on filter criteria.GET <cluster-ip>/intent/api/v1/images/\${imageId}/productNames/\${productNameOrdinal} Update the list of sites for the network device product name assigned to the software image.GET <cluster-ip>/dna/intent/api/v1/siteWiseProductNames Get network device product names for a site.POST <cluster-ip>/dna/intent/api/v1/images/\${imageId}/productNames Assign network device product name and sites for the given image identifier.GET <cluster-ip>/dna/intent/api/v1/siteWiseProductNames/count Get the count of network device product names for the given filters.DELETE <cluster-ip>/dna/intent/api/v1/images/\${imageId}/productNames/\${productNameOrdinal} Removes the network device product name from all the sites for the given software image.PUT <cluster-ip> /dna/intent/api/v1/images/\${imageId}/productNames/\${productNameOrdinal} Update the list of sites for the network device product name assigned to the software image.GET <cluster-ip>/dna/intent/api/v1/images/count Count of images available under the given site and product name.GET <cluster-ip>/dna/intent/api/v1/images/\${id}/addonImages Retrieves the list of applicable add-on images if available for the given software image.GET <cluster-ip>/dna/intent/api/v1/images/\${id}/addonImages/count Count of add-on images available for the given software image identifier.GET <cluster-ip>/dna/intent/api/v1/images/distributionServerSettings Retrieve the list of remote image distribution servers.POST <cluster-ip>/dna/intent/api/v1/images/distributionServerSettings Add image distribution server for distributing software images.GET <cluster-ip>/dna/intent/api/v1/images/distributionServerSettings/\${id} Get image distribution server for specified server identifier.PUT <cluster-ip>/dna/intent/api/v1/images/distributionServerSettings/\${id} Update remote image distribution server.DELETE <cluster-ip>/dna/intent/api/v1/images/distributionServerSettings/\${id} Delete remote image distribution server.



2.3.7.9 release notes

For detailed information about the APIs, see the Cisco Catalyst Center APIs on Cisco DevNet .	
Table 9. New and changed features in Catalyst Center platform 2.3.7.9	
Feature	Description
New APIs	
Applications APIs	<p>Catalyst Center platform supports the following Applications APIs:</p> <ul style="list-style-type: none">• GET <cluster-ip>/dna/data/api/v1/networkApplications Retrieves the list of network applications along with experience and health metrics.• GET <cluster-ip>/dna/data/api/v1/networkApplications/count Retrieves the total count of network applications by applying basic filtering.• POST <cluster-ip>/dna/data/api/v1/networkApplications/trendAnalytics Retrieves the Trend analytics data related to network applications. <p>To access the new Applications APIs, click the menu icon and choose Platform > Developer Toolkit > APIs. Expand the Know Your Network drop-down list and choose Applications.</p>
Application Policy APIs	<p>Catalyst Center platform supports the following Application Policy APIs:</p> <ul style="list-style-type: none">• GET <cluster-ip>/dna/intent/api/v1/applicationVisibility/networkDevices Retrieve the list of network devices with their application visibility status.• GET <cluster-ip>/dna/intent/api/v1/applicationVisibility/networkDevices/count Retrieve the count of network devices for the given application visibility status filters.• POST <cluster-ip>/dna/intent/api/v1/applicationVisibility/networkDevices/enableAppTelemetry Enable application telemetry feature on multiple network devices.• POST <cluster-ip>/dna/intent/api/v1/applicationVisibility/networkDevices/disableAppTelemetry Disable application telemetry feature on multiple network devices.• POST <cluster-ip>/dna/intent/api/v1/applicationVisibility/networkDevices/enableCbar Enable CBAR feature on multiple network devices.• POST <cluster-ip>/dna/intent/api/v1/applicationVisibility/networkDevices/disableCbar Disable CBAR feature on multiple network devices.• GET <cluster-ip>/dna/intent/api/v1/qosPolicySetting Retrieves the application QoS policy setting.• PUT <cluster-ip>/dna/intent/api/v1/qosPolicySetting Updates the application QoS policy setting. <p>To access the new Application Policy APIs, click the menu icon and choose Platform > Developer Toolkit > APIs. Expand the Policy drop-down list and choose Application Policy.</p>
Cisco Integrated Management Controller (IMC) APIs	<p>Catalyst Center platform supports the following Cisco IMC APIs:</p> <ul style="list-style-type: none">• GET <cluster-ip>/dna/system/api/v1/ciscolmcs Retrieves Cisco IMC configurations for Catalyst Center nodes.• POST <cluster-ip>/dna/system/api/v1/ciscolmcs Adds Cisco IMC configuration to a Catalyst Center node.• GET <cluster-ip>/dna/system/api/v1/ciscolmcs/{id} Retrieves the Cisco IMC configuration for a Catalyst Center node.• PUT <cluster-ip>/dna/system/api/v1/ciscolmcs/{id} Updates the Cisco IMC configuration for a Catalyst Center node.• DELETE <cluster-ip>/dna/system/api/v1/ciscolmcs/{id} Deletes the Cisco IMC configurations for a Catalyst Center node. <p>To access the new Cisco IMC APIs, click the menu icon and choose Platform > Developer Toolkit > APIs. Expand the Appliance drop-down list and choose Cisco IMC.</p>
Compliance APIs	<p>Catalyst Center platform supports the following Compliance APIs:</p> <ul style="list-style-type: none">• POST <cluster-ip>/dna/intent/api/v1/networkBugs/trials Creates a trial for bugs detection on network devices.• GET <cluster-ip>/dna/intent/api/v1/networkBugs/trials Get trial details for bugs detection on network devices.• POST <cluster-ip>/dna/intent/api/v1/networkBugs/triggerScan
Configuration Archive APIs	<p>Catalyst Center platform supports the following Configuration Archive APIs:</p> <ul style="list-style-type: none">• GET <cluster-ip>/dna/intent/api/v1/networkDeviceConfigFiles Get Network Device Configuration File Details.• GET <cluster-ip>/dna/intent/api/v1/networkDeviceConfigFiles/count Count of Network Device Configuration Files.• GET <cluster-ip>/dna/intent/api/v1/networkDeviceConfigFiles/{id} Get Configuration File Details by ID.• POST <cluster-ip>/dna/intent/api/v1/networkDeviceConfigFiles/{id}/downloadMasked Download masked device configuration.• POST <cluster-ip>/dna/intent/api/v1/networkDeviceConfigFiles/{id}/downloadUnmasked Download Unmasked (raw) Device Configuration as ZIP. <p>To access the new Configuration Templates APIs, click the menu icon and choose Platform > Developer Toolkit > APIs. Expand the Site Management drop-down list and choose Configuration Archive APIs.</p>
Configuration Templates APIs	<p>Catalyst Center platform supports the following Configuration Templates APIs:</p> <ul style="list-style-type: none">• GET <cluster-ip>/dna/intent/api/v1/templates/{templateId}/networkProfilesForSites Retrieve the network profiles attached to a CLI template.• GET <cluster-ip>/dna/intent/api/v1/templates/{templateId}/networkProfilesForSites/count Retrieve count of network profiles attached to a CLI template.• POST <cluster-ip>/dna/intent/api/v1/templates/{templateId}/networkProfilesForSites Attach network profile to a Day-N CLI template.• POST <cluster-ip>/dna/intent/api/v1/templates/{templateId}/networkProfilesForSites/bulk Attach a list of network profiles to a Day-N CLI template.• DELETE <cluster-ip>/dna/intent/api/v1/templates/{templateId}/networkProfilesForSites/bulk Detach a list of network profiles from a Day-N CLI template.• DELETE <cluster-ip>/dna/intent/api/v1/templates/{templateId}/networkProfilesForSites/{profileId} Detach a network profiles from a Day-N CLI template.• GET <cluster-ip>/templates/{templateId}/versions Get Template Versions.• GET <cluster-ip>/dna/intent/api/v1/templates/{templateId}/versions/{versionId} Get Template Version.• GET <cluster-ip>/dna/intent/api/v1/templates/{templateId}/versions/count Get Template Versions Count.• POST <cluster-ip>/dna/intent/api/v1/templates/{templateId}/versions/commit Commit Template For a New Version.• GET <cluster-ip>/dna/intent/api/v1/projects Get Template Projects.• POST <cluster-ip>/dna/intent/api/v1/projects Create Template Project.• PUT <cluster-ip>/dna/intent/api/v1/projects/{projectId} Update Template Project.• GET <cluster-ip>/dna/intent/api/v1/projects/{projectId} Get Template Project.• DELETE <cluster-ip>/dna/intent/api/v1/projects/{projectId} Delete Template Project.• GET <cluster-ip>/dna/intent/api/v1/projects/count Get Template Project Count. <p>To access the new Configuration Templates APIs, click the menu icon and choose Platform > Developer Toolkit > APIs. Expand the Site Management drop-down list and choose Configuration Templates APIs.</p>
Devices APIs	<p>Catalyst Center platform supports the following Devices APIs:</p> <ul style="list-style-type: none">• POST <cluster-ip>/dna/intent/api/v1/networkDevices/deleteWithoutCleanup Delete a network device without configuration cleanup.• POST <cluster-ip>/dna/intent/api/v1/networkDevices/deleteWithCleanup

3.1.5 release notes

Site Design API Operations	The <code>siteHierarchyId</code> attribute is included in the response of these API operations: <ul style="list-style-type: none">• GET <cluster-ip>/dna/intent/api/v1/areas/\${id}• Gets an area.• GET <cluster-ip>/dna/intent/api/v2/buildings/\${id}• Gets a building.• GET <cluster-ip>/dna/intent/api/v2/floors/\${id}• Gets a floor.• GET <cluster-ip>/dna/intent/api/v1/sites• Get sites.		
Wireless API Operations	The <code>featureTemplates</code> attribute is included in the query of these API operations: <ul style="list-style-type: none">• POST <cluster-ip>/dna/intent/api/v1/wirelessProfiles• Create Wireless Profile.• PUT <cluster-ip>/dna/intent/api/v1/wirelessProfiles/\${id}• Update Wireless Profile.• POST <cluster-ip>/dna/intent/api/v1/wirelessControllers/\${deviceId}/provision• Wireless Controller Provision. The <code>featureTemplates</code> attribute is included in the response of these API operations: <ul style="list-style-type: none">• GET <cluster-ip>/dna/intent/api/v1/wirelessProfiles• Get Wireless Profiles.• GET <cluster-ip>/dna/intent/api/v1/wirelessProfiles/\${id}• Get Wireless Profile by ID. The <code>neighbourApName</code> attribute is included in the response and two new filters <code>meshAp</code> and <code>Get Mesh Ap Neighbours</code> . <ul style="list-style-type: none">• GET <cluster-ip>/dna/intent/api/v1/wirelessControllers/meshAp/Neighbours The <code>beamState</code> attribute is included as a query parameter in the API operation: <ul style="list-style-type: none">• POST <cluster-ip>/dna/intent/api/v1/wirelessAccessPoints/provision• AP Provision. With this release, <code>ssidRadioType</code> , <code>ghz24Policy</code> , <code>ghz60PolicyClientSteering</code> and <code>overridable</code> attributes.		
Deprecated API Operations	The <code>policyProfileName</code> attribute is included in the query of these API operations: <ul style="list-style-type: none">• POST <cluster-ip>/dna/intent/api/v1/ssid• Create SSID.• PUT <cluster-ip>/dna/intent/api/v1/ssid/\${id}• Update SSID.• POST <cluster-ip>/dna/intent/api/v1/ssid/\${id}/override• Update or Override SSID.• POST <cluster-ip>/dna/intent/api/v1/ssid/\${id}/update• Update Wireless Profile.		
Devices API Operations	Catalyst Center platform supports the following Devices API operations: <ul style="list-style-type: none">• POST <cluster-ip>/dna/data/api/v1/energy/networkDevices/query• Query devices energy.• POST <cluster-ip>/dna/data/api/v1/energy/networkDevices/query/count• Count devices energy from query.• GET <cluster-ip>/dna/data/api/v1/energy/networkDevices/count• Count devices energy.• GET <cluster-ip>/dna/data/api/v1/energy/networkDevices/\${id}• Get device energy by ID.• GET <cluster-ip>/dna/data/api/v1/energy/networkDevices• Get devices energy.• GET <cluster-ip>/dna/intent/api/v1/networkDevices/\${networkDeviceId}/portChannels/count• Retrieve port channels count for a network device.• GET <cluster-ip>/dna/intent/api/v1/networkDevices/\${networkDeviceId}/portChannels/\${id}• Retrieve information for the given port channel on a specific network device.• GET <cluster-ip>/dna/intent/api/v1/networkDevices/\${networkDeviceId}/portChannels• Retrieve the list of port channels for the network device. To access the new Devices API operations, click the menu icon and choose Platform > Developer Toolkit > API . Expand the Know Your Network drop-down list and choose Devices .		
Energy Analytics API Operations	Catalyst Center platform supports the following energy analytics API operations: <ul style="list-style-type: none">• POST <cluster-ip>/dna/data/api/v1/energy/trendAnalytics• Get energy trend analytics.• POST <cluster-ip>/dna/data/api/v1/energy/summaryAnalytics• Get energy summary analytics. To access the new energy analytics API operations, click the menu icon and choose Platform > Developer Toolkit > API . Expand the Know Your Network drop-down list and choose the API .		
Industrial Configuration API Operations	Catalyst Center platform supports the following Industrial Configuration API operations: <ul style="list-style-type: none">• GET <cluster-ip>/dna/intent/api/v1/fabric/repRings/\${id}• Get the REP ring based on the ring ID.• POST <cluster-ip>/dna/intent/api/v1/fabric/repRings/query• Retrieve the list of REP rings.• POST <cluster-ip>/dna/intent/api/v1/fabric/repRings/deploy• Configure a REP Ring on NON-FABRIC deployment.• POST <cluster-ip>/dna/intent/api/v1/fabric/repRings/delete• Delete REP ring configured in the NON-FABRIC deployment.• DELETE <cluster-ip>/dna/intent/api/v1/fabric/repRings/delete• Delete REP ring configured in the NON-FABRIC deployment.• POST <cluster-ip>/dna/intent/api/v1/fabric/repRings/count• Retrieve the count of REP rings.• POST <cluster-ip>/dna/intent/api/v1/fabric/repRings/members• Retrieve the list of MRP rings.• GET <cluster-ip>/dna/intent/api/v1/fabric/repRings/members• Retrieve the list of network devices part of MRP ring.• GET <cluster-ip>/dna/intent/api/v1/fabric/repRings/members/count• Retrieve the count of MRP ring members. To access the new Industrial Configuration API operations, click the menu icon and choose Platform > Developer Toolkit > API . Expand the Know Your Network drop-down list and choose Industrial Configuration .		
LAN Automation Port Channel API Operations	Catalyst Center platform supports the following LAN Automation Port Channel API operations: <ul style="list-style-type: none">• POST <cluster-ip>/dna/intent/api/v1/lanAutomation/portChannels• Create a New Port Channel between devices.• GET <cluster-ip>/dna/intent/api/v1/lanAutomation/portChannels• Get Port Channels.• GET <cluster-ip>/dna/intent/api/v1/lanAutomation/portChannels/\${id}• Get Port Channel Information by ID.• DELETE <cluster-ip>/dna/intent/api/v1/lanAutomation/portChannels/\${id}• Delete Port Channel.• POST <cluster-ip>/dna/intent/api/v1/lanAutomation/portChannels/\${id}/addLink• Add a LAN Automated link to a Port Channel.• POST <cluster-ip>/dna/intent/api/v1/lanAutomation/portChannels/\${id}/removeLink• Remove a link from Port Channel. To access the LAN Automation API operations, click the menu icon and choose Platform > Developer Toolkit > API . Expand the Site Management drop-down list and choose LAN Automation .		
Sites API Operations	Catalyst Center platform supports the following Sites API operations: <ul style="list-style-type: none">• GET <cluster-ip>/dna/data/api/v1/energy/sites/\${id}• Get site energy by ID.• GET <cluster-ip>/dna/data/api/v1/energy/sites• Get sites energy.• GET <cluster-ip>/dna/data/api/v1/energy/sites/count• Count sites energy.• POST <cluster-ip>/dna/data/api/v1/energy/sites/query• Submit request to query sites energy.• POST <cluster-ip>/dna/data/api/v1/energy/sites/query/count• Submit request to count sites energy from query. To access the new Sites API operations, click the menu icon and choose Platform > Developer Toolkit > API . Expand the Know Your Network drop-down list and choose Sites .		
Software Image Management (SWIM) API Operations	Catalyst Center platform supports the following SWIM API operations: <ul style="list-style-type: none">• GET <cluster-ip>/dna/intent/api/v1/networkDeviceImages• Get the list of network devices with image details.• GET <cluster-ip>/dna/intent/api/v1/networkDeviceImages/count• Count of network devices for the given status filters.• GET <cluster-ip>/dna/intent/api/v1/networkDeviceImages/\${id}• Fetch network device with image details.• POST <cluster-ip>/dna/intent/api/v1/networkDeviceImages/\${id}/activate• Update Images on the network devices.• POST <cluster-ip>/dna/intent/api/v1/networkDeviceImages/\${id}/distribute• Distribute Images on the network devices.• POST <cluster-ip>/dna/intent/api/v1/networkDeviceImages/activate/bulk• Bulk update images on network devices.• POST <cluster-ip>/dna/intent/api/v1/networkDeviceImages/distribute/bulk• Bulk distribute images on network devices.• POST <cluster-ip>/dna/intent/api/v1/networkDeviceImages/\${id}/readinessChecks• Trigger update readiness for network device.• GET <cluster-ip>/dna/intent/api/v1/networkDeviceImages/validationResults• Network device image update validation results.• GET <cluster-ip>/dna/intent/api/v1/networkDeviceImages/validationResults/count• Count of network device image update validation results.• GET <cluster-ip>/dna/intent/api/v1/productSeries• Retrieve the list of network device product series.• GET <cluster-ip>/dna/intent/api/v1/productSeries/count• Count of network product series.		
Wireless API Operations	Catalyst Center platform supports the following Wireless API operations: <ul style="list-style-type: none">• PUT <cluster-ip>/dna/intent/api/v1/systemSettings/apPhpLocation• Update AP Php Location Setting.• GET <cluster-ip>/dna/intent/api/v1/systemSettings/apPhpLocation• Get AP Php Location Setting.• DELETE <cluster-ip>/dna/intent/api/v1/sites/\${siteId}/wirelessSettings/flexConnectNativeVlan• Delete Native Vlan Settings By Site.• PUT <cluster-ip>/dna/intent/api/v1/sites/\${siteId}/wirelessSettings/flexConnectNativeVlan• Update Native Vlan Settings By Site.• GET <cluster-ip>/dna/intent/api/v1/sites/\${siteId}/wirelessSettings/flexConnectNativeVlan• Get Native Vlan Settings By Site.• DELETE <cluster-ip>/dna/intent/api/v1/sites/\${siteId}/wirelessSettings/flexConnectAaaOverride• Delete AAA Override Vlan Settings By Site.• PUT <cluster-ip>/dna/intent/api/v1/sites/\${siteId}/wirelessSettings/flexConnectAaaOverride• Update AAA Override Vlan Settings By Site.• GET <cluster-ip>/dna/intent/api/v1/sites/\${siteId}/wirelessSettings/flexConnectAaaOverride• Get AAA Override Vlan Settings By Site.• POST <cluster-ip>/dna/intent/api/v1/featureTemplates/wireless/eventDrivenRRMConfigurations• Create Event Driven RRM Configuration Feature Template.• GET <cluster-ip>/dna/intent/api/v1/featureTemplates/wireless/eventDrivenRRMConfigurations/\${id}• Get Event Driven RRM Configuration Feature Template.• PUT <cluster-ip>/dna/intent/api/v1/featureTemplates/wireless/eventDrivenRRMConfigurations/\${id}• Update Event Driven RRM Configuration Feature Template.• DELETE <cluster-ip>/dna/intent/api/v1/featureTemplates/wireless/eventDrivenRRMConfigurations/\${id}• Delete Event Driven RRM Configuration Feature Template.• POST <cluster-ip>/dna/intent/api/v1/featureTemplates/wireless/multicastConfigurations• Create Multicast Configuration Feature Template.• GET <cluster-ip>/dna/intent/api/v1/featureTemplates/wireless/multicastConfigurations/\${id}• Get Multicast Configuration Feature Template.• PUT <cluster-ip>/dna/intent/api/v1/featureTemplates/wireless/multicastConfigurations/\${id}• Update Multicast Configuration Feature Template.• DELETE <cluster-ip>/dna/intent/api/v1/featureTemplates/wireless/multicastConfigurations/\${id}• Delete Multicast Configuration Feature Template.• POST <cluster-ip>/dna/intent/api/v1/featureTemplates/wireless/dot11axConfigurations• Create Dot11ax Configuration Feature Template.• PUT <cluster-ip>/dna/intent/api/v1/featureTemplates/wireless/dot11axConfigurations/\${id}• Update Dot11ax Configuration Feature Template.		
Applications API Operations	Catalyst Center platform supports the following Applications API operations: <ul style="list-style-type: none">• POST <cluster-ip>/dna/data/api/v1/networkApplications/\${id}/trendAnalytics• Retrieve the Trend analytics related to specific network application.• POST <cluster-ip>/dna/data/api/v1/networkApplications/summaryAnalytics• Retrieve summary analytics data related to network applications along with health metrics.• GET <cluster-ip>/dna/data/api/v1/thousandeyesTestResults/trendAnalytics• The trend analytics data for ThousandEyes test results in the specified time range.• GET <cluster-ip>/dna/data/api/v1/thousandeyesTestResults• Retrieve the list of ThousandEyes test results along with related metrics.• GET <cluster-ip>/dna/data/api/v1/thousandeyesTestResults/count• Retrieve the total count of ThousandEyes test results. To access the new Applications API operations, click the menu icon and choose Platform > Developer Toolkit > API . Expand the Know Your Network drop-down list and choose Applications .		
Backup API Operations	Catalyst Center platform supports the following Backup APIs operations: <ul style="list-style-type: none">• GET <cluster-ip>/dna/system/api/v1/backupStorages• Get Backup Storages.• GET <cluster-ip>/dna/system/api/v1/backups/\${id}• Get Backup By ID.• POST <cluster-ip>/dna/system/api/v1/backupNfsConfigurations• Create NFS Configuration.• DELETE <cluster-ip>/dna/system/api/v1/backups/\${id}• Delete Backup.• GET <cluster-ip>/dna/system/api/v1/backupRestoreExecutions/\${id}• Get Backup And Restore Execution.• DELETE <cluster-ip>/dna/system/api/v1/backupNfsConfigurations/\${id}• Delete NFS Configuration.• GET <cluster-ip>/dna/system/api/v1/backupNfsConfigurations• Get All NFS Configuration.• GET <cluster-ip>/dna/system/api/v1/backups• Get All Backup.• GET <cluster-ip>/dna/system/api/v1/backupRestoreExecutions• Get Backup And Restore Executions.• POST <cluster-ip>/dna/system/api/v1/backupConfiguration• Create Backup.• POST <cluster-ip>/dna/system/api/v1/backupConfiguration• Create Backup Configuration.• GET <cluster-ip>/dna/system/api/v1/backupConfiguration• Get Backup Configuration.• POST <cluster-ip>/dna/system/api/v1/backups/\${id}/restore• Restore Backup. To access the new Backup API operations, click the menu icon and choose Platform > Developer Toolkit > API . Expand the System drop-down list and choose Backup .		
Clients API Operations	Catalyst Center platform supports the following Clients API operations: <ul style="list-style-type: none">• GET <cluster-ip>/dna/data/api/v1/energy/clients/count• Count clients energy.• POST <cluster-ip>/dna/data/api/v1/energy/clients/query• Query clients energy.• GET <cluster-ip>/dna/data/api/v1/energy/clients• Get clients energy.• GET <cluster-ip>/dna/data/api/v1/energy/clients/\${id}• Get client energy by ID.• POST <cluster-ip>/dna/data/api/v1/energy/clients/query/count• Count clients energy.		



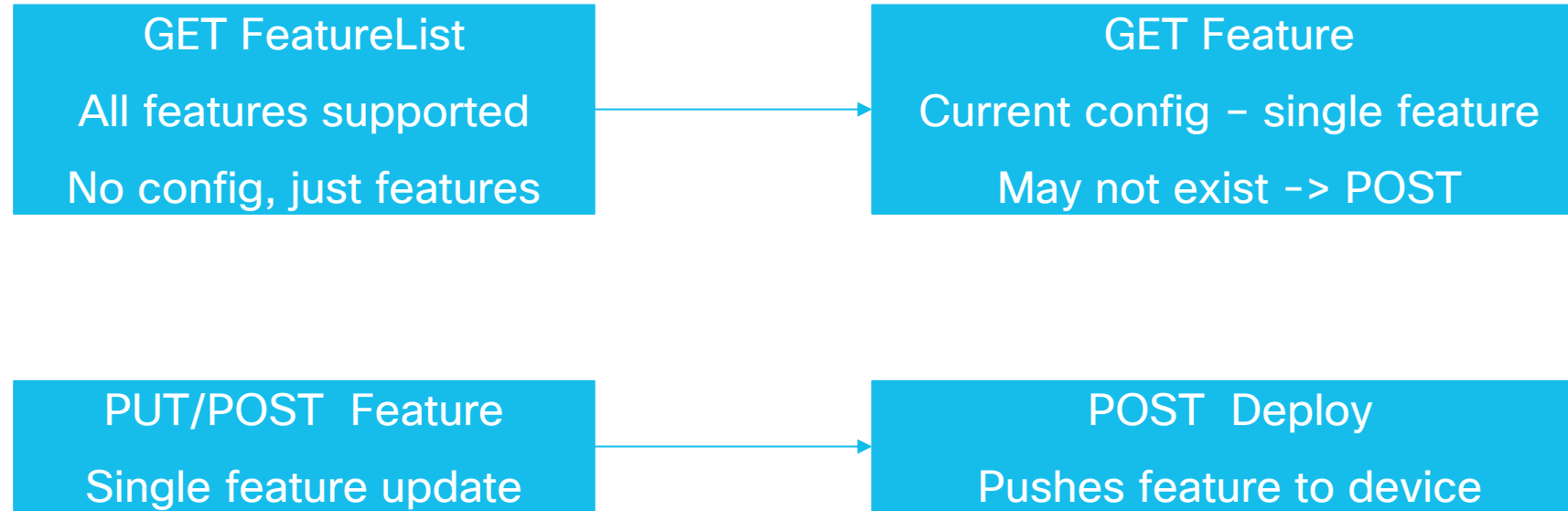
3.1.5 release notes

Compliance API Operations	<p>Catalyst Center platform supports the following Compliance API operations:</p> <ul style="list-style-type: none">• POST <cluster-ip>/dna/intent/api/v1/compliancePolicies Create a new policy.• GET <cluster-ip>/dna/intent/api/v1/compliancePolicies Retrieve the policies.• GET <cluster-ip>/dna/intent/api/v1/compliancePolicies/count Retrieve the count of policies.• GET <cluster-ip>/dna/intent/api/v1/compliancePolicies/\${id} Retrieve a specific policy.• PUT <cluster-ip>/dna/intent/api/v1/compliancePolicies/\${id} Update an existing policy.• DELETE <cluster-ip>/dna/intent/api/v1/compliancePolicies/\${id} Delete a specific policy.• POST <cluster-ip>/dna/intent/api/v1/compliancePolicies/\${policyId}/rules Create a new rule.• GET <cluster-ip>/dna/intent/api/v1/compliancePolicies/\${policyId}/rules Retrieve the rules.• GET <cluster-ip>/dna/intent/api/v1/compliancePolicies/\${policyId}/rules/count Retrieve the count of rules.• GET <cluster-ip>/dna/intent/api/v1/compliancePolicies/\${policyId}/rules/\${id} Retrieve a specific rule.• PUT <cluster-ip>/dna/intent/api/v1/compliancePolicies/\${policyId}/rules/\${id} Update an existing rule.• DELETE <cluster-ip>/dna/intent/api/v1/compliancePolicies/\${policyId}/rules/\${id} Delete a specific rule.• POST <cluster-ip>/dna/intent/api/v1/compliancePolicies/\${policyId}/rules/\${ruleId}/conditions Create a new condition• GET <cluster-ip>/dna/intent/api/v1/compliancePolicies/\${policyId}/rules/\${ruleId}/conditions Retrieve the conditions.• GET <cluster-ip>/dna/intent/api/v1/compliancePolicies/\${policyId}/rules/\${ruleId}/conditions/count Retrieve the count of conditions.• GET <cluster-ip>/dna/intent/api/v1/compliancePolicies/\${policyId}/rules/\${ruleId}/conditions/\${id} Retrieve a specific condition.• PUT <cluster-ip>/dna/intent/api/v1/compliancePolicies/\${policyId}/rules/\${ruleId}/conditions/\${id} Update an existing condition.• DELETE <cluster-ip>/dna/intent/api/v1/compliancePolicies/\${policyId}/rules/\${ruleId}/conditions/\${id} Delete a specific condition.• POST <cluster-ip>/dna/intent/api/v1/compliancePolicies/\${policyId}/rules/\${ruleId}/variables Create a new variable.• GET <cluster-ip>/dna/intent/api/v1/compliancePolicies/\${policyId}/rules/\${ruleId}/variables Retrieve the variables.• GET <cluster-ip>/dna/intent/api/v1/compliancePolicies/\${policyId}/rules/\${ruleId}/variables/count Retrieve the count of variables.• GET <cluster-ip>/dna/intent/api/v1/compliancePolicies/\${policyId}/rules/\${ruleId}/variables/\${id} Retrieve a specific variable.• PUT <cluster-ip>/dna/intent/api/v1/compliancePolicies/\${policyId}/rules/\${ruleId}/variables/\${id} Update an existing variable.• DELETE <cluster-ip>/dna/intent/api/v1/compliancePolicies/\${policyId}/rules/\${ruleId}/variables/\${id} Delete a specific variable.• PUT <cluster-id>/dna/intent/api/v1/compliancePolicies/\${policyId}/siteAssignments Set site assignments for policy.• GET <cluster-id>/dna/intent/api/v1/compliancePolicies/\${policyId}/siteAssignments
---------------------------	---

Devices API Operations	<p>Catalyst Center platform supports the following Devices API operations:</p> <ul style="list-style-type: none">• GET <cluster-ip>/dna/intent/api/v1/filterGroups Get the filter groups for given search criteria.• POST <cluster-ip>/dna/intent/api/v1/filterGroups Create filter group.• GET <cluster-ip>/dna/intent/api/v1/filterGroups/\${id} Get the filter group details for the given ID.• PUT <cluster-ip>/dna/intent/api/v1/filterGroups/\${id} Update filter group.• DELETE <cluster-ip>/dna/intent/api/v1/filterGroups/\${id} Delete a filter group.• GET <cluster-ip>/dna/intent/api/v1/filterGroupAssociations Get the filter group associations.• DELETE <cluster-ip>/dna/intent/api/v1/filterGroupAassociations/\${id} Delete filter group association.• POST <cluster-ip>/dna/intent/api/v1/filterGroupAssociations Create filter group association. <p>To access the new Filter Groups API operations, click the menu icon and choose Platform. Expand the Know Your Network drop-down list and choose Devices.</p>
User and Roles API Operations	<p>Catalyst Center platform supports the following User and Roles API operations:</p> <ul style="list-style-type: none">• POST <cluster-ip>/dna/system/api/v2/roles Add role v2.• POST <cluster-ip>/dna/system/api/v1/accessGroups Add access group.• GET <cluster-ip>/dna/system/api/v1/accessGroups/\${id} Get access group.• DELETE <cluster-ip>/dna/system/api/v1/accessGroups/\${id} Delete access group.• PUT <cluster-ip>/dna/system/api/v1/accessGroups/\${id} Update access group.• GET <cluster-ip>/dna/system/api/v1/accessGroups Get access groups.• GET <cluster-ip>/dna/system/api/v1/accessGroups/count Get access group count.• DELETE <cluster-ip>/dna/system/api/v2/roles/\${id} Delete role v2.• GET <cluster-ip>/dna/system/api/v2/roles/Permissions Get permissions v2.• GET <cluster-ip>/dna/system/api/v2/roles/\${id} Get role v2.• PUT <cluster-ip>/dna/system/api/v2/roles/\${id} Update role v2.• GET <cluster-ip>/dna/system/api/v2/roles Get roles v2. <p>To access the new User and Roles API operations, click the menu icon and choose Platform. Expand the System drop-down list and choose User and Roles.</p>
API Operation Changes	



API Overview



Which features are supported?

```
GET dna/intent/api/v1/wired/networkDevices/<deviceid>/configFeatures/supported/layer2
```

```
cdpGlobalConfig, cdpInterfaceConfig, dhcpSnoopingGlobalConfig,  
dhcpSnoopingInterfaceConfig, dot1xGlobalConfig, dot1xInterfaceConfig,  
igmpSnoopingGlobalConfig, lldpGlobalConfig, lldpInterfaceConfig,  
mabInterfaceConfig, mldSnoopingGlobalConfig, portchannelConfig,  
stpGlobalConfig, stpInterfaceConfig, switchportInterfaceConfig,  
trunkInterfaceConfig, vlanConfig, vtpGlobalConfig, vtpInterfaceConfig
```

GET a feature

```
GET dna/intent/api/v1/wired/networkDevices/<deviceid/configFeatures/deployed/layer2/vtpGlobalConfig
{
  "response": {
    "vtpGlobalConfig": {
      "items": [
        {
          "configType": "VTP_GLOBAL",
          "mode": "TRANSPARENT",
          "version": "VERSION_1",
          "isPruningEnabled": false
        }
      ]
    }
  },
  "version": "1.0"
}
```

Update a feature

```
PUT /dna/intent/api/v1/wired/networkDevices/<deviceid>/configFeatures/intended/layer2/switchportInterfaceConfig
```

```
{
  "switchportInterfaceConfig": {
    "items": [
      {
        "configType": "SWITCHPORT_INTERFACE",
        "interfaceName": "FortyGigabitEthernet1/1/1",
        "mode": "DYNAMIC_AUTO",
        "accessVlan": 10,
        "adminStatus": "UP",
        "trunkAllowedVlans": "1",
        "nativeVlan": 1
      }
    ]
  }
}
```

Poll the task

```
GET /dna/intent/api/v1/task/0196428b-090c-7647-aeaa-e4c6708049c4
```

```
{
  "response": {
    "startTime": 1744873130253,
    "progress": "Profile Update Task completed successfully",
    "data": "[{\"profileIdentity\":{\"id\":\"ec24581b-6e40-4a64-b47b-41e08aefa4f3\"},\"name\":\"DCP.ec24581b-6e40-4a64-b47b-41e08aefa4f3\"},\"version\":54}]]",
    "version": 1744873130396,
    "endTime": 1744873130396,
    "serviceType": "Network Profile Service",
    "username": "system",
    "isError": false,
    "instanceTenantId": "5d817bf369136f00c74cb23b",
    "id": "0196428b-090c-7647-aeaa-e4c6708049c4"
  },
  "version": "1.0"
}
```

Deploy the feature

```
POST /dna/intent/api/v1/wired/networkDevices/<deviceid>/configFeatures/intended/deploy
```

No body required.

```
GET /dna/intent/api/v1/task/1df6688d-58e8-4b8e-9d61-a3cbb09676ae
```

```
{
  "response": {
    "startTime": 1744874529347,
    "progress": "New Schedules were added. Successfully created a task schedule. 1df6688d-58e8-4b8e-9d61-a3cbb09676ae",
    "version": 1744874529432,
    "endTime": 1744874529432,
    "serviceType": "NCSS",
    "username": "admin",
    "additionalStatusURL": "/dna/intent/api/v1/activities/1df6688d-58e8-4b8e-9d61-a3cbb09676ae",
    "isError": false,
    "instanceTenantId": "5d817bf369136f00c74cb23b",
    "id": "1df6688d-58e8-4b8e-9d61-a3cbb09676ae"
  },
  "version": "1.0"
}
```

Poll the activity

```
GET /dna/intent/api/v1/activities/1df6688d-58e8-4b8e-9d61-a3cbb09676ae
```

```
{
  "response": {
    "recurring": false,
    "description": "Deploy Intended Config Features on ec24581b-6e40-4a64-b47b-41e08aefa4f3",
    "startTime": 1744874529419,
    "id": "1df6688d-58e8-4b8e-9d61-a3cbb09676ae",
    "endTime": 1744874529432,
    "type": "DEFAULT",
    "status": "COMPLETED"
  },
  "version": "1.0"
}
```

Closing and Q&A

Complete your session evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.



Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live Events app.

Continue your education



Visit the Cisco Stand for related demos



Book your one-on-one Meet the Expert meeting



Attend the interactive education with Capture the Flag, and Walk-in Labs



Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact me at: cisco.com/go/catalyst-center / cs.co/dnac-resources

Thank you

CISCO Live !

