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

BRKOPS-2697

Adam Radford, Distinguished Solutions Engineer @adamradford123

Lila Rousseaux, Principal Solutions Engineer @lila_rousseaux

June 2025

Cisco Webex App

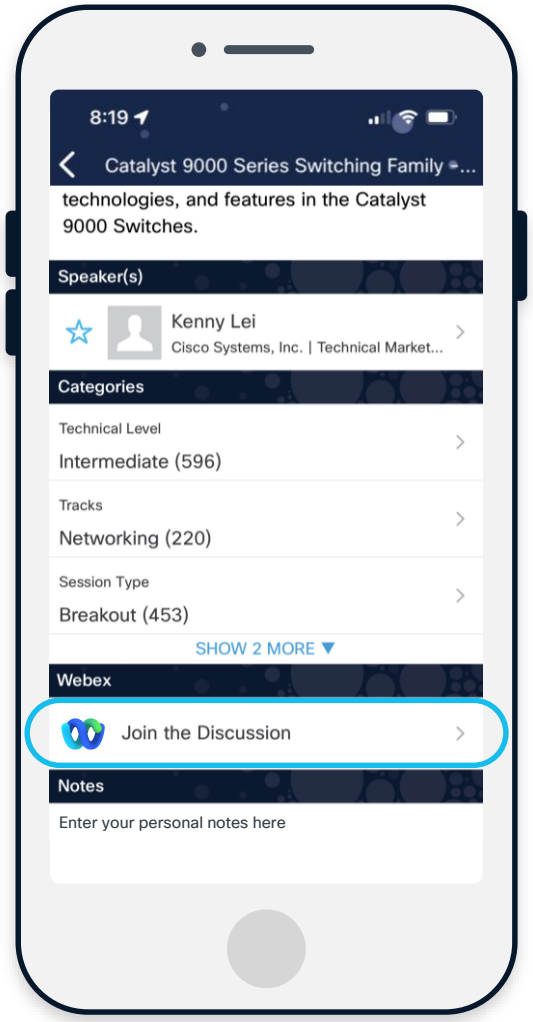
Questions?

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 manually[1]

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

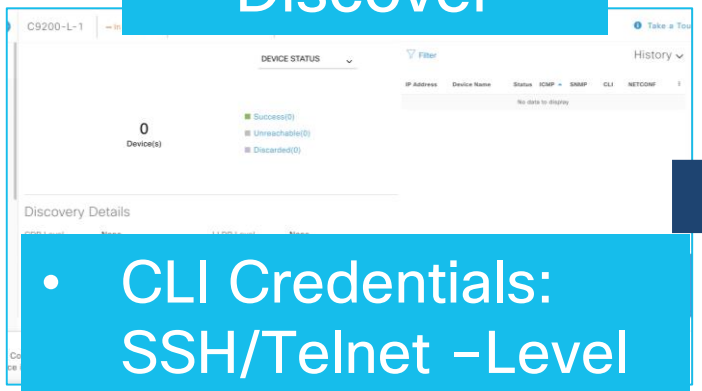
1. Onboard Devices to Catalyst Center
2. Assign Devices to Sites
3. Populate Network Settings (Servers)
4. Create Network Profiles
5. Provision Devices

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

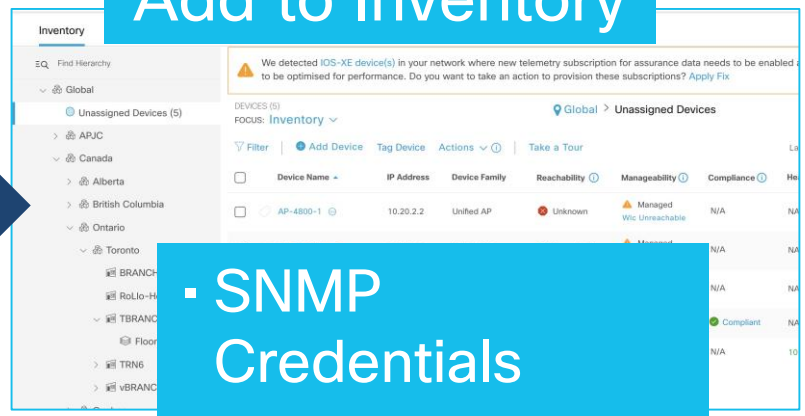
Brownfield device onboarding

Discover



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

Add to Inventory



- SNMP Credentials
- NETCONF

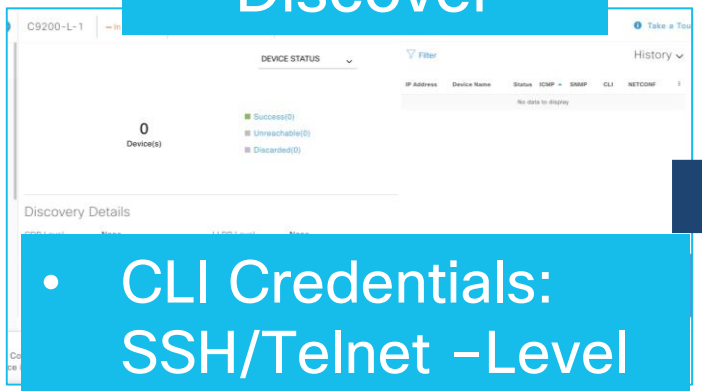
Note: Devices can be onboarded through other methods like PnP, PDMT and others

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

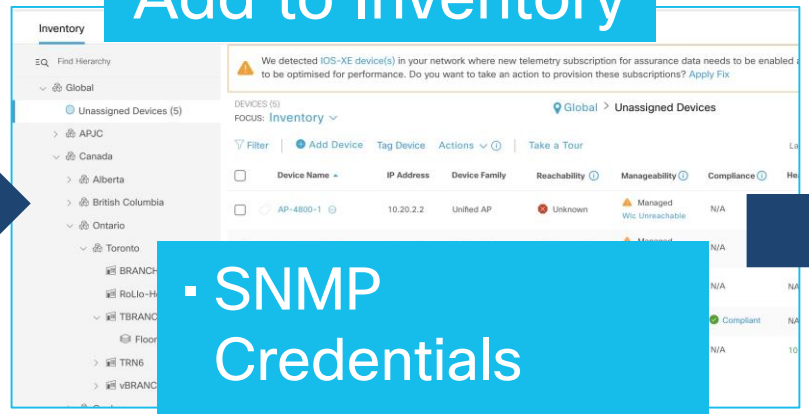
Brownfield device onboarding

Discover



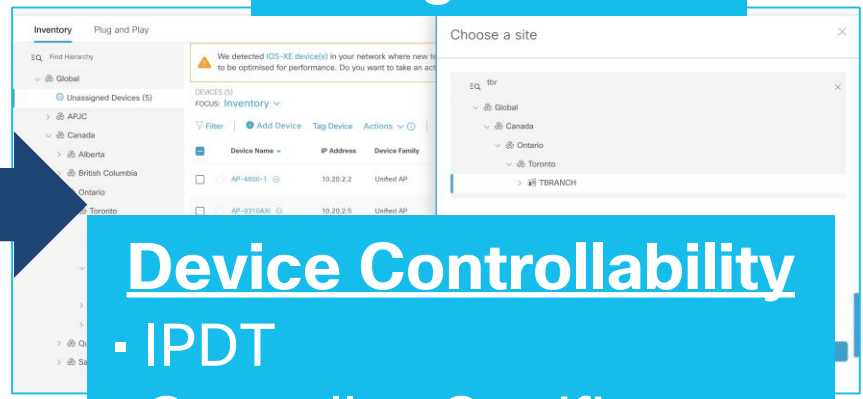
- CLI Credentials: SSH/Telnet –Level 15 or enable password
- At least SNMPv2c read
- Netconf enabled (WLC)

Add to Inventory



- SNMP Credentials
- NETCONF

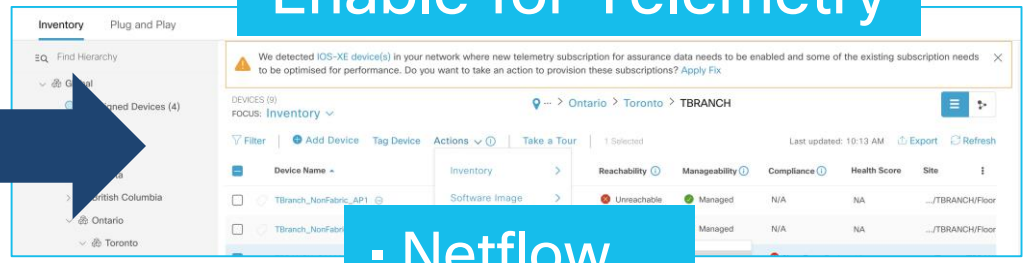
Assign to Site



Device Controllability

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

Enable for Telemetry



- Netflow

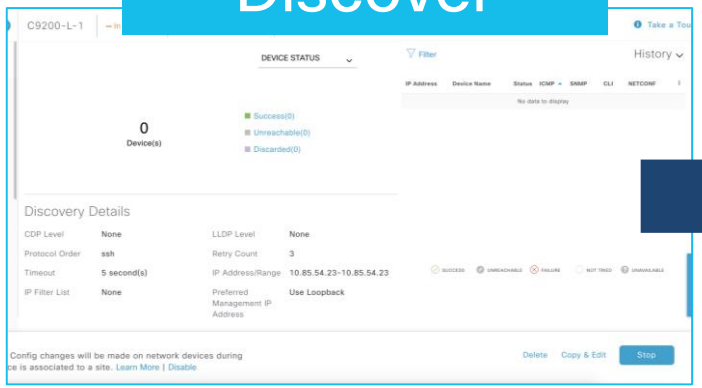
Steps for Device Provisioning using Intent Based Automation

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

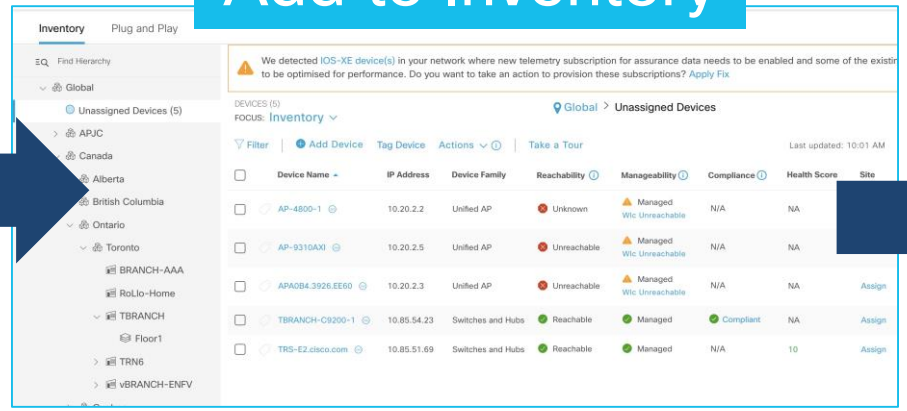
Associated to Site

Brownfield device automation

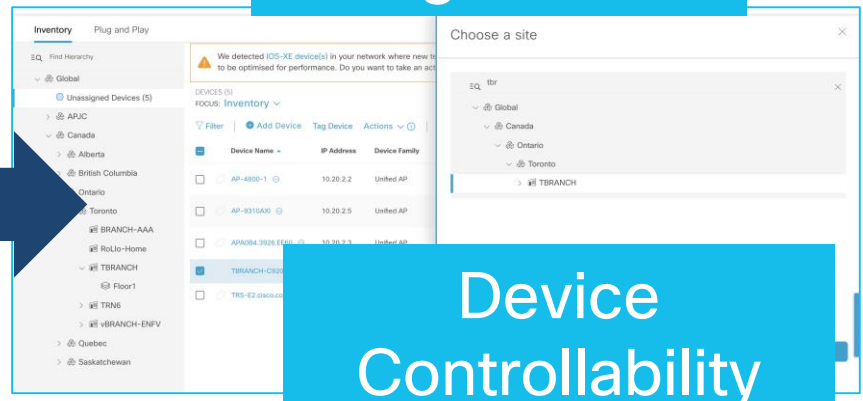
Discover



Add to Inventory

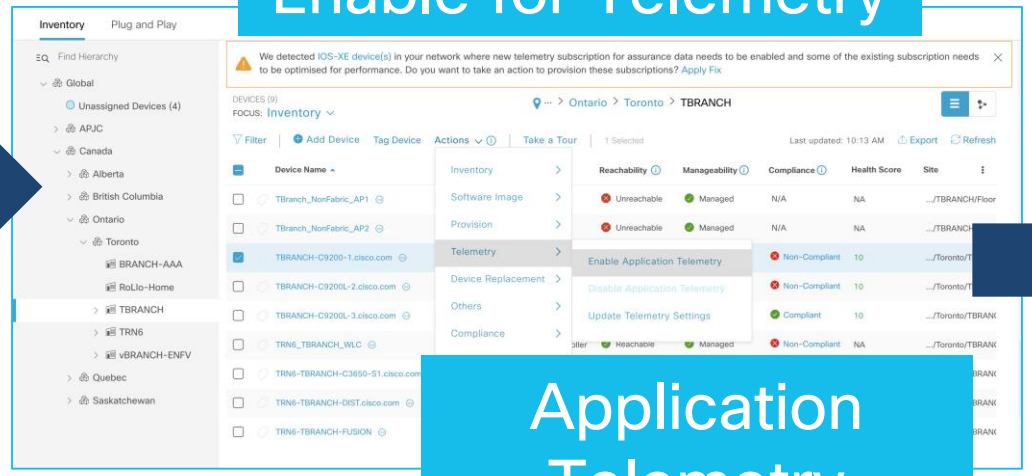


Assign to Site



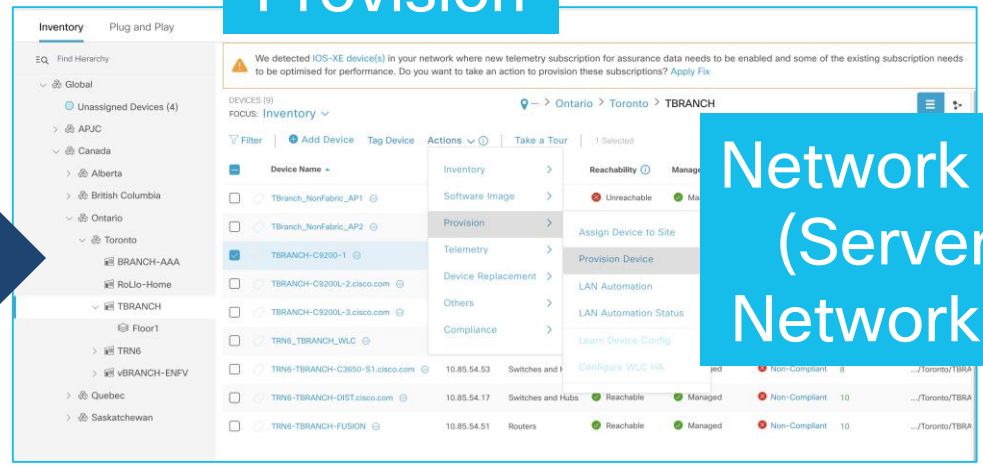
Device Controllability

Enable for Telemetry



Application Telemetry

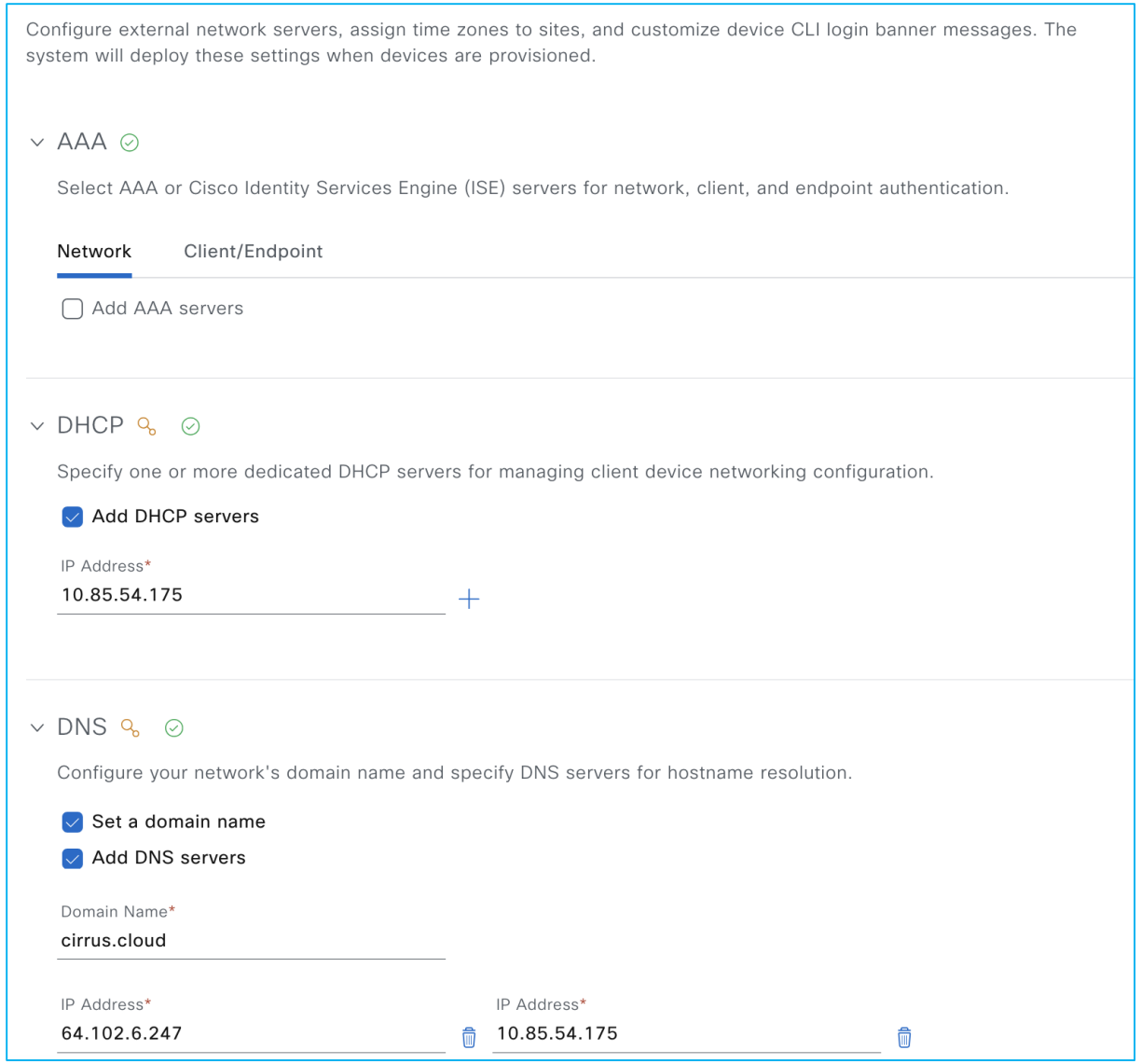
Provision



Network Settings (Servers) and Network Profiles

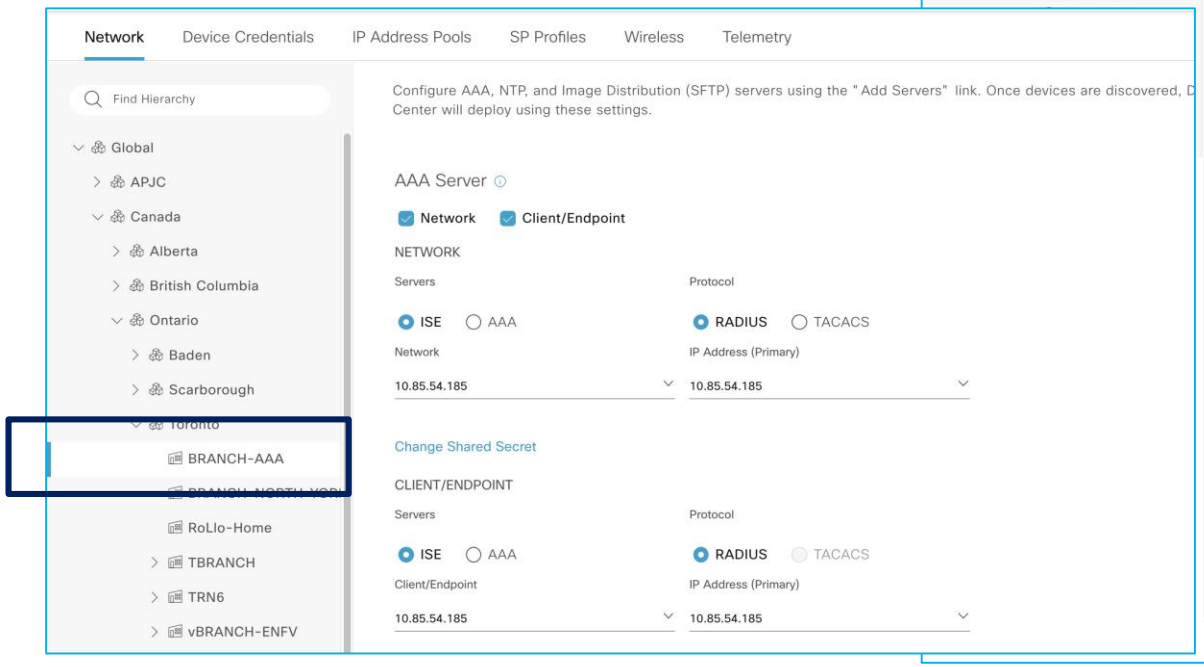
Network Settings - Servers

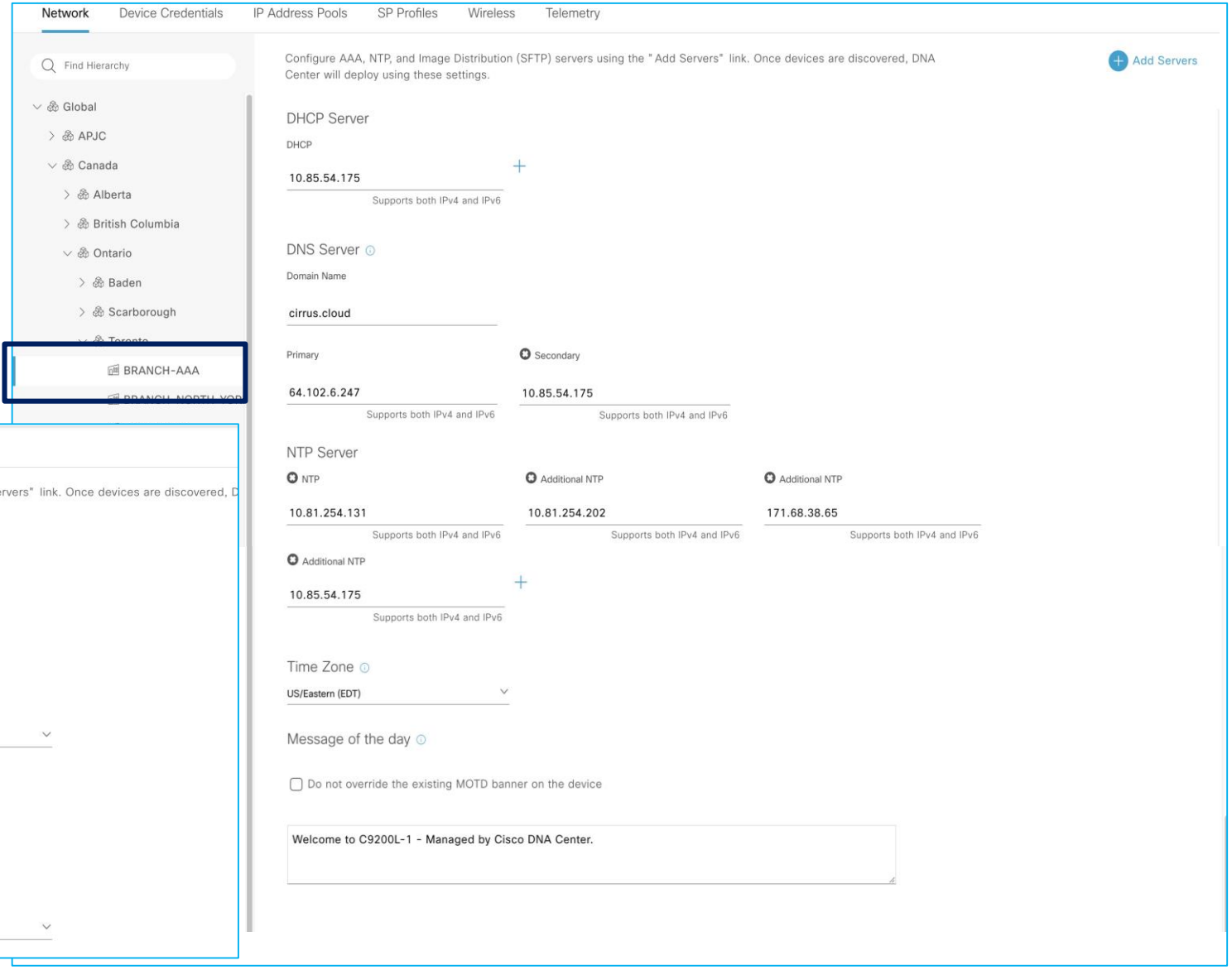
- AAA (Network Client/Endpoint)
- DHCP
- DNS and Domain
- Stealthwatch Flow Destination
- Image Distribution
- NTP
- Time Zone
- Message of the Day



Network Settings - Servers

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





Steps for Device Provisioning using Intent Based Automation

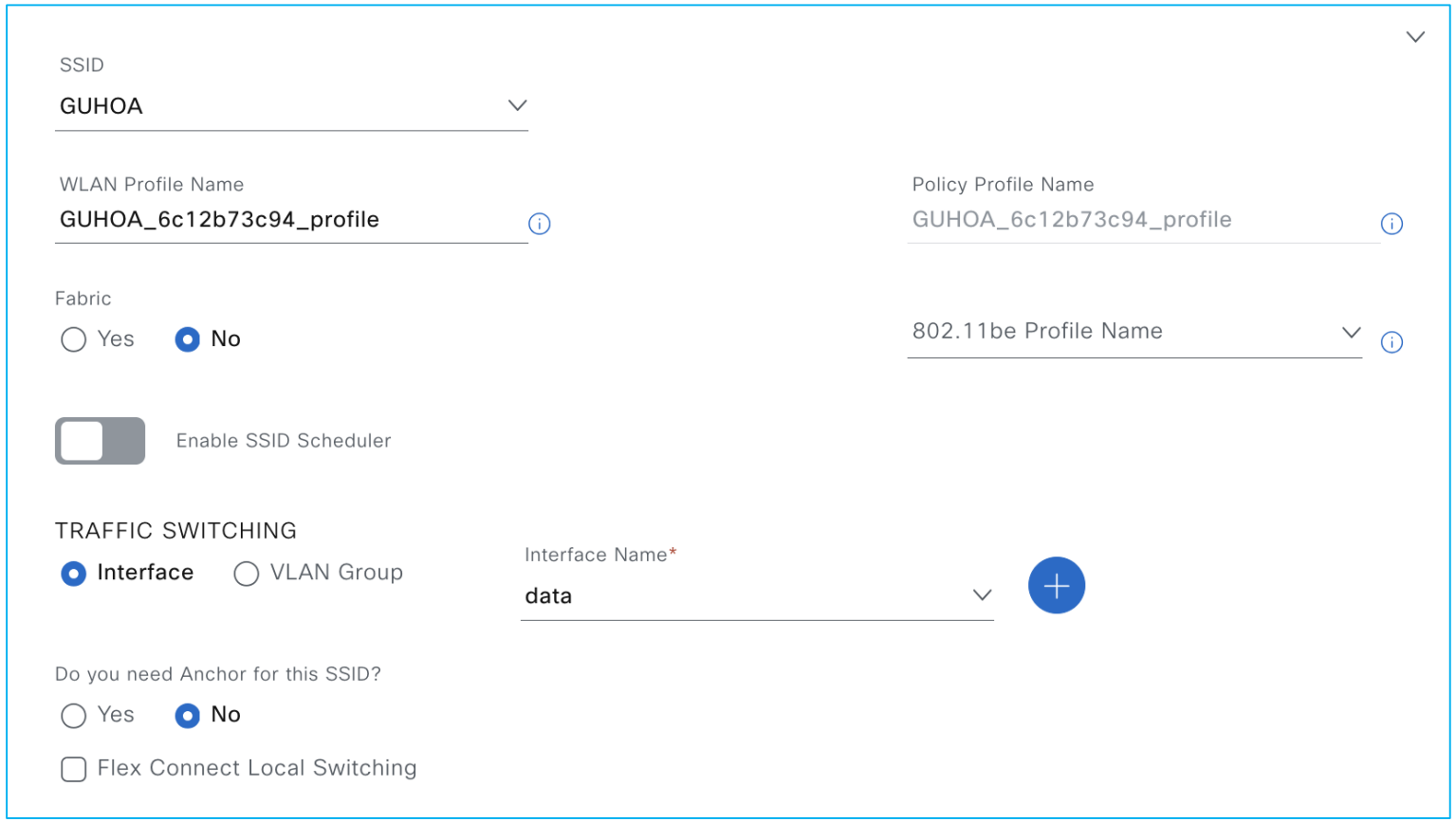
1. Onboard Devices to Catalyst Center
2. Assign Devices to Sites
3. Populate Network Settings (Servers)
4. **Create Network Profiles**

} **Associated to Site**

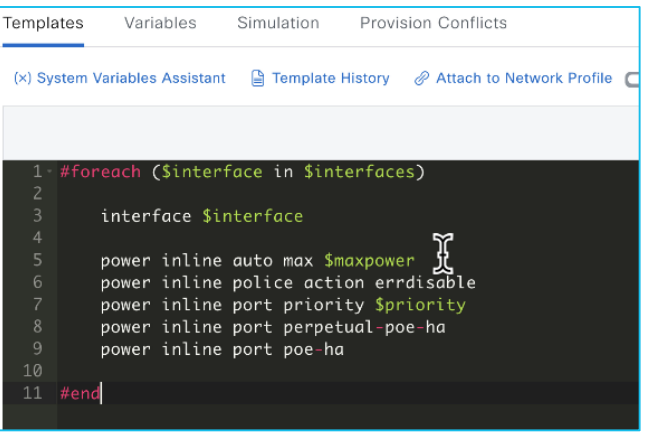
5. Provision Devices

Network Profiles

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



Catalyst Center – Intent Based Configuration Switches



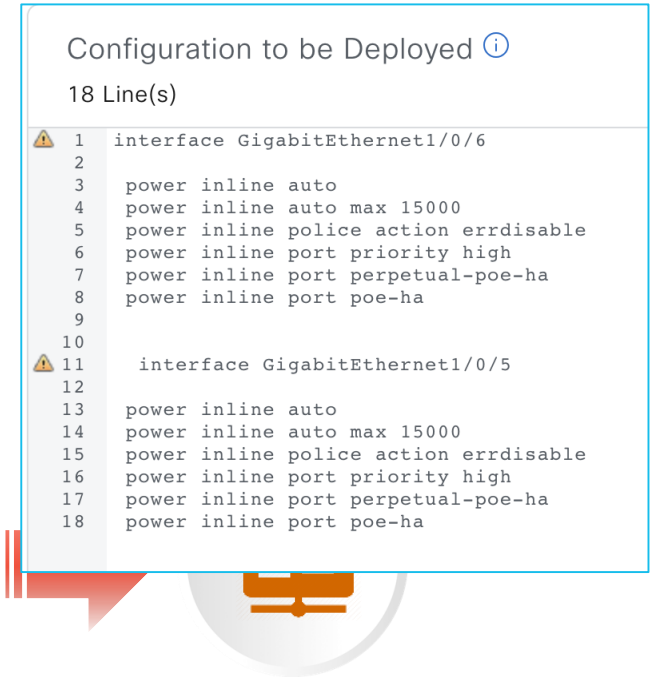
Day N Template

Network Settings

PROFILE

Switches

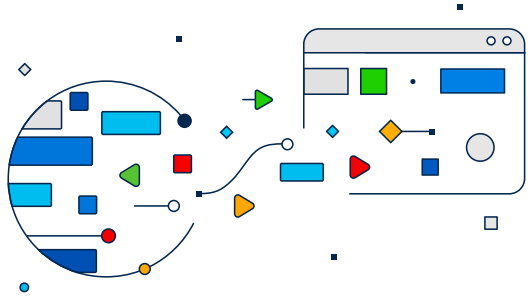
SITE



Provision

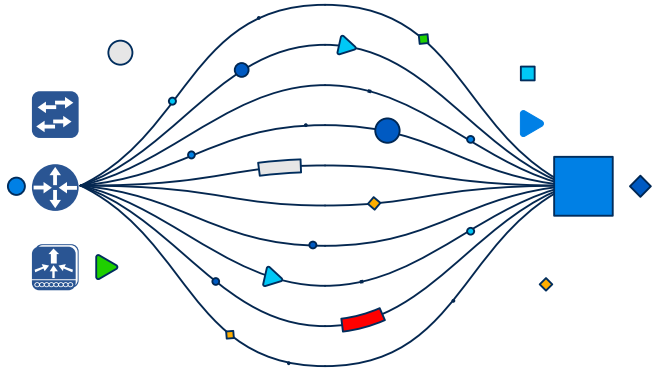
Evolution to Per-Device Configuration for Wired

Catalyst Center- Per-Device Configuration



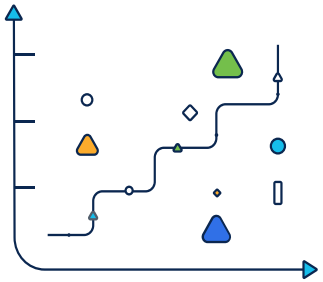
Discover

Add devices from existing infrastructure



Learn

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

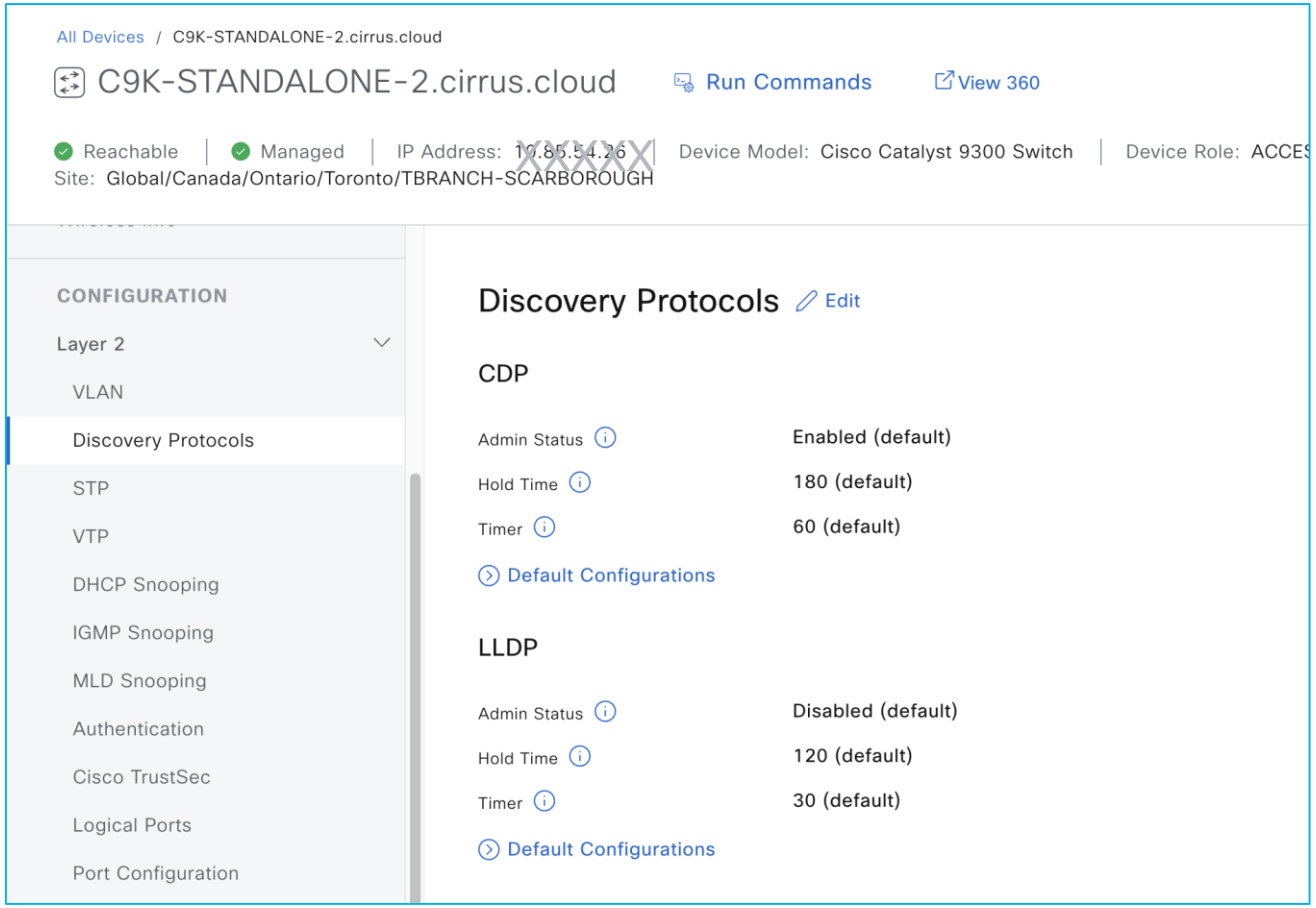


Manage

Simplified configuration read/write at an Element Level

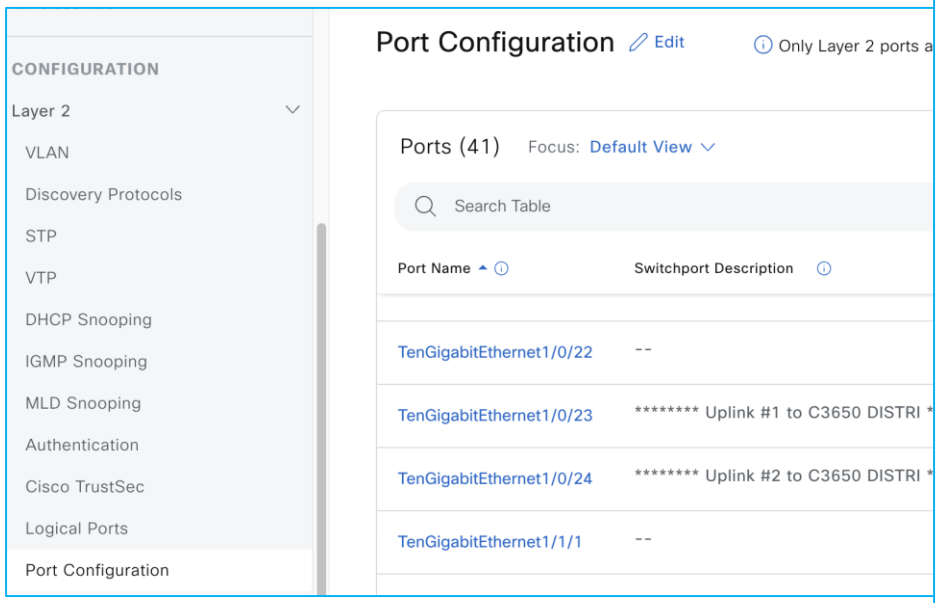
Simplified View and Edit of Switch Configuration

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

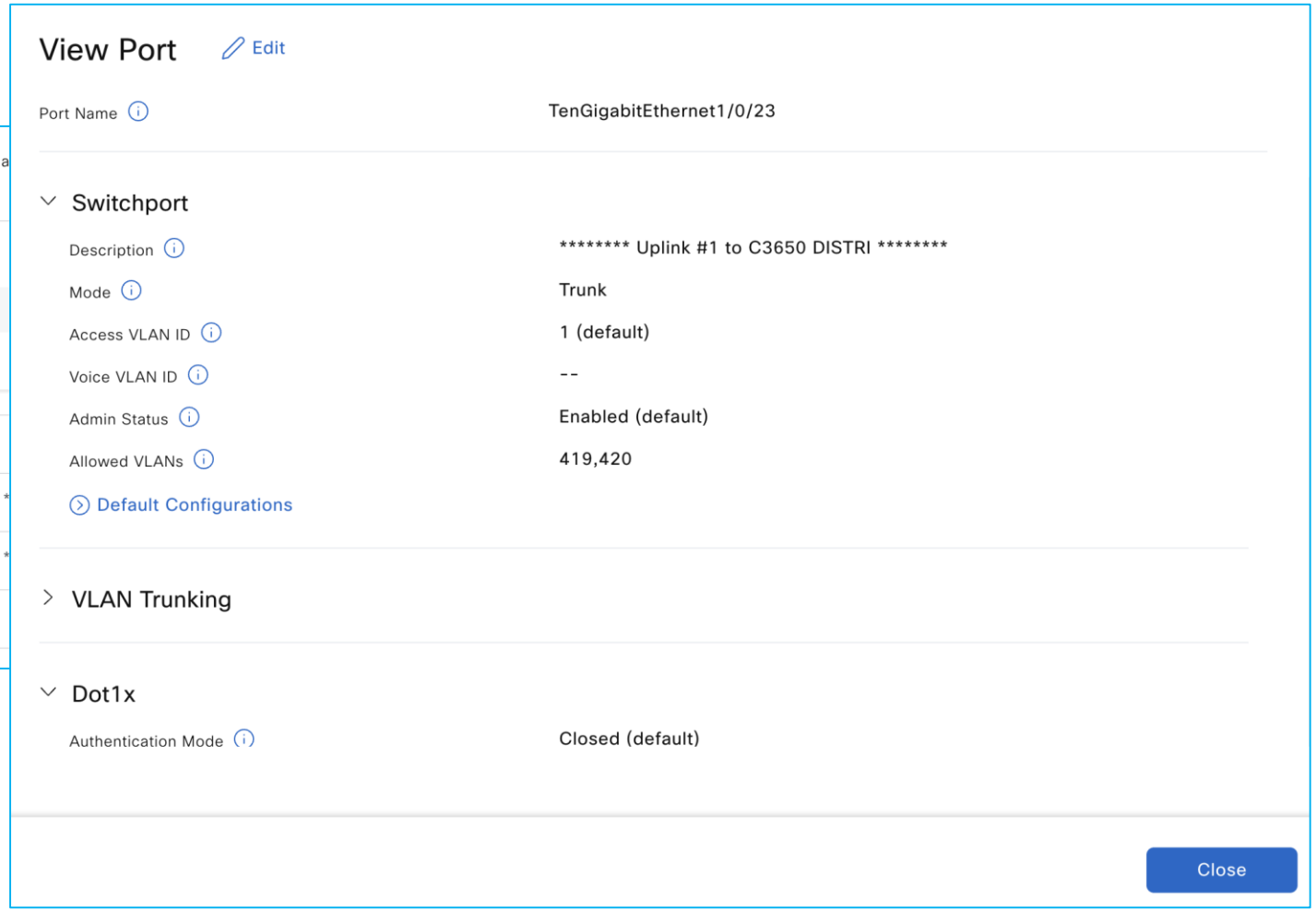


Catalyst Center- Per-Device Configuration - Switches

Phase 1: Layer 2 configurations

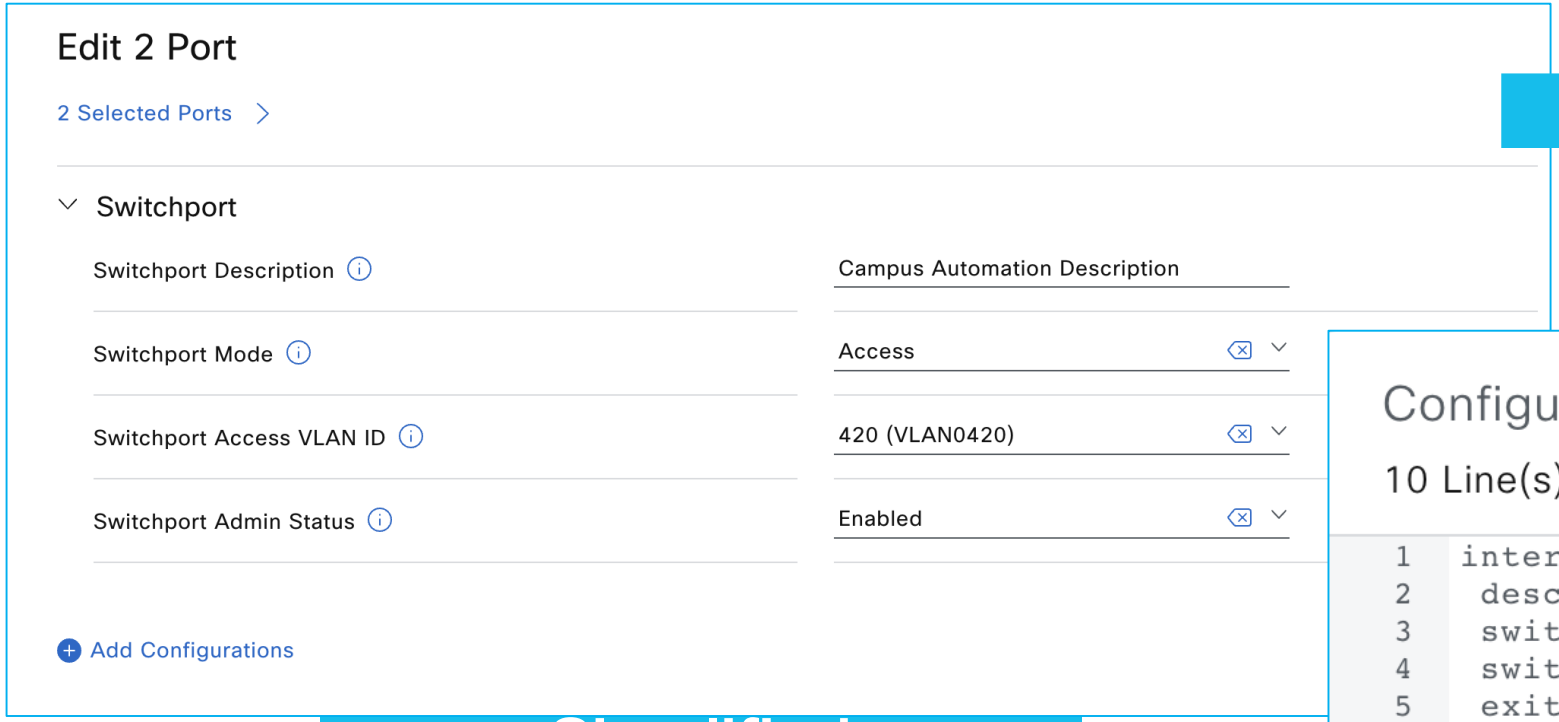


Simplified visualization

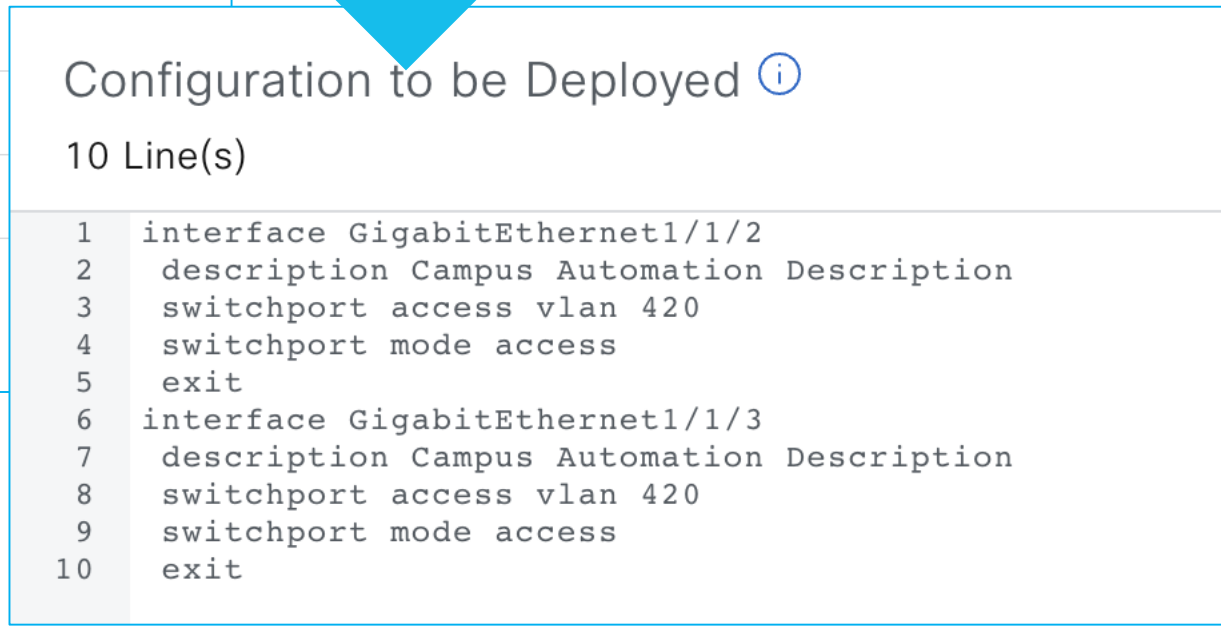


Catalyst Center- Per-Device Configuration - Switches

Phase 1: Layer 2 configurations



Simplified Configuration

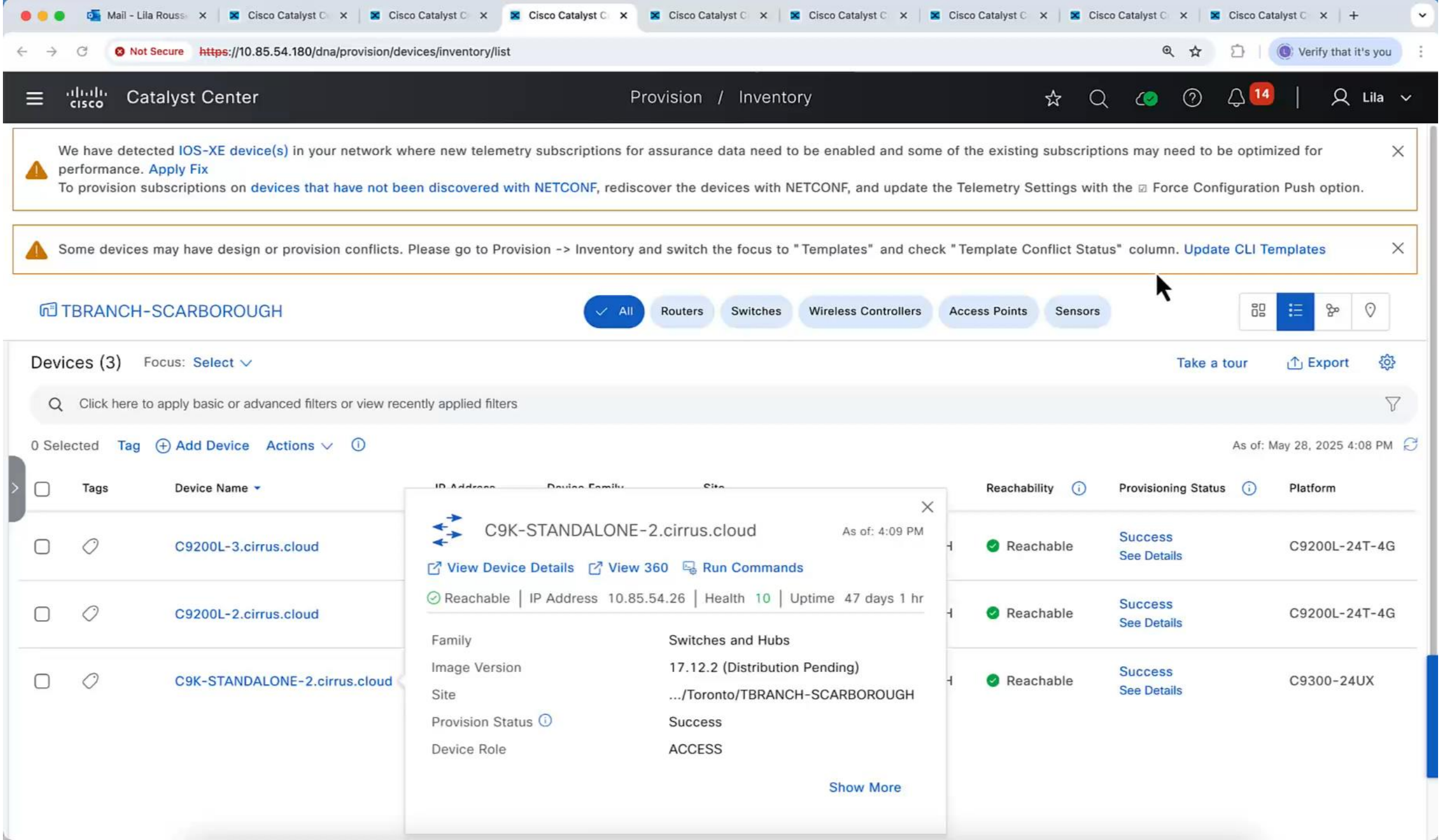


Catalyst Center- Per-Device Configuration - **Switches**

Reference

Pre-Requisites

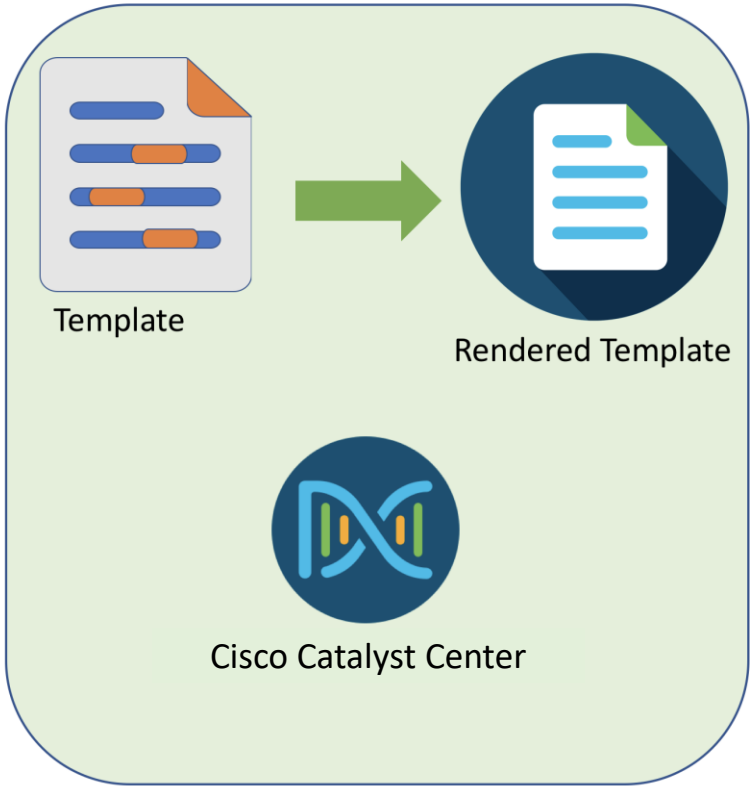
- Catalyst 9000 Series Switches running Cisco IOS-XE 17.3 or later
- Cisco Catalyst Center version 2.3.7.9 or later
  - L2 Configurations available
- For devices provisioned using SDA, only Config Visibility is supported

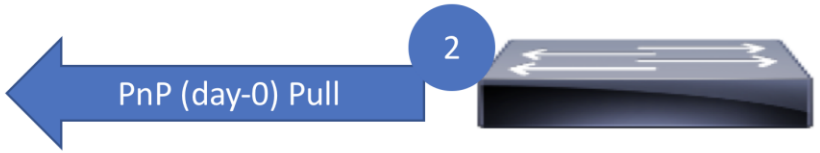

Not Secure https://10.85.54.180/dna/provision/devices/inventory/list
Verify that it's you
Catalyst Center
Provision / Inventory
14
Lila
We have detected IOS-XE device(s) in your network where new telemetry subscriptions for assurance data need to be enabled and some of the existing subscriptions may 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
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
Reachability
Provisioning Status
Platform
C9200L-3.cirrus.cloud
Reachable
Success
See Details
C9200L-24T-4G
C9200L-2.cirrus.cloud
Reachable
Success
See Details
C9200L-24T-4G
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

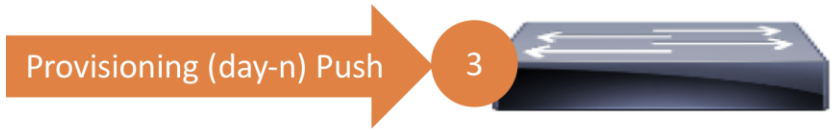
Templates

Day0 vs Day-N

Reference







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

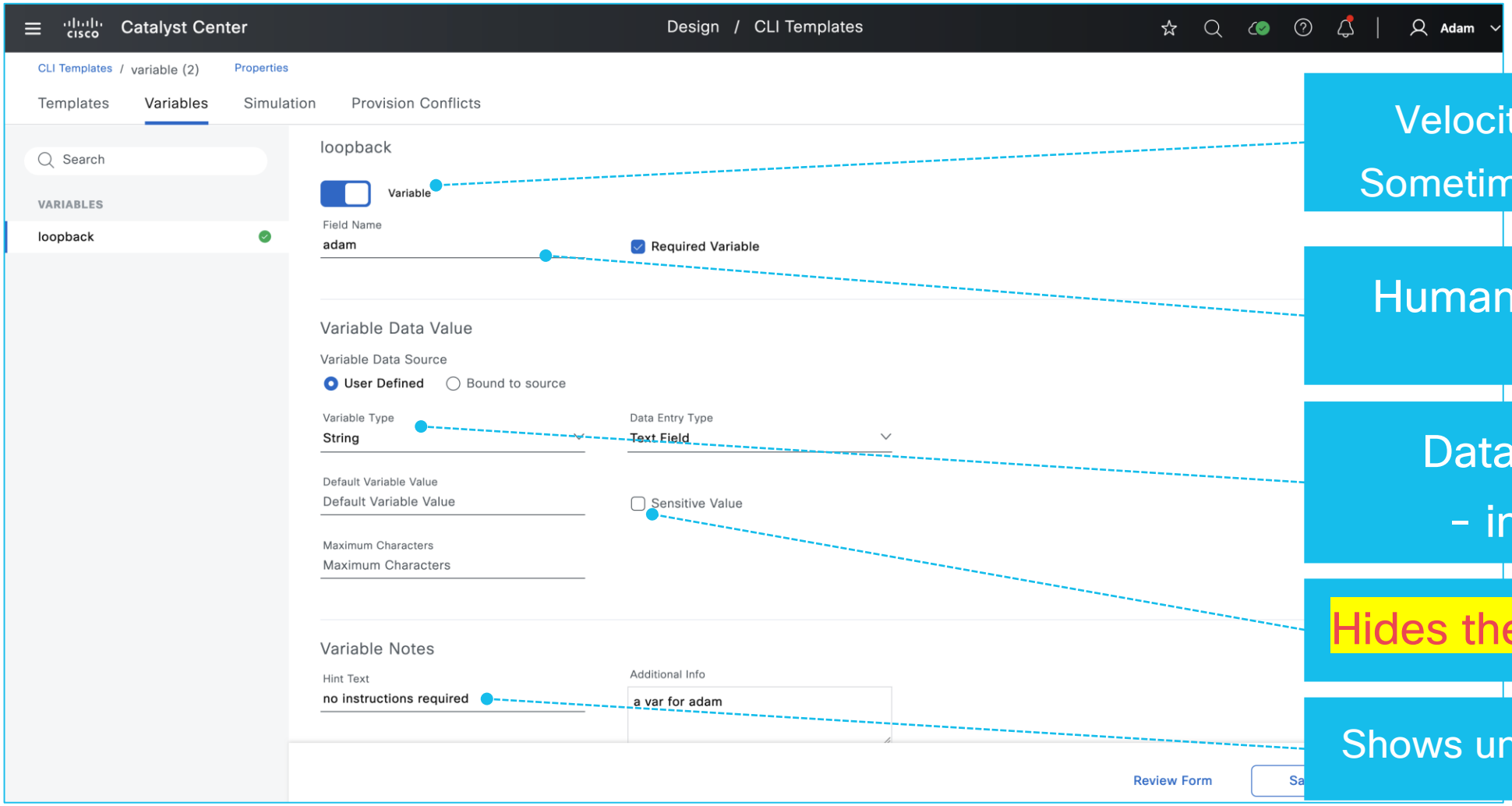
	velocity	jinja
variable reference	`$loopback`	`{{loopback}}`
assignment	`#set ($loopback = "10.10.10.1")`	`{% set loopback = "10.10.10.1" %}`

conditional	`#if ($hostname == "border01")`
	`  foo`
	`#end`
		`{% if hostname == "border01" %}`
		`foo`
		`{% endif %}`

loop	`#foreach ($number in [0..3])`
	`  int gig1/${number}/24`
	`  shutdown`
	`#end`
		`{% for number in range(3) %}`
		`  int gig1/{{ number }}/24`
		`  shutdown`
		`{% endfor %}`

implicit variables	`#foreach ($interface in $__interfaces)`	`{% for interface in __interface %}`
interactive mode	yes	yes
ENABLE and MULTLINE	yes	yes
filters	no	yes

Introduction to variables



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

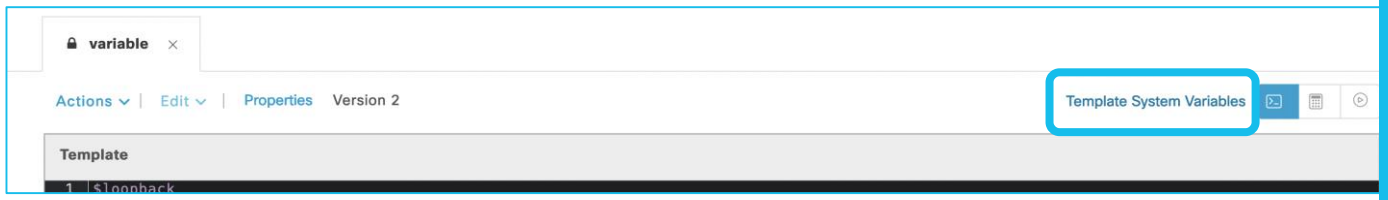
"introspect" data Catalyst Center has about the device

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

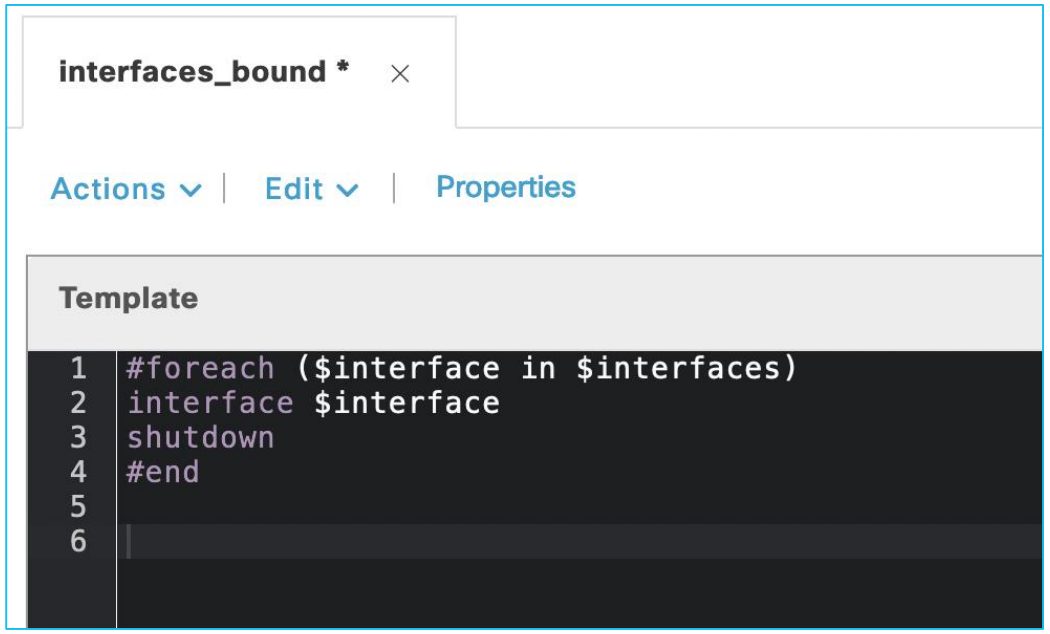
Filter

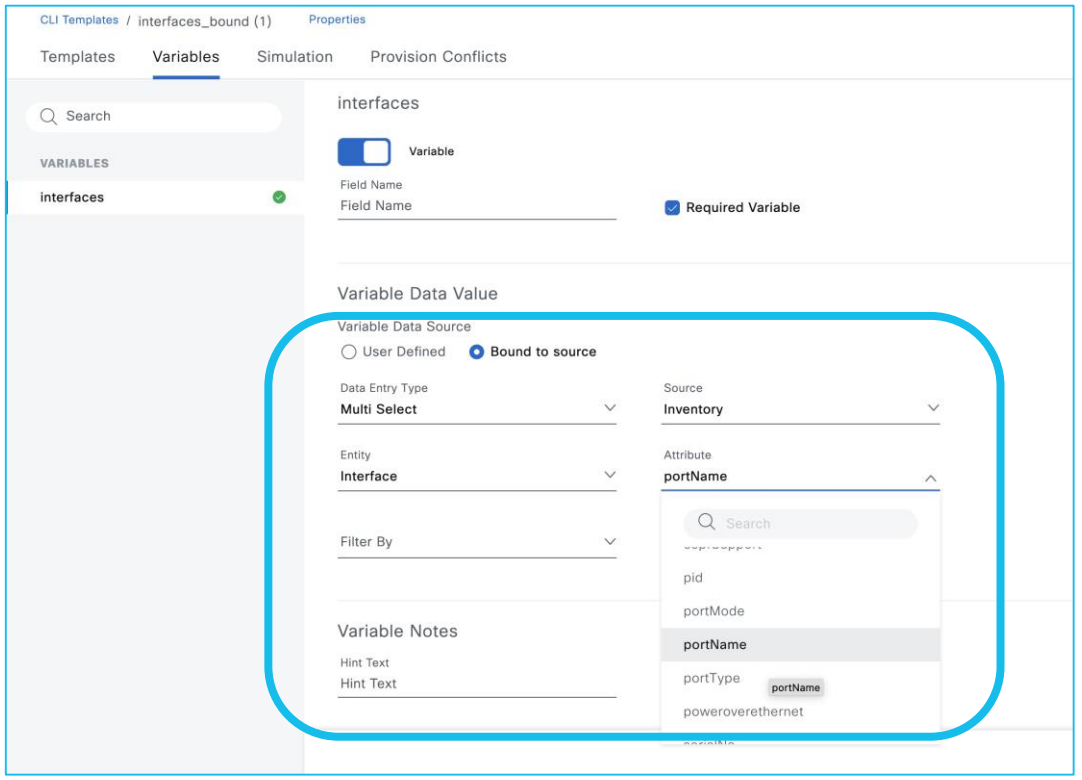
Source	Entity	Variable Name	Attribute Name
NetworkProfile	SSID	__ssid	
NetworkProfile	SSID	__ssid[index].wlanId	wlanId
NetworkProfile	SSID	__ssid[index].wlanProfileName	wlanProfileName
NetworkProfile	Policy Profile	__policyprofile	
NetworkProfile	AP Group	__apgroup	
NetworkProfile	Flex Group	__flexgroup	
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

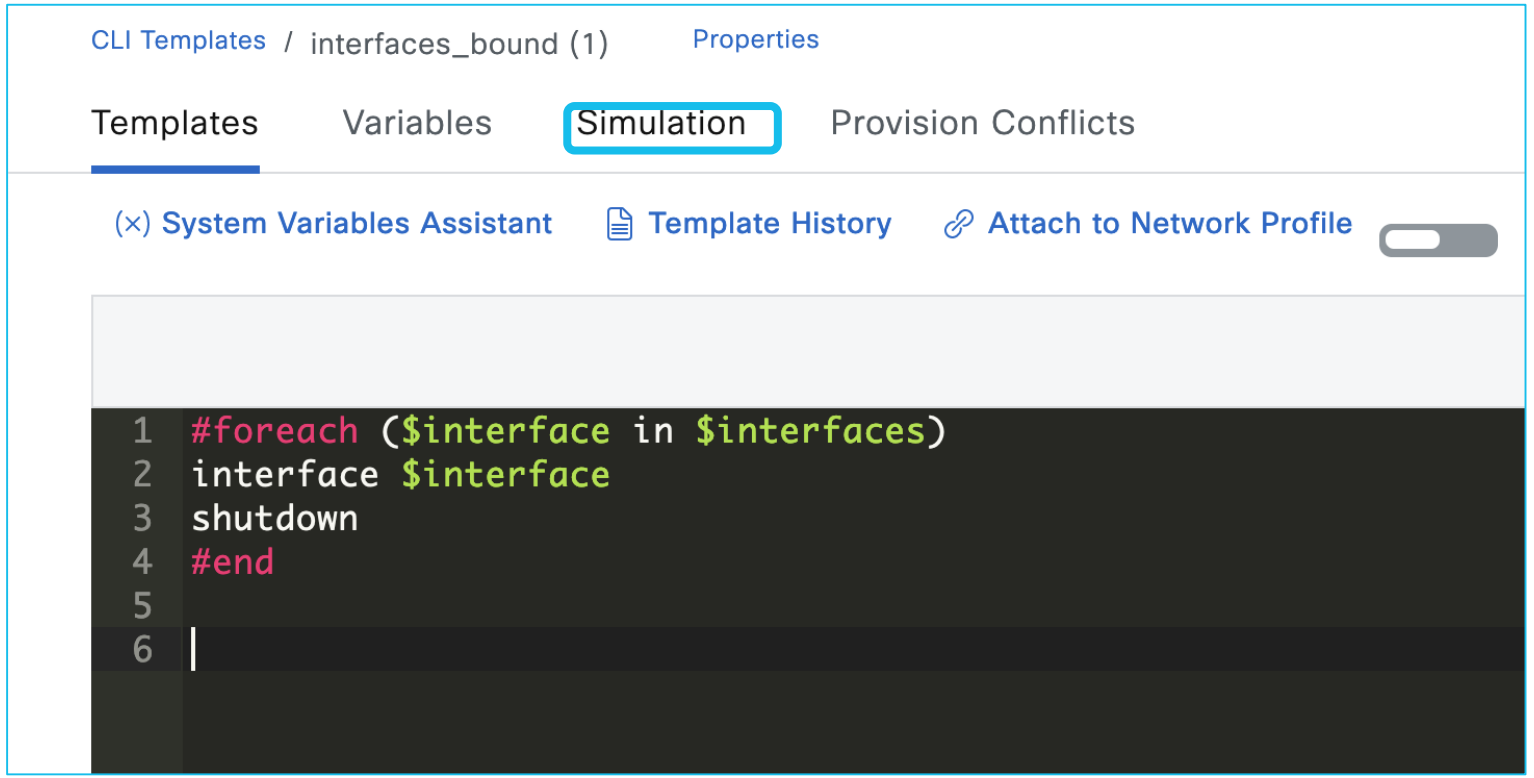
Take a system variable and map to a variable inside the template.
- e.g. template to shut a list of interfaces
- Inventory -> interface -> portName



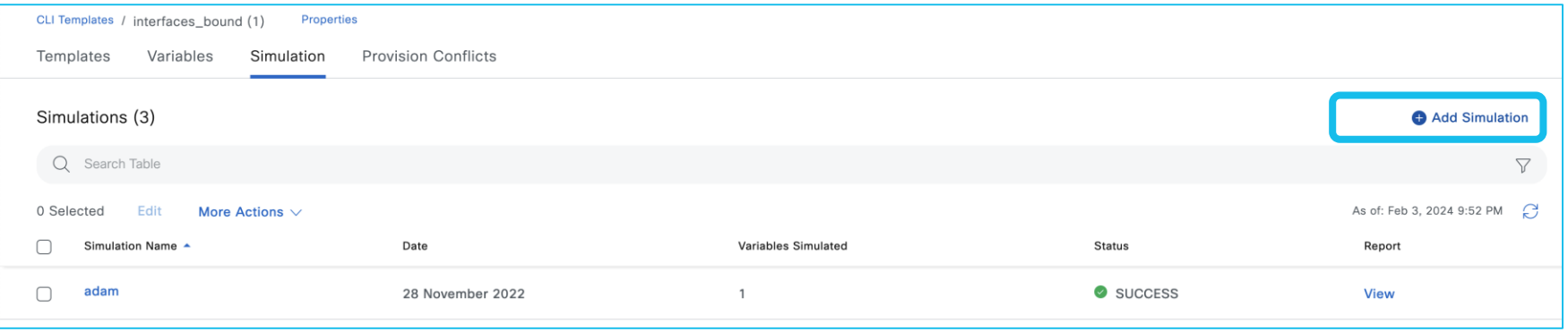


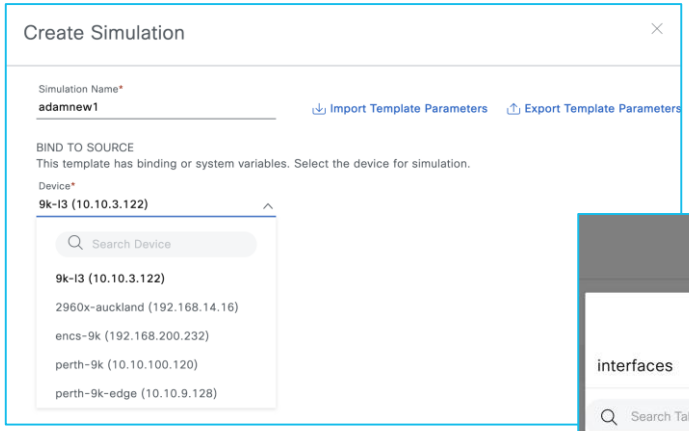
Simulation

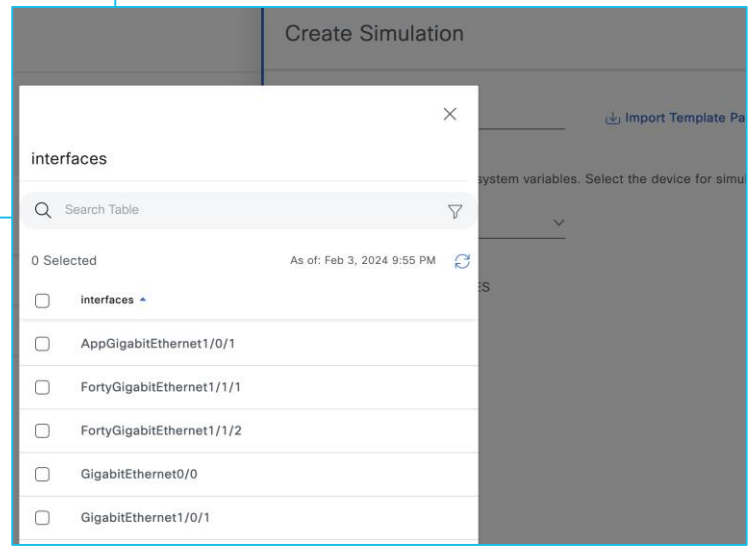
- Select "Simulation" on far right
- Create Simulation



Simulation - #2

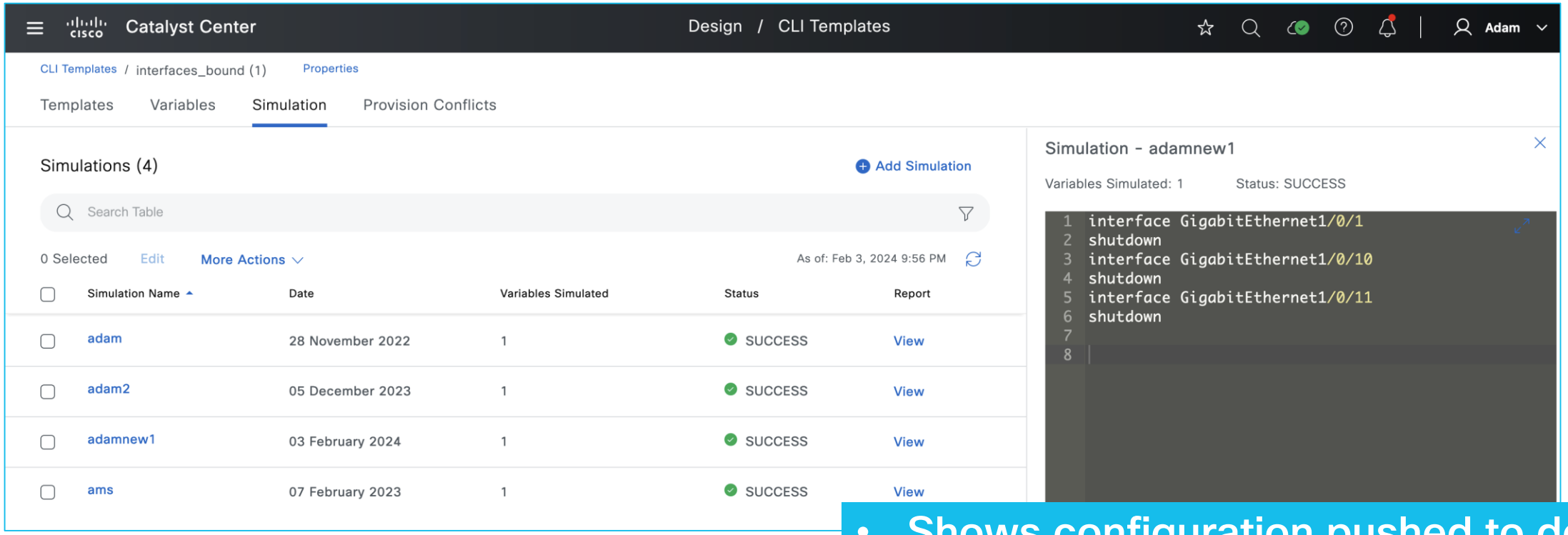






- Click link to select device
- Choose device from list
- Interfaces will be assigned to a list (multi-select)

Simulation #3

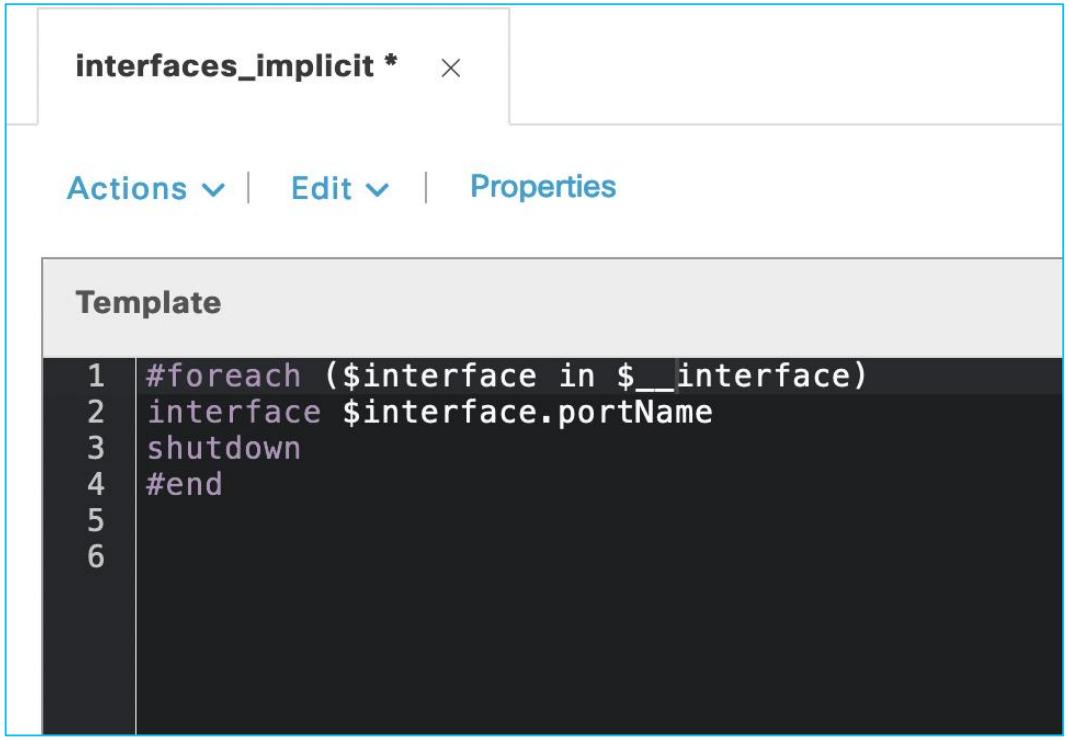


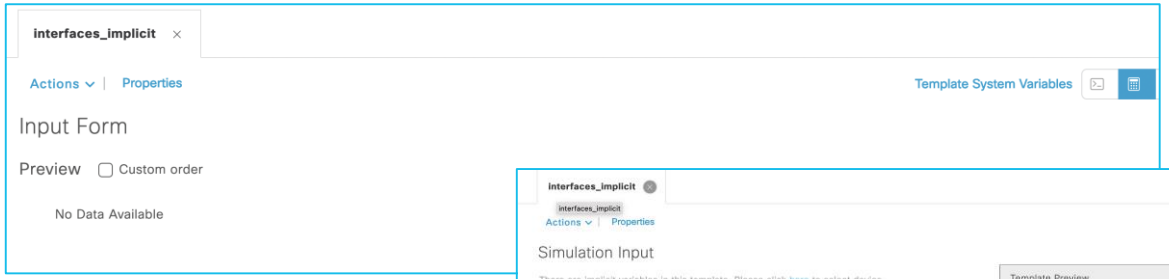
- Shows configuration pushed to device
- Lots of options for more intelligent templates
- Can send all interface attributes and pick those needed

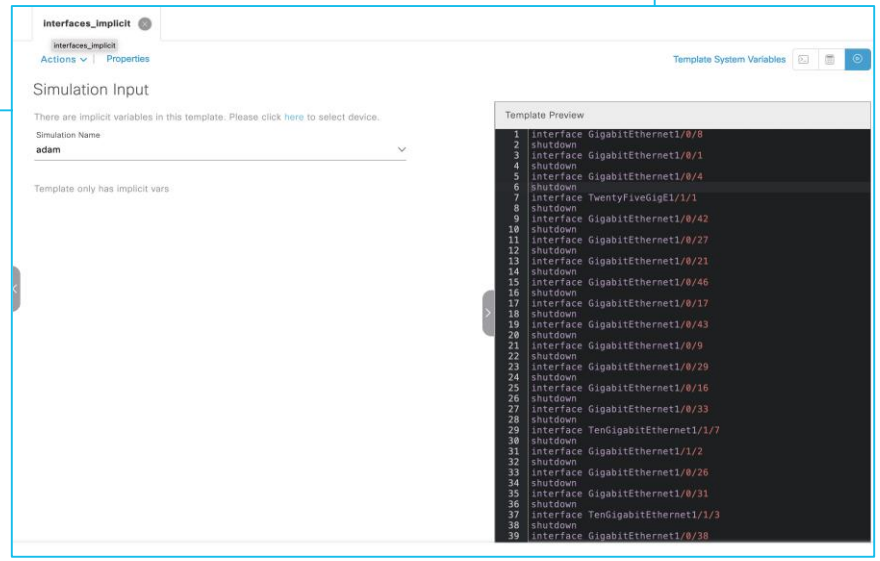
Implicit Variables

- 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!







Real Example

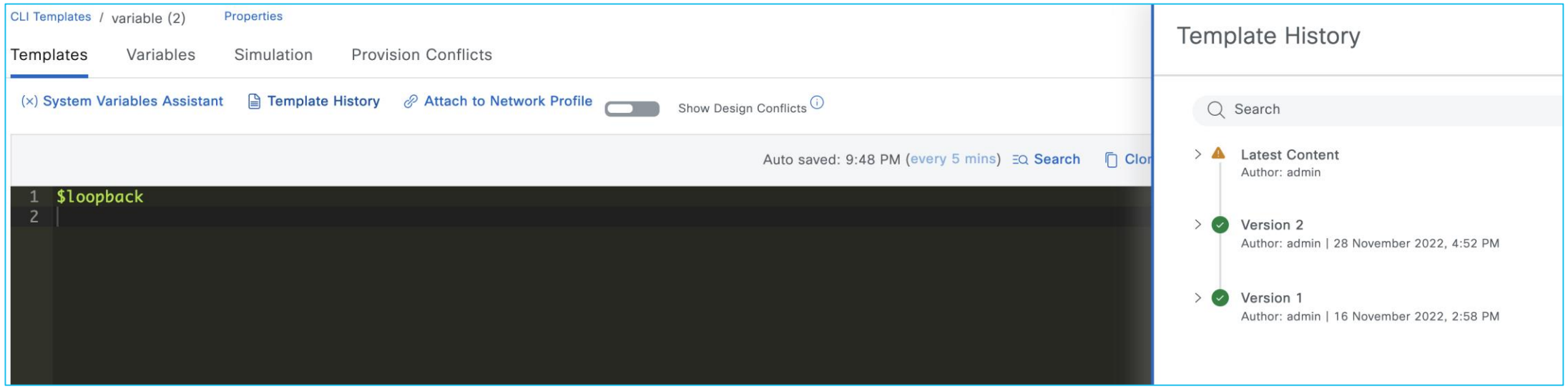
appX_implicit

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



- 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

(×) 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

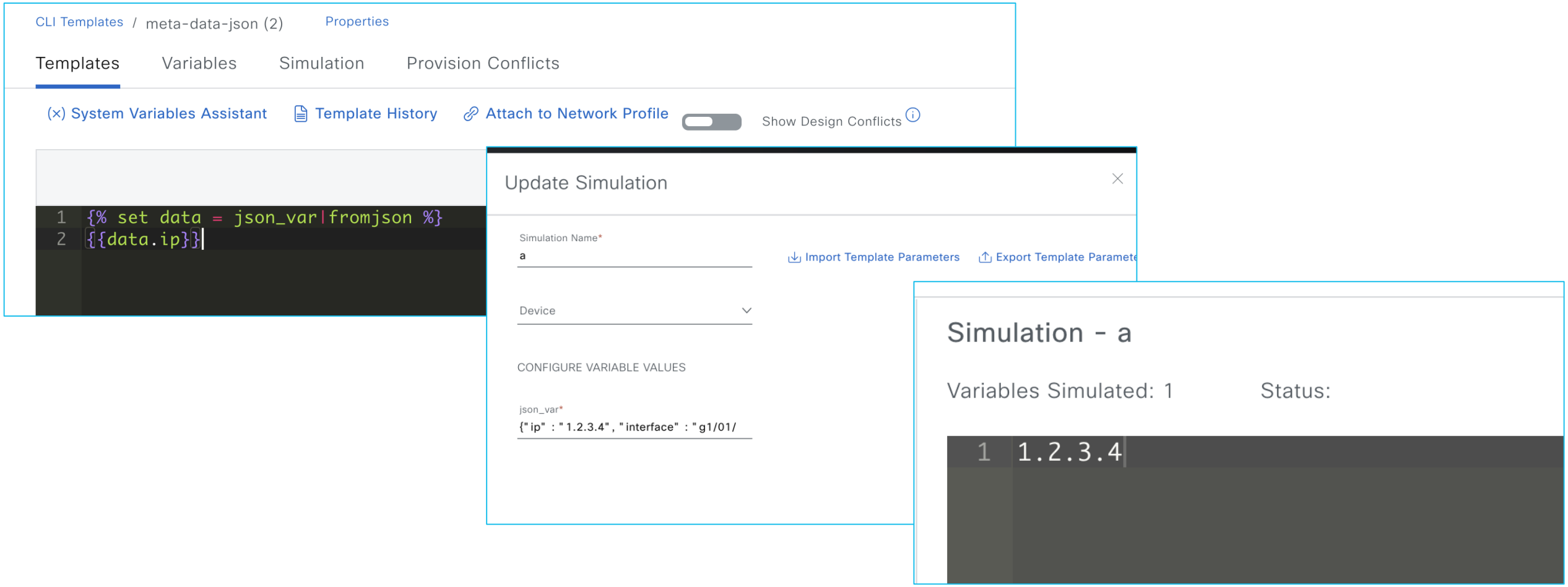
```
{# this was the original.  Needed a throwaway var so the True command was supressed #}
{% set physicalInterfaces = __interface | selectattr("interfaceType", "equalto", "Physical") | list %}
{% set interfaceNames = [] %}

{% for dict_item in physicalInterfaces %}
    {% for key, value in dict_item.items() %}
        {% if key == 'portName' %}
            {% set _ = interfaceNames.append(value) %}
        {% endif %}
    {% endfor %}
{% endfor %}

{{ interfaceNames }}
```

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

{{ interfaceNames }}
```

"selectattr" and "map" are filters

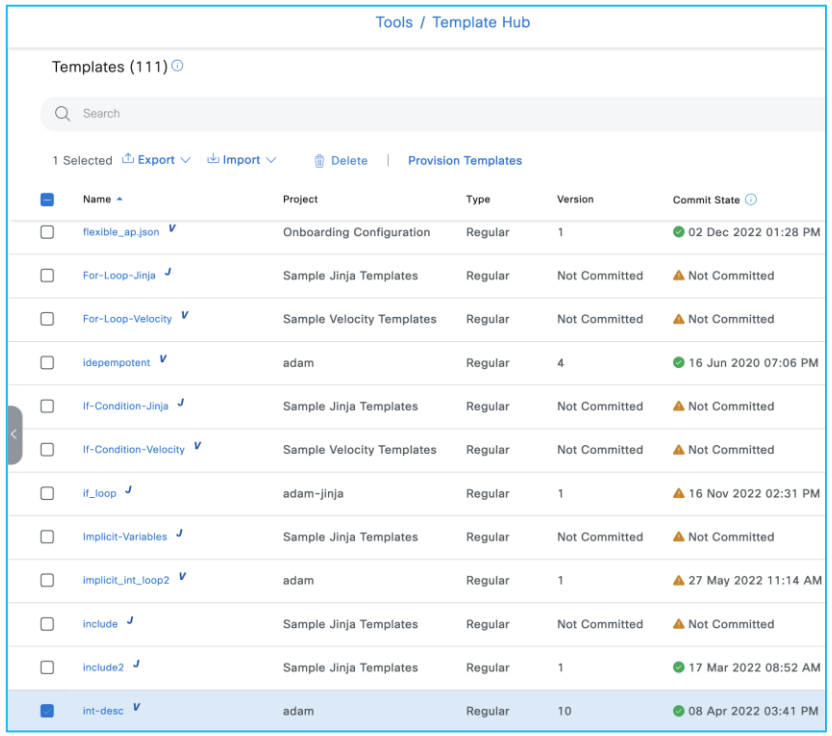
- selectattr: if the attribute "interfaceType" == "Physical"
- map: just pick the attribute "portName" (vs all attributes)

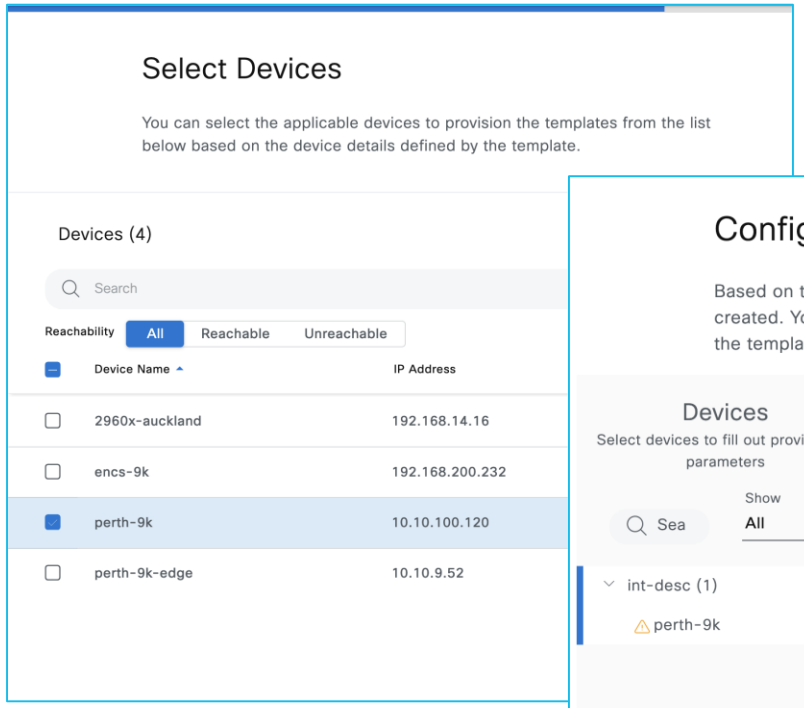
Structured Data as input (vs strings)

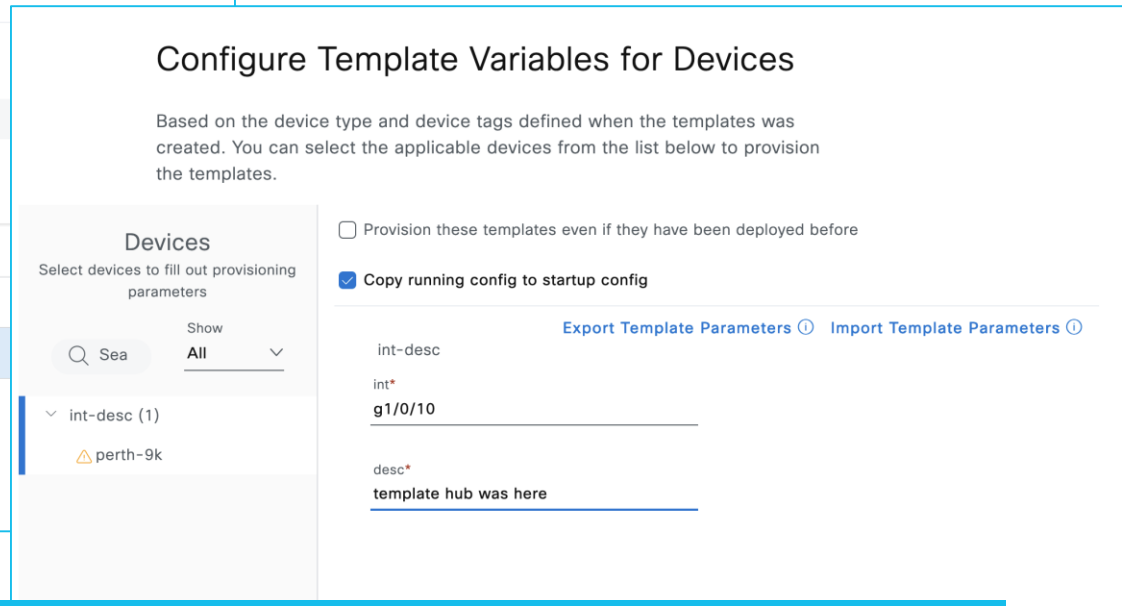


- Can do this via API.
- Also possible through UI (using a filter "fromjson")

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

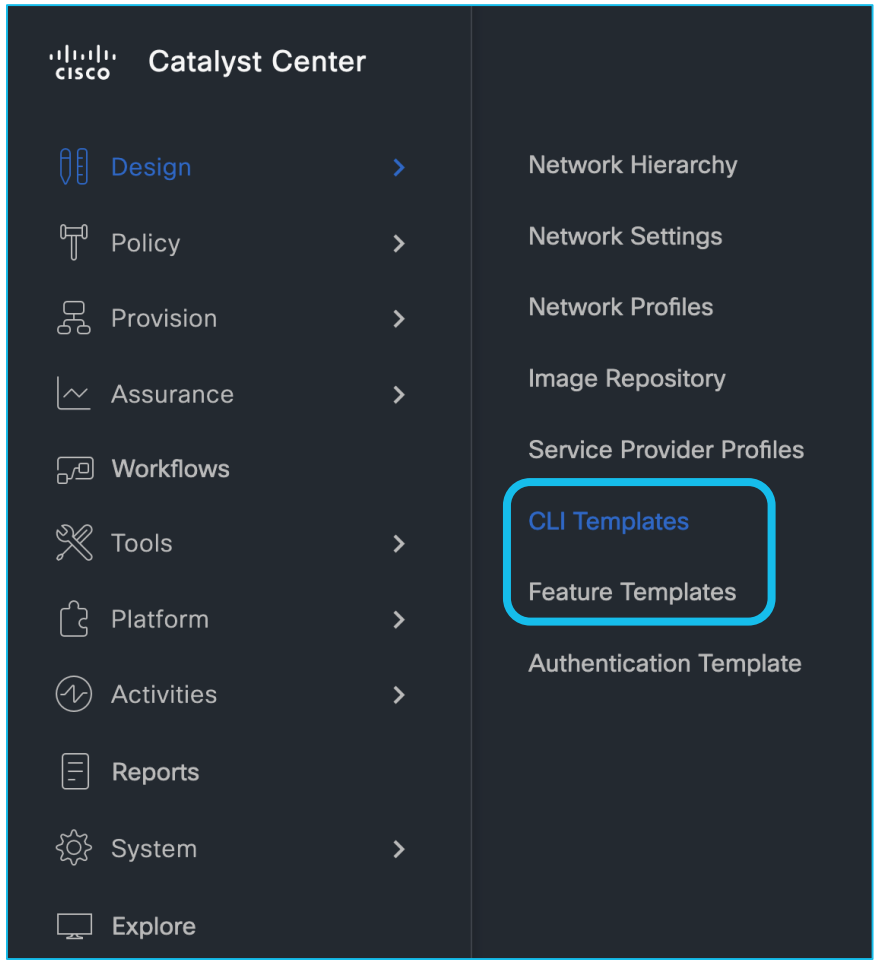


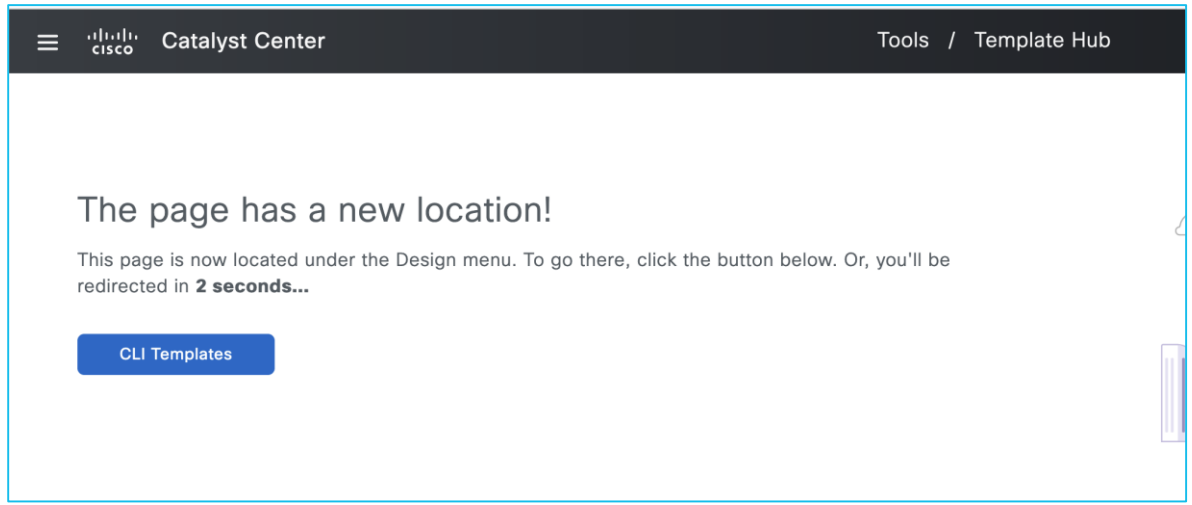




- Shows network profiles using templates
- Attach template to network profile
- Allows selective templates to be directly applied to devices – no need to do full provision (e.g. WLC)

New Location, Same functionality – 2.3.7.4

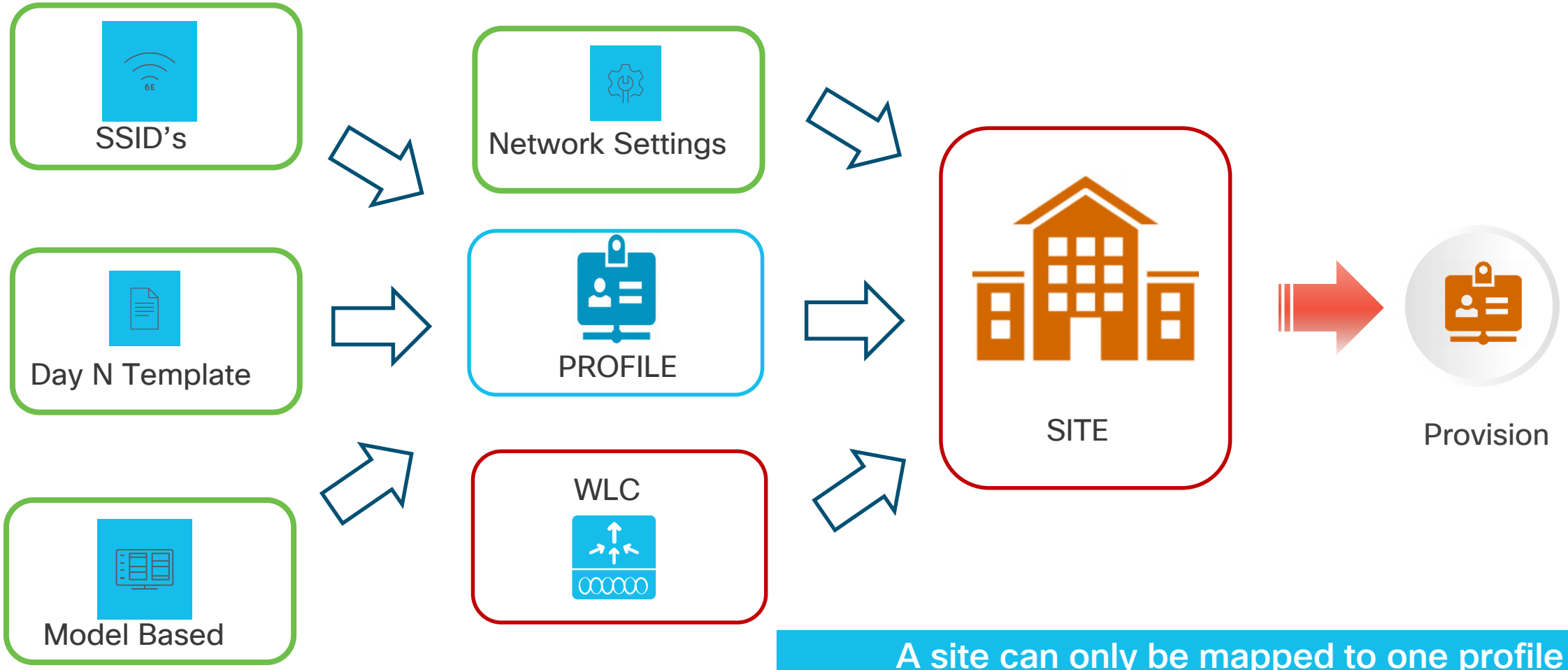




- Moved from tools to design. Old Menu gives a redirect
- "feature templates" also moved (was Model Config Editor)

Intent Based Automation for Wireless Networks

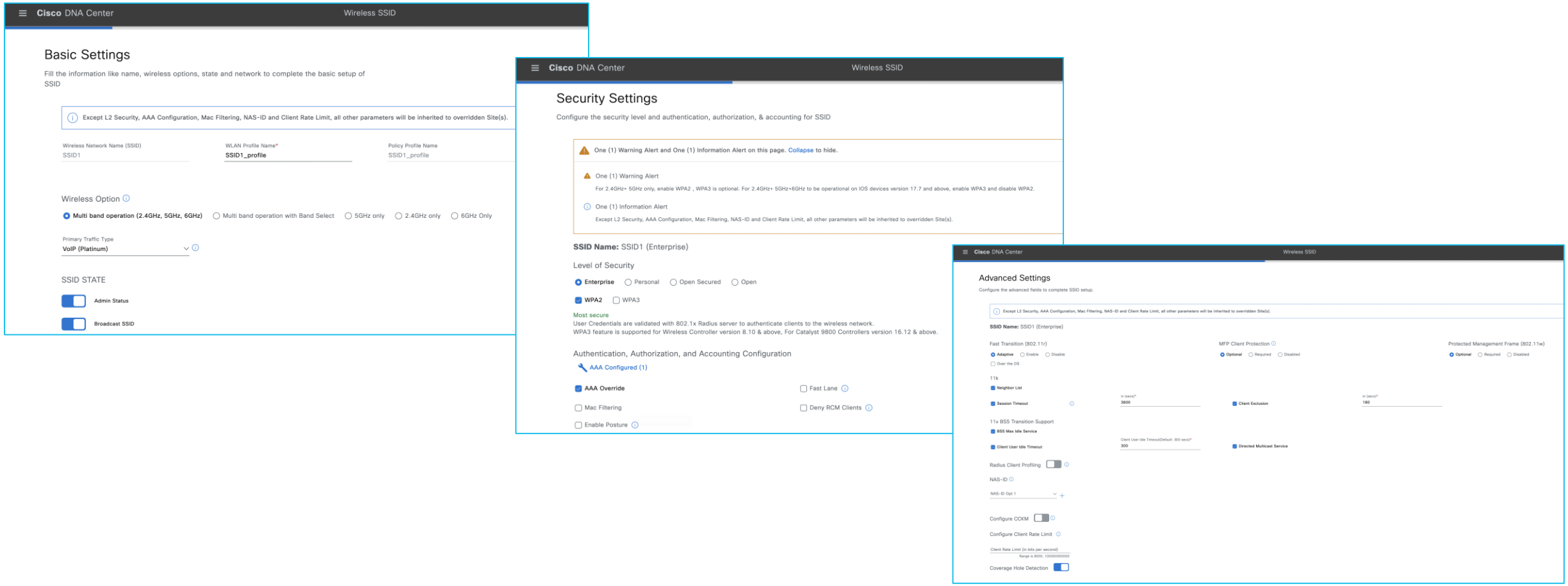
Wireless Provisioning – intent based



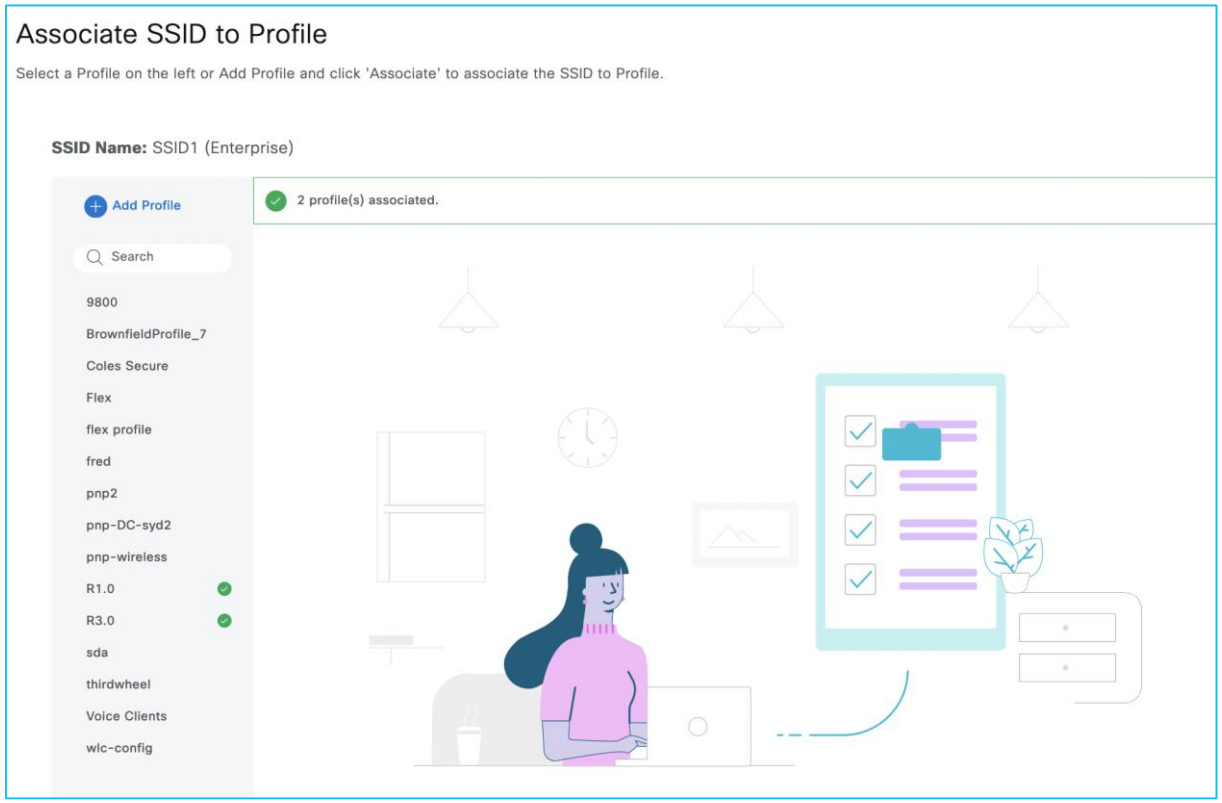
A site can only be mapped to one profile
A profile can contain many sites

Step 1 : SSID Configuration

Design->Network Settings->Wireless

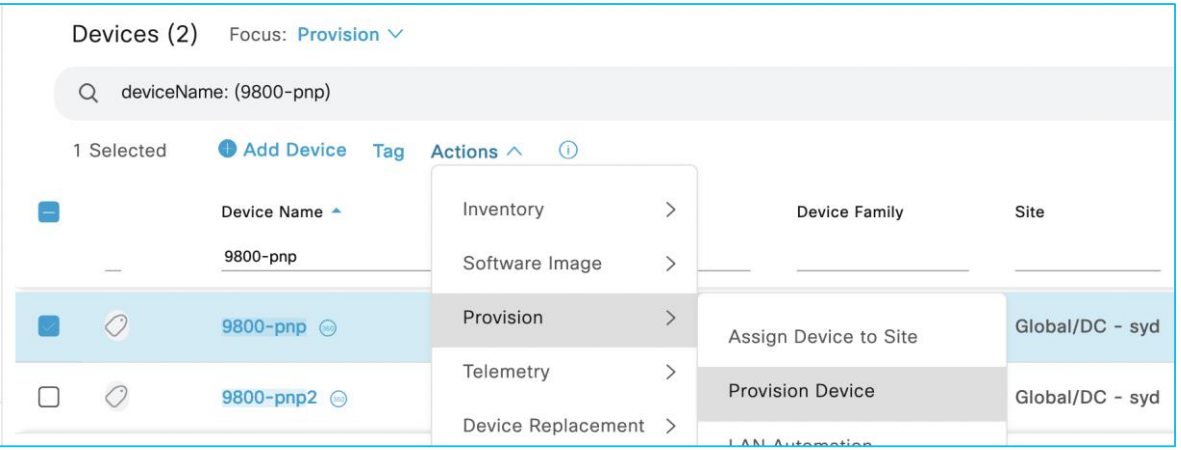


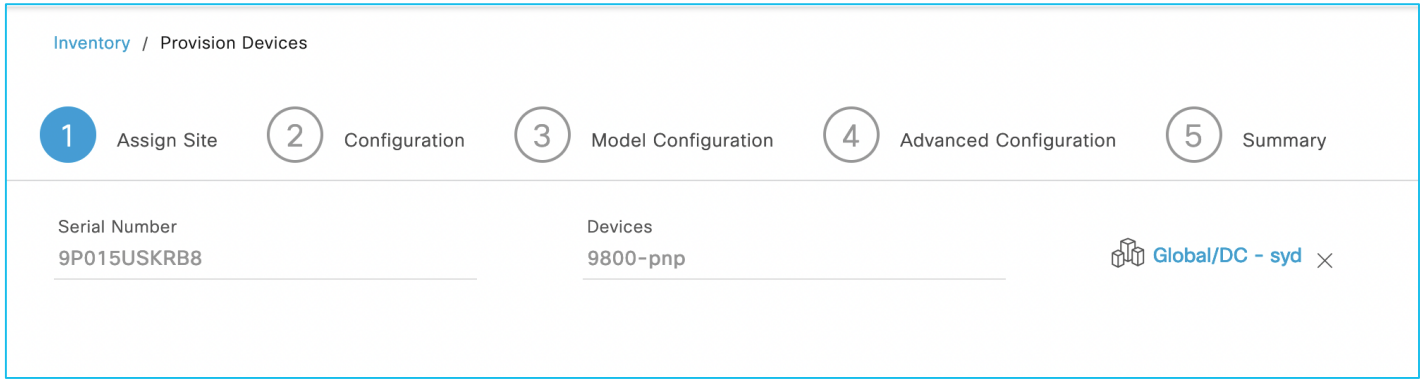
Step 2: Associate to wireless network profile



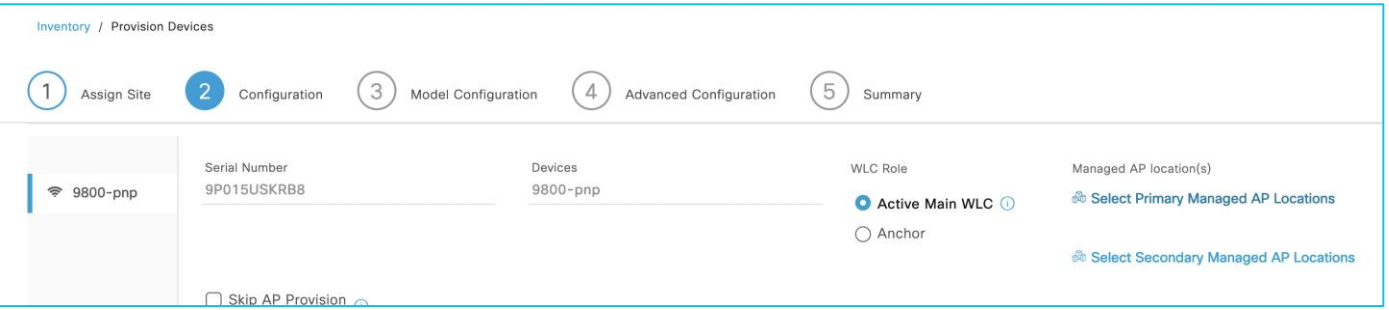
Can then assign a set of sites to the wireless network profile

Provision one WLC

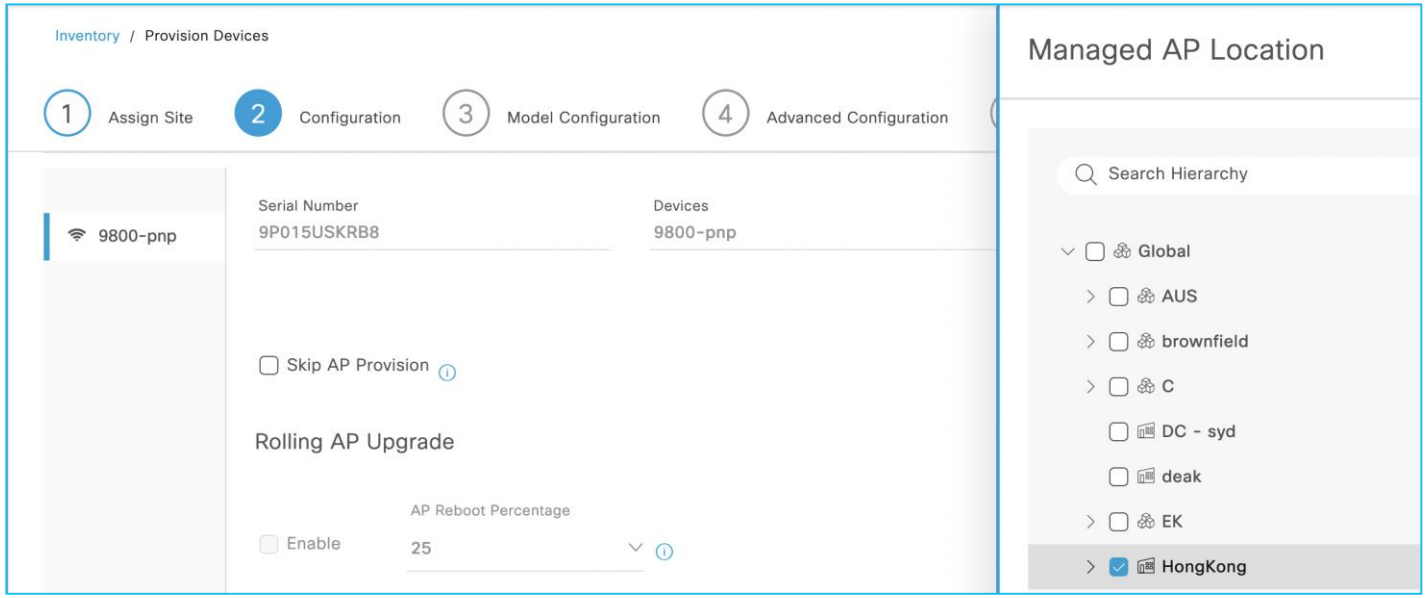




Select managed sites

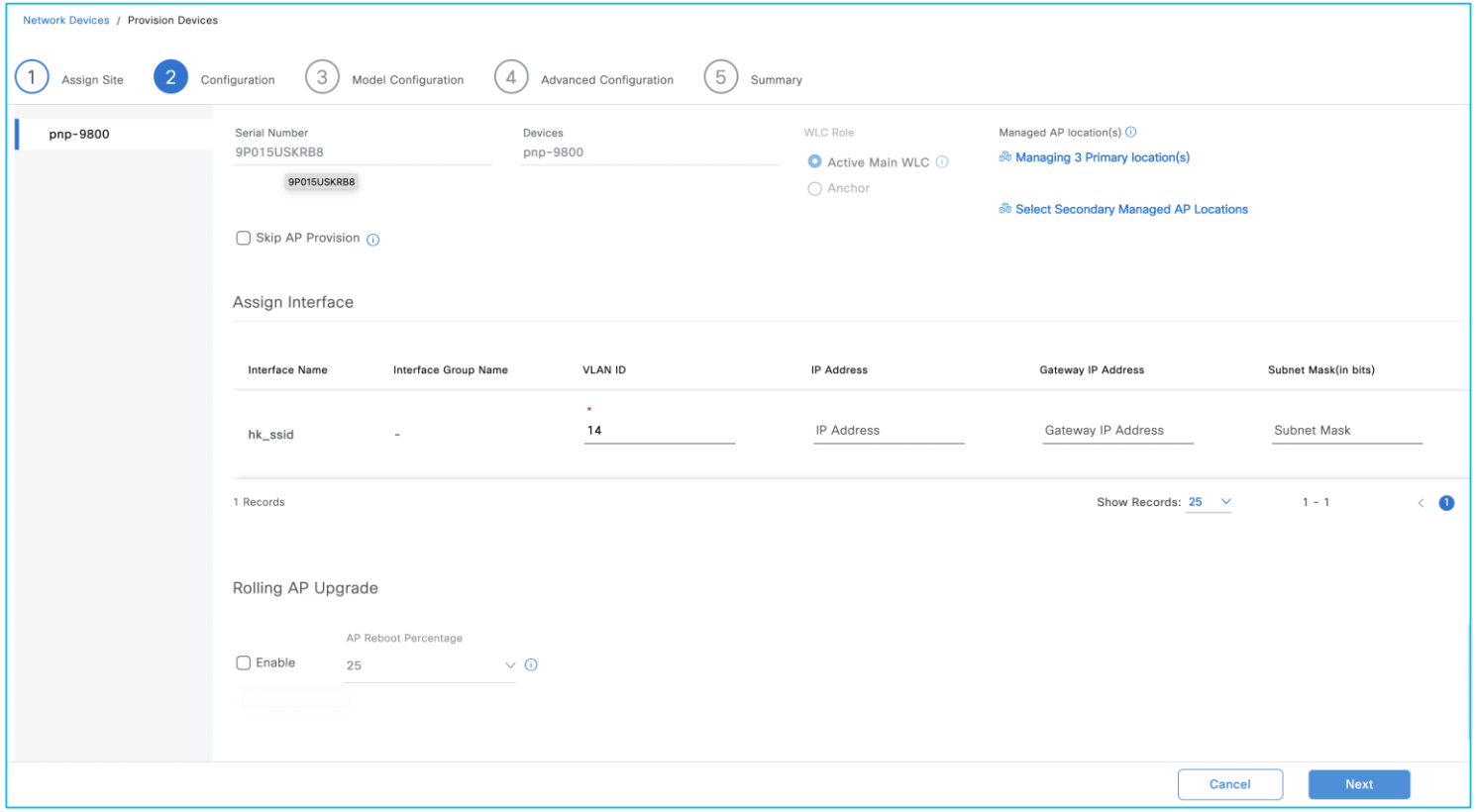


- The sites WLC manages determines the relevant wireless network profiles (WNP)
- Secondary sites are for N+1 config
- AP are assigned to a site -> configuration pushed to AP
- Some commands are disruptive, so option to skip AP provisioning until later

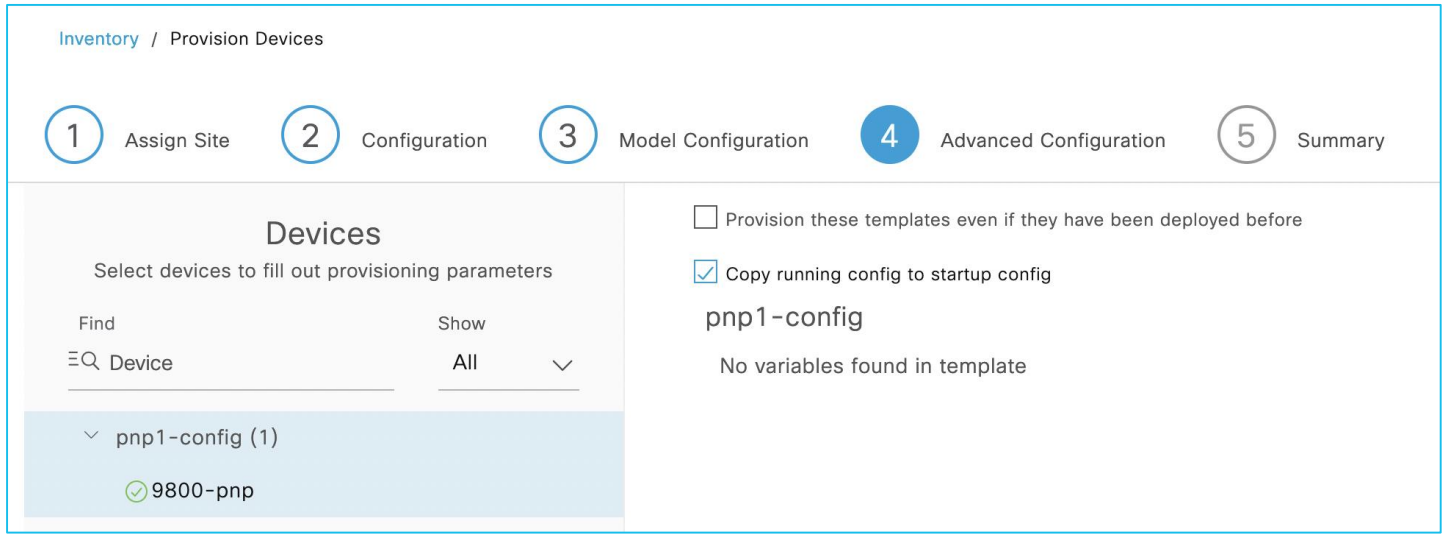


SSID interfaces

L3 configuration is not best practice

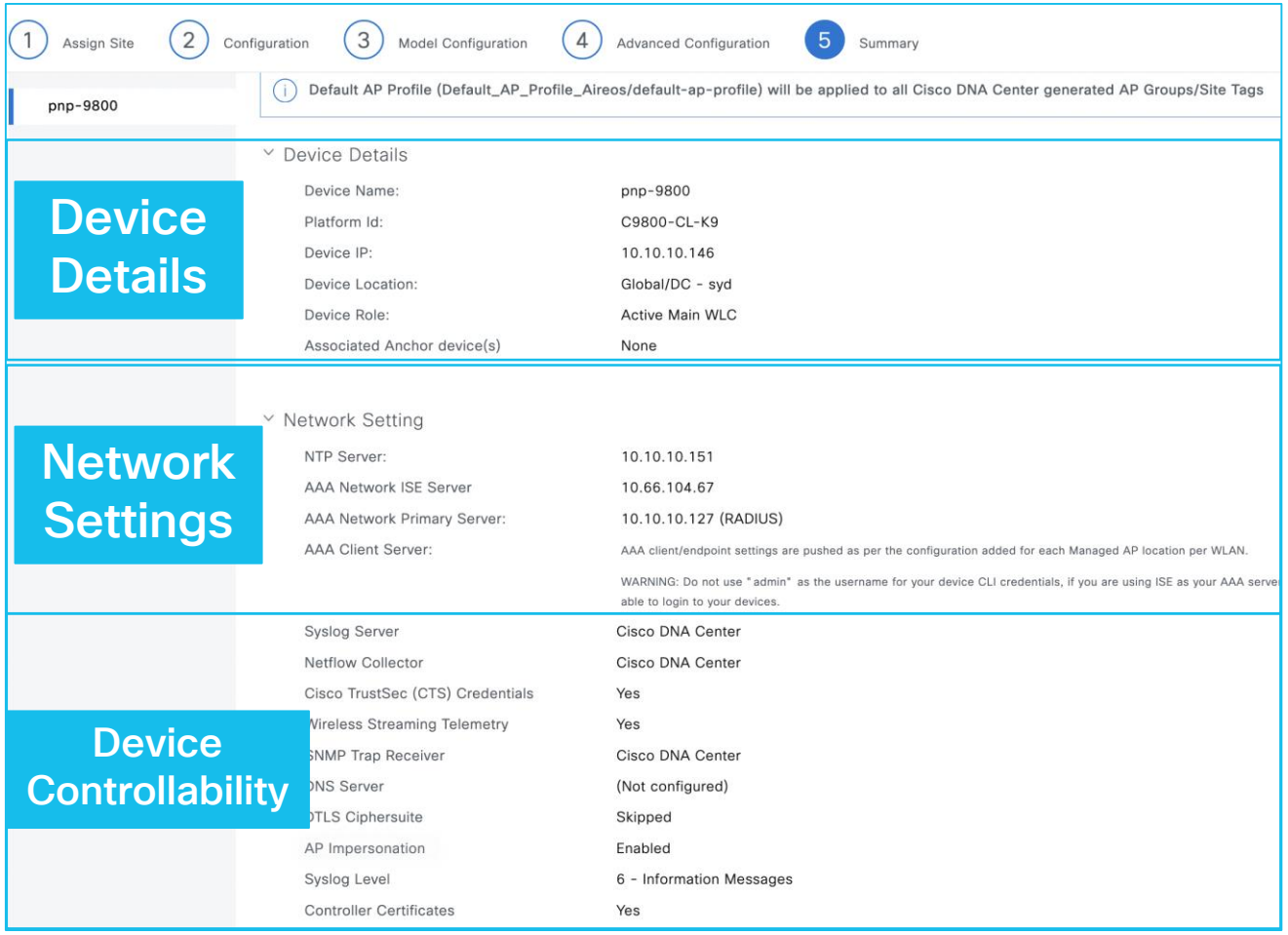


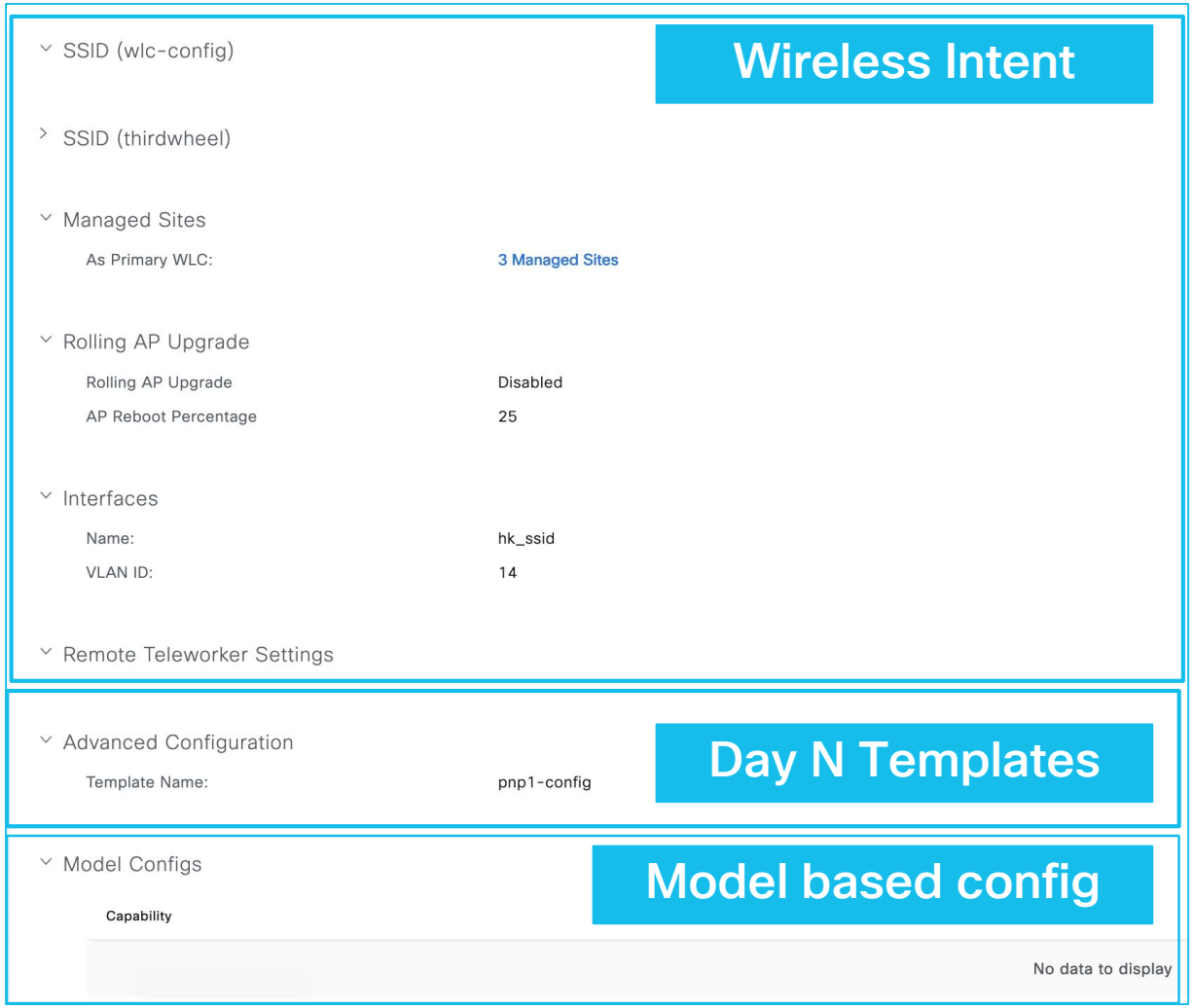
Template




```
# 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
```

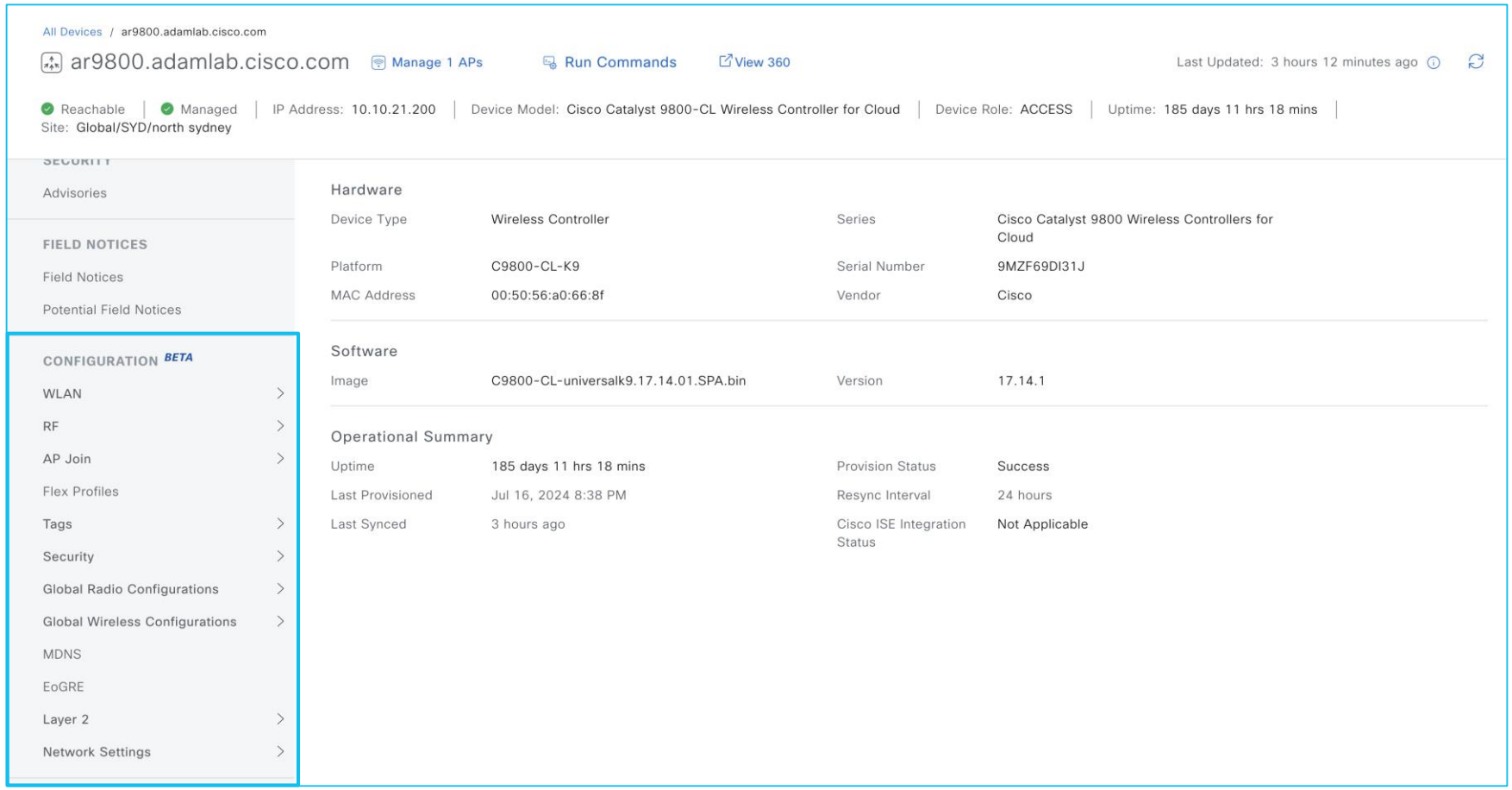
Wireless Provisioning - Summary





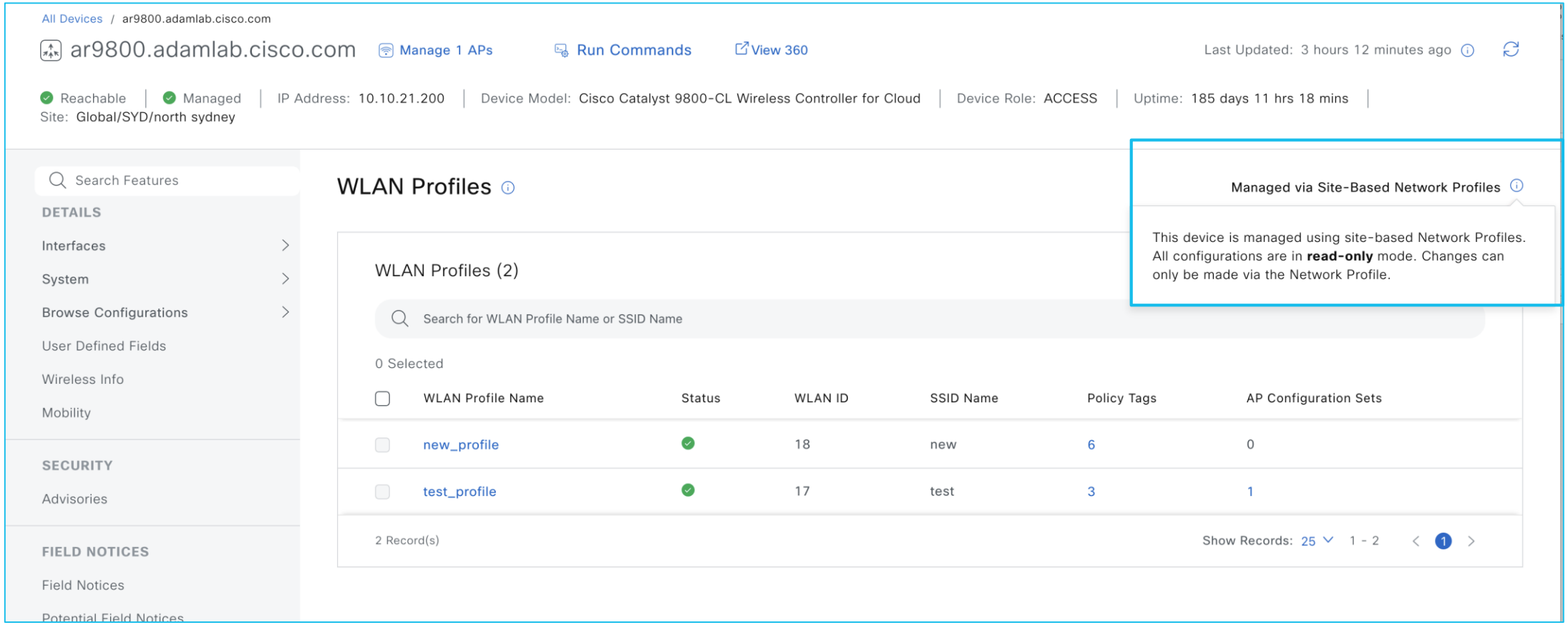
Per-Device Configuration for Wireless

9800 WLC – Per device configuration

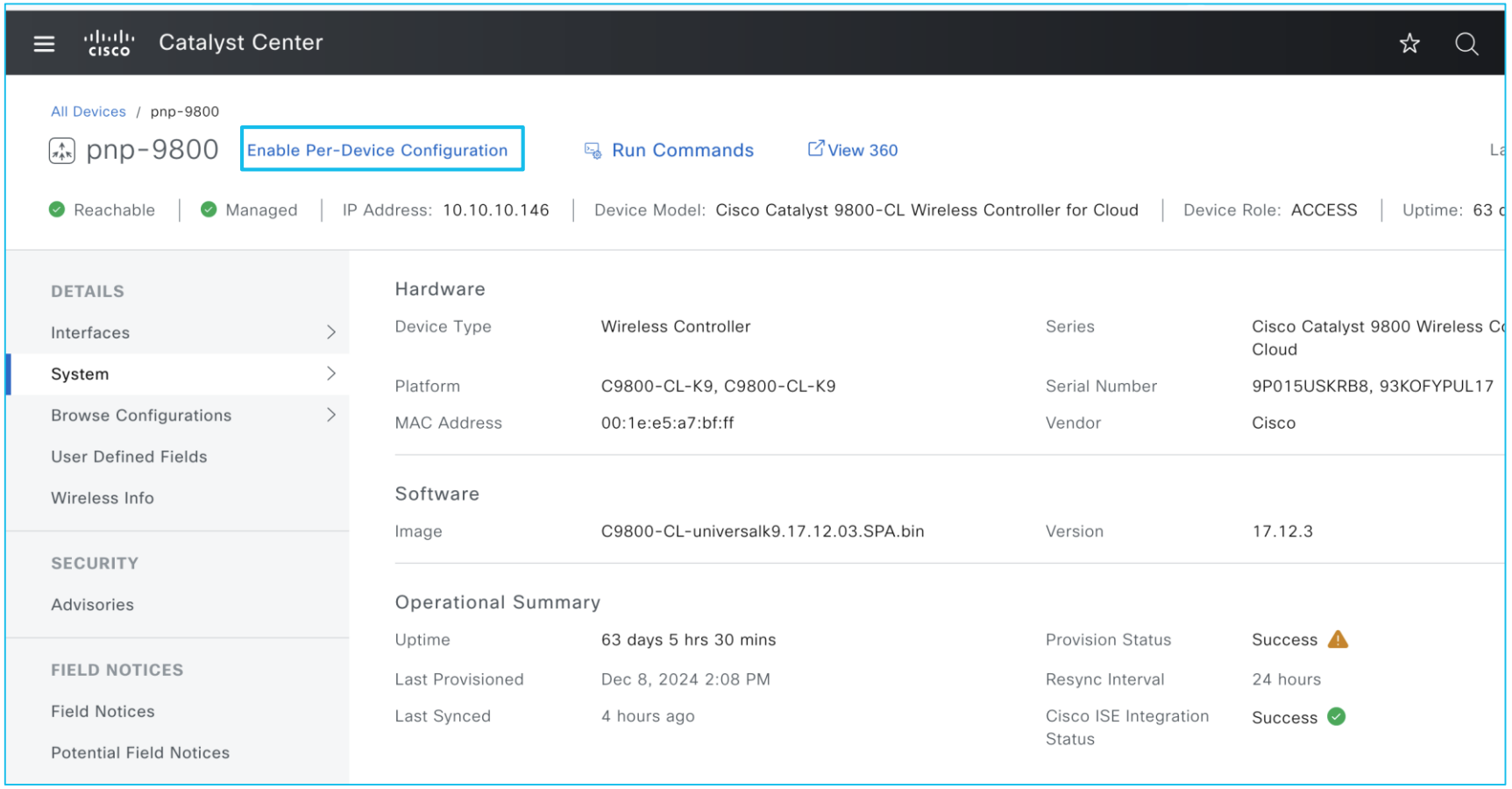


Private Beta: 2.3.7.6
Beta 2.3.7.9

Management choice: **Site-Based** or **Per-device**

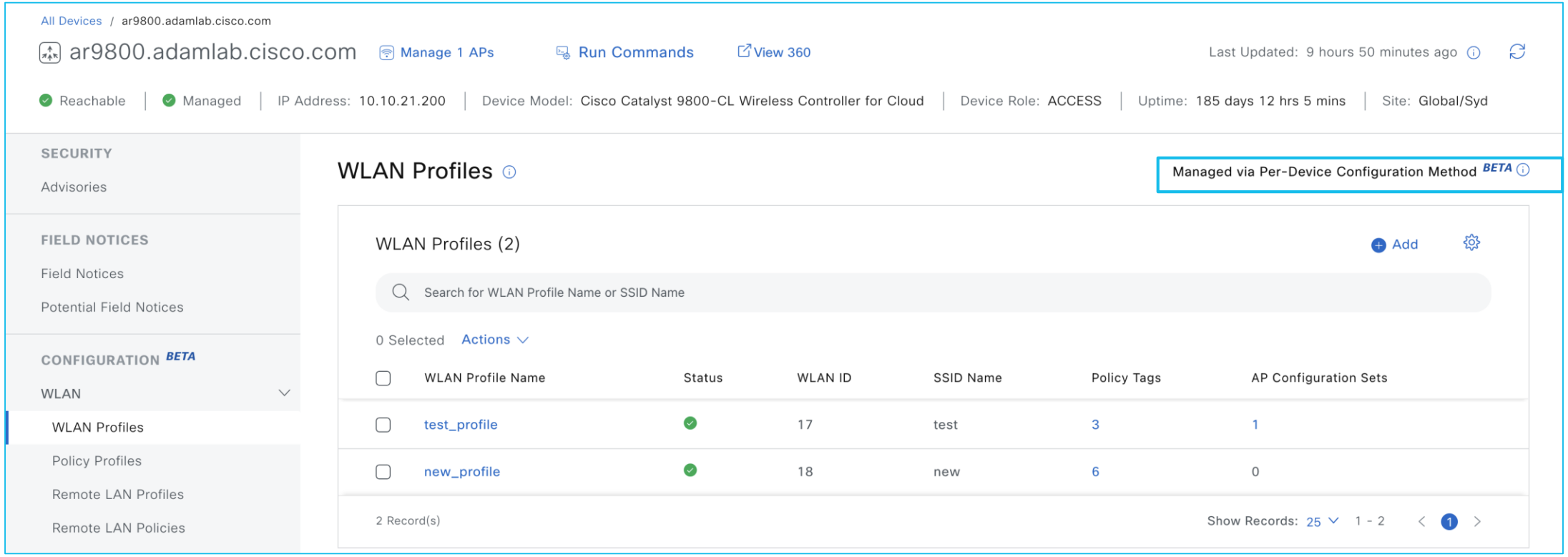


2.3.7.9 – Convert to per-device mode



Only applies if using intent based config

Per-Device configuration mode



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

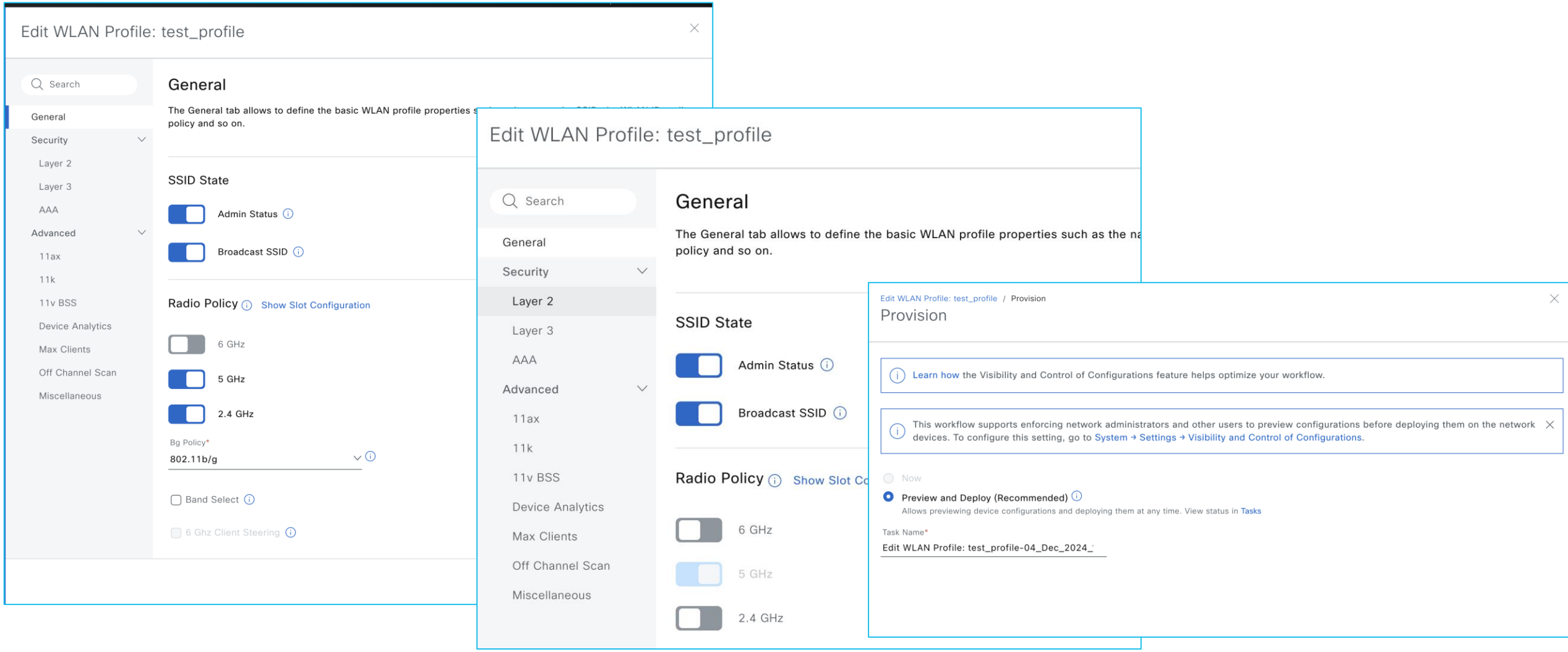
Layer 3
- Routing

Administration
- Device

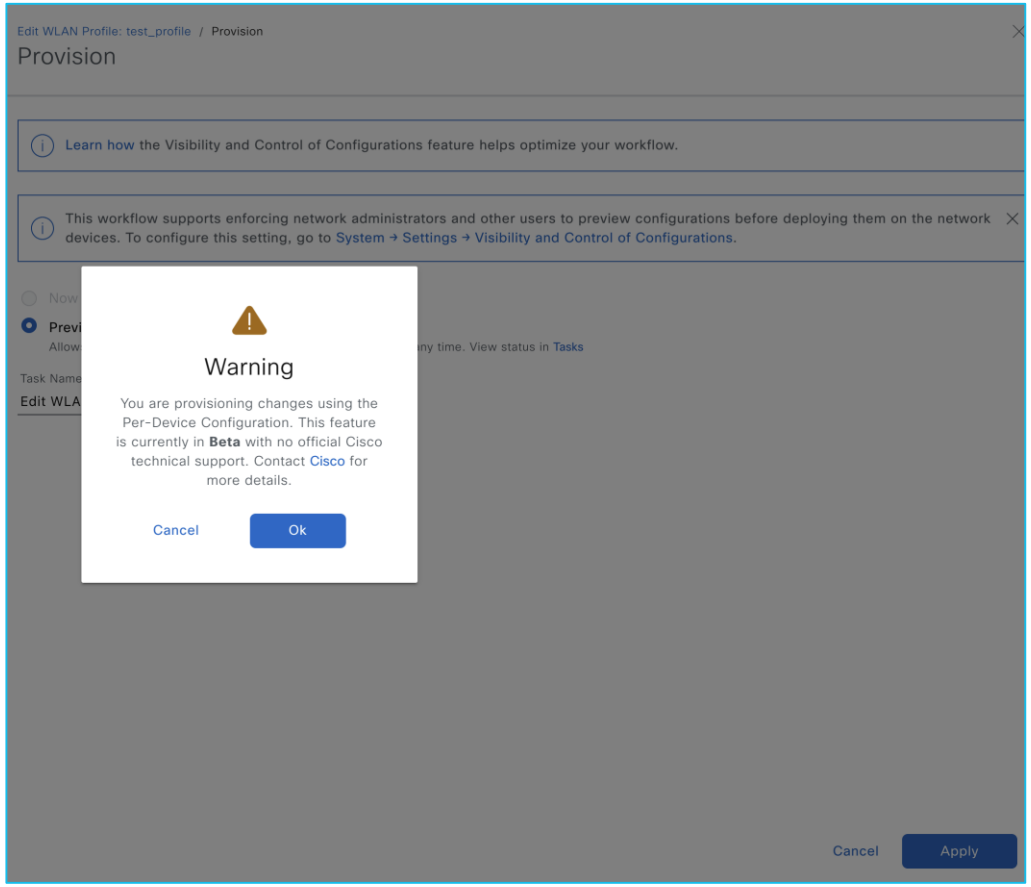
Mobility

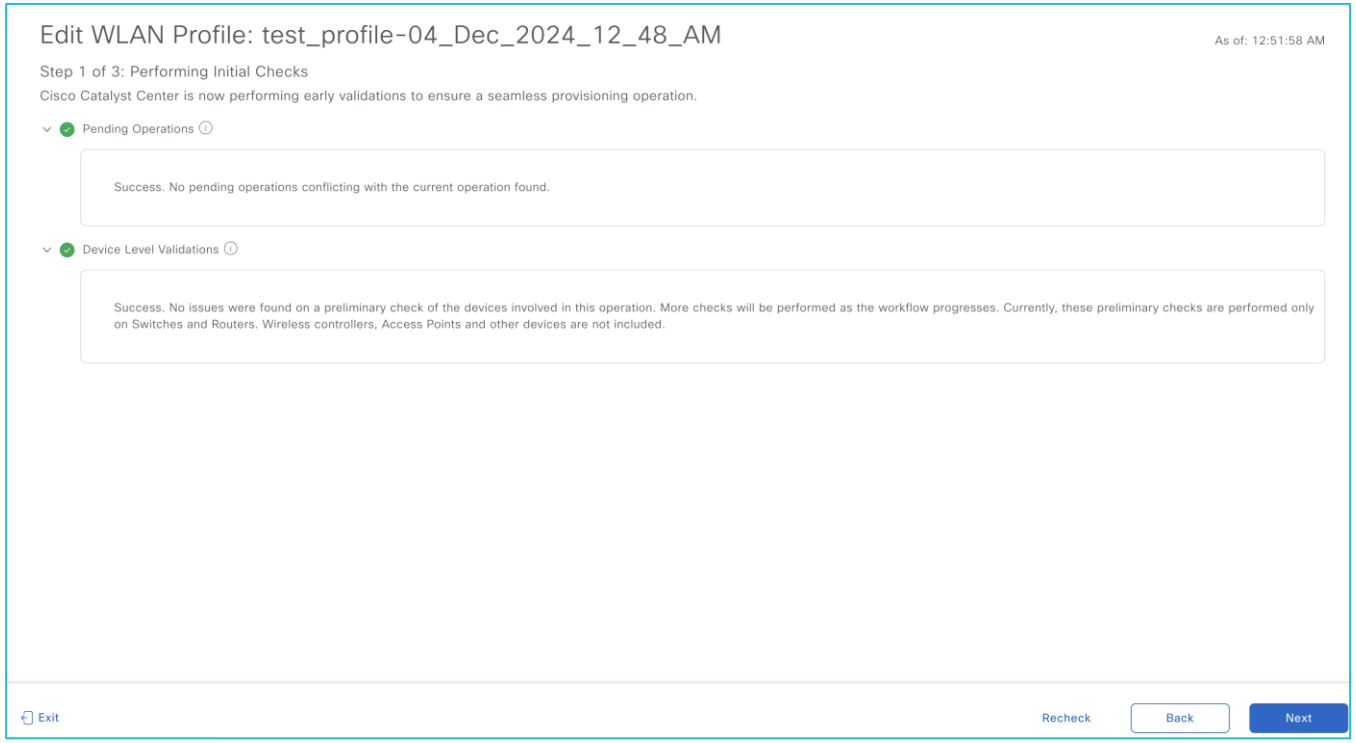
New in 2.3.7.9

Example: Turn off 2.4GHz

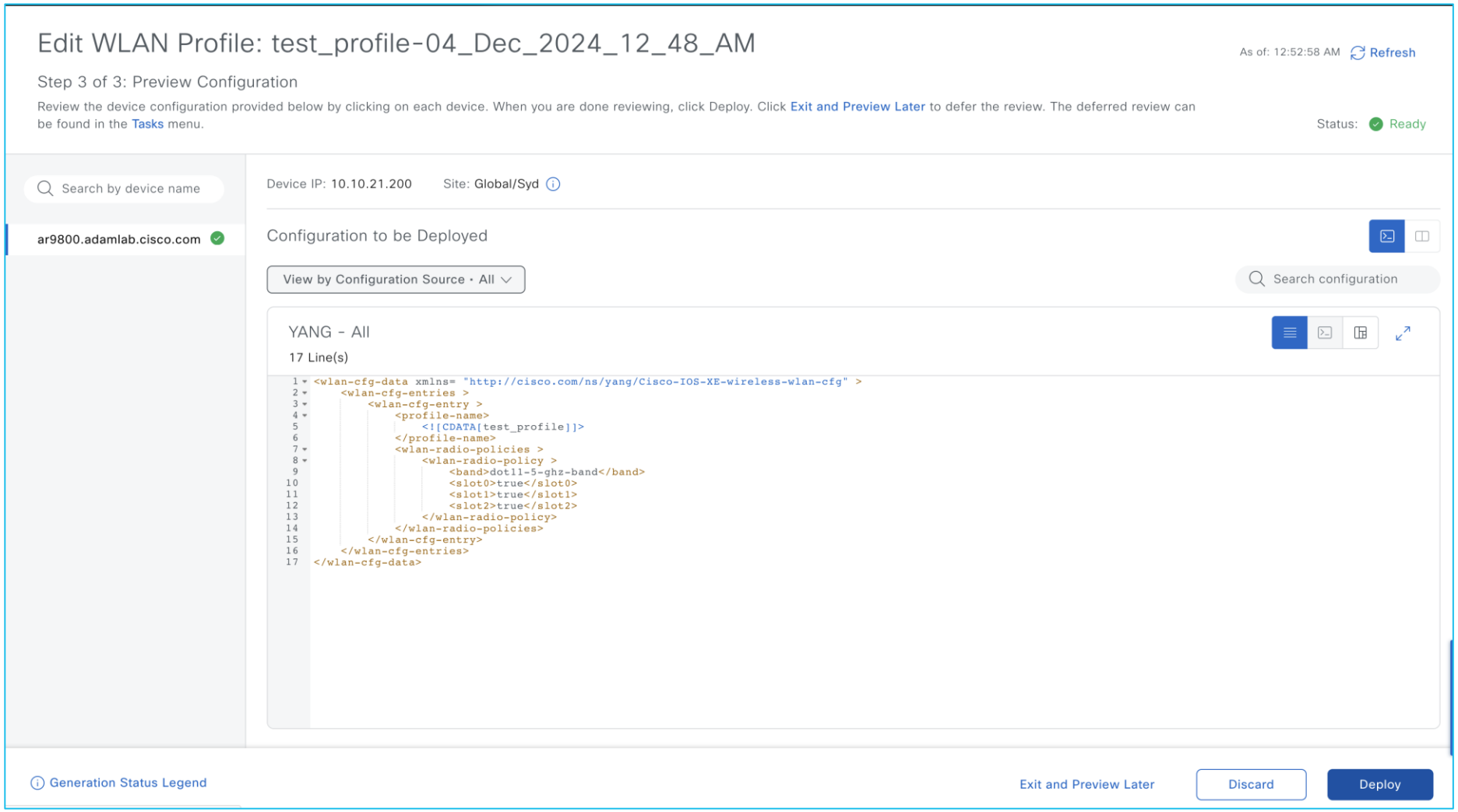


Now in VCR mode

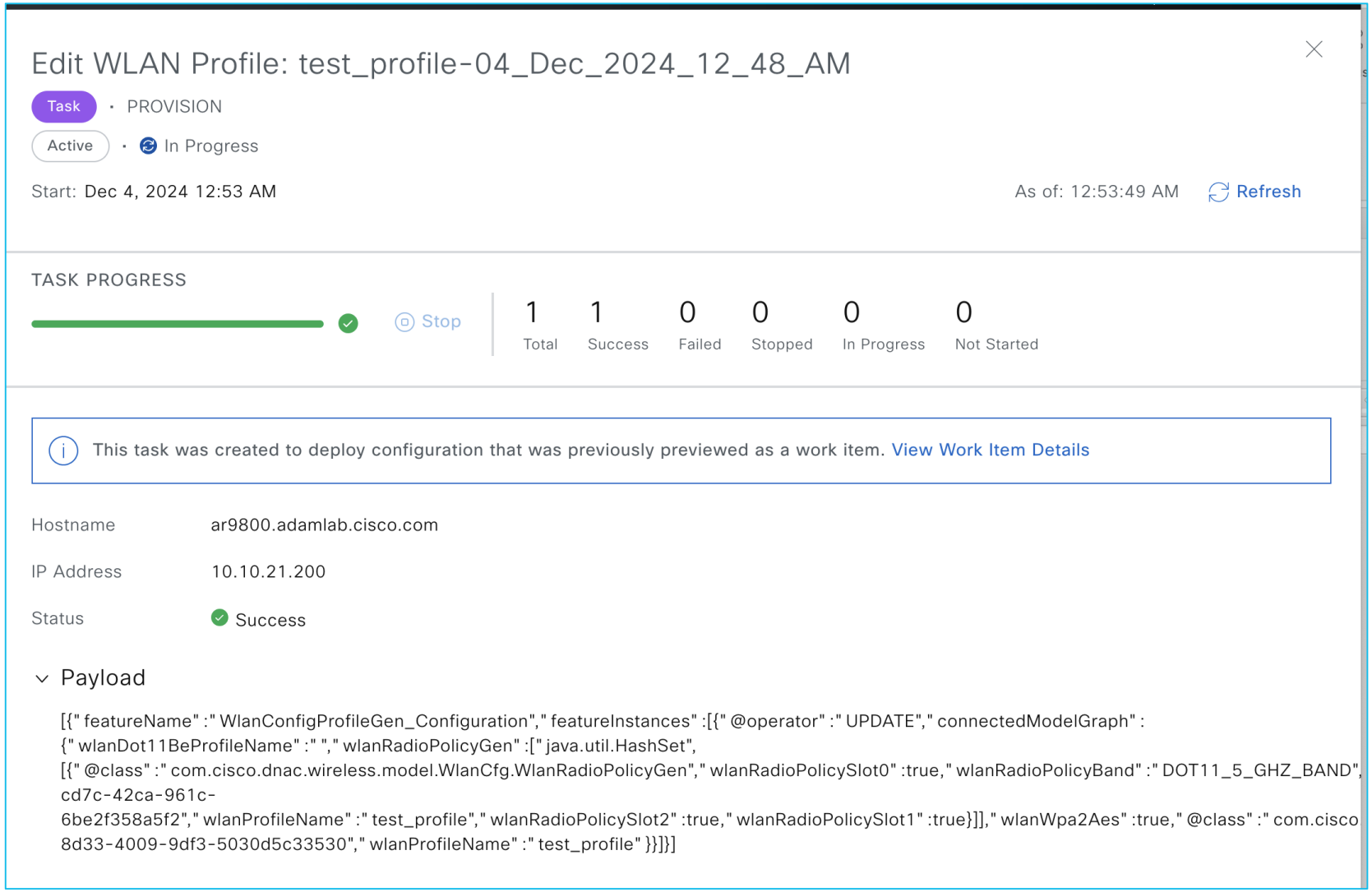




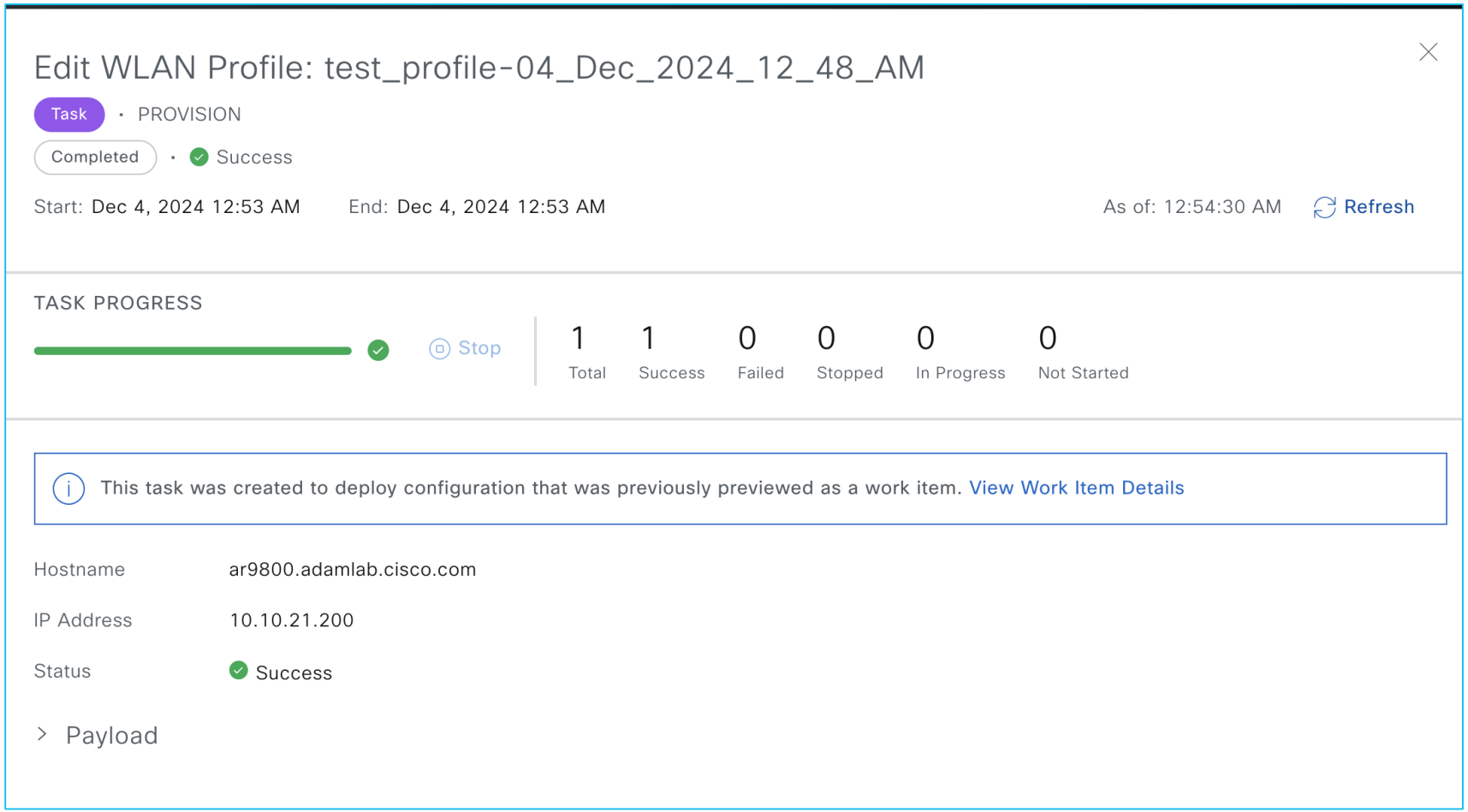
Visibility



Provisioning Task

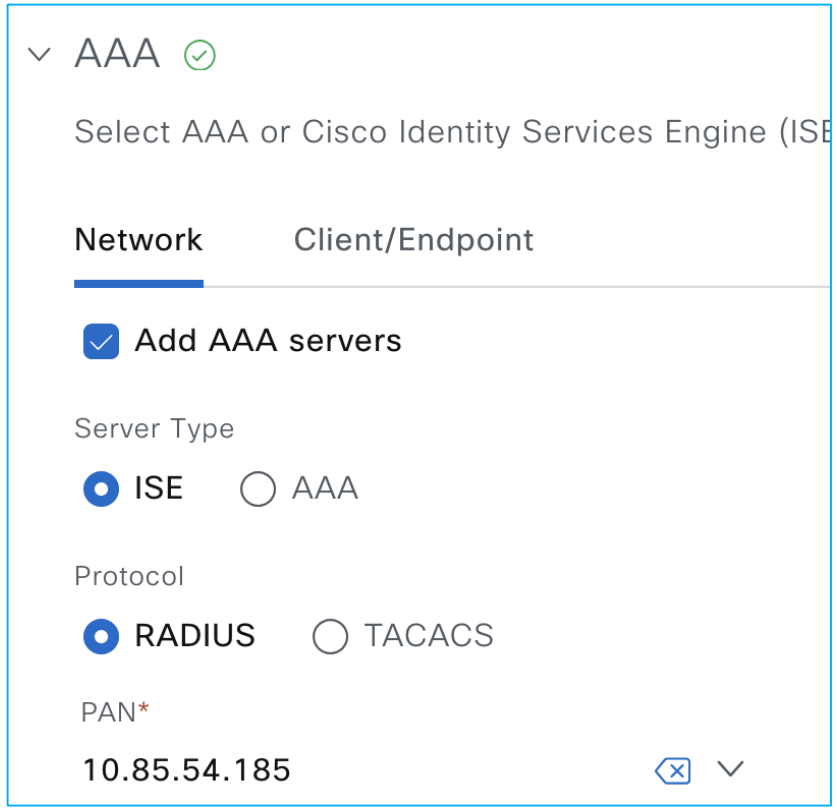


Success

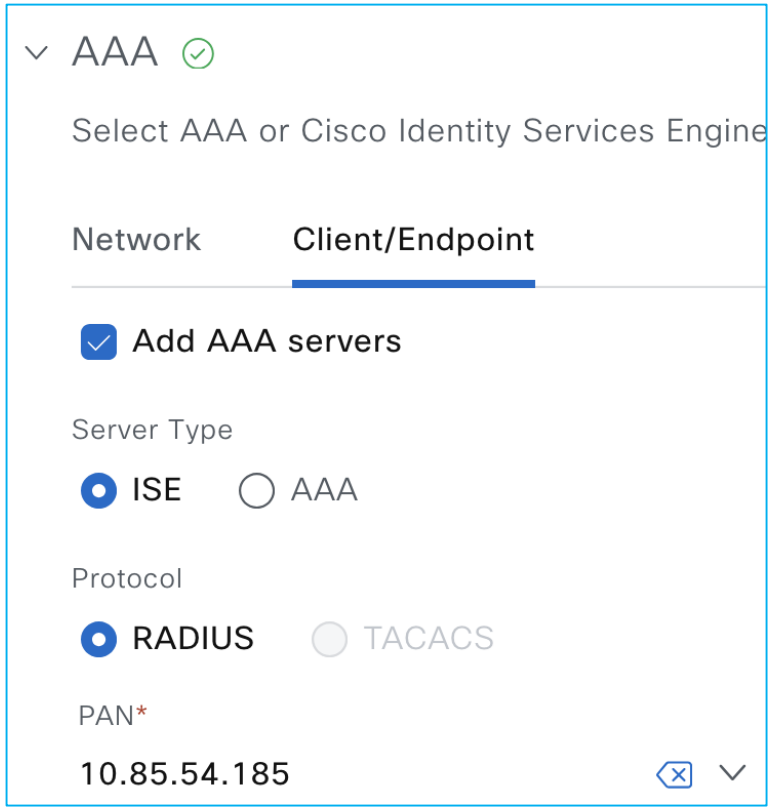


AAA and Management of Credentials

Network Settings: AAA

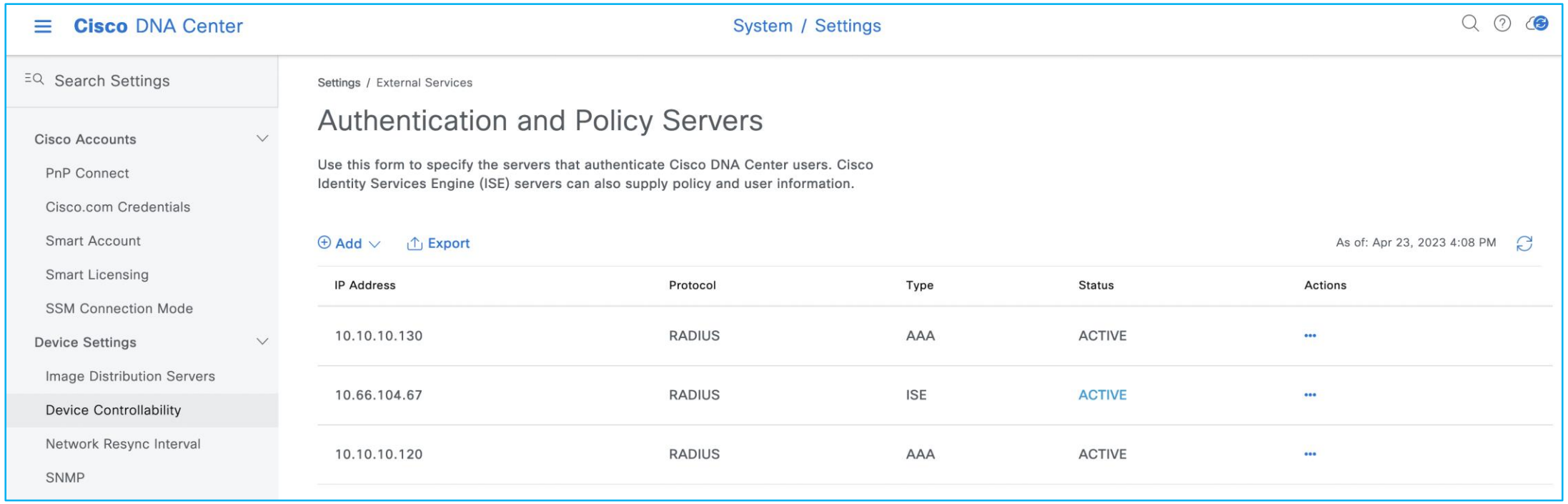


- ISE or other AAA
- RADIUS or TACACS



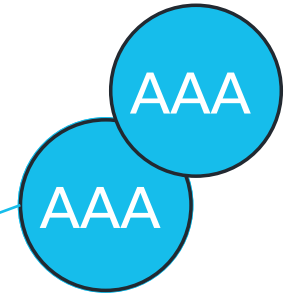
- ISE or other AAA
- RADIUS

ISE and Catalyst Center Integration



- 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

AAA config pushed to devices

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)

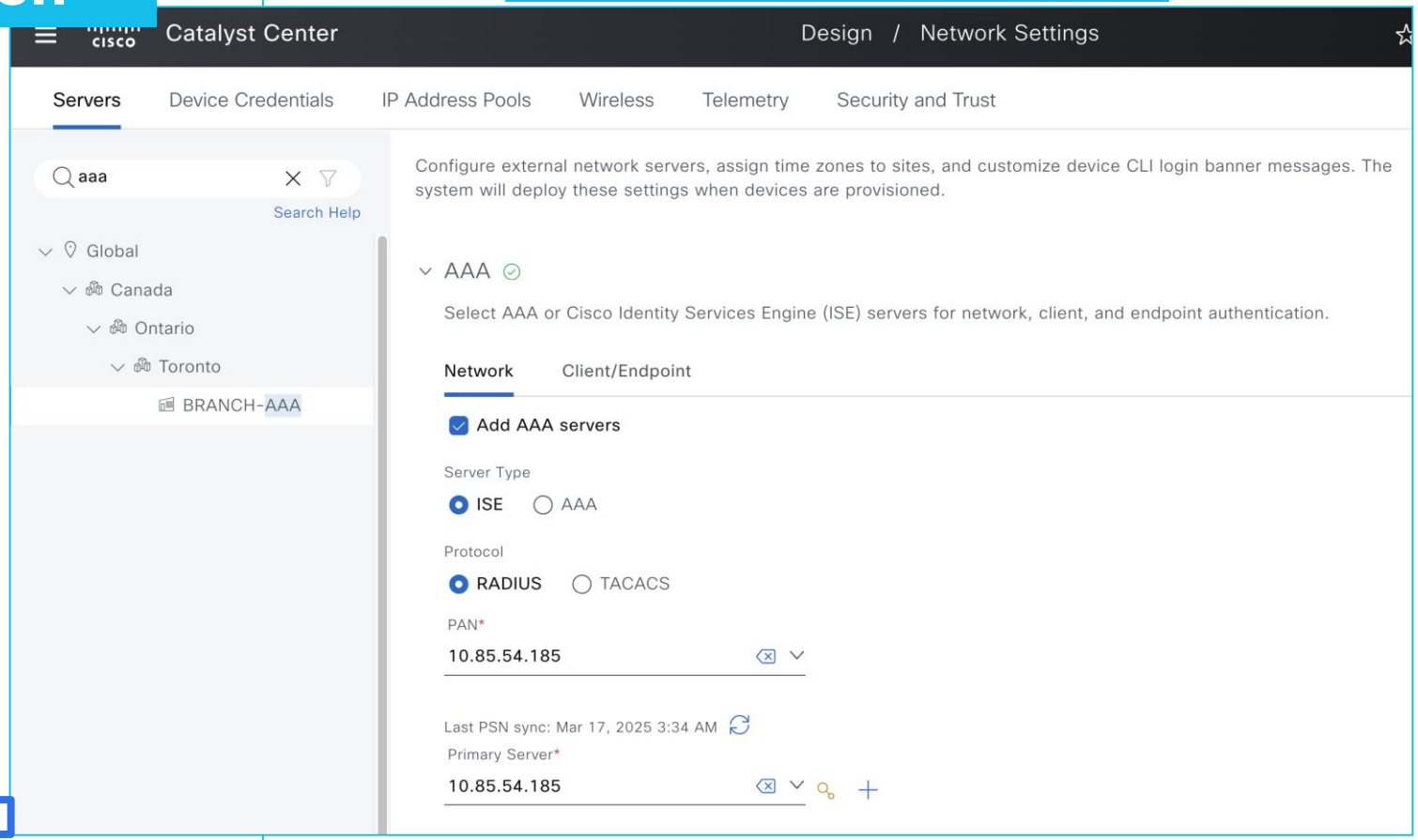
Devices with AAA configured

Provision with Network AAA in Network Settings

Device Configuration before Provision

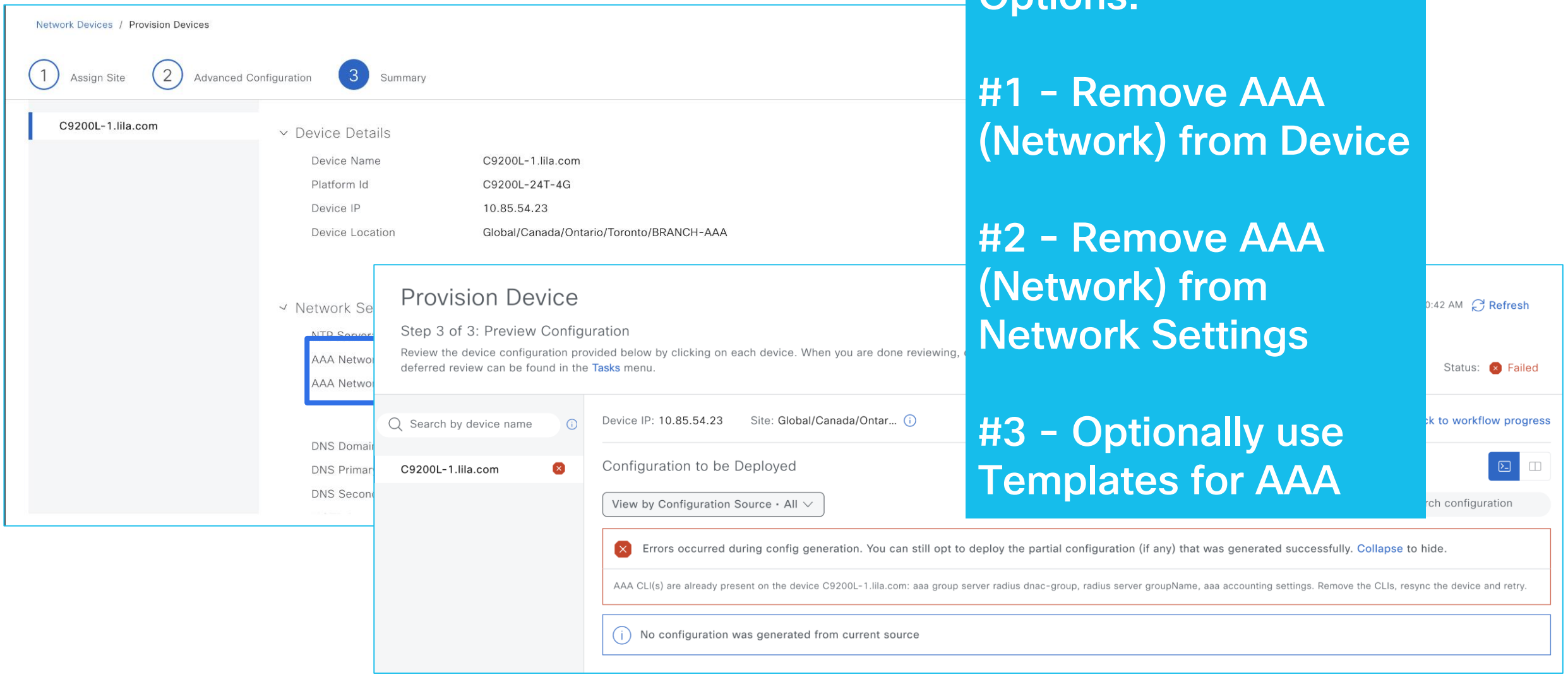
```
C9200L-1#show run
Building configuration...

Current configuration : 34587 byte
!
! 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_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
!
```

Network Settings



Devices with AAA configured

Provision with Network AAA in Network Settings



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

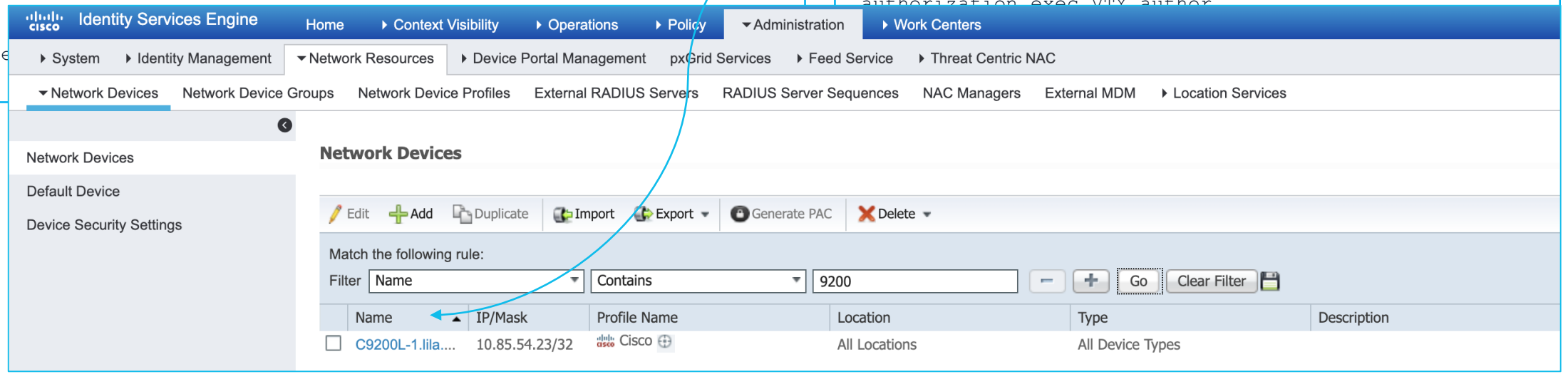
Provision with Network AAA in Network Settings

```
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
                                  d nas-port-detail mac-only
                                  ne 5 tries 3


                                  5.54.185
                                  n-port 1812 acct-port 1813


                                  y ignore-acct-port probe-on
 pac key 7 123A5404110428ZA0B6A
!
line vty 0 4
 authorization exec VTY_author
 login authentication VTY_authen
line vty 5 15
 authorization exec VTY_author
```

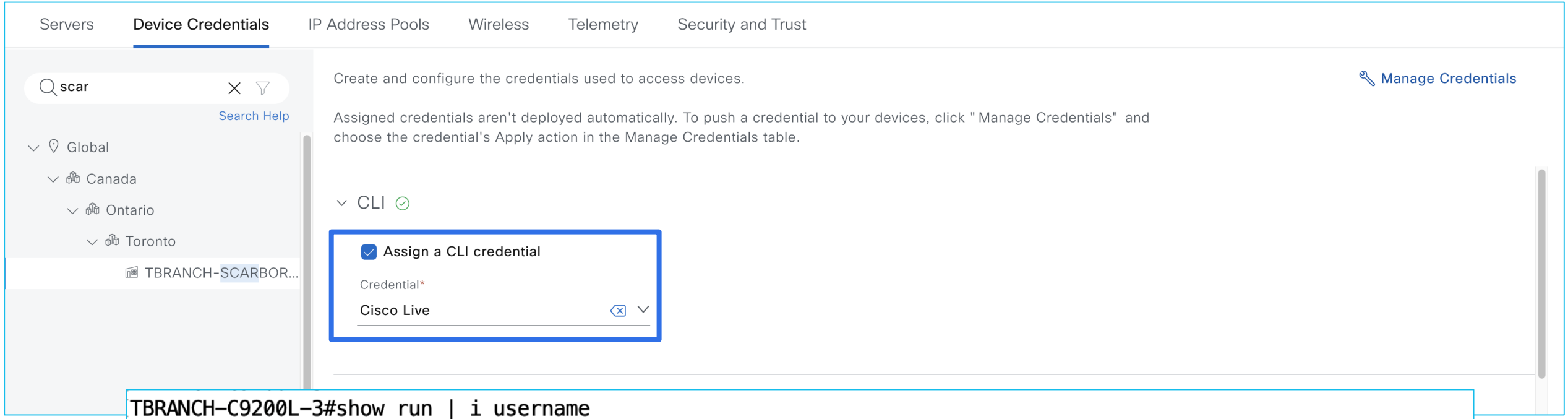
Sample AAA config sent to device

Device added in ISE

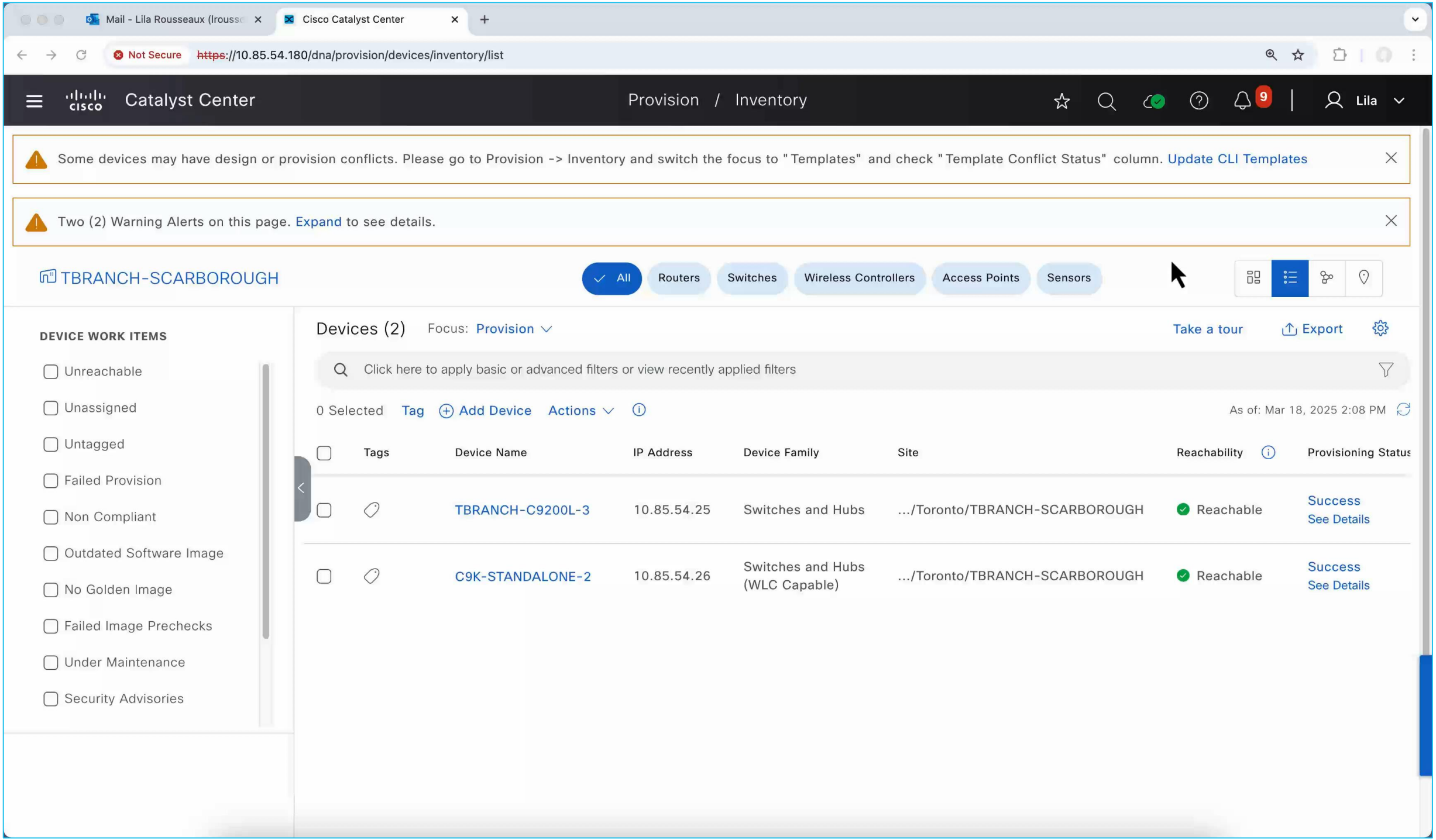


Devices with local credentials

Changing local credential passwords



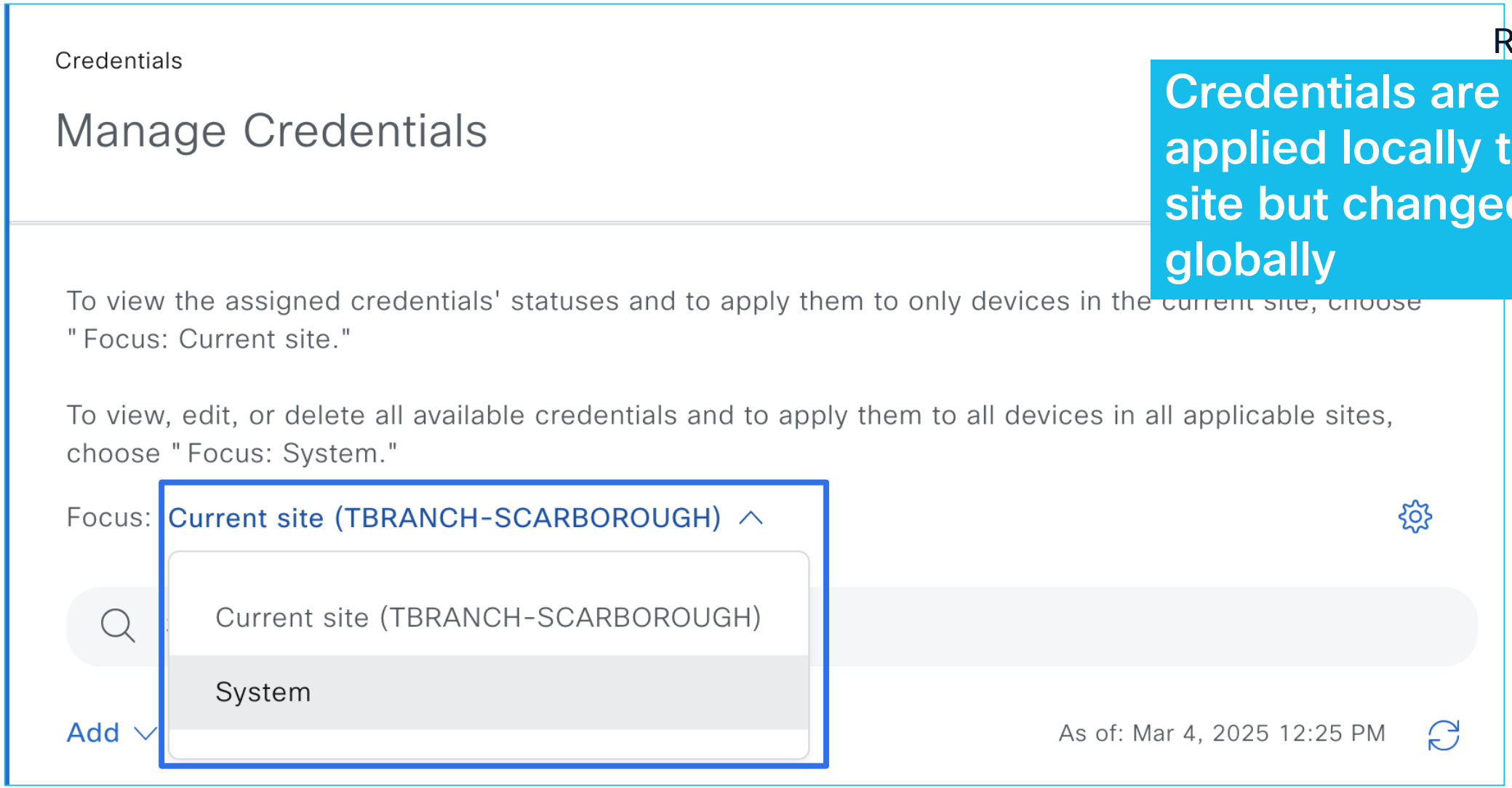

```
TBRANCH-C9200L-3#show run | i username
username netadmin privilege 15 password 7 04785A150C2E68602858
username ciscolive privilege 15 secret 8 $8$MHEMy6OT0Qp.fk$eQBNEVYBCW7umuAarXnNbxDnyhZrk4o2ORVYyQEFG.A
username lila privilege 15 secret 8 $8$YZ4SK4Hb4X9dmk$.Fi1.LkfwxF.YdjvLytRJ8R8V.jfN1aWuCaE9a0jTt6
```


Mail - Lila Rousseaux (lrousse
Cisco Catalyst Center
Not Secure
https://10.85.54.180/dna/provision/devices/inventory/list
Catalyst Center
Provision / Inventory
9
Lila
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
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
TBRANCH-C9200L-3
10.85.54.25
Switches and Hubs
.../Toronto/TBRANCH-SCARBOROUGH
Reachable
Success
See Details
C9K-STANDALONE-2
10.85.54.26
Switches and Hubs (WLC Capable)
.../Toronto/TBRANCH-SCARBOROUGH
Reachable
Success
See Details

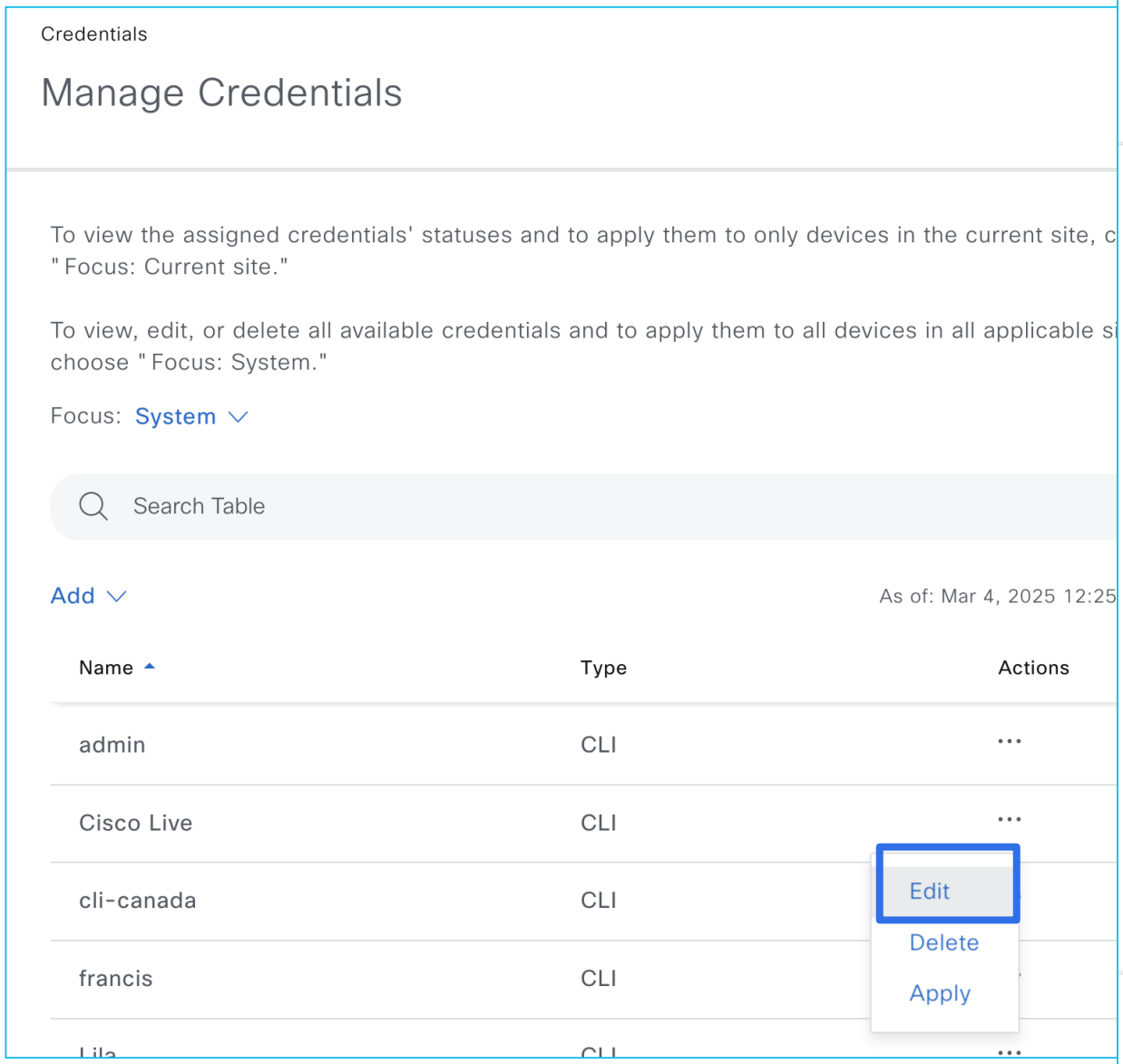
Changing local credential passwords

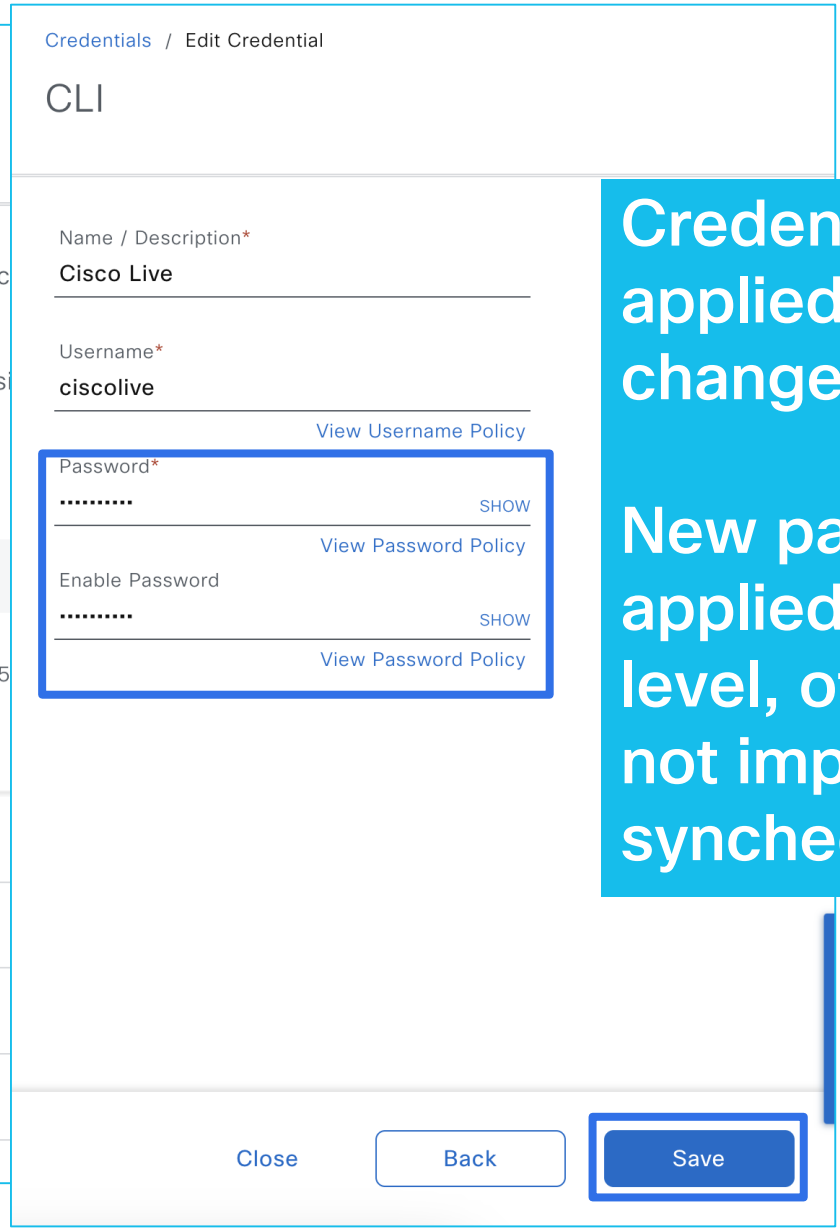
Reference

Credentials are applied locally to the site but changed globally



Changing local credential passwords



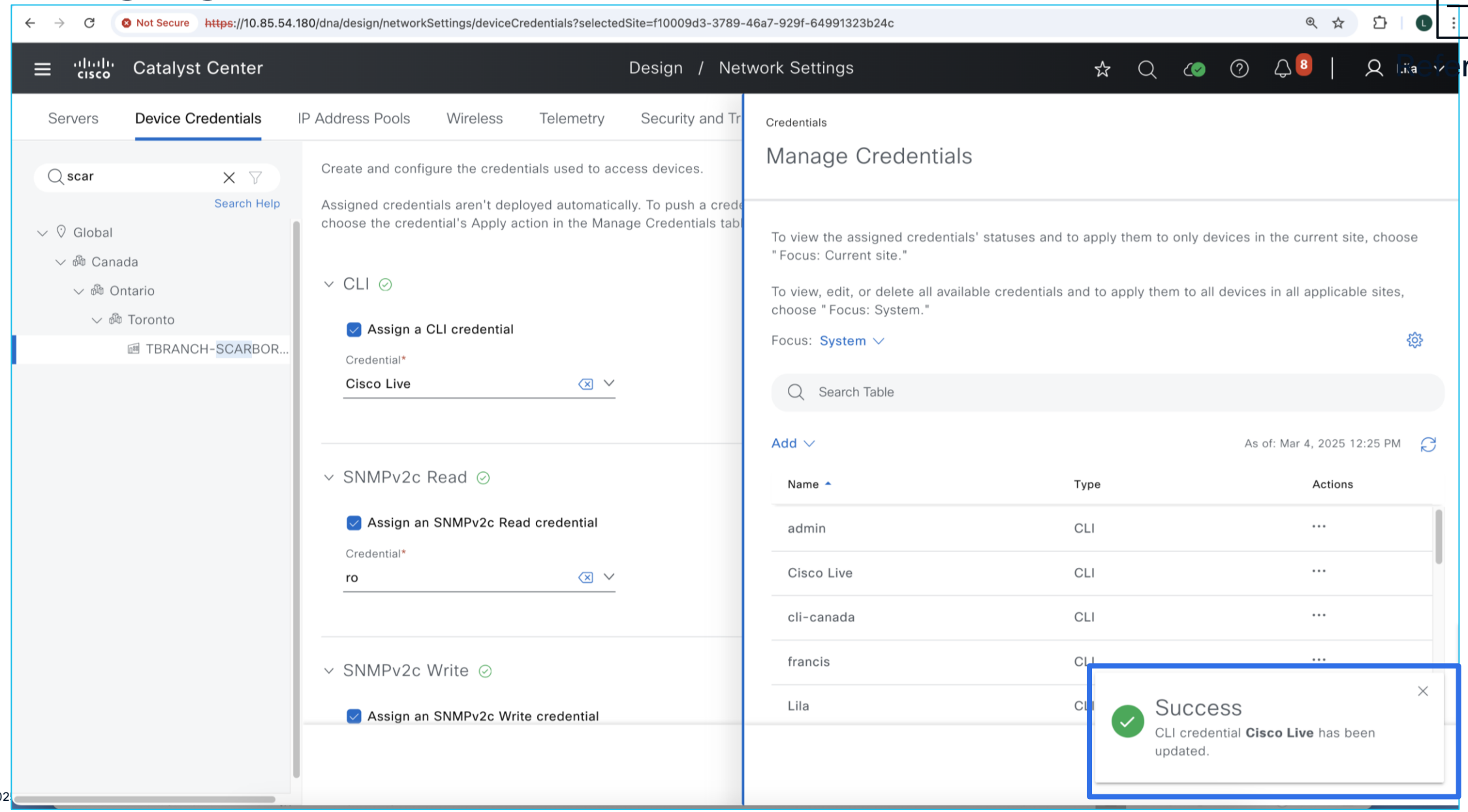


Reference

Credentials are applied locally but changed globally

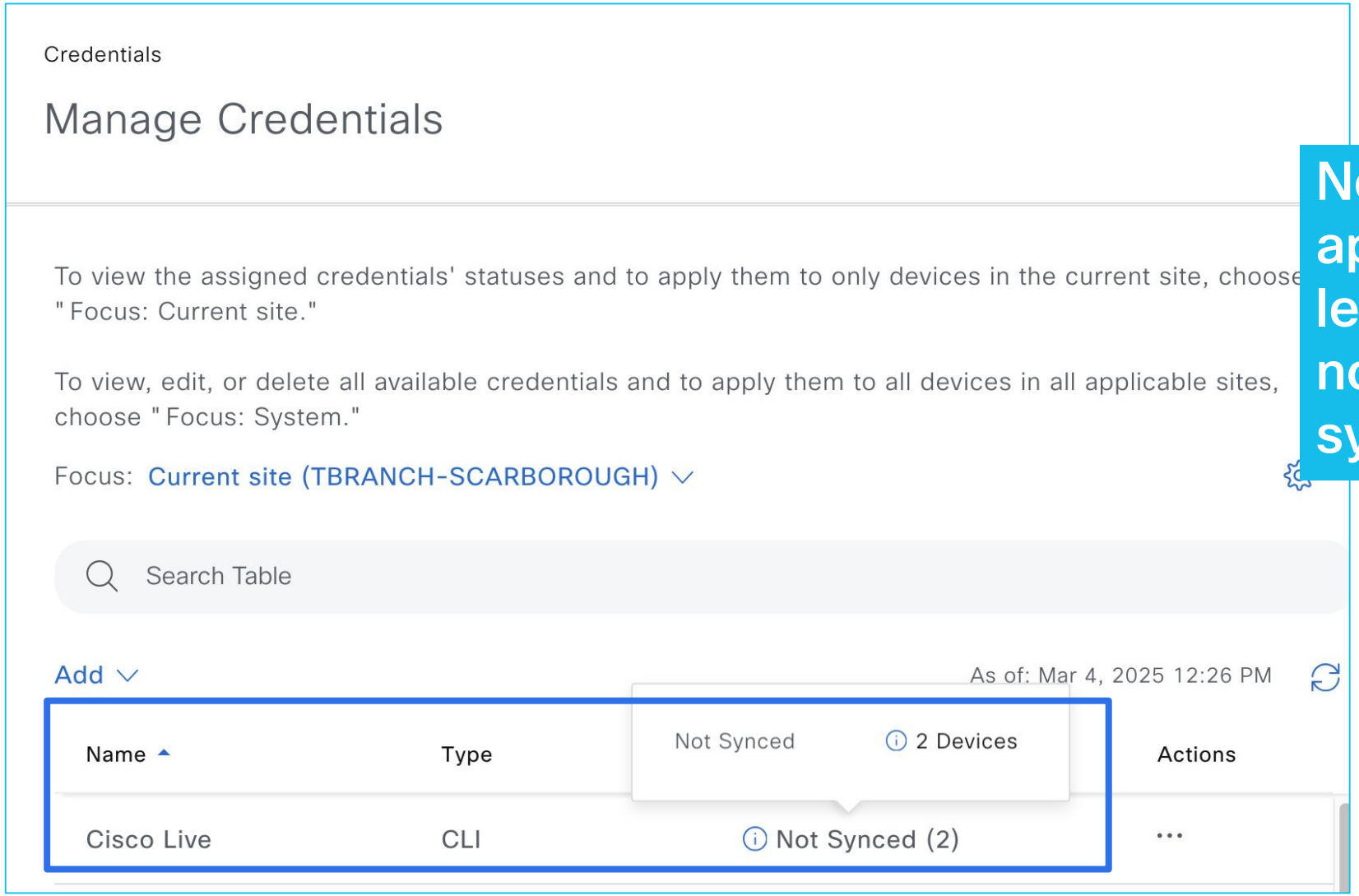
New password applied at the site level, other sites not impacted until synched

Changing local credential passwords



Changing local credential passwords

Reference

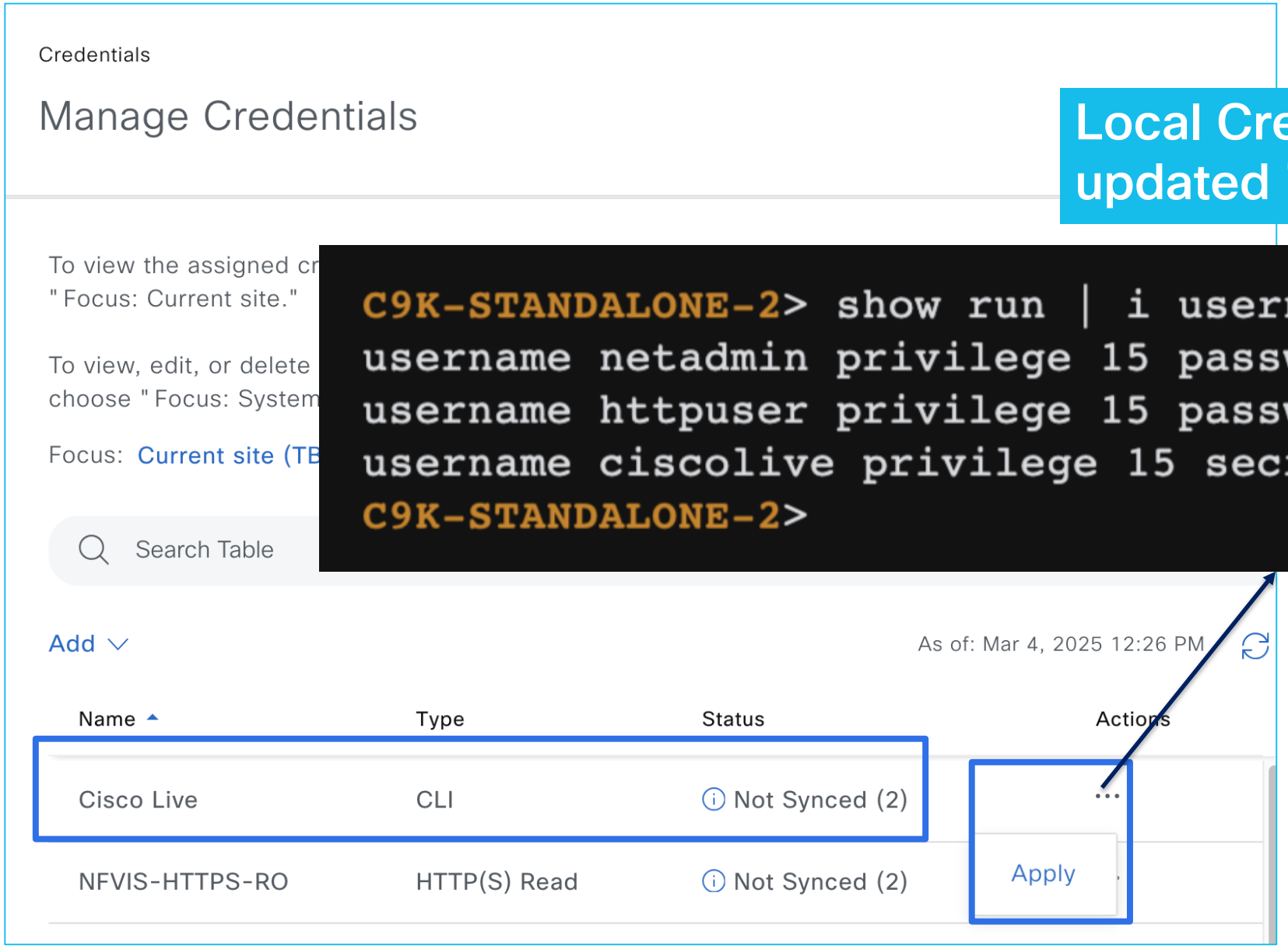


New password applied at the site level, other sites not impacted until synched

Changing local credential passwords

Reference

Local Credentials updated in device




```
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>
```

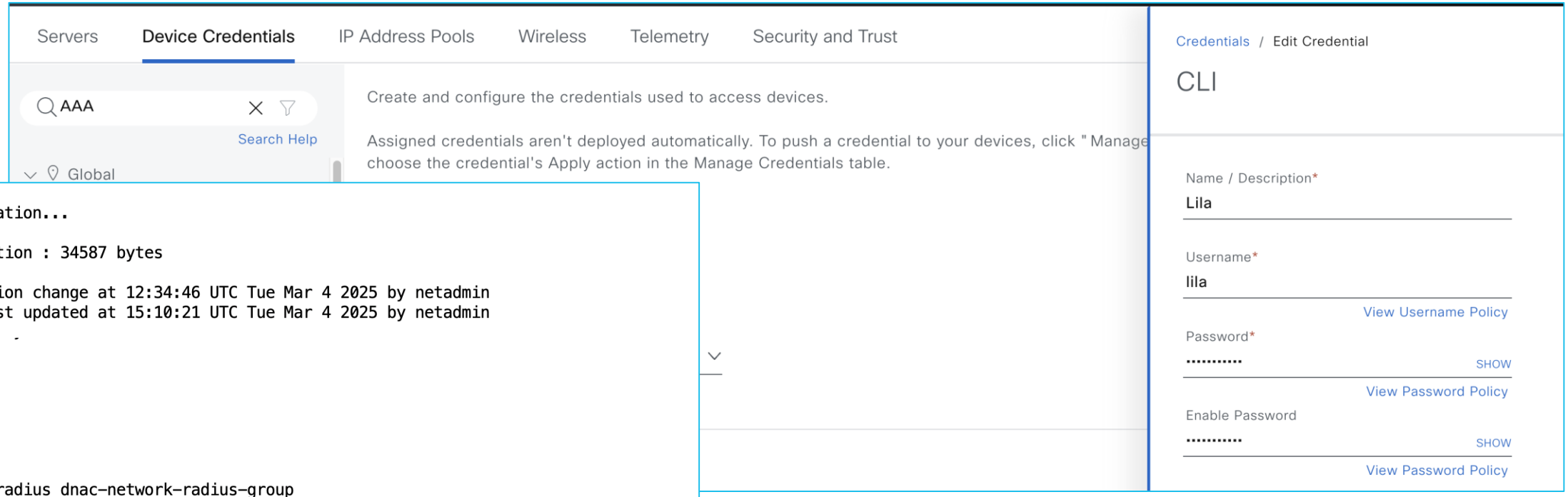
Changing local credential passwords

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' Succe
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

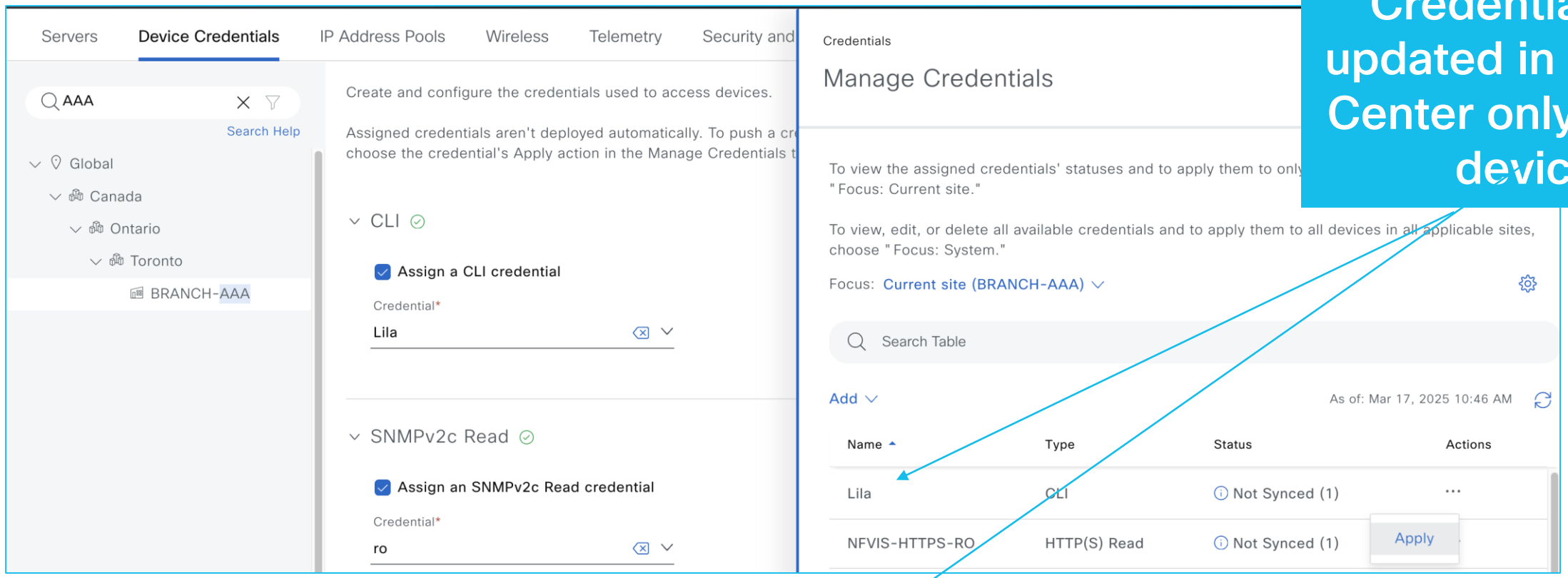



```
C9200L-1#show run
Building configuration...

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

Changing credentials passwords for devices with AAA for Network Devices

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



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

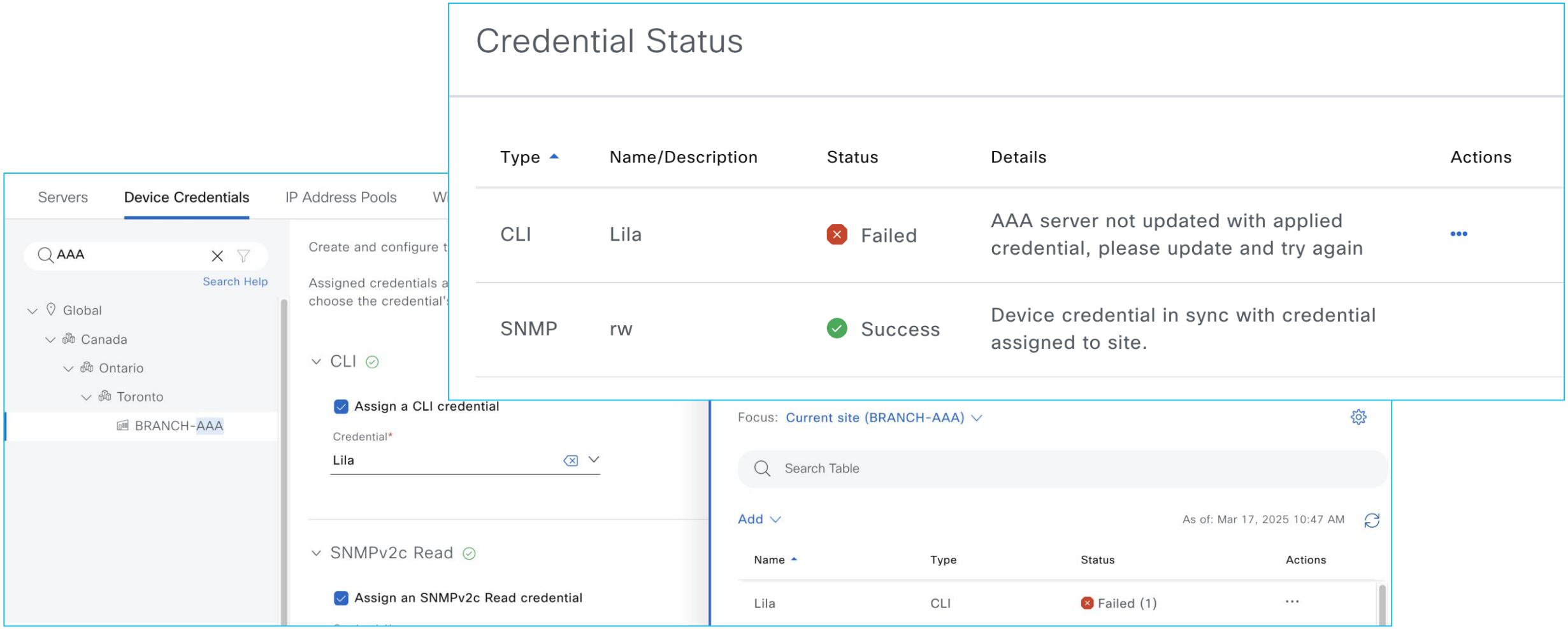
Brownfield AAA, Template-Based AAA or AAA Configured via Network Settings

```
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-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

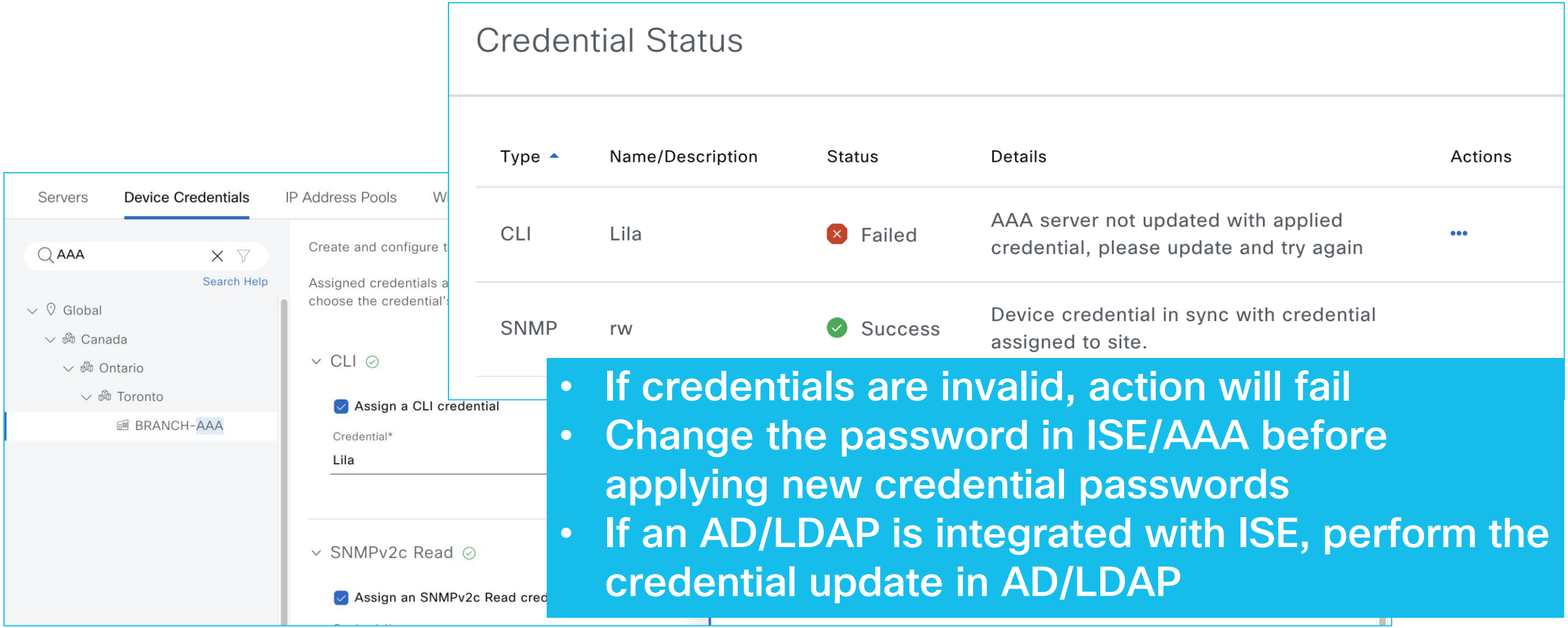
Changing credentials passwords for devices with AAA for Network Devices

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



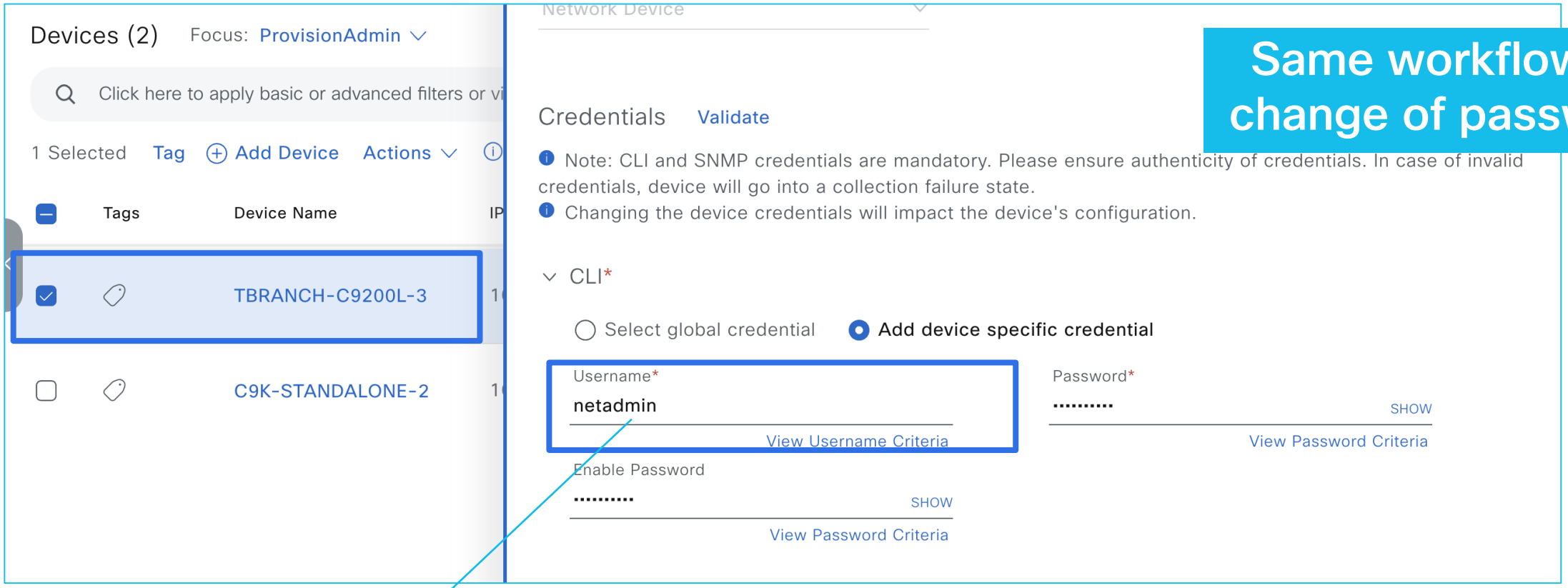
Changing credentials passwords for devices with AAA for Network Devices

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



- 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

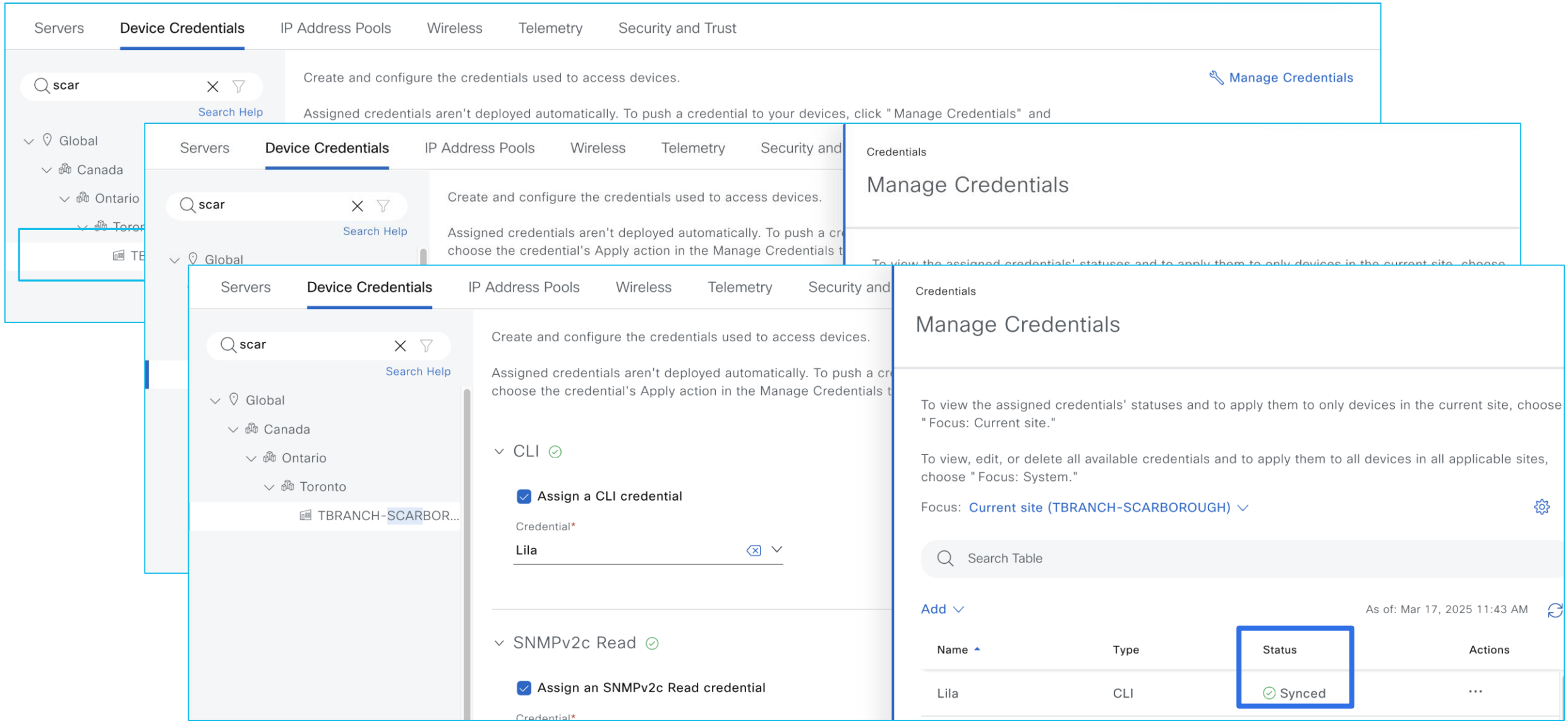
Adding and applying new credentials to devices



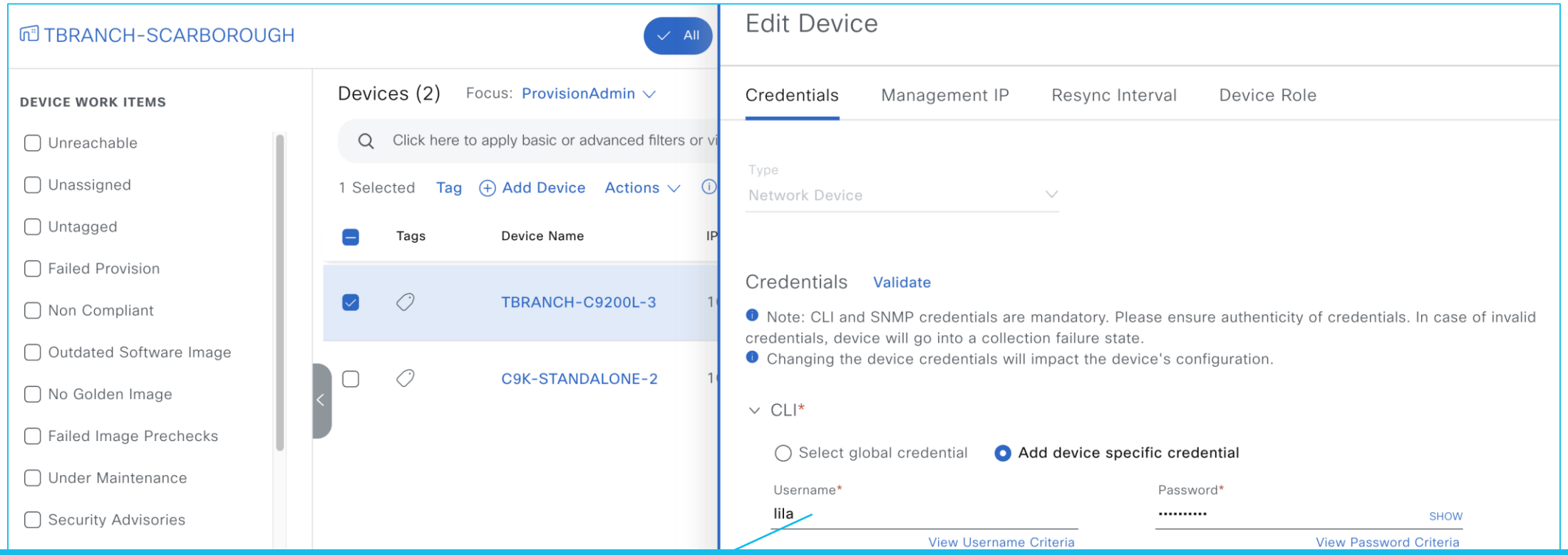
Same workflow as change of password

```
TBRANCH-C9200L-3#show run | i username
username netadmin privilege 15 password 7 04785A150C2E68602858
username ciscolive privilege 15 secret 8 $8$MHEMy6OT0Qp.fk$eQBNEVYBCW7umuAarXnNbxDnyhZrk4o2ORVYyQEFG.A
```

Adding and applying new credentials to devices



Adding and applying new credentials to devices

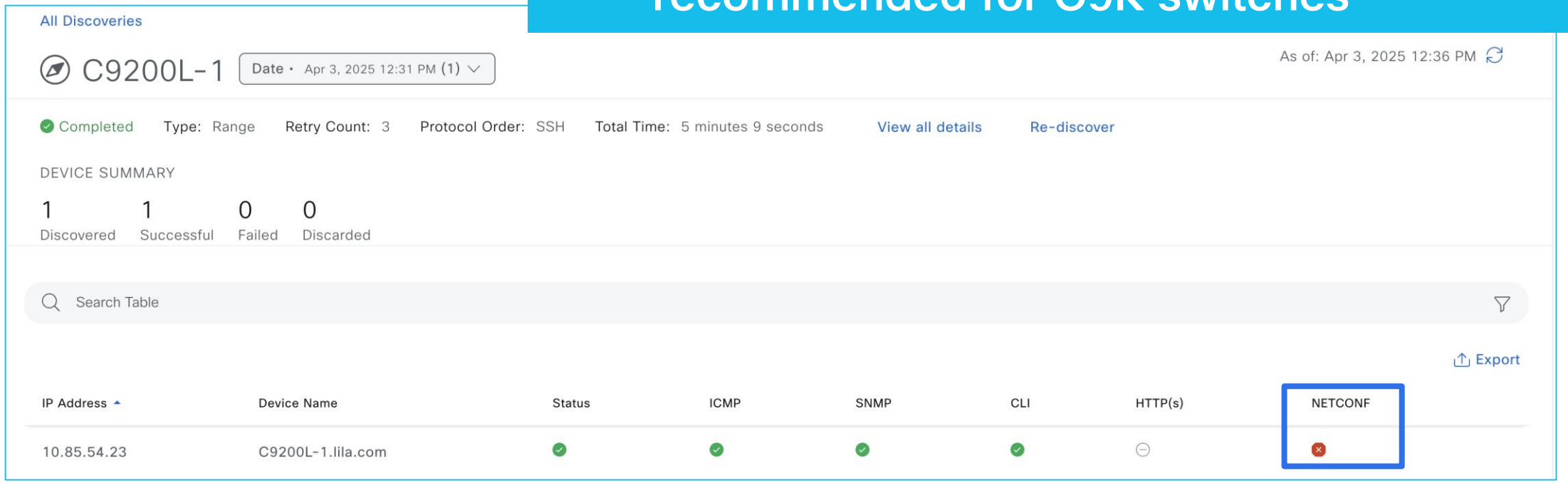


- For local authentication – new username will be added in device config
- For AAA authentication – new user needs to be added manually in AAA server

```
TBRANCH-C9200L-3#show run | i username
username netadmin privilege 15 password 7 04785A150C2E68602858
username ciscolive privilege 15 secret 8 $8$MHEMy6OT0Qp.fk$eQBNEVYBCW7umuAarXnNbxDnyhZrk4o2ORVYyQEFG.A
username lila privilege 15 secret 8 $8$YZ4SK4Hb4X9dmk$.Fi1.LkfwxF.YdjvLytRJ8R8V.jfN1aWuCaE9a0jTt6
```

Netconf failure

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



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

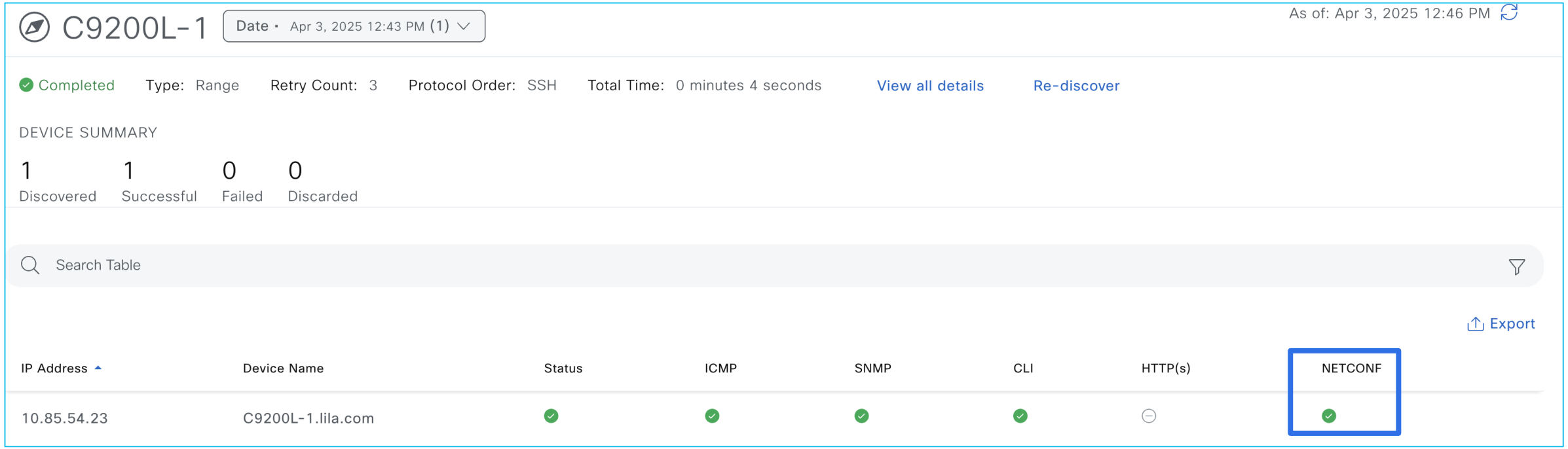
    aaa authorization exec default <local or radius/tacacs group>

    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



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
```

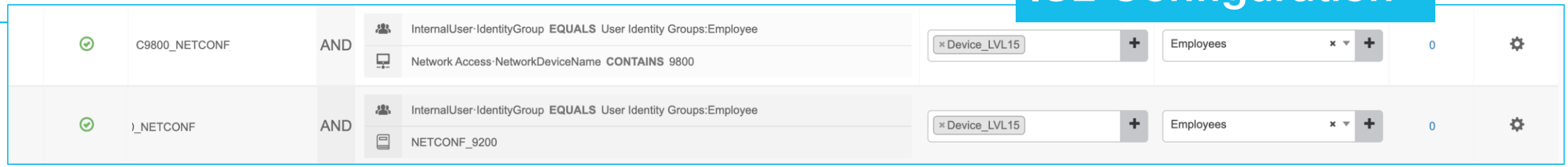
```
C9200L-1#
Apr  3 16:43:16.910: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: netadmin] [Source: 10.85.54.180] [localport: 22] at 16:43:16 UTC Thu Apr 3 2025
Apr  3 16:43:16.998: %SYS-6-LOGOUT: User netadmin has exited tty session 2(10.85.54.180)
C9200L-1#
Apr  3 16:43:17.286: %SEC_LOGIN-5-LOGIN_SUCCESS: 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

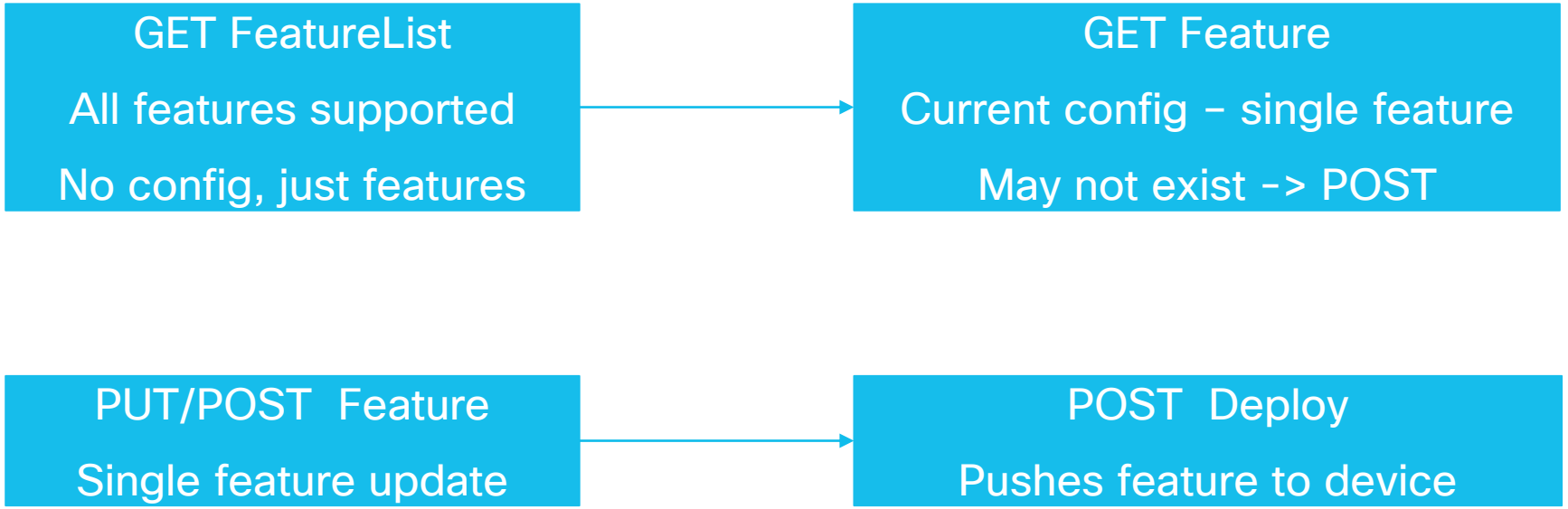
```
aaa new-model
!
!
aaa group server radius dnac-network-radius-group
 server name dnac-radius_10.85.54.185
 ip radius source-interface Vlan419
!
aaa authentication login VTY1 authen group dnac-network-radius-group local
aaa authentication login netconf-authn group dnac-network-radius-group local
aaa authorization exec VTY1 author 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

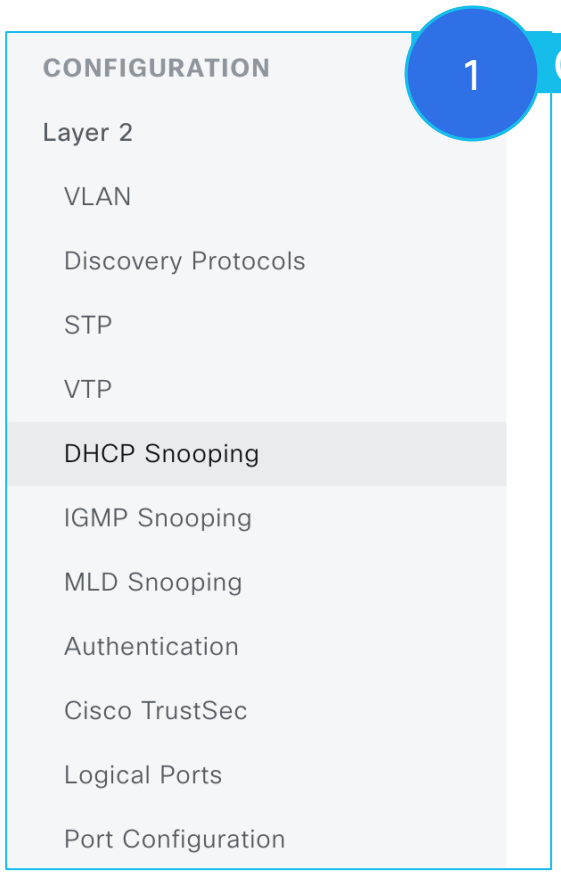


Automation beyond the UI: API’s

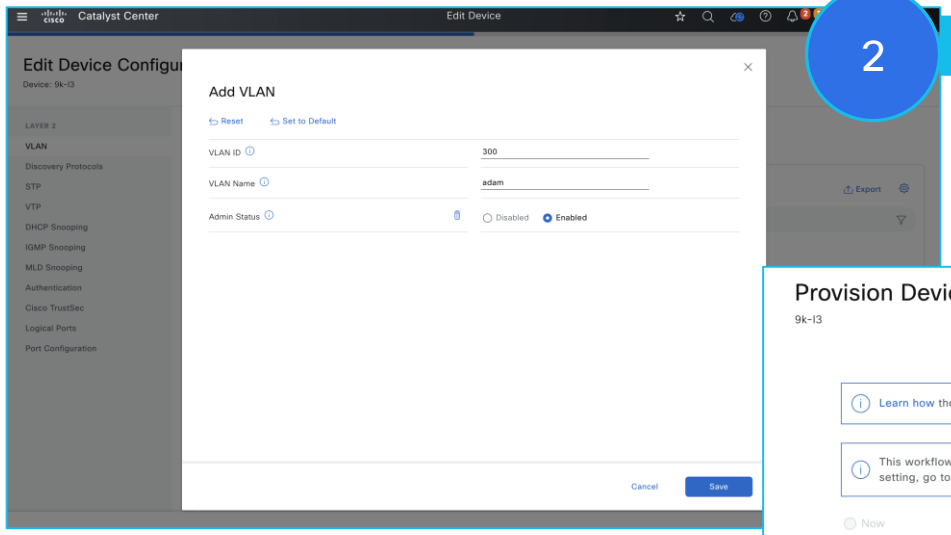
API Overview



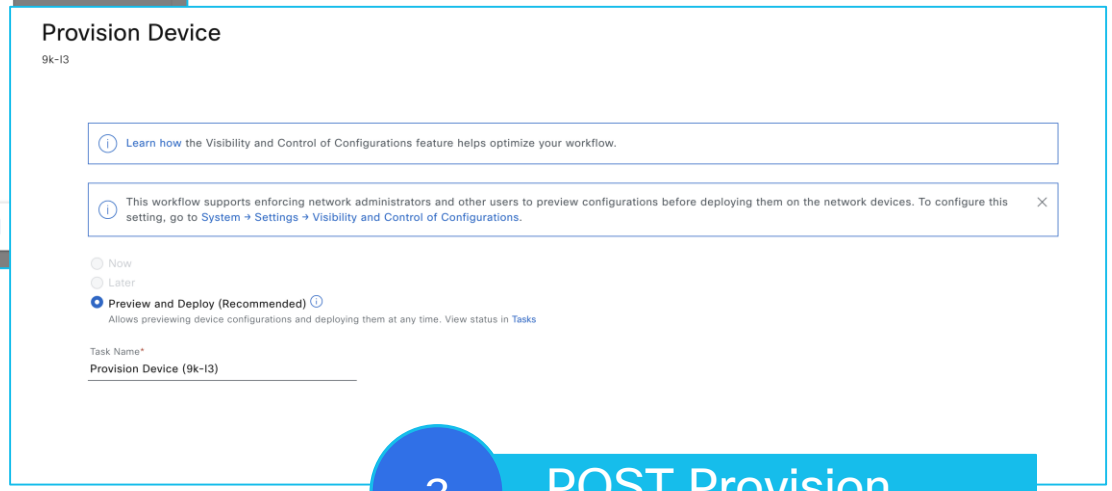
Mapping to the UI



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-aeea-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-aeea-e4c6708049c4"
  },
  "version": "1.0"
}
```

Deploy the feature

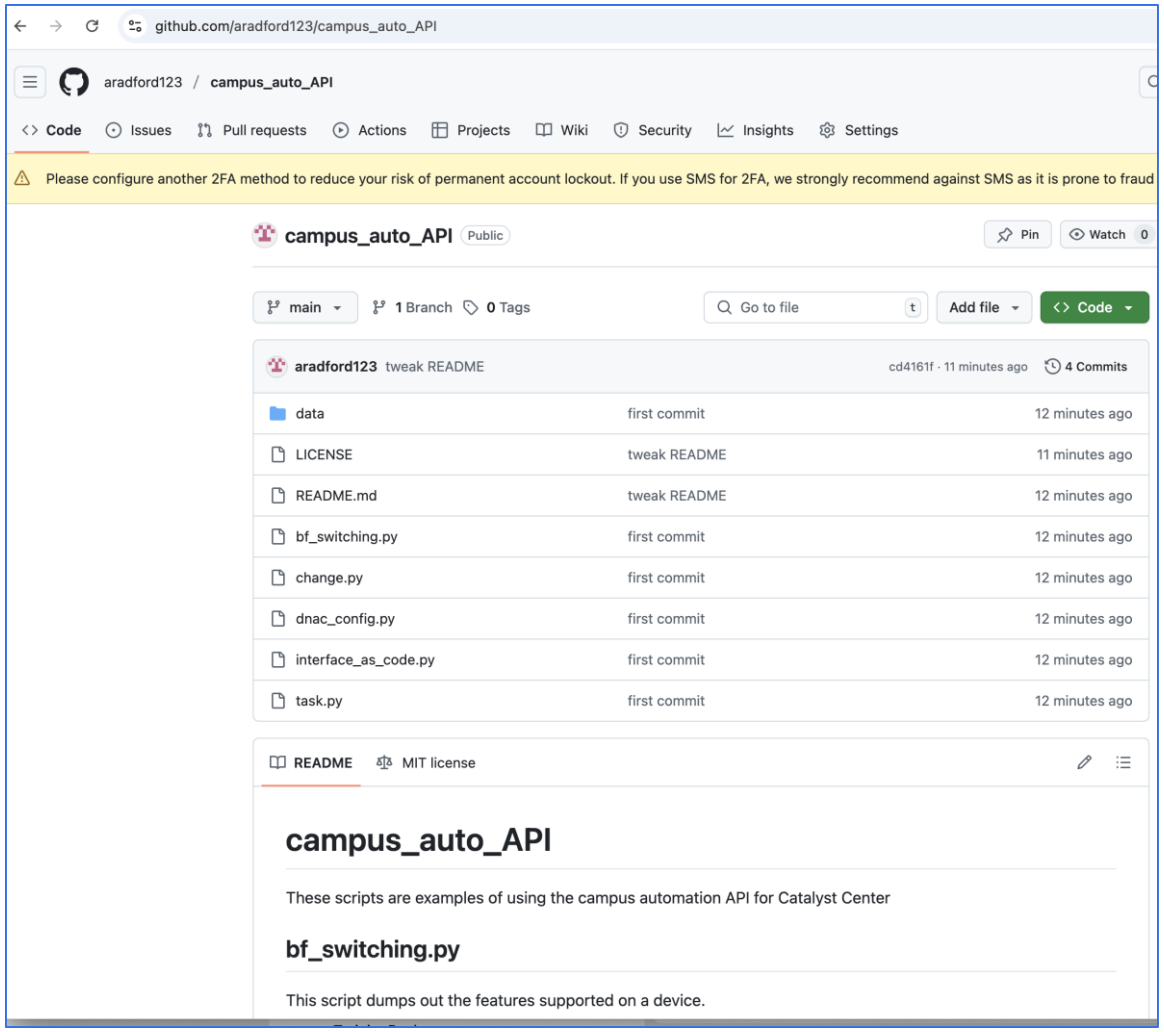
```
POST /dna/intent/api/v1/wired/networkDevices/<deviceid>/configFeatures/intended/deploy

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



Closing and Q&A

Complete your session evaluations

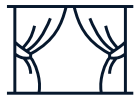
Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to win 1 of 5 full conference passes to Cisco Live 2026.

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

Cisco Community

cs.co/dnac-resources

Thank you

cisco Live !


CISCO