

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

CISCO Live !

BRKOPS-2697

Adam Radford, Distinguished Solutions
Engineer @adamradford123

Lila Rousseaux, Principal Solutions
Engineer @lila_rousseau

June 2025

Cisco Webex App

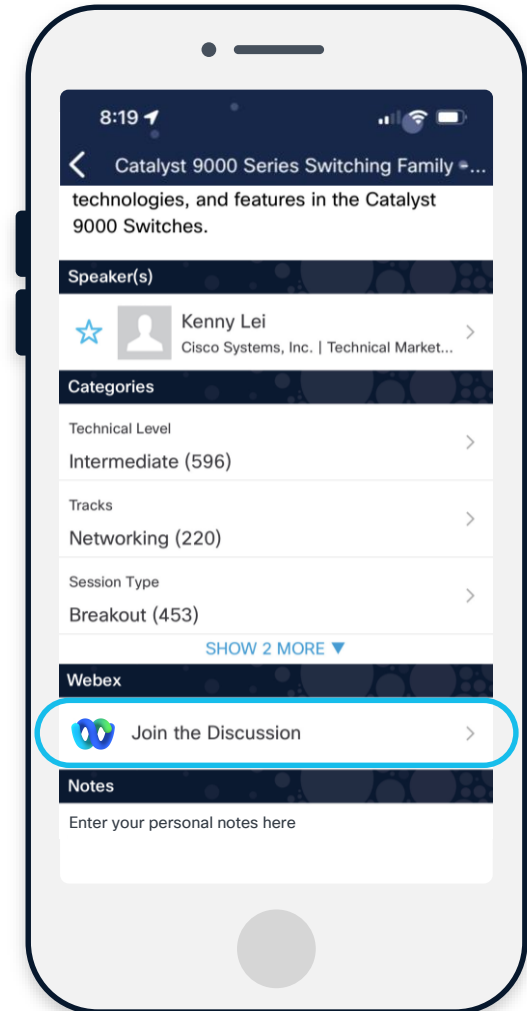
Questions?

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 June 13, 2025.



Agenda

- 01 Intent Based Automation Framework
- 02 Intent Based Automation for Wired
- 03 Evolution to Per-Device Configuration for Wired
- 04 Templates
- 05 Intent Based Automation for Wireless
- 06 Per-Device Configuration for Wireless
- 07 AAA and Management of Credentials
- 08 Automation beyond the UI: API's

Why a session on Network Automation



Assurance



SWIM



PnP



Traditional Network Configuration ²



65%
Network changes performed manually¹

75%
of Opex spent on changes and troubleshooting

70%
of Policy Violations are due to human error



1: Gartner: "Market Guide for Network Automation Tools"
Published 22 February 2022 - ID G00735443
2 : Non Sd-Access Networks

Intent Based Automation Framework

Steps for Device Provisioning using Intent Based Automation

- 1 Onboard Devices to Catalyst Center
- 2 Assign Devices to Sites
- 3 Populate Network Settings (Servers)
- 4 Create Network Profiles
- 5 Provision Devices

Steps for Device Provisioning using Intent Based Automation

- 1 **Onboard Devices to Catalyst Center**
- 2 Assign Devices to Sites
- 3 Populate Network Settings (Servers)
- 4 Create Network Profiles
- 5 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

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

Steps for Device Provisioning using Intent Based Automation

- 1 Onboard Devices to Catalyst Center
- 2 **Assign Devices to Sites**
- 3 Populate Network Settings (Servers)
- 4 Create Network Profiles
- 5 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

- 1 Onboard Devices to Catalyst Center
 - 2 Assign Devices to Sites
 - 3 **Populate Network Settings (Servers)**
 - 4 Create Network Profiles
 - 5 Provision Devices
- } **Associated to Site**

Brownfield device automation

Discover

Add to Inventory

Assign to Site

Device Controllability

Enable for Telemetry

Provision

Network Settings (Servers) and Network Profiles

Application Telemetry

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 interface for configuring servers. The left sidebar shows a hierarchical tree structure with 'BRANCH-AAA' selected. The main content area is divided into sections for AAA Server, DHCP Server, DNS Server, and NTP Server.

AAA Server Configuration:

- Network: Network, Client/Endpoint
- Network Section:
 - Protocol: RADIUS, TACACS
 - Network: 10.85.54.185
 - IP Address (Primary): 10.85.54.185
- Client/Endpoint Section:
 - Protocol: RADIUS, TACACS
 - Client/Endpoint: 10.85.54.185
 - IP Address (Primary): 10.85.54.185

DHCP Server Configuration:

- DHCP: 10.85.54.175 (Supports both IPv4 and IPv6)

DNS Server Configuration:

- Domain Name: cirrus.cloud
- Primary: 64.102.6.247 (Supports both IPv4 and IPv6)
- Secondary: 10.85.54.175 (Supports both IPv4 and IPv6)

NTP Server Configuration:

- NTP: 10.81.254.131 (Supports both IPv4 and IPv6)
- Additional NTP: 10.81.254.202 (Supports both IPv4 and IPv6)
- Additional NTP: 171.68.38.65 (Supports both IPv4 and IPv6)
- Additional NTP: 10.85.54.175 (Supports both IPv4 and IPv6)

Time Zone: US/Eastern (EDT)

Message of the day: Do not override the existing MOTD banner on the device. Text: Welcome to C9200L-1 - Managed by Cisco DNA Center.

Steps for Device Provisioning using Intent Based Automation

- 1 Onboard Devices to Catalyst Center
- 2 Assign Devices to Sites
- 3 Populate Network Settings (Servers)
- 4 **Create Network Profiles**
- 5 Provision Devices

} **Associated to Site**

Network Profiles

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

The screenshot shows a configuration page for a Wireless SSID profile. The SSID is set to 'GUHOA'. The WLAN Profile Name is 'GUHOA_6c12b73c94_profile' and the Policy Profile Name is also 'GUHOA_6c12b73c94_profile'. The Fabric is set to 'No'. The 'Enable SSID Scheduler' toggle is turned off. Under 'TRAFFIC SWITCHING', 'Interface' is selected. The Interface Name is 'data'. The 'Do you need Anchor for this SSID?' is set to 'No'. There is also an unchecked checkbox for 'Flex Connect Local Switching'.

SSID
GUHOA

WLAN Profile Name
GUHOA_6c12b73c94_profile

Policy Profile Name
GUHOA_6c12b73c94_profile

Fabric
 Yes No

Enable SSID Scheduler

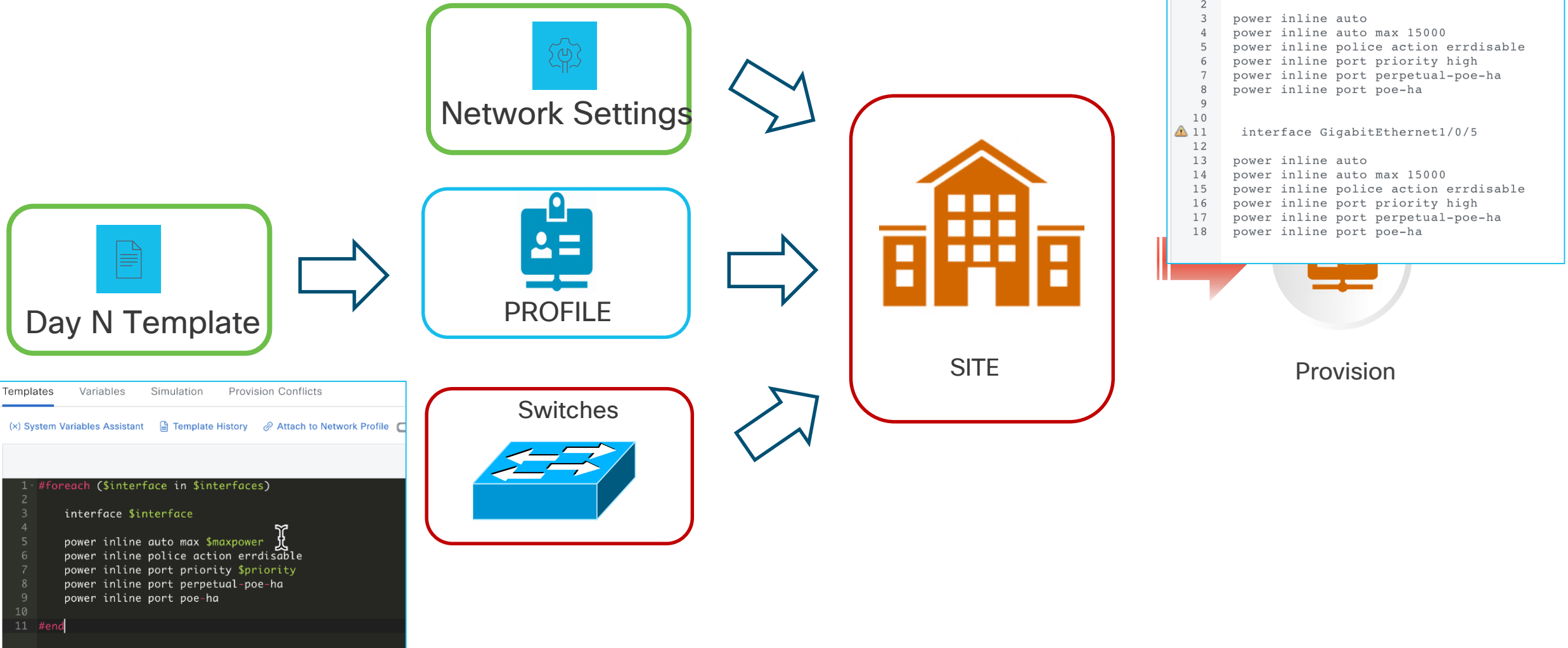
TRAFFIC SWITCHING
 Interface VLAN Group

Interface Name*
data

Do you need Anchor for this SSID?
 Yes No

Flex Connect Local Switching

Catalyst Center - Intent Based Configuration Switches



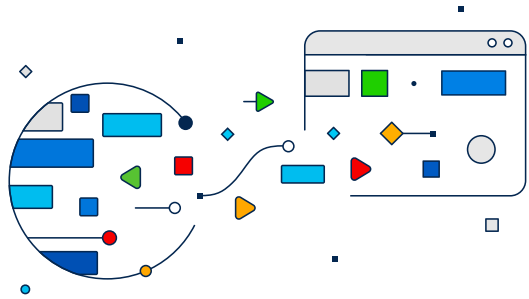
Templates Variables Simulation Provision Conflicts

(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
```

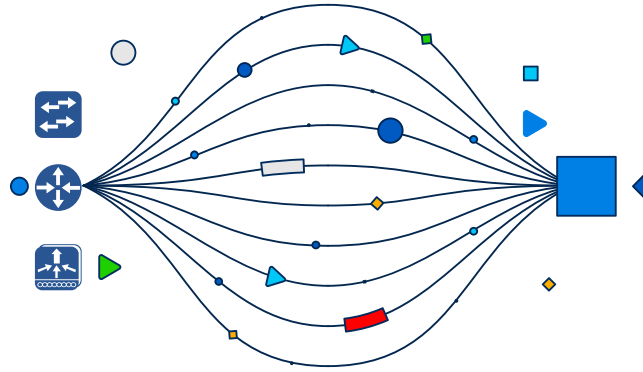
Evolution to Per-Device Configuration for Wired

Catalyst Center- Per-Device Configuration



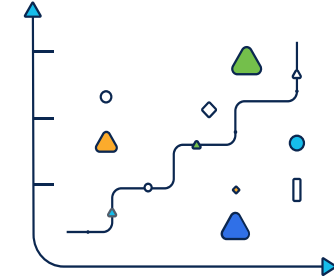
Discover

Add devices from
existing infrastructure



Learn

Visualize the network
architecture and learn from
existing per-device
configurations



Manage

Simplified configuration
read/write at an Element Level

Simplified View and Edit of Switch Configuration

Summary View of Configurations

Actionable Switch Ports

Instant Edit and Provisioning

View/Edit of Detailed Configurations

The screenshot shows a web-based configuration interface for a Cisco switch. At the top, it displays the device name 'C9K-STANDALONE-2.cirrus.cloud' and provides options to 'Run Commands' and 'View 360'. Below this, status indicators show the device is 'Reachable' and 'Managed', with an IP address of 10.85.54.26. The device is identified as a 'Cisco Catalyst 9300 Switch' with a role of 'ACCESS'. A left-hand navigation menu is titled 'CONFIGURATION' and includes categories like 'Layer 2', 'VLAN', 'Discovery Protocols', 'STP', 'VTP', 'DHCP Snooping', 'IGMP Snooping', 'MLD Snooping', 'Authentication', 'Cisco TrustSec', 'Logical Ports', and 'Port Configuration'. The 'Discovery Protocols' section is currently selected and expanded, showing settings for CDP and LLDP. CDP is set to 'Enabled (default)' with a 'Hold Time' of 180 and a 'Timer' of 60. LLDP is set to 'Disabled (default)' with a 'Hold Time' of 120 and a 'Timer' of 30. Both sections include a link to '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 [Edit](#) Only Layer 2 ports a

Ports (41) Focus: Default View

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	--

View Port [Edit](#)

Port Name [i](#) TenGigabitEthernet1/0/23

Switchport

Description [i](#) ***** Uplink #1 to C3650 DISTRI *****

Mode [i](#) Trunk

Access VLAN ID [i](#) 1 (default)

Voice VLAN ID [i](#) --

Admin Status [i](#) Enabled (default)

Allowed VLANs [i](#) 419,420

[Default Configurations](#)

VLAN Trunking

Dot1x

Authentication Mode [i](#) Closed (default)

[Close](#)

Simplified visualization

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

Simplified Configuration

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
```



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

We have detected IOS-XE device(s) in your network where new telemetry subscriptions for assurance data need to be enabled and some of the existing subscriptions may need to be optimized for performance. Apply Fix To provision subscriptions on devices that have not been discovered with NETCONF, rediscover the devices with NETCONF, and update the Telemetry Settings with the Force Configuration Push option.

Some devices may have design or provision conflicts. Please go to Provision -> Inventory and switch the focus to "Templates" and check "Template Conflict Status" column. Update CLI Templates

TBRANCH-SCARBOROUGH

- All Routers Switches Wireless Controllers Access Points Sensors

Grid, List, Map, Location icons

Devices (3) Focus: Select

Take a tour Export

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

0 Selected Tag Add Device Actions

As of: May 28, 2025 4:08 PM

Tags	Device Name	ID Address	Device Family	Site	Reachability	Provisioning Status	Platform
<input type="checkbox"/>	C9200L-3.cirrus.cloud				Reachable	Success See Details	C9200L-24T-4G
<input type="checkbox"/>	C9200L-2.cirrus.cloud				Reachable	Success See Details	C9200L-24T-4G
<input type="checkbox"/>	C9K-STANDALONE-2.cirrus.cloud				Reachable	Success See Details	C9300-24UX

C9K-STANDALONE-2.cirrus.cloud As of: 4:09 PM

[View Device Details](#) [View 360](#) [Run Commands](#)

Reachable | IP Address 10.85.54.26 | Health 10 | Uptime 47 days 1 hr

Family	Switches and Hubs
Image Version	17.12.2 (Distribution Pending)
Site	.../Toronto/TBRANCH-SCARBOROUGH
Provision Status	Success
Device Role	ACCESS

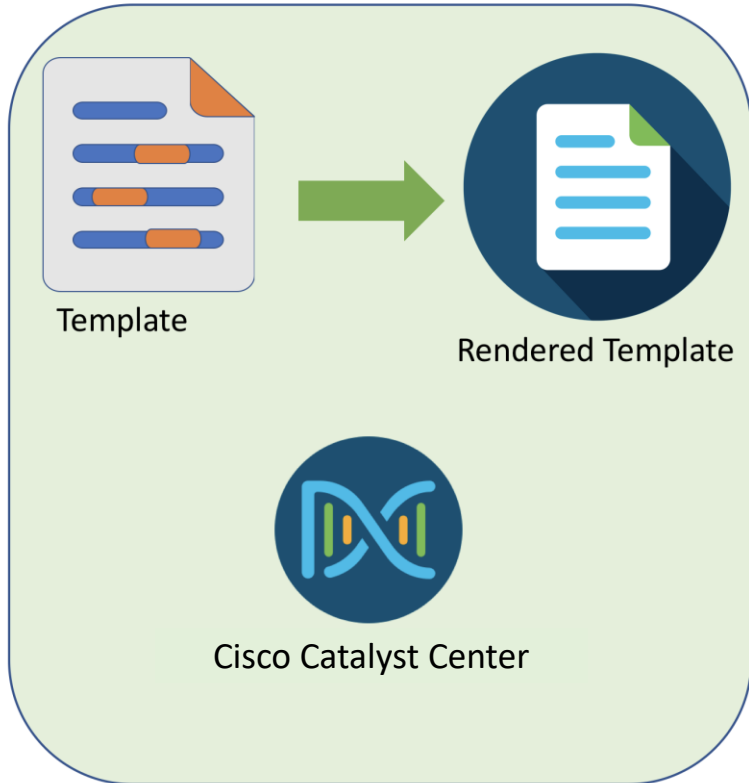
[Show More](#)

Templates

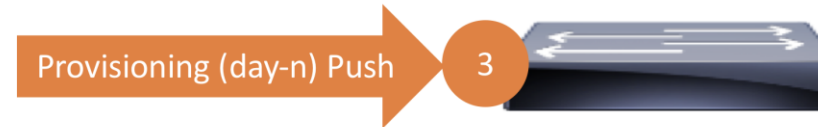
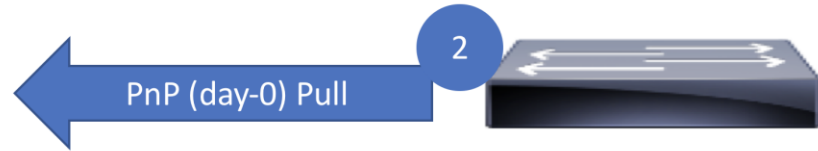
Day0 vs Day-N



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 Catalyst Center interface for configuring a variable. The variable is named 'loopback' and is currently set to 'adam'. The configuration includes a 'Required Variable' checkbox which is checked, a 'Variable Data Source' set to 'User Defined', and a 'Variable Type' set to 'String'. The 'Data Entry Type' is set to 'Text Field'. There is also a 'Sensitive Value' checkbox which is unchecked. The 'Variable Notes' section contains the text 'no instructions required' and 'a var for adam'.

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

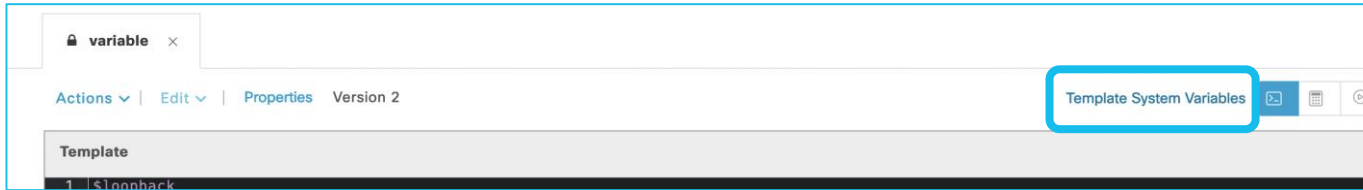
"introspect" data Catalyst Center has about the device

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



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

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

Search

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

Source

Inventory

Entity

Interface

Attribute

portName

Filter By

Variable Notes

Hint Text

Hint Text

Search

pid

portMode

portName

portType



poweroverethernet

Simulation

- Select "Simulation" on far right
- Create 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 |
```

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
<input type="checkbox"/> 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-l3 (10.10.3.122)

Search Device

- 9k-l3 (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-l3 (10.10.3.122)

Search Device

interfaces

Search Table

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

interfaces
<input type="checkbox"/> AppGigabitEthernet1/0/1
<input type="checkbox"/> FortyGigabitEthernet1/1/1
<input type="checkbox"/> FortyGigabitEthernet1/1/2
<input type="checkbox"/> GigabitEthernet0/0
<input type="checkbox"/> GigabitEthernet1/0/1

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

Simulation #3

The screenshot displays the Cisco Catalyst Center interface for managing CLI templates. The main navigation bar includes the Cisco logo, 'Catalyst Center', and the current path 'Design / CLI Templates'. The user 'Adam' is logged in. The breadcrumb trail shows 'CLI Templates / interfaces_bound (1) Properties'. Below this, there are tabs for 'Templates', 'Variables', 'Simulation', and 'Provision Conflicts', with 'Simulation' being the active tab.

The 'Simulations (4)' section features a search bar and a table of simulation records. The table has columns for 'Simulation Name', 'Date', 'Variables Simulated', 'Status', and 'Report'. All four simulations listed ('adam', 'adam2', 'adamnew1', 'ams') have a status of 'SUCCESS'.

The 'Simulation - adamnew1' detail view shows the following configuration:

```
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!

```
interfaces_implicit * x
Actions v | Edit v | Properties
Template
1 #foreach ($interface in $__interface)
2 interface $interface.portName
3 shutdown
4 #end
5
6
```

interfances_implicit x

Actions v | Properties

Template System Variables [?] [x]

Input Form

Preview Custom order

No Data Available

interfances_implicit

Simulation Input

There are implicit variables in this template. Please click here to select device.

Simulation Name: adam

Template only has implicit vars

Template Preview

```
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 window shows a CLI editor with the following content:

```
1 $loopback
2
```

The interface includes a top navigation bar with tabs for Templates, Variables, Simulation, and Provision Conflicts. Below the editor, there are several utility buttons: (x) System Variables Assistant, Template History, Attach to Network Profile, and Show Design Conflicts. A status bar at the bottom of the editor indicates "Auto saved: 9:48 PM (every 5 mins)".

The right-hand panel, titled "Template History", shows a search bar and 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

Templates Variables Simulation Provision Conflicts

(x) System Variables Assistant  Template History  Attach 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

FiltersJinja

```
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)

CLI Templates / meta-data-json (2) Properties

Templates Variables Simulation Provision Conflicts

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

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

Update Simulation

Simulation Name*

a

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

Device



CONFIGURE VARIABLE VALUES

json_var*

{ "ip" : " 1.2.3.4", "interface" : "g1/01/"

Simulation - a

Variables Simulated: 1

Status:

```
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

Tools / Template Hub

Templates (111)

Search

1 Selected Export Import Delete Provision Templates

Name	Project	Type	Version	Commit State
flexible_apjson	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)

Search

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

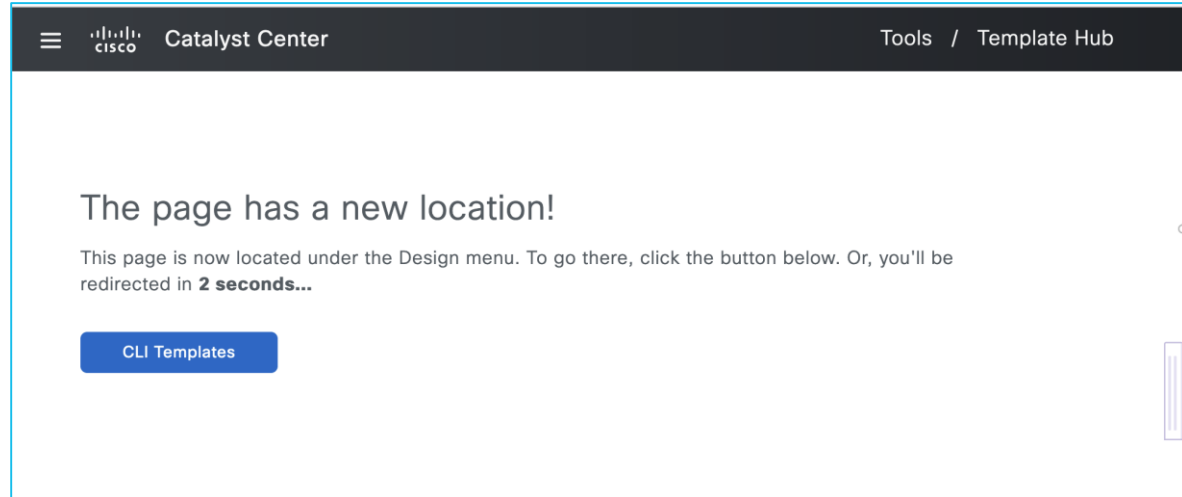
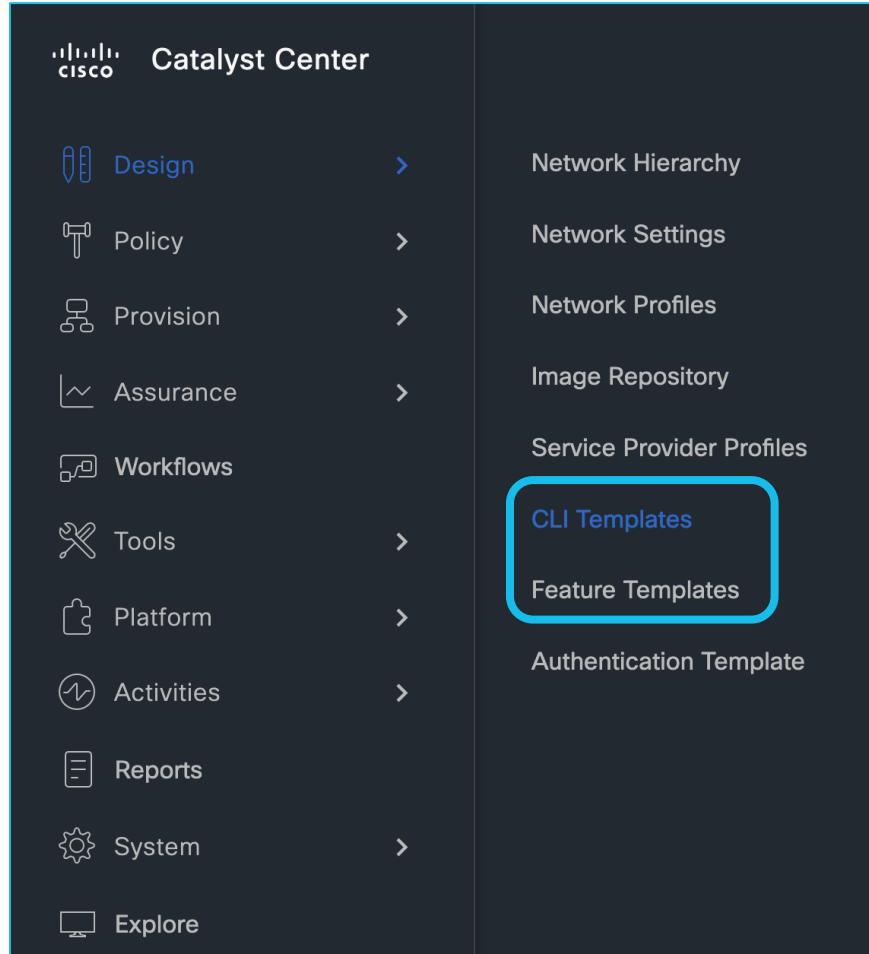
int-desc

int*
g1/0/10

desc*
template hub was here

- 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)

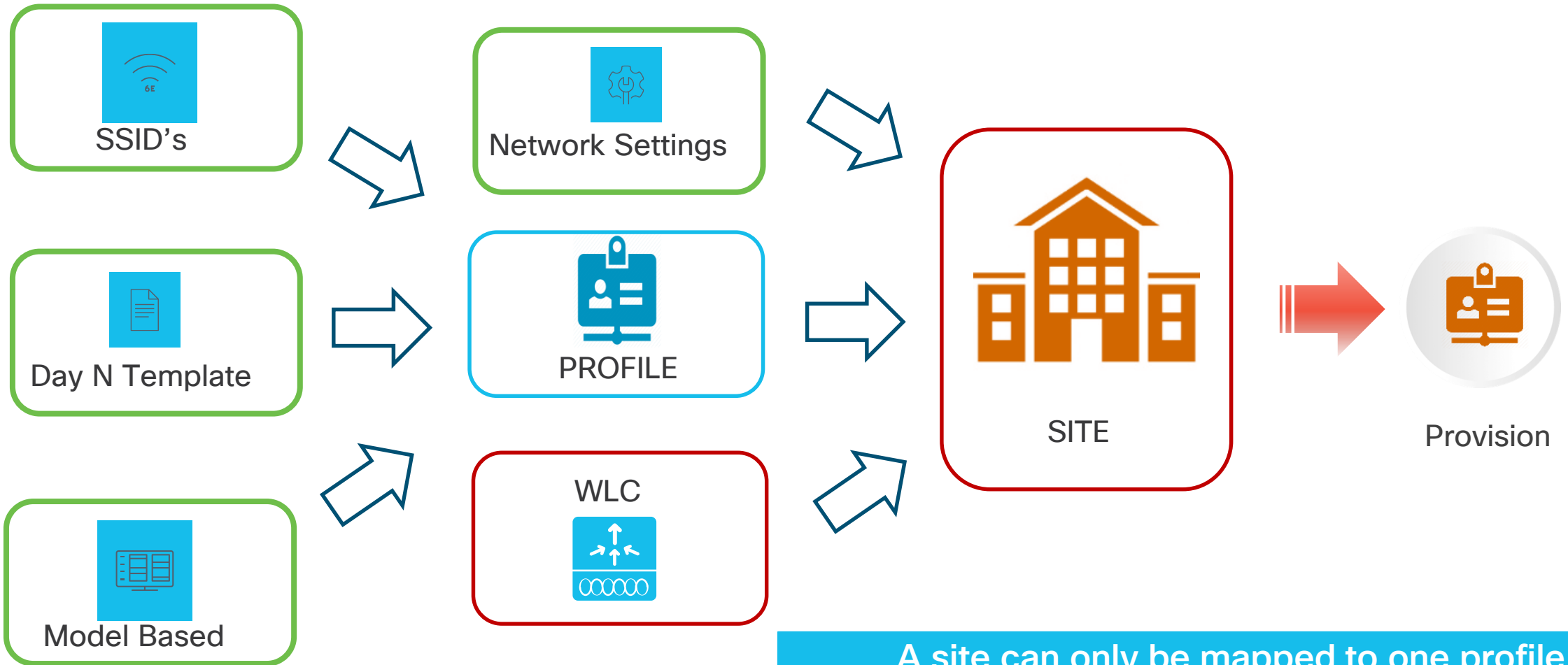
New Location, Same functionality – 2.3.7.4



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

Intent Based Automation for Wireless Networks

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

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

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

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

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

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.

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

Advanced Settings
Configure the advanced fields to complete SSID setup.

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 (802.11k)
 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: 3600
 Client Exclusion: 180

11v BSS Transition Support
 BSS Max Idle Service
 Client User Idle Timeout: 300
 Directed Multicast Service

Radius Client Profiling: On

NAS-ID: On

NAS-ID Opt 1: On

Configure CCKM: On

Configure Client Rate Limit: On

Client Rate Limit (in bits per second)
Range: 0-1000000000

Coverage Hole Detection: On

Step 2: Associate to wireless network profile

Associate SSID to Profile

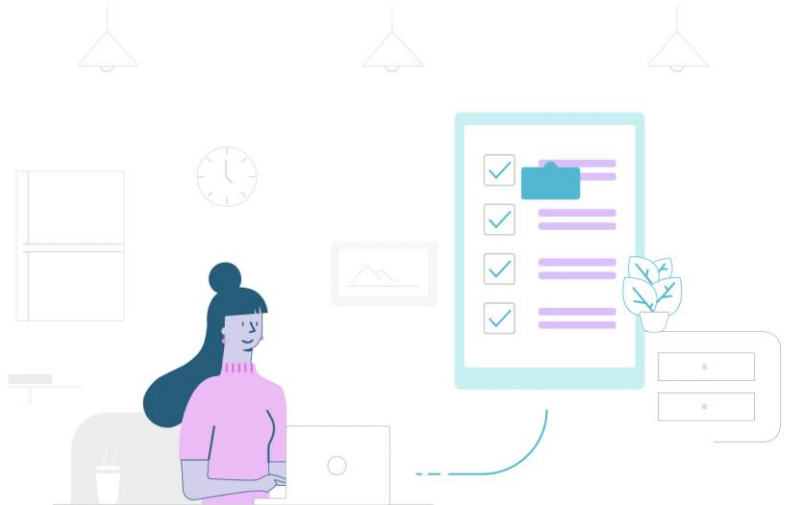
Select a Profile on the left or Add Profile and click 'Associate' to associate the SSID to Profile.

SSID Name: SSID1 (Enterprise)

+ Add Profile 2 profile(s) associated.

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

An illustration of a person with long dark hair, wearing a pink top, sitting at a desk with a laptop. A checklist with four items, each with a checkmark, is overlaid on the scene. The background includes a window, a clock, and a potted plant.

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

Provision one WLC

Devices (2) Focus: Provision

Q deviceName: (9800-pnp)

1 Selected Add Device Tag Actions

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

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

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 ⓘ

Anchor

Managed AP location(s)

[Select Primary Managed AP Locations](#)

[Select Secondary Managed AP Locations](#)

Skip AP Provision ⓘ

- 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

9800-pnp

Serial Number 9P015USKRB8

Devices 9800-pnp

Skip AP Provision ⓘ

Rolling AP Upgrade

Enable

AP Reboot Percentage 25 ⓘ

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: 9P015USKRBB
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

Cancel Next

Template

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 Show

▼ 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

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

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

Device Name: pnp-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

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 able to login to your devices.

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

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

Advanced Configuration

Template Name: pnp1-config

Day N Templates

Model Configs

Capability

No data to display

Per-Device Configuration for Wireless

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

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 [Info](#) [Refresh](#)

✔ 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

DETAILS

- Interfaces >
- System >
- Browse Configurations >
- User Defined Fields
- Wireless Info
- Mobility

SECURITY

- Advisories

FIELD NOTICES

- Field Notices
- Potential Field Notices

WLAN Profiles [Info](#)

Managed via Site-Based Network Profiles [Info](#)

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.

WLAN Profiles (2)

0 Selected

<input type="checkbox"/>	WLAN Profile Name	Status	WLAN ID	SSID Name	Policy Tags	AP Configuration Sets
<input type="checkbox"/>	new_profile	✔	18	new	6	0
<input type="checkbox"/>	test_profile	✔	17	test	3	1

2 Record(s) Show Records: 25 < 1 >

2.3.7.9 – Convert to per-device mode

The screenshot shows the Cisco Catalyst Center interface for a device named 'pnp-9800'. At the top, there is a navigation bar with the Cisco logo and 'Catalyst Center'. Below this, the breadcrumb 'All Devices / pnp-9800' is visible. The device name 'pnp-9800' is followed by a red-bordered button labeled 'Enable Per-Device Configuration'. Other buttons include 'Run Commands' and 'View 360'. Below the buttons, there are status indicators: 'Reachable' (green checkmark), 'Managed' (green checkmark), 'IP Address: 10.10.10.146', 'Device Model: Cisco Catalyst 9800-CL Wireless Controller for Cloud', 'Device Role: ACCESS', and 'Uptime: 63 d'. The main content area is divided into sections: 'DETAILS', 'SECURITY', and 'FIELD NOTICES'. Under 'DETAILS', there are sub-sections for 'Hardware', 'Software', and 'Operational Summary'. The 'Hardware' section includes 'Device Type: Wireless Controller', 'Platform: C9800-CL-K9, C9800-CL-K9', and 'MAC Address: 00:1e:e5:a7:bf:ff'. The 'Software' section includes 'Image: C9800-CL-universalk9.17.12.03.SPA.bin' and 'Version: 17.12.3'. The 'Operational Summary' section includes 'Uptime: 63 days 5 hrs 30 mins', 'Last Provisioned: Dec 8, 2024 2:08 PM', 'Last Synced: 4 hours ago', 'Provision Status: Success ⚠️', 'Resync Interval: 24 hours', and 'Cisco ISE Integration Status: Success ✅'. A left-hand navigation menu contains items like 'Interfaces', 'System', 'Browse Configurations', 'User Defined Fields', 'Wireless Info', 'Advisories', 'Field Notices', and 'Potential Field Notices'.

Only applies if using intent based config

Per-Device configuration mode

All Devices / ar9800.adamlab.cisco.com

ar9800.adamlab.cisco.com [Manage 1 APs](#) [Run Commands](#) [View 360](#) Last Updated: 9 hours 50 minutes ago [i](#) [refresh](#)

✓ Reachable | ✓ Managed | IP Address: 10.10.21.200 | Device Model: Cisco Catalyst 9800-CL Wireless Controller for Cloud | Device Role: ACCESS | Uptime: 185 days 12 hrs 5 mins | Site: Global/Syd

SECURITY

Advisories

FIELD NOTICES

Field Notices

Potential Field Notices

CONFIGURATION *BETA*

WLAN [v](#)

- WLAN Profiles
- Policy Profiles
- Remote LAN Profiles
- Remote LAN Policies

WLAN Profiles [i](#)

Managed via Per-Device Configuration Method *BETA* [i](#)

WLAN Profiles (2) [+ Add](#) [gear](#)

0 Selected [Actions v](#)

<input type="checkbox"/>	WLAN Profile Name	Status	WLAN ID	SSID Name	Policy Tags	AP Configuration Sets
<input type="checkbox"/>	test_profile	✓	17	test	3	1
<input type="checkbox"/>	new_profile	✓	18	new	6	0

2 Record(s) Show Records: 25 [v](#) 1 - 2 [<](#) [1](#) [>](#)

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
- 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

mDNS

EoGRE

Layer 2

- VLAN
- Interfaces
- Discovery Protocols

Network Settings

- DHCP Pools
- HTTP/HTTPS
- SNMP
- NTP

Layer 3

- Routing Administration
- Device Mobility

New in 2.3.7.9

Example: Turn off 2.4GHz

Edit WLAN Profile: test_profile

Search

General

The General tab allows to define the basic WLAN profile properties such as the name, 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 ⓘ

General

Security

Layer 2

Layer 3

AAA

Advanced

11ax

11k

11v BSS

Device Analytics

Max Clients

Off Channel Scan

Miscellaneous

Edit WLAN Profile: test_profile

Search

General

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

SSID State

Admin Status ⓘ

Broadcast SSID ⓘ

Radio Policy ⓘ Show Slot Configuration

6 GHz

5 GHz

2.4 GHz

General

Security

Layer 2

Layer 3

AAA

Advanced

11ax

11k

11v BSS

Device Analytics

Max Clients

Off Channel Scan

Miscellaneous

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

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**

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

Device IP: 10.10.21.200 Site: Global/Syd ⓘ

ar9800.adamlab.cisco.com ✔

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

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": ["java.util.HashSet", [{"@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}], "wlanWpa2Aes": true, "@class": "com.cisco.8d33-4009-9df3-5030d5c33530", "wlanProfileName": "test_profile"}]}]}
```

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

 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

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 bar and a list of settings categories: Cisco Accounts, PnP Connect, Cisco.com Credentials, Smart Account, Smart Licensing, SSM Connection Mode, Device Settings, 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 descriptive paragraph: '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 three servers with columns for IP Address, Protocol, Type, Status, and Actions. The table data is as follows:

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	...

The table also shows a timestamp 'As of: Apr 23, 2023 4:08 PM' and a refresh icon.

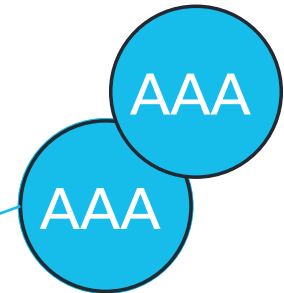
- Only one ISE integration can be done per Catalyst Center.
- Other AAA servers can be added, but as an AAA server only (even if they are ISE servers)

Difference between ISE and AAA integration

ISE



Cisco
Catalyst
Center



AAA config
pushed to
devices

- 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

The screenshot shows the 'Provision Device' modal in the Cisco provisioning interface. The modal is titled 'Provision Device' and is at 'Step 3 of 3: Preview Configuration'. It displays the configuration for device 'C9200L-1.lila.com' with IP '10.85.54.23'. The configuration to be deployed is shown, but there are two error messages:

- Error 1:** Errors occurred during config generation. You can still opt to deploy the partial configuration (if any) that was generated successfully. Collapse to hide.
- Error 2:** 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.
- Info:** No configuration was generated from current source

The interface also shows a list of devices with a search bar and a 'View by Configuration Source' dropdown set to 'All'. The device 'C9200L-1.lila.com' is highlighted with a red 'x' icon, indicating an error.

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 if
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
```

```
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 32 nas-port-detail mac-only
radius-server attribute 5 tries 3
radius-server host 10.85.54.185
radius-server port 1812 acct-port 1813
radius-server timeout 30
radius-server ignore-acct-port probe-on
```

Sample AAA config sent to device

Device added in ISE

```
line vty 0 4
 authorization exec VTY_author
 login authentication VTY_authen
line vty 5 15
 authorization exec VTY_author
```

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Network Resources > Device Portal Management. The main content area is titled "Network Devices" and includes a filter bar with the following configuration: Filter Name Contains 9200. Below the filter is a table of network devices.

Name	IP/Mask	Profile Name	Location	Type	Description
<input type="checkbox"/> 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 configuration interface for Device Credentials. The top navigation bar includes 'Servers', 'Device Credentials' (selected), 'IP Address Pools', 'Wireless', 'Telemetry', and 'Security and Trust'. A search bar on the left contains 'scar' and a filter icon. Below the search bar is a 'Search Help' link. The left sidebar shows a hierarchical view of locations: Global, Canada, Ontario, and Toronto, with 'TBRANCH-SCARBOR...' selected. The main content area has a heading 'Create and configure the credentials used to access devices.' and a 'Manage Credentials' link. Below this is a paragraph explaining that assigned credentials are not deployed automatically and that the 'Manage Credentials' link should be used to choose the credential's 'Apply' action. A dropdown menu for 'CLI' is open, showing a checked option 'Assign a CLI credential' and a text input field for 'Credential*' containing '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
```

Some devices may have design or provision conflicts. Please go to Provision -> Inventory and switch the focus to "Templates" and check "Template Conflict Status" column. [Update CLI Templates](#)

Two (2) Warning Alerts on this page. [Expand](#) to see details.

TBRANCH-SCARBOROUGH

- All
- Routers
- Switches
- Wireless Controllers
- Access Points
- Sensors

Grid, List, Map, Location icons

DEVICE WORK ITEMS

- Unreachable
- Unassigned
- Untagged
- Failed Provision
- Non Compliant
- Outdated Software Image
- No Golden Image
- Failed Image Prechecks
- Under Maintenance
- Security Advisories

Devices (2) Focus: Provision Take a tour Export

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

0 Selected Tag Add Device Actions As of: Mar 18, 2025 2:08 PM

Tags	Device Name	IP Address	Device Family	Site	Reachability	Provisioning Status
<input type="checkbox"/>	TBRANCH-C9200L-3	10.85.54.25	Switches and Hubs	.../Toronto/TBRANCH-SCARBOROUGH	Reachable	Success See Details
<input type="checkbox"/>	C9K-STANDALONE-2	10.85.54.26	Switches and Hubs (WLC Capable)	.../Toronto/TBRANCH-SCARBOROUGH	Reachable	Success See Details

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)** ^



Current site (TBRANCH-SCARBOROUGH)

System

Add ✓

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** ▾

Search Table

Add ▾ As of: Mar 4, 2025 12:25

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

- Edit
- Delete
- Apply

Credentials / Edit Credential

CLI

Name / Description*
Cisco Live

Username*
cicolive
[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 synced

Changing local credential passwords



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

Catalyst Center Design / Network Settings

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 credential to devices, 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

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.

© 2025 Cisco

reference

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: **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)	...

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

Changing local credential passwords



Reference

Credentials

Manage Credentials

Local Credentials updated in device

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

To view, edit, or delete a credential, choose "Focus: System."

Focus: [Current site \(TE\)](#)

```
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)	

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 S
1) using crypto cipher 'aes128-ctr', hmac 'hmac-sha2-256-etm@openssh.com' Succ
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

The screenshot displays the Cisco configuration interface with the 'Device Credentials' tab selected. The main content area shows instructions: 'Create and configure the credentials used to access devices.' and 'Assigned credentials aren't deployed automatically. To push a credential to your devices, click "Manage" and choose the credential's Apply action in the Manage Credentials table.'

On the right, the 'Edit Credential' form is visible, showing a credential named 'Lila' with the following fields:

- Name / Description*: Lila
- Username*: lila (with a link to 'View Username Policy')
- Password*: (masked with dots) (with a link to 'View Password Policy')
- Enable Password: (masked with dots) (with a link to 'View Password Policy')

On the left, a terminal window shows the output of the 'show run' command on a C9200L-1 device. The configuration includes AAA settings for a RADIUS server and local authentication. The line 'aaa authentication login VTY_authen group dnac-network-radius-group local' is highlighted with a blue box.

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

The screenshot shows the Cisco Catalyst Center interface for managing credentials. On the left, a navigation pane shows the hierarchy: Servers > Device Credentials > IP Address Pools > Wireless > Telemetry > Security and Compliance. The main area is titled 'Manage Credentials' and includes instructions on how to view and apply credentials. Below the instructions is a table of credentials. The table has columns for Name, Type, Status, and Actions. Two credentials are listed: 'Lila' (CLI) and 'NFVIS-HTTPS-RO' (HTTP(S) Read). Both are marked as 'Not Synced (1)'. An 'Apply' button is visible next to the 'NFVIS-HTTPS-RO' row. A blue callout box on the right contains the text: 'Credentials are updated in Catalyst Center only (not on device)'. Two blue arrows point from this callout box to the 'Lila' and 'NFVIS-HTTPS-RO' rows in the table.

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

```
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-Authenticato[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-Authenticato[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

The screenshot displays the Cisco configuration interface for Device Credentials. The main view shows a table of credential status for the 'Current site (BRANCH-AAA)'. The table has columns for Type, Name/Description, Status, Details, and Actions.

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.	

Below the main table, there are sections for assigning credentials to specific device types:

- Assign a CLI credential
- Credential*
Lila
- Assign an SNMPv2c Read credential

On the right side, there is a search table for the current site:

Focus: Current site (BRANCH-AAA)

Search Table

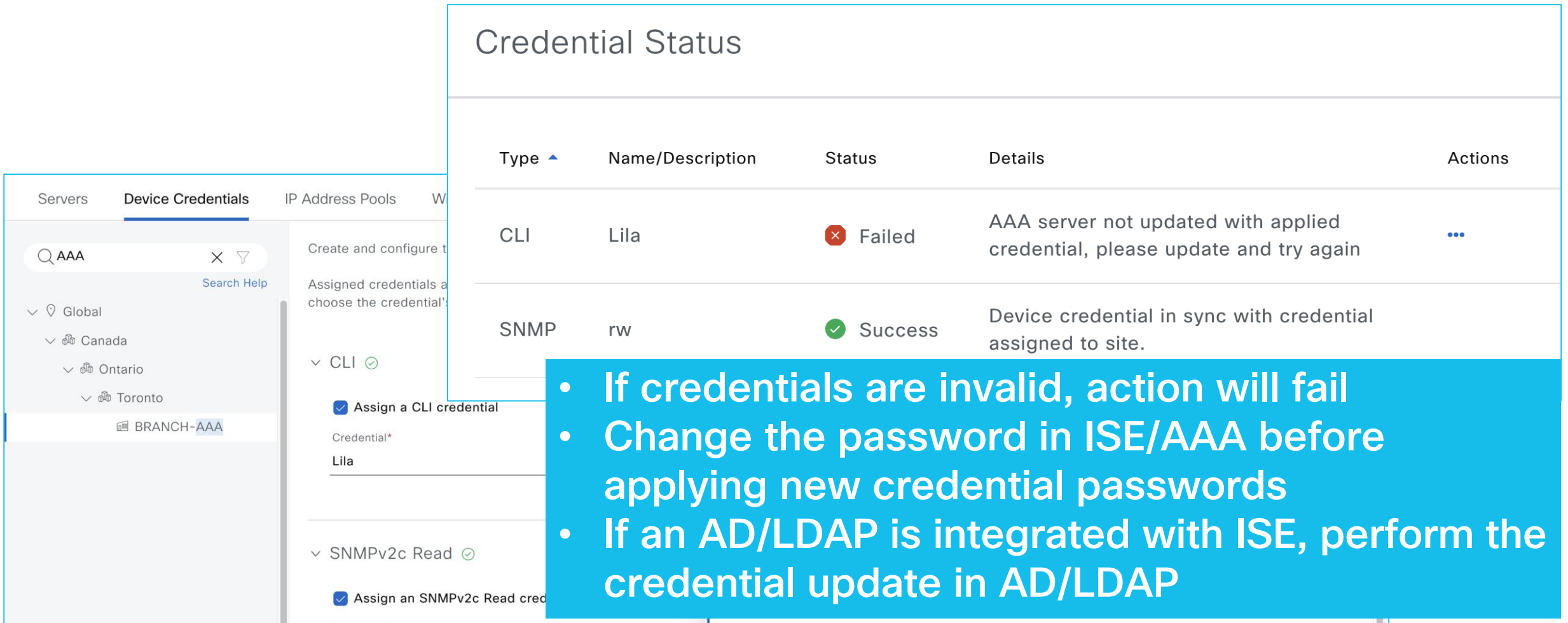
Add

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



The screenshot shows the Cisco ISE Device Credentials configuration page. The left sidebar contains a navigation menu with 'Servers', 'Device Credentials', and 'IP Address Pools'. The main content area shows a search bar for 'AAA' and a list of credentials. A table titled 'Credential Status' is overlaid on the right side of the page, showing the status of two credentials: 'Lila' (CLI) and 'rw' (SNMP).

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

Adding and applying new credentials to devices

Same workflow as change of password

Devices (2) Focus: ProvisionAdmin

Click here to apply basic or advanced filters or view

1 Selected Tag Add Device Actions

Tags	Device Name	IP
<input checked="" type="checkbox"/>	TBRANCH-C9200L-3	10.10.10.10
<input type="checkbox"/>	C9K-STANDALONE-2	10.10.10.10

Network Device

Credentials Validate

- Note: CLI and SNMP credentials are mandatory. Please ensure authenticity of credentials. In case of invalid credentials, device will go into a collection failure state.
- Changing the device credentials will impact the device's configuration.

CLI*

Select global credential Add device specific credential

Username* Password* SHOW

[View Username Criteria](#) [View Password Criteria](#)

Enable Password SHOW

[View Password Criteria](#)

```
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
```

Adding and applying new credentials to devices

The screenshots illustrate the process of adding and applying new credentials to devices. The top screenshot shows the 'Device Credentials' page with a search bar containing 'scar' and a 'Manage Credentials' button. The middle screenshot shows the 'Manage Credentials' page with a 'Focus: Current site' dropdown. The bottom screenshot shows the 'Manage Credentials' page with a table of credentials, where the 'Status' column for 'Lila' is highlighted with a blue box.

Device Credentials Page:

- Search: scar
- Instructions: Create and configure the credentials used to access devices.
- Text: Assigned credentials aren't deployed automatically. To push a credential to your devices, click "Manage Credentials" and
- Buttons: Search Help, Manage Credentials

Manage Credentials Page:

- Section: Credentials
- Section: Manage Credentials
- Text: To view the assigned credentials' statuses and to apply them to only devices in the current site, choose "Focus: Current site."
- Text: 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
- As of: Mar 17, 2025 11:43 AM

Table of Credentials:

Name	Type	Status	Actions
Lila	CLI	Synced	...

Adding and applying new credentials to devices

The screenshot displays the Cisco ICM interface. On the left, a sidebar titled 'DEVICE WORK ITEMS' lists various device states like 'Unreachable', 'Unassigned', etc. The main area shows a list of devices, with 'TBRANCH-C9200L-3' selected. The 'Edit Device' panel is open, showing the 'Credentials' tab. Under the 'CLI*' section, the option 'Add device specific credential' is selected. The 'Username*' field contains 'lila' and the 'Password*' field is masked with dots. A 'SHOW' button is located to the right of the password field.

- For local authentication – new username will be added in device config
- For AAA authentication – new user needs to be added manually in AAA server

```
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.YdjvLytrRJ8R8V.jfN1aWuCaE9a0jTt6
```

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 Discovered 1 Successful 0 Failed 0 Discarded

Search Table ⌵ ↑ Export

IP Address ▾	Device Name	Status	ICMP	SNMP	CLI	HTTP(s)	NETCONF
10.85.54.23	C9200L-1.lila.com	✔	✔	✔	✔	⊖	✘

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](#)

IP Address ▾	Device Name	Status	ICMP	SNMP	CLI	HTTP(s)	NETCONF
10.85.54.23	C9200L-1.lila.com	✔	✔	✔	✔	⊖	✔

Netconf failure solved

```
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 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#
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

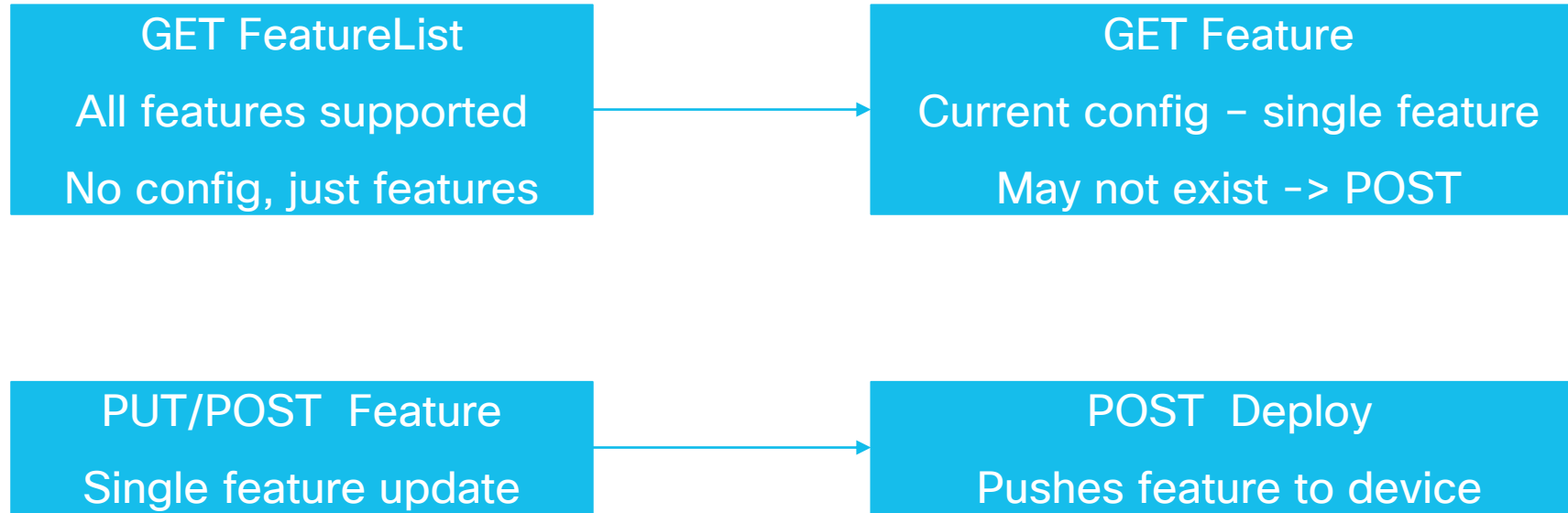
```
aaa new-model
!  
!  
aaa group server radius dnac-network-radius-group
  server name dnac-radius_10.85.54.185
  ip radius source-interface Vlan419
!  
aaa authentication login VTY1 authn group dnac-network-radius-group local
aaa authentication login netconf-authn group dnac-network-radius-group 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="× Device_LVL15"/> +	<input type="text" value="Employees"/> × ▾ +	0	
	_NETCONF	AND	InternalUser-IdentityGroup EQUALS User Identity Groups:Employee	<input type="text" value="× Device_LVL15"/> +	<input type="text" value="Employees"/> × ▾ +	0	
			Network Access-NetworkDeviceName CONTAINS 9800				
			NETCONF_9200				

Automation beyond the UI: API's

API Overview



Mapping to the UI

CONFIGURATION

Layer 2

VLAN

Discovery Protocols

STP

VTP

DHCP Snooping

IGMP Snooping

MLD Snooping

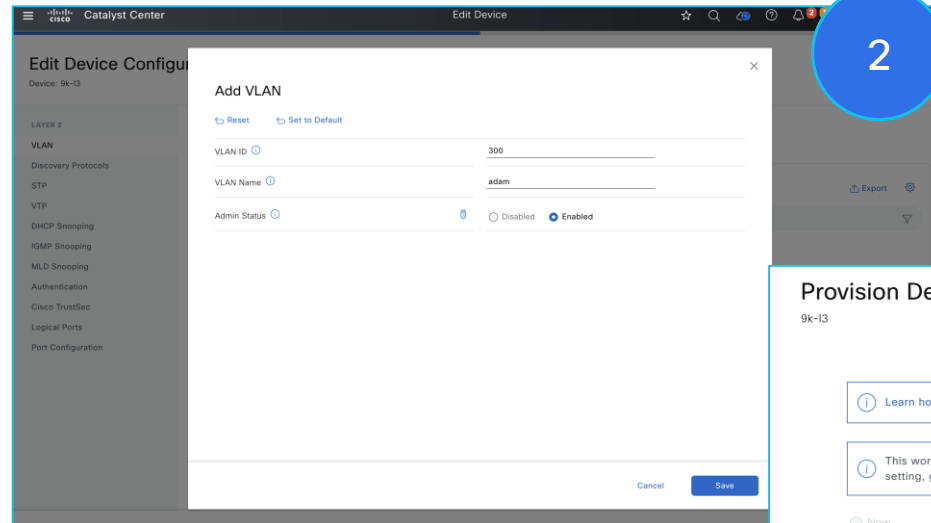
Authentication

Cisco TrustSec

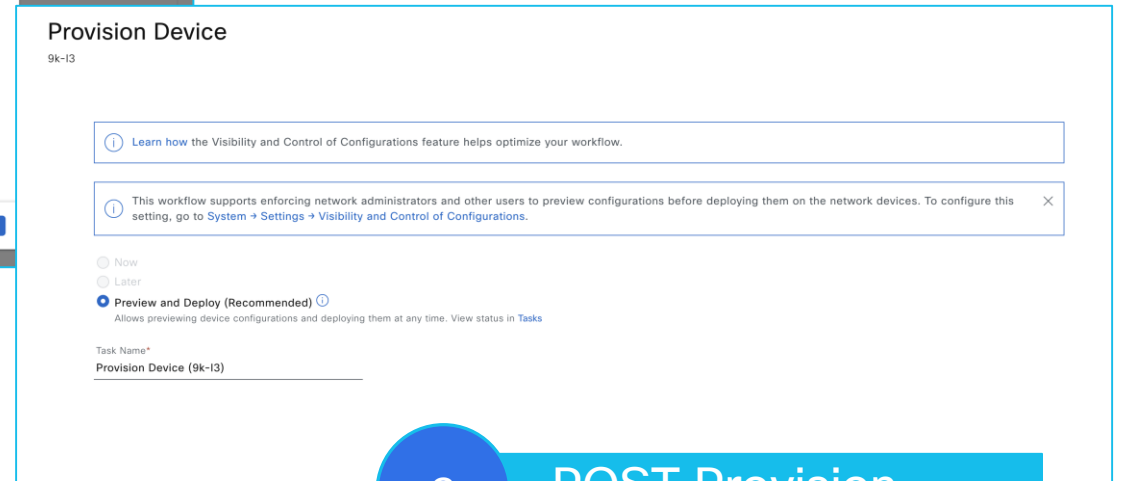
Logical Ports

Port Configuration

1 GET FeatureList



2 PUT Feature



3 POST Provision

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"  
}
```

https://github.com/aradford123/campus_auto_API

The screenshot shows a GitHub repository page for 'campus_auto_API' by user 'aradford123'. The repository is public and has 1 branch (main) and 0 tags. The commit history shows a recent commit 'tweak README' by 'aradford123' 11 minutes ago, with 4 commits in total. The file list includes 'data', 'LICENSE', 'README.md', 'bf_switching.py', 'change.py', 'dnac_config.py', 'interface_as_code.py', and 'task.py'. The README file is selected, showing the title 'campus_auto_API' and the text: 'These scripts are examples of using the campus automation API for Catalyst Center' and 'bf_switching.py' with the description 'This script dumps out the features supported on a device.'

File	Commit	Time
data	first commit	12 minutes ago
LICENSE	tweak README	11 minutes ago
README.md	tweak README	12 minutes ago
bf_switching.py	first commit	12 minutes ago
change.py	first commit	12 minutes ago
dnac_config.py	first commit	12 minutes ago
interface_as_code.py	first commit	12 minutes ago
task.py	first commit	12 minutes ago

Closing and Q&A

Complete your session evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to win 1 of 5 full conference passes to Cisco Live 2026.



Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live mobile app.

Continue your education



Visit the Cisco Showcase for related demos



Book your one-on-one Meet the Engineer meeting



Attend the interactive education with DevNet, 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

Continue your education

cisco.com/go/catalyst-center



cs.co/dnac-resources

Thank you

CISCO Live !

