Discovering and Managing Brownfield Deployment with Cisco Catalyst Center

(formerly Cisco DNA Center)

Sneha Amarapuram - Customer Success Specialist
Ramkumar Chellappa - Technical Leader, TME

BRKOPS-1461

Webex App

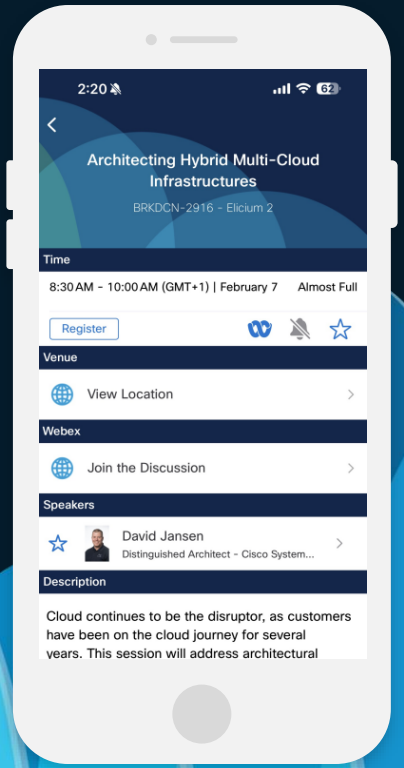
Questions?

Use the Webex app to chat with the speaker after the session

How

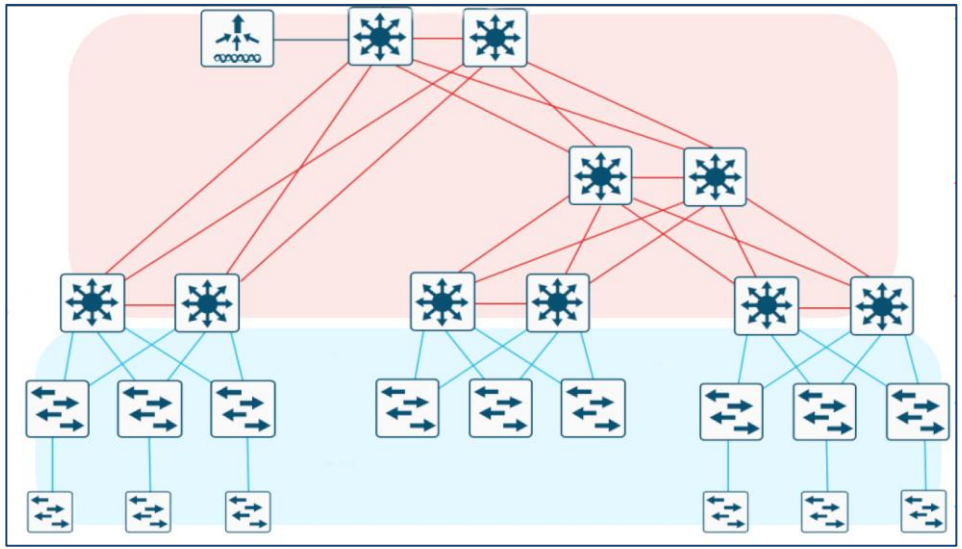
1. Find this session in the Cisco Events mobile app
2. Click “Join the Discussion”
3. Install the Webex app or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until February 28, 2025.



Navigating Amsterdam: A Biker’s Journey

Navigating Brownfield: A Network Admin's Journey



Agenda

Introduction to Catalyst Center

- Planning Catalyst Center Deployments
- Starting your Journey

Pre-requisites to Onboard

- Pre-requisites on Catalyst Center
- Pre-requisites on Network Devices

Device Onboarding Workflow

- Device Onboarding Workflow
- Site Assignment Workflow

Managing your Brownfield Deployment

- Provisioning (CLI Templates & Per Device Workflow)
- Compliance
- Software Image Management
- Device Refresh & RMA

For Your Reference

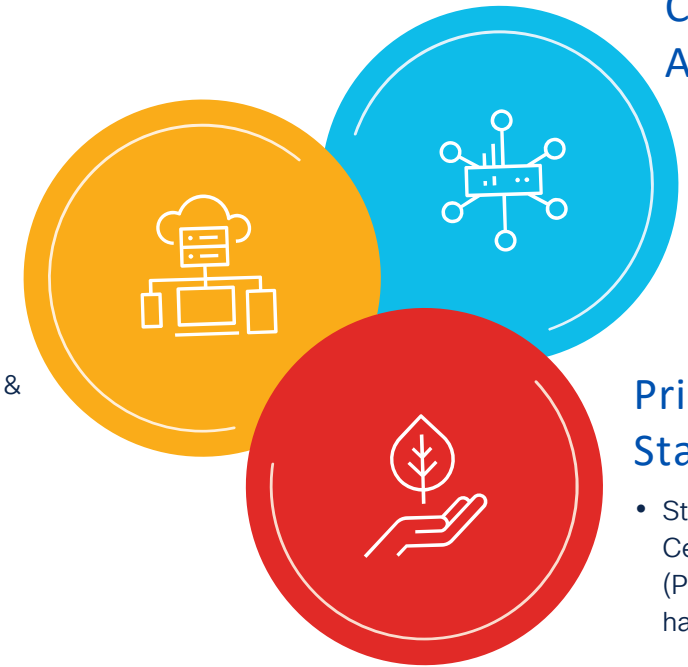
There are slides in your PDF that will not be presented, or quickly presented

They are valuable, but included only “For your reference”

Planning Catalyst Center Deployment & Migration

Plan Deployment

- Physical/AWS/ESXi
- High Availability
- Gather the required IPs information
- Latency requirement
- Device Compatibility(HW & SW)
- License
- SDA/ Non-SDA



Cable and Install Appliances

- Open the required ports/URLS
- Reachability between appliances and network devices

Prime Migration or Start Fresh

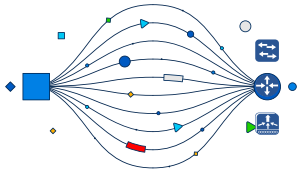
- Start from scratch on Catalyst Center or migrate from Prime (Prime Data Migration Tool makes it hassle free)

Catalyst Center- NetOps Journey Map

Onboarding & Inventory

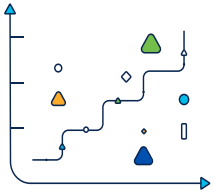
- Plug and Play
- Discovery
- Inventory
- Network Hierarchy & Design
- Config Visibility

Network Configuration



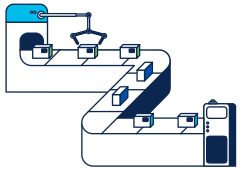
- Device Provisioning
- CLI Templates, Feature Templates, Wireless Design
- Workflows
- Network Services
- Per Device Configuration

Network Conformance



- Config Drifts
- Config Compliance & Remediation
- Change Audits (Visibility & Control)

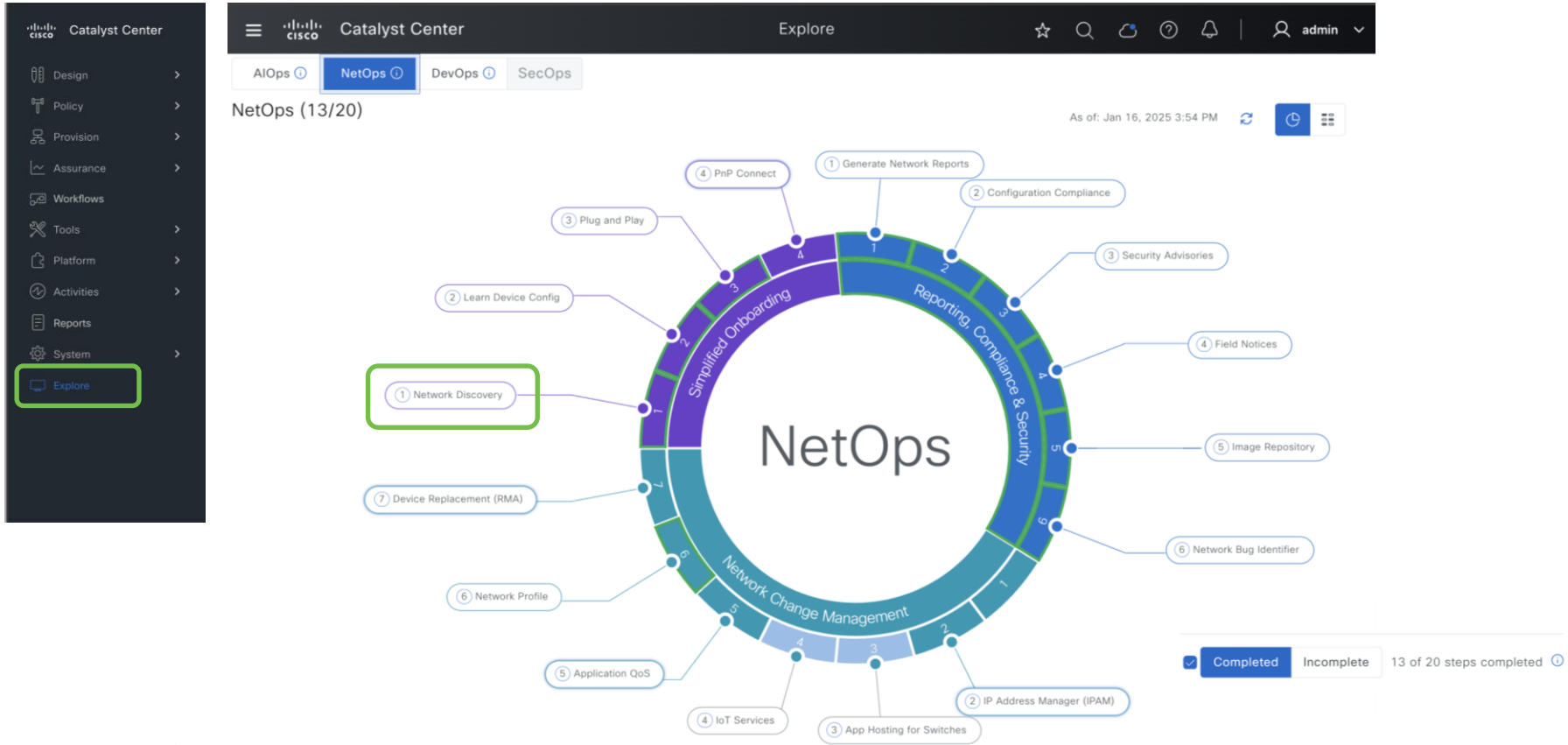
Lifecycle Management



- Software Image & Patch Updates
- Device RMA
- IOS-XE Switch & AP Device Refresh
- Security Advisories, Field Notices, EoX Status

Day-0 | Day-1 | Day-N

Start your Journey

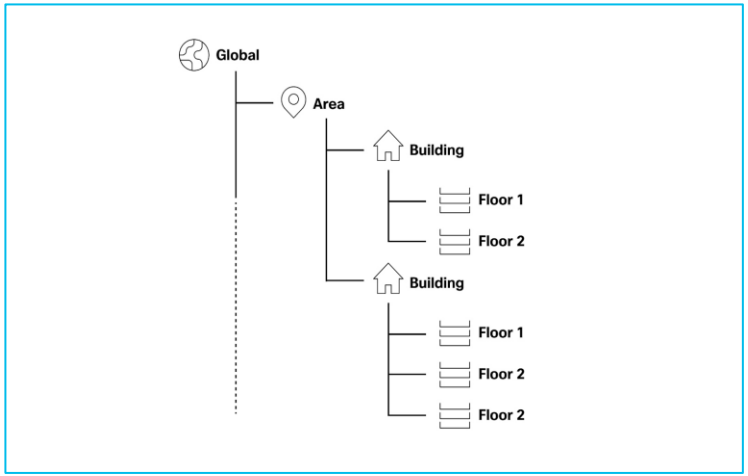


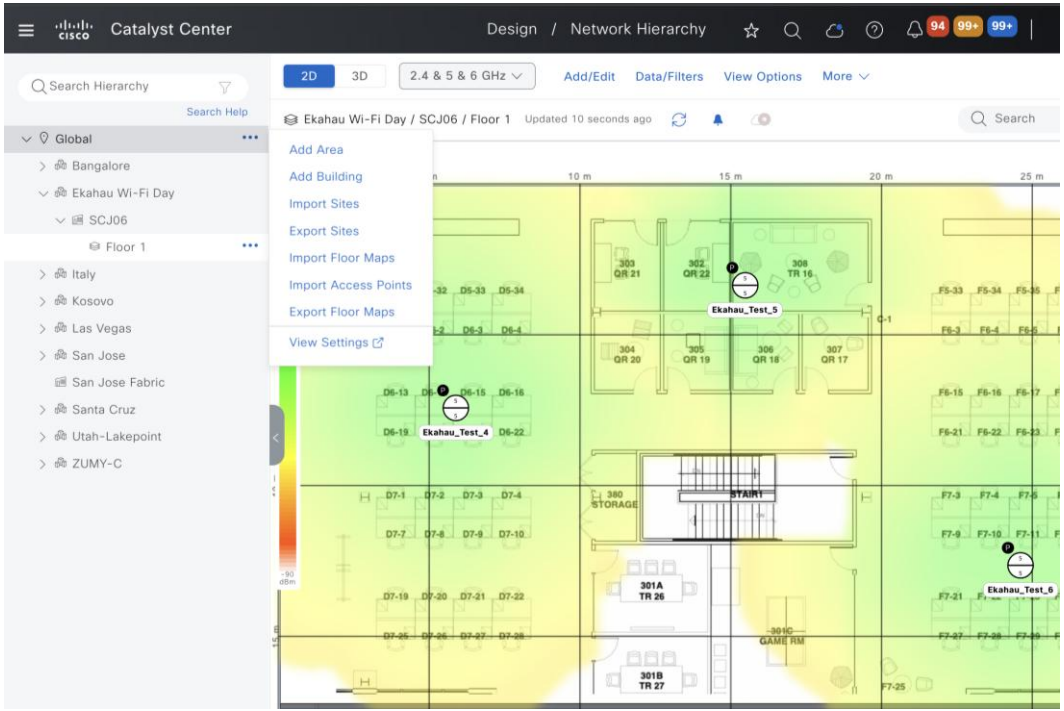
Pre-requisites to Onboard

cisco Live!

Creating Site Hierarchy

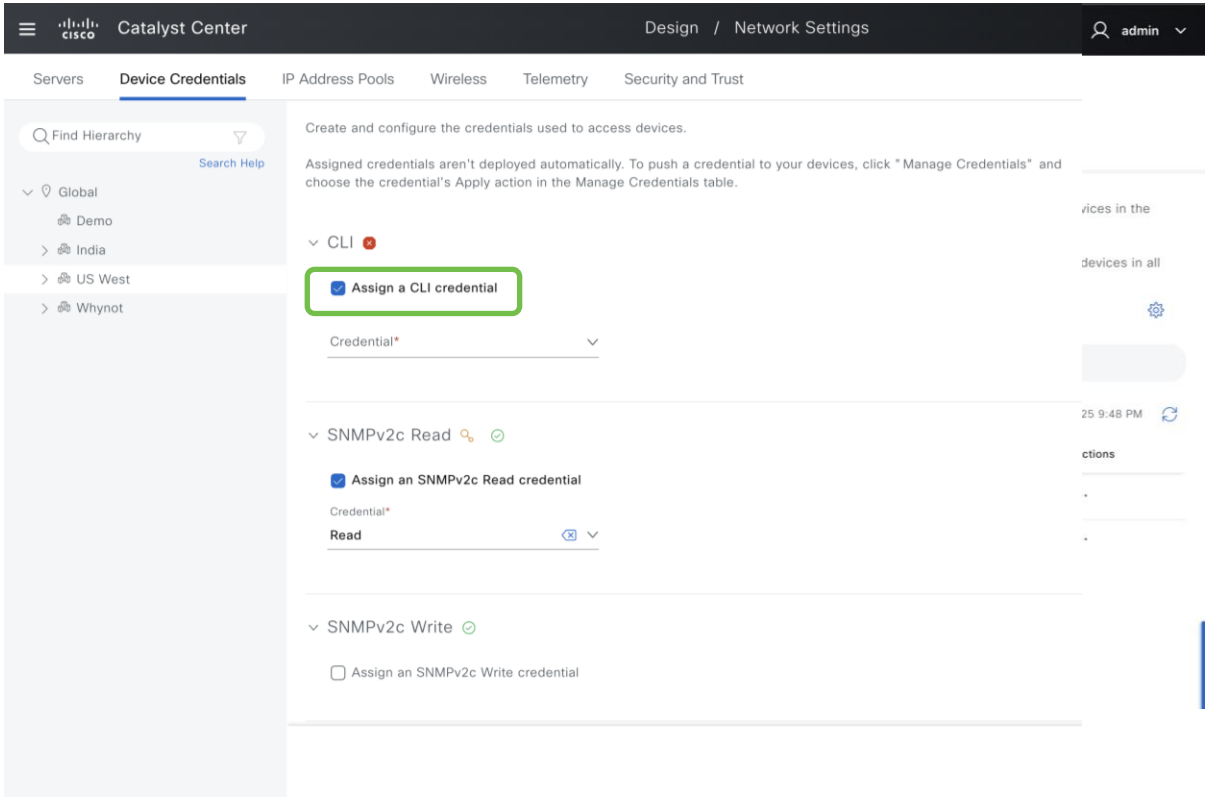
Create the structure and framework of your network, including the physical topology, network settings, and device type profiles that you can apply to devices throughout your network.





Designing Network Settings- Device Credentials

- Create CLI, SNMP v2/v3,HTTPS credentials at “System” level
- “Assign” credentials to Global or Specific Sites



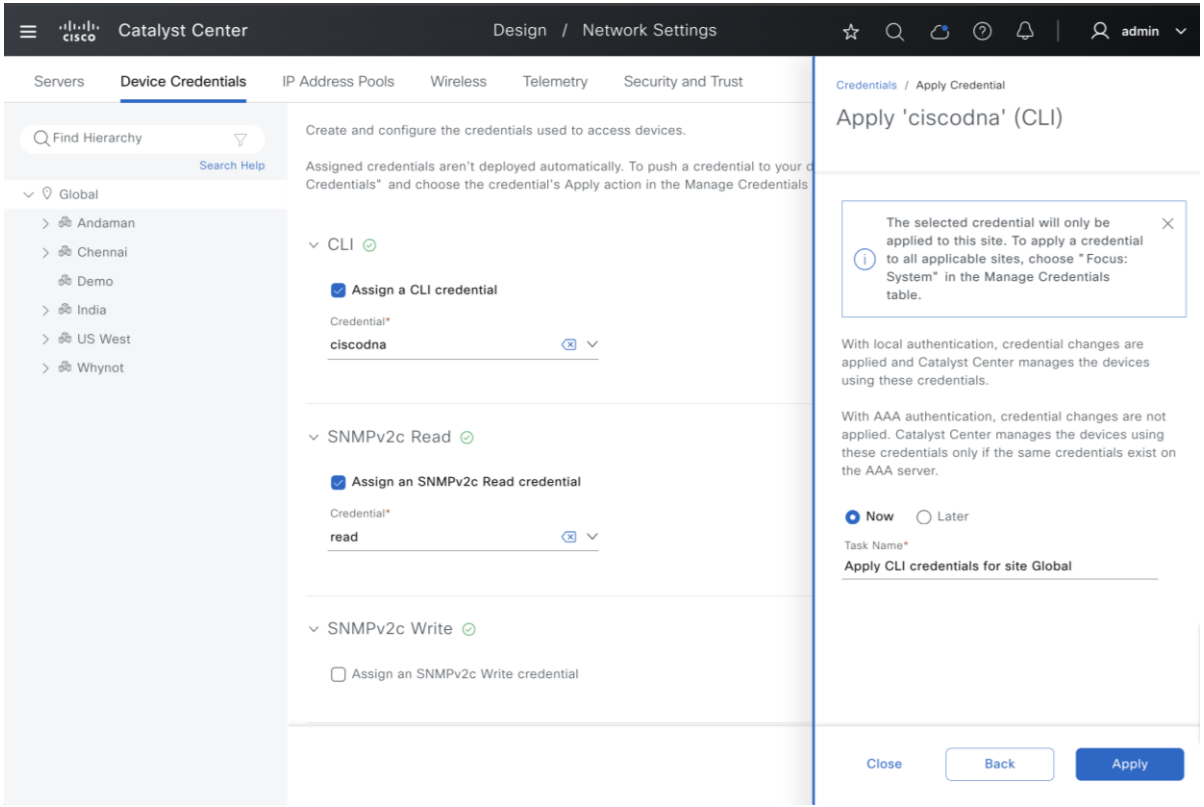
Designing Network Settings- Device Credentials

- Create CLI, SNMP v2/v3 credentials at “System” level
- “Assign” credentials to Global or Specific Sites
- “Apply” credentials workflow

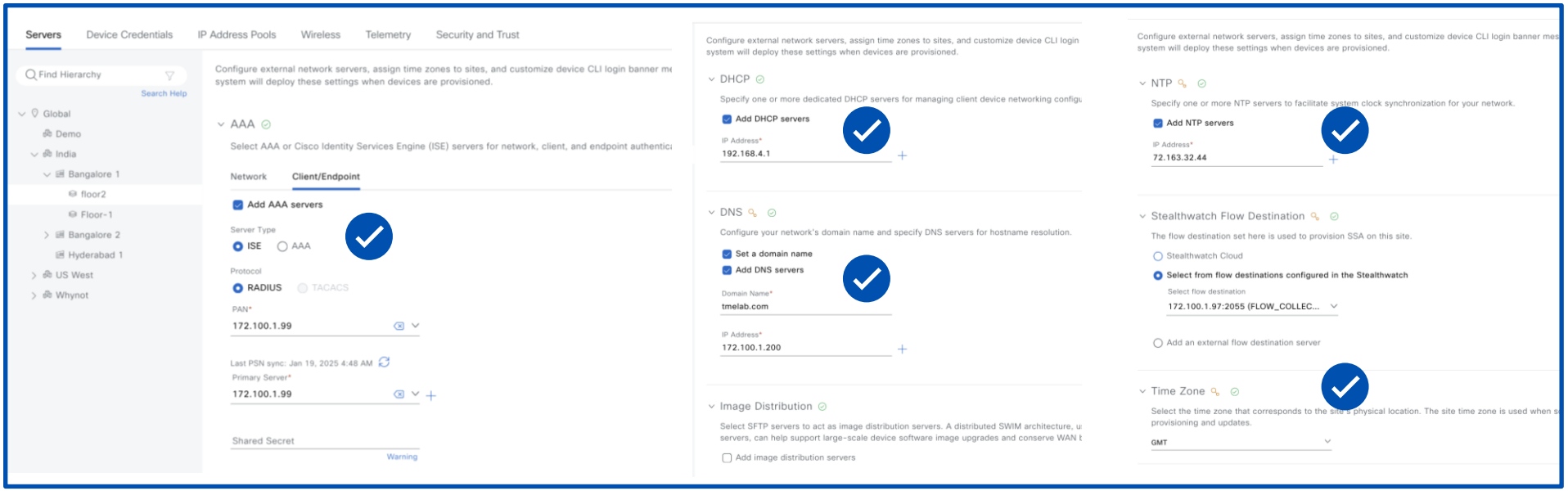
A. Local Credentials: Push Credentials to device and update inventory

B. AAA Credentials:
   - Ensure local credentials match those on the AAA server.

Note: For password rotation, first update the AAA server credentials or service account, then use the Apply Credential workflow in Catalyst Center



Designing Network Settings- Servers

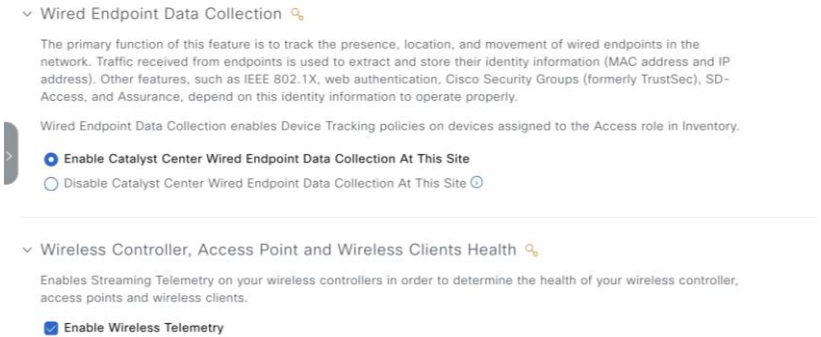


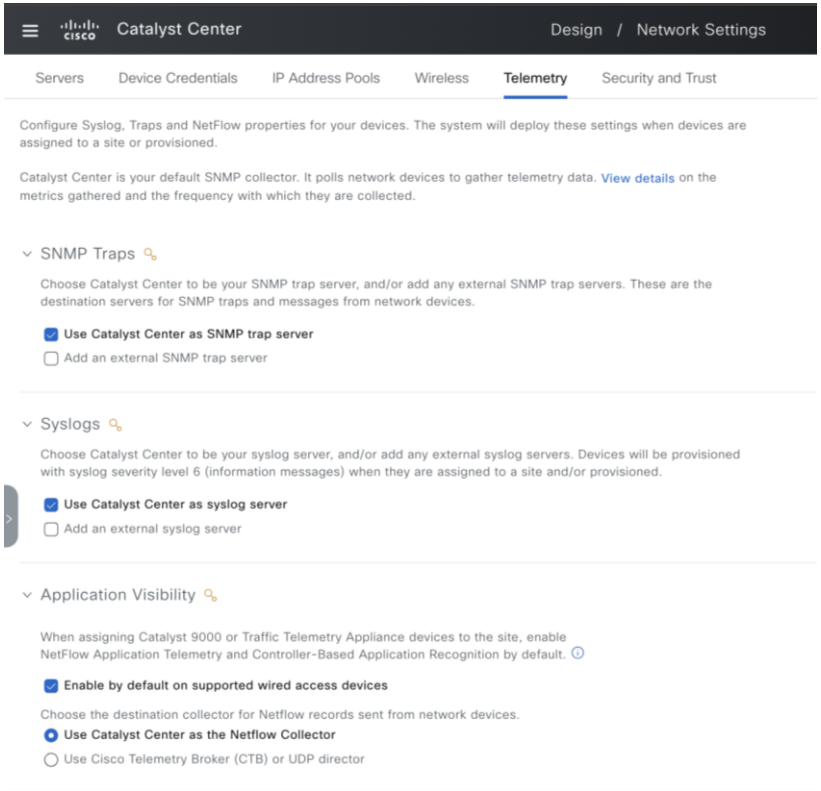
Ensure Network Settings are configured for configurations to be deployed during “Site Assignment” or “Provisioning” workflows

Designing Network Settings- Telemetry

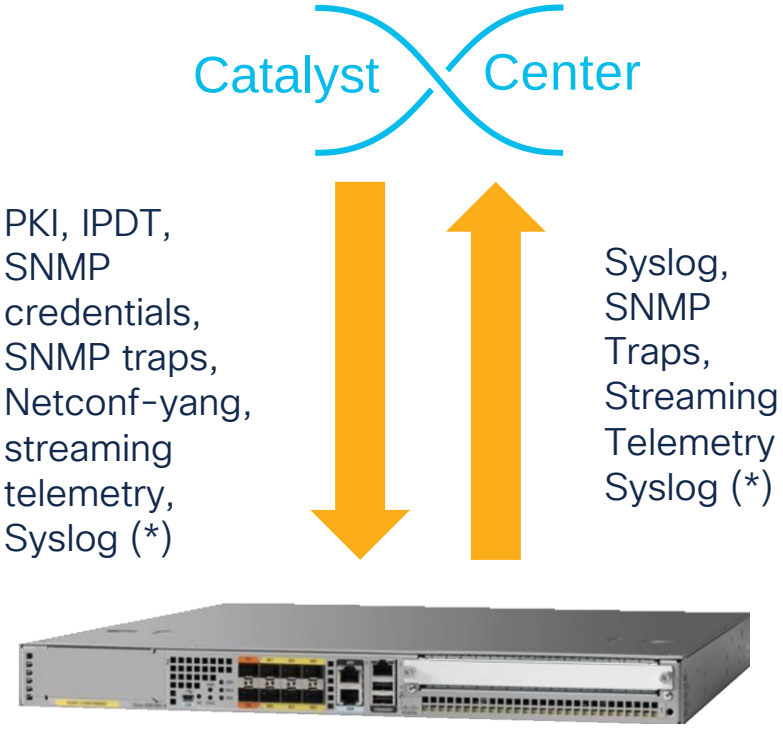
Ensure Telemetry settings are configured, to send Syslog/ SNMP/ NetFlow collectors as Catalyst Center

For Brownfield Devices, to avoid overwriting configured IPDT policies, recommendation is to keep the Wired Endpoint Data Collection “Disabled”



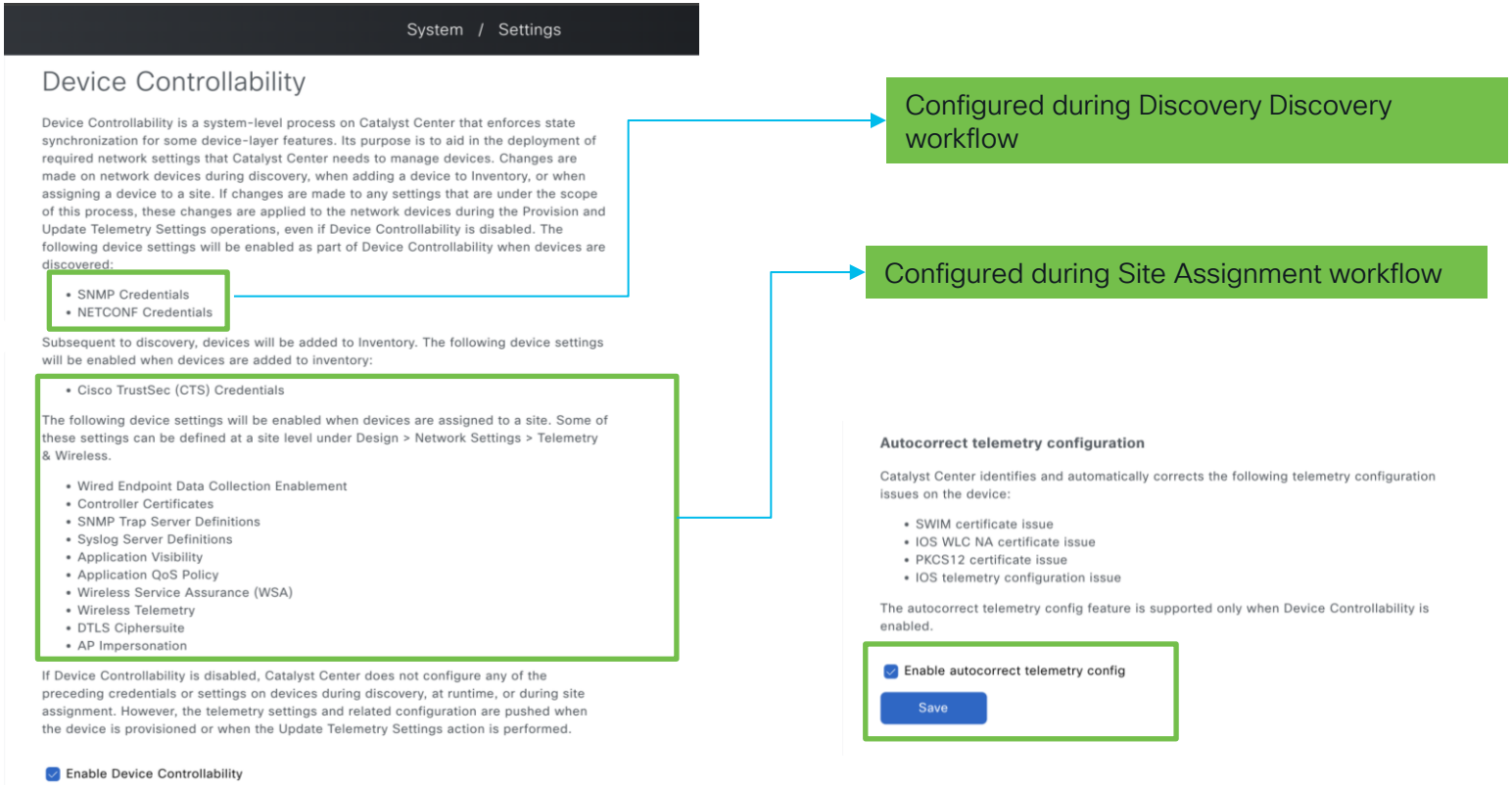


Why We Need Telemetry?

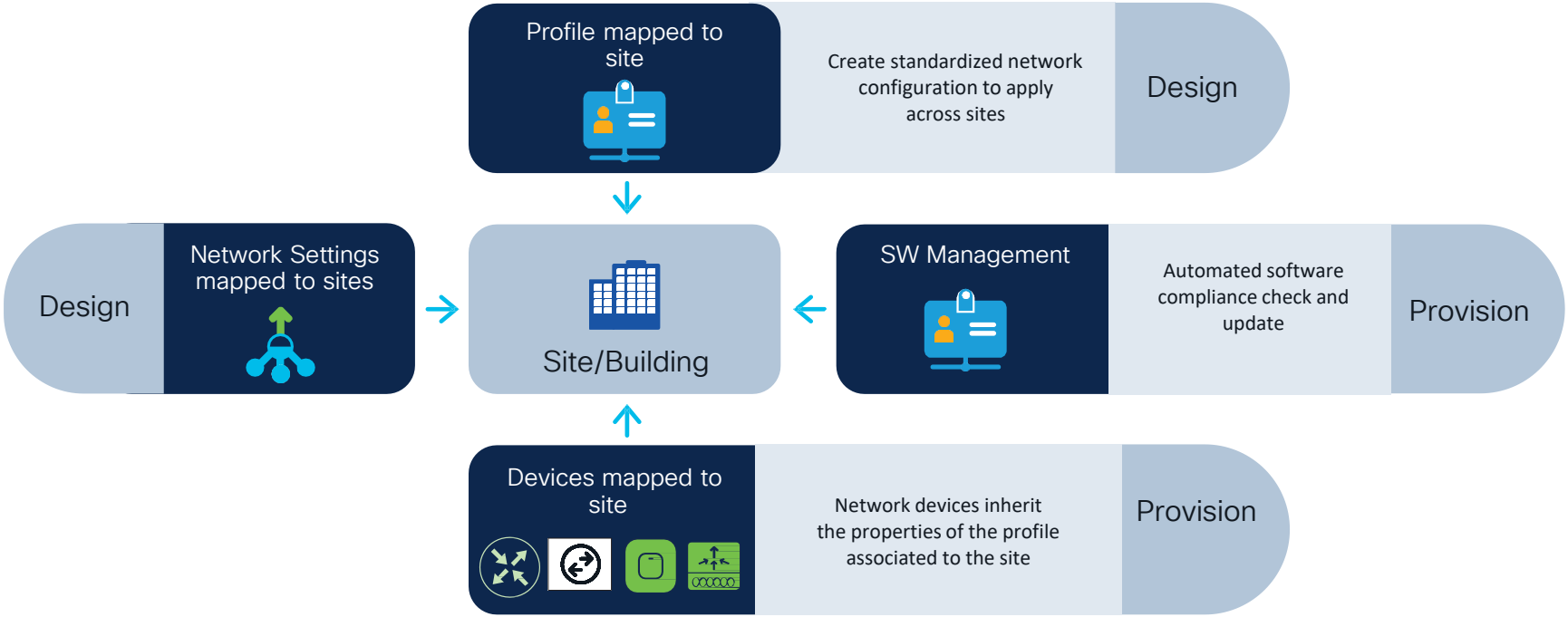


1. Network and Client Health
2. Application Health
3. Network Services (AAA, DHCP, DNS)
4. View and Manage Issues
5. Visibility into Wi-Fi 6/6E Readiness
6. Monitor Power over Ethernet
7. EoX Insights
8. Inventory Insights
9. Network Trends and Insights

How do we push Telemetry?

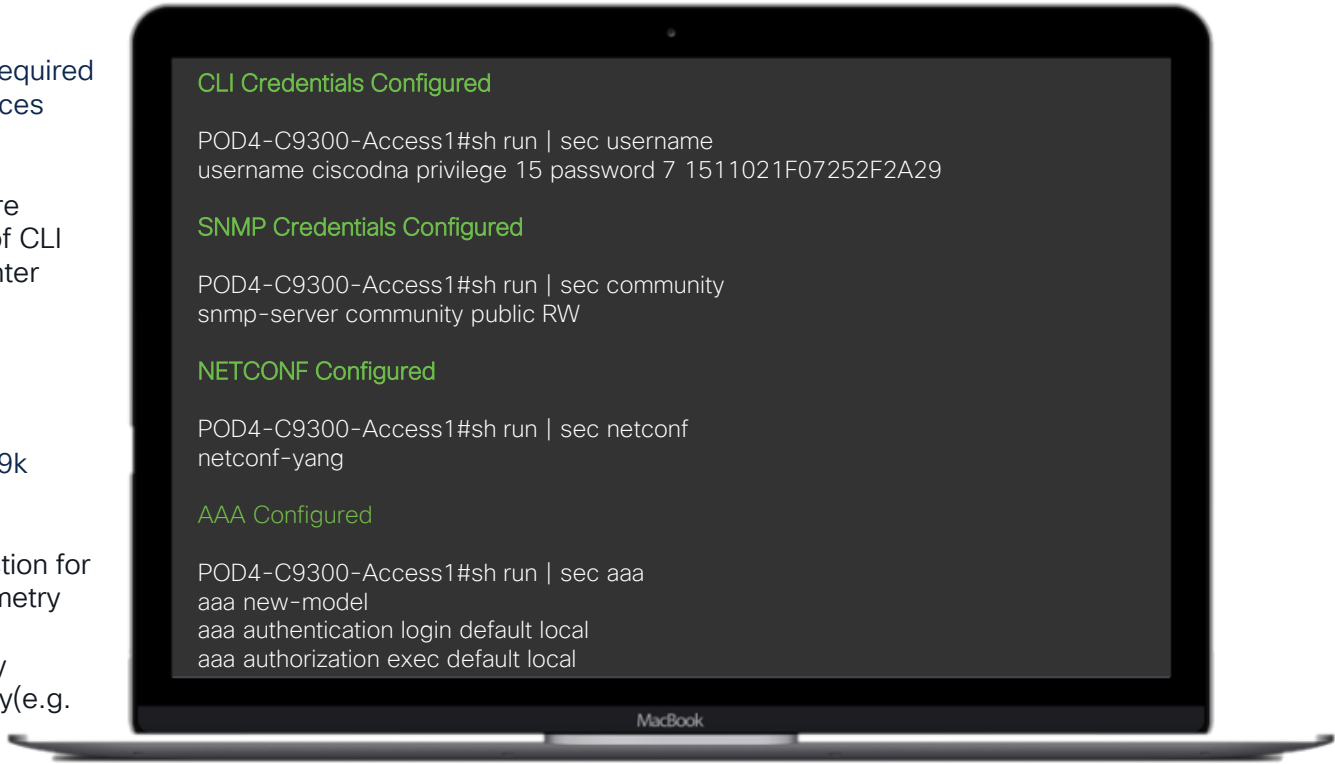


Site as a Focal Point in Catalyst Center



Pre-requisites before Onboarding devices

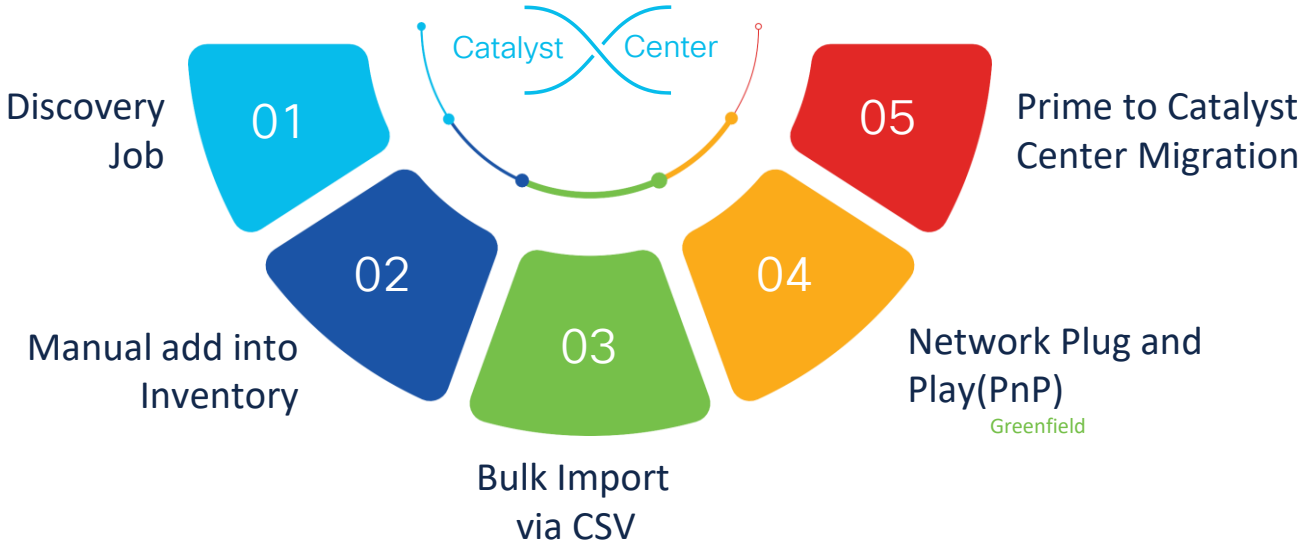
- Minimal CLI and SNMP details are required for Catalyst Center to discover devices
  - SSH/Telnet Login – EXEC mode(level 15) or configure enable password as part of CLI credentials in Catalyst Center
  - At least SNMPv2c read
- NETCONF for Cat9800 WLC & Cat 9k switches
  - The majority of data collection for WLC is via streaming telemetry
  - Advanced features employ Netconf-yang for telemetry(e.g. POE status)



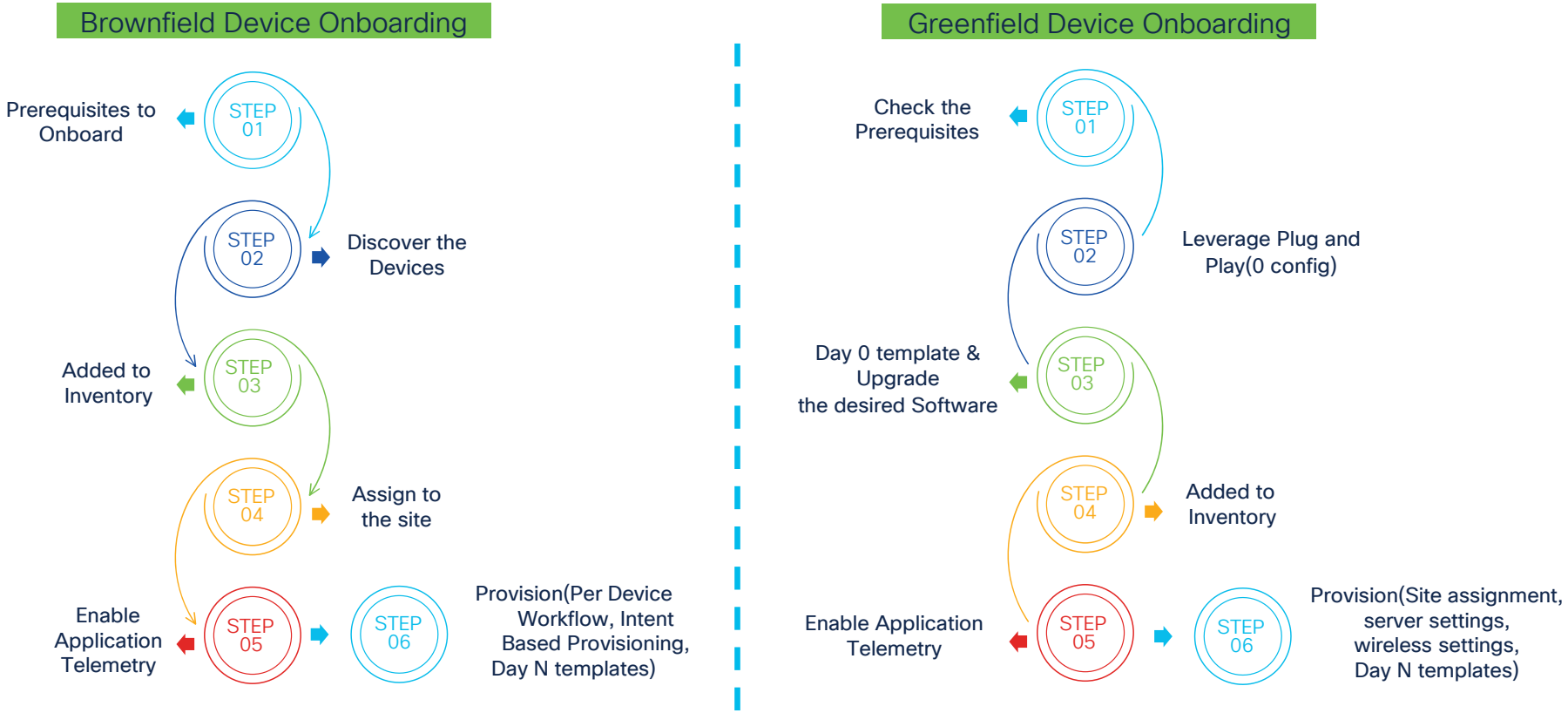
Device Onboarding Workflow

cisco Live!

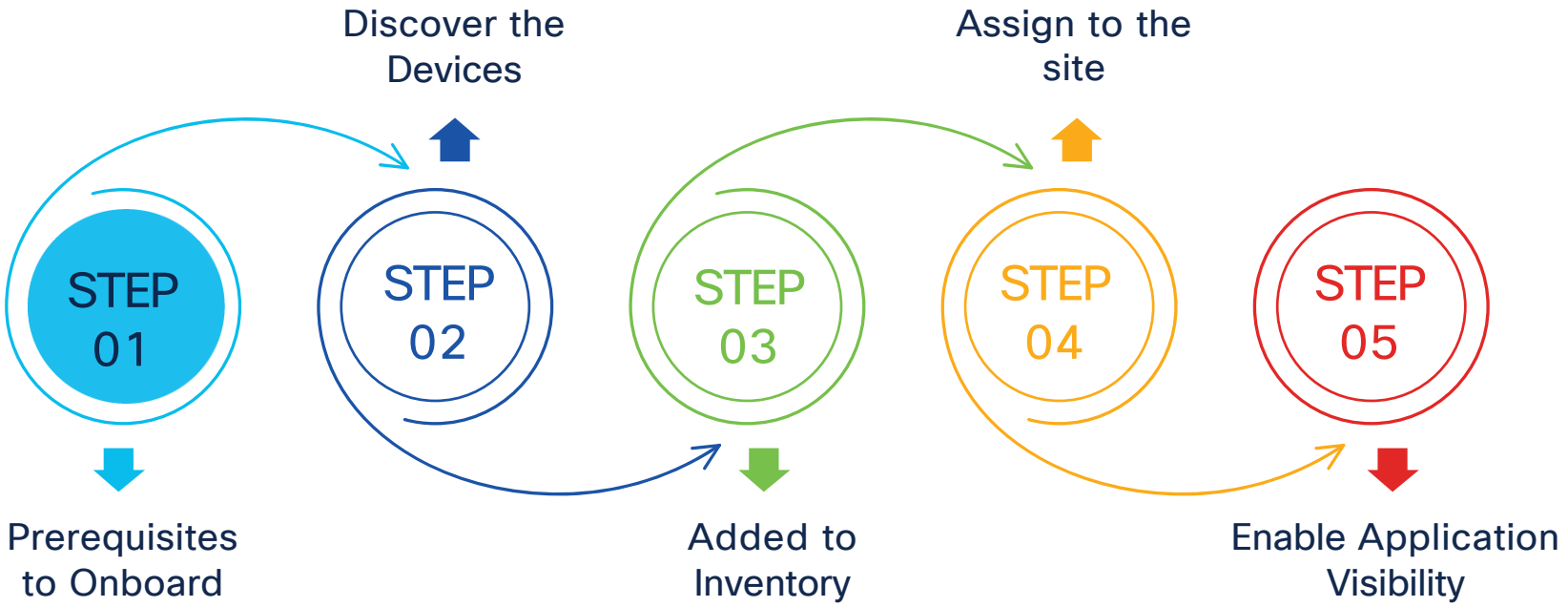
Various Ways To Onboard Devices Into Catalyst Center



Brownfield vs Greenfield Device Onboarding



Brownfield Device Onboarding



Discovery Tool

Discover Devices

Begin by naming this discovery job. Then select your preferred type of discovery. The discovered devices can be assigned to a site later in this workflow. Access Points associated with discovered wireless controllers will be automatically added to Inventory.

Discovery Job Name*
Edge Devices

DISCOVERY TYPE

CDP | IP Address Range | LLDP | CIDR

This workflow is used to discover Cisco Network Devices. Third party devices can be manually added in the inventory page.

IP Address* (Info)

CDP Level*
16 (Info)

Subnet Filter (Info)

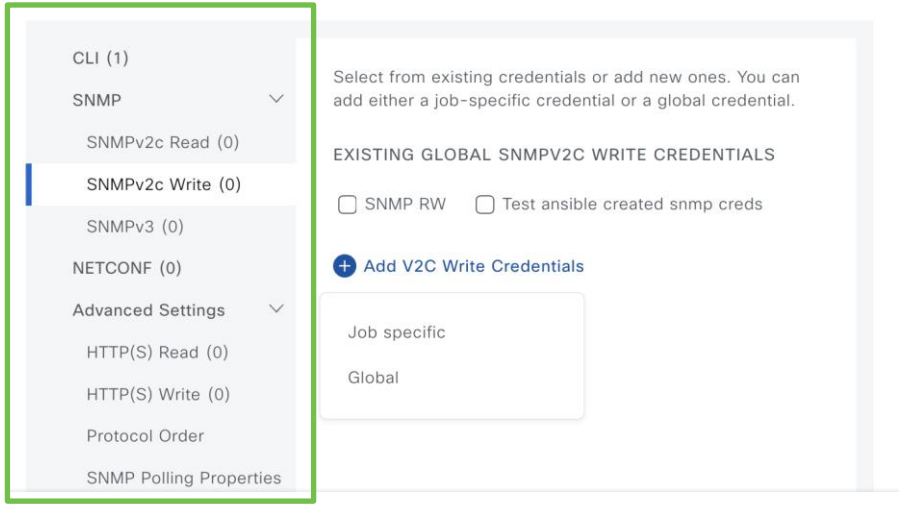
PREFERRED MANAGEMENT IP ADDRESS

None | Use Loopback (If Applicable)

Provide Credentials

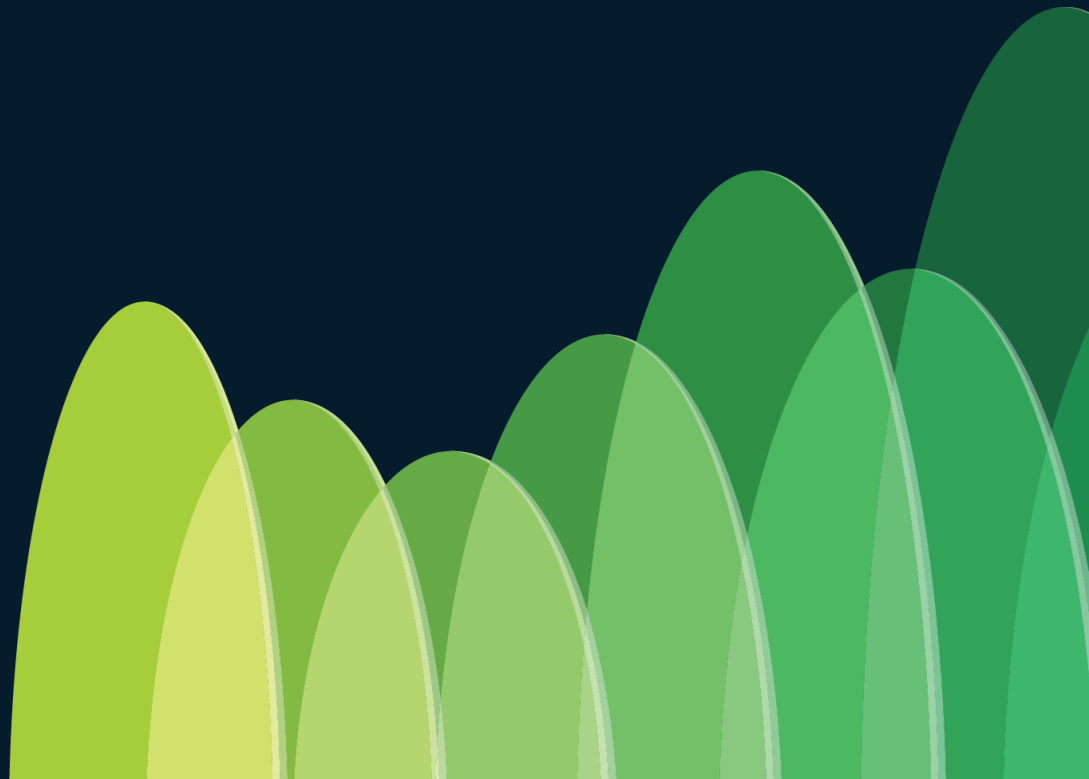
Global credentials are provided only for ease of use when entering credentials. At the device level, only the device-specific credentials are saved. The device-to-global-credentials association isn't saved.

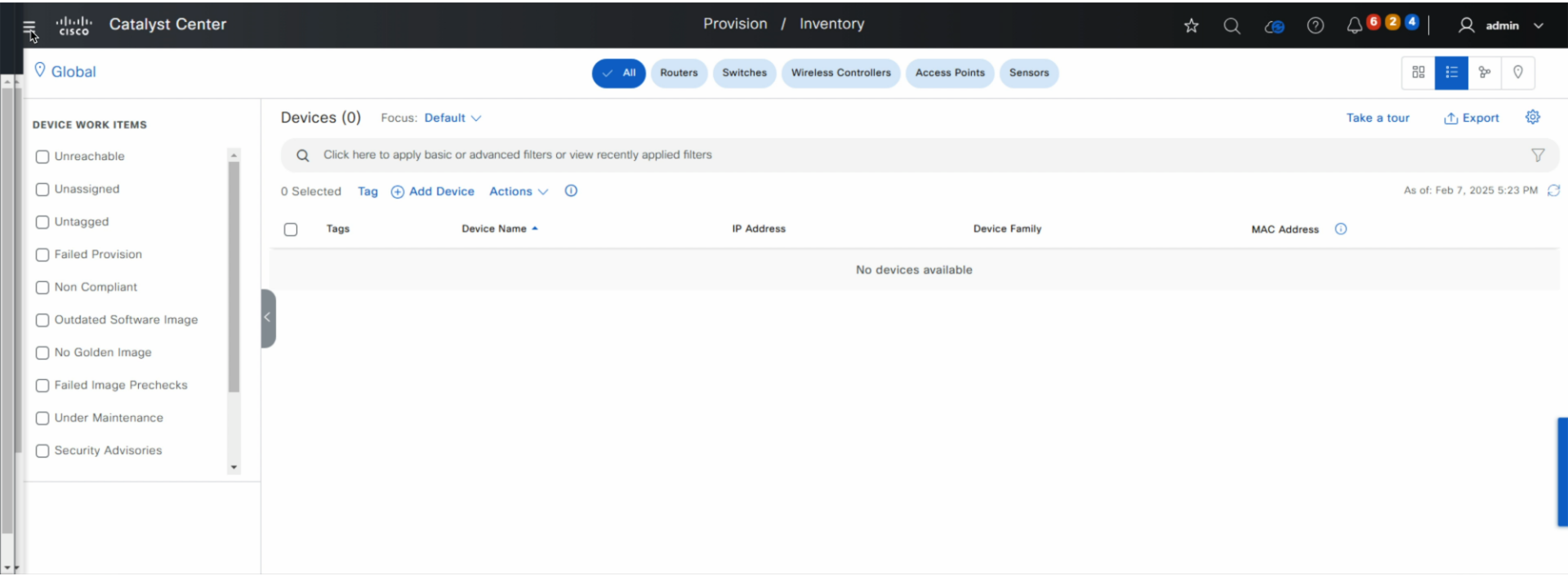
Next, confirm the credentials that Catalyst Center uses for the devices it discovers. At least one CLI credential and one SNMP credential are required. You can have a maximum of five global credentials and one task-specific credential for each type. Optionally, you can update SNMP properties and protocols used for CLI.



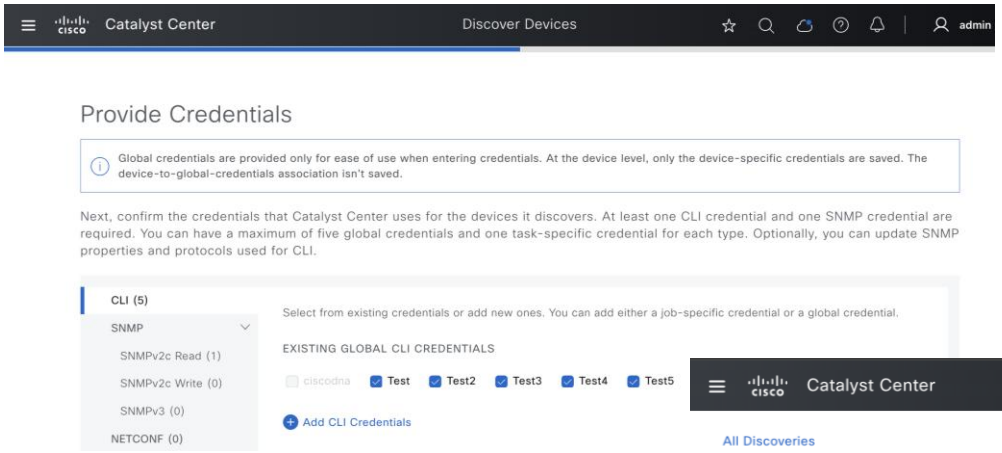
Note: WLC should be discovered using the management port for assurance
APs that have joined the WLC automatically get added to the inventory. No need to discover them.

Demo

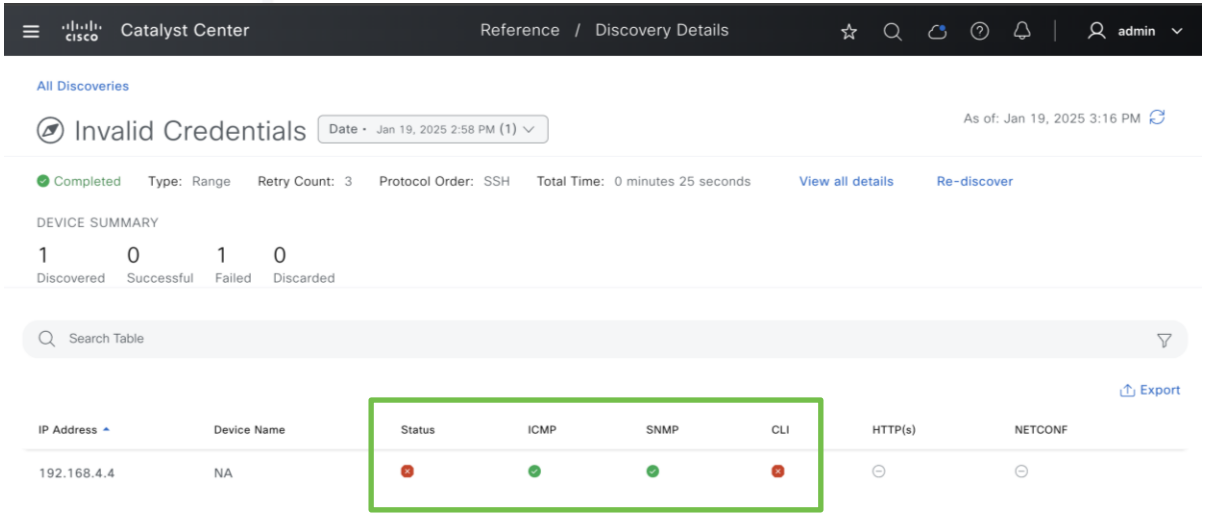




What If…? – Scenario-1



CLI Credentials configured in device does not match credentials in Catalyst Center



Discovery Fails for the devices with Invalid Credentials

What If…? – Scenario-2

SNMP v2 Credentials mismatch between Device and Catalyst Center

SNMP Manual Config on devices	SNMP Config on Catalyst Center	Result
snmp-server community public RO	Catalyst Center configured with SNMPv3 Credentials	SNMPv3 credentials appended to existing config. No changes made to v2 config
snmp-server community demo RO	Catalyst Center Configured with RO community and name “public”	SNMP community name is overridden

SNMP v3 Credentials mismatch between Device and Catalyst Center

SNMP Manual Config on devices	SNMP Config on Catalyst Center	Result
snmp-server user admin default v3 auth sha cisco priv aes 128 cisco snmp-server group default v3 priv	Catalyst Center Configured with “snmp-server user admin default v3 auth sha ciscodna priv aes 128 **ciscodna**”	SNMP Credentials are overridden

What If...? – Scenario-2

Device Configured with SNMP ACL vs What Catalyst Center pushes

SNMP Brownfield Config on devices	SNMP Config on Catalyst Center	Result
C9300-Access(config)#access-list 99 permit 172.25.1.0 0.0.0.255 C9300-Access(config)#access-list 99 permit host 10.1.1.1 C9300-Access(config)#access-list 99 deny any C9300-Access(config)#snmp-server community ORARO ro 99	Snmp-server community ORARO RO	SNMP ACL is removed

Mitigation Action :

- Make sure to have Catalyst Center Enterprise VIP/IP added to SNMP ACL Allowed list
- Use CLI templates to append ACL string to SNMP. No impact to the managed network devices

Device is not configured with any SNMP community

Catalyst Center configures the devices with SNMP credentials selected for device Discovery → snmp-server community public ro
snmp-server community public rw

What If...? Scenario-3 (Discovery with NETCONF)

NETCONF configuration in devices	Catalyst Center Discovery workflow	Result
Device does not have NETCONF enabled	Configured with NETCONF port 830	NETCONF configs are pushed to devices netconf-yang ssh port 830 netconf-yang
Devices configured with NETCONF but no AAA enabled		Devices discovered successfully with NETCONF
Devices configured with NETCONF and AAA (custom method-list for TACACS)		NETCONF discovery fails, Device added to inventory without NETCONF port • No Config pushed to devices to overwrite the existing AAA configs. • Device completely managed in Inventory

Why NETCONF Discovery Failed

What is configured on the devices	vs	What Catalyst Center expects on the devices

aaa authentication login dnac-cts-list group dnac-client-radius-group local
aaa authentication login DEMO group isetme3 local
aaa authentication dot1x default group dnac-client-radius-group
aaa authorization exec DEMO group isetme3 local if-authenticated
aaa authorization network default group dnac-client-radius-group
aaa authorization network dnac-cts-list group dnac-client-radius-group
aaa accounting exec default start-stop group isetme3
aaa accounting Identity default start-stop group dnac-client-radius-group
aaa accounting update newinfo periodic 2880
username ciscodna privilege 15 password 7 094F471A1A0A131C0A

IOS XE < 17.9.x, default method list needs to be specified for NETCONF

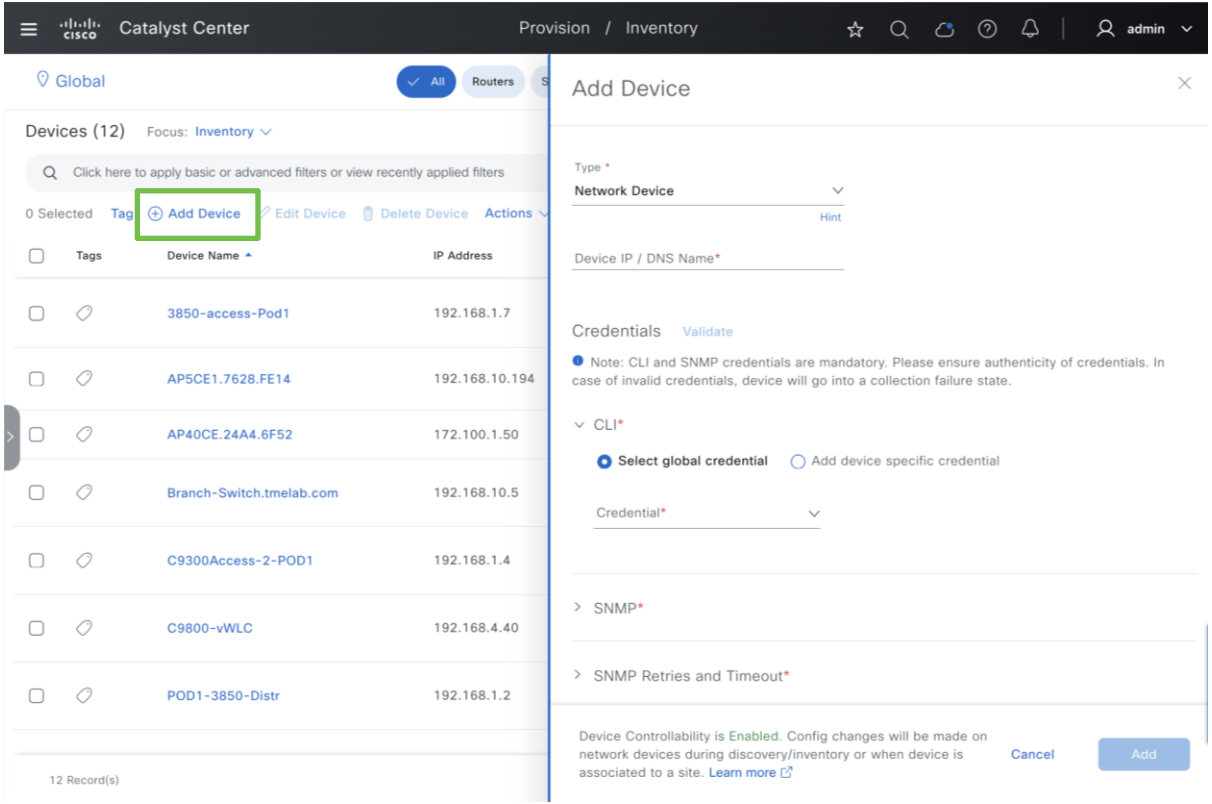
aaa authorization exec default <local or radius/tacacs group>
aaa authentication login default <local or radius/tacacs group>

IOS XE > 17.9.x, custom method can be specified for NETCONF

yang-interfaces aaa authentication method-list <custom method list>
yang-interfaces aaa authorization method-list <custom method list>

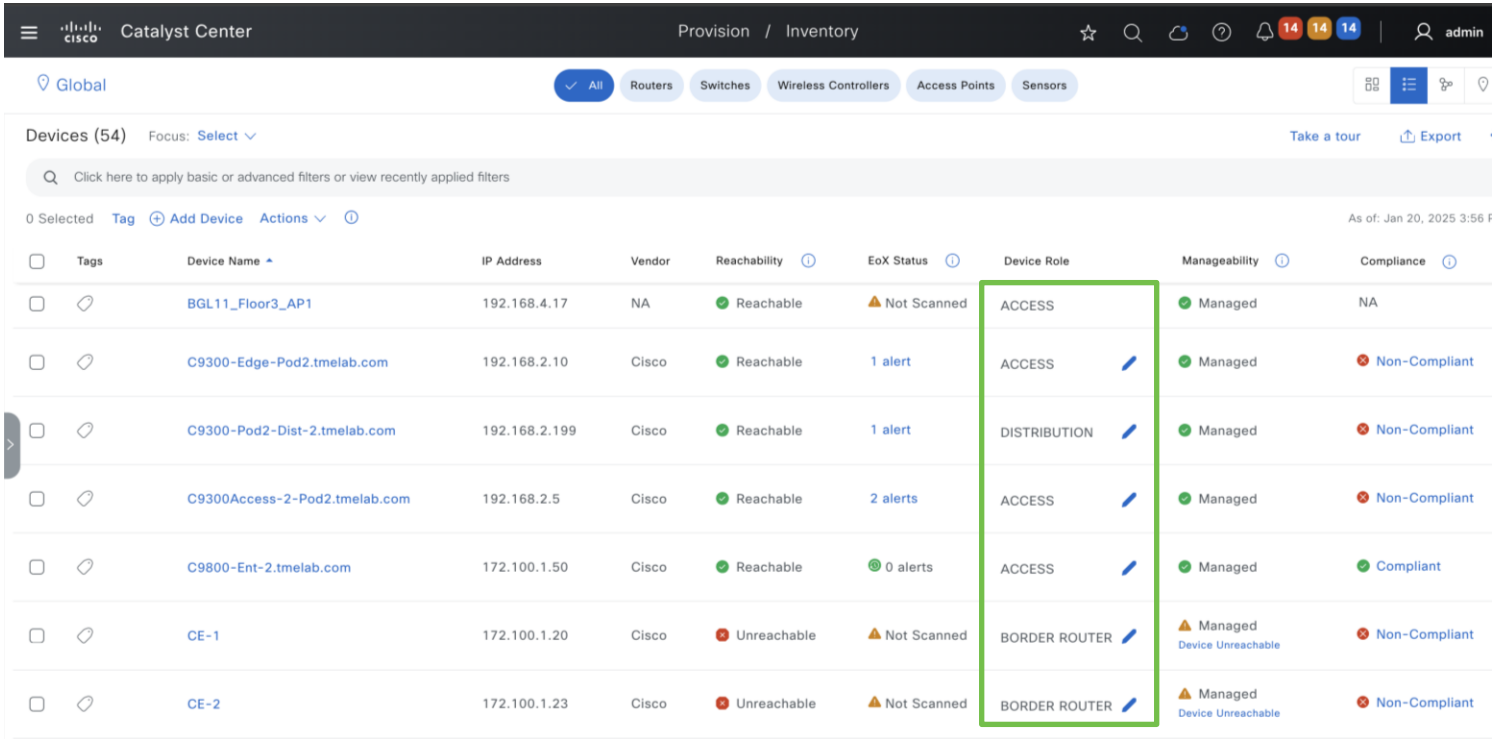
Discovery vs Manual Add Devices

- Add either Single Device or perform Bulk Import of Devices to Inventory
- During Single Device add or Bulk import of devices from CSV
  - If any of the credentials CLI/SNMP does not match with device credential => Device add fails
  - Mismatch to NETCONF port requirements will place the device in “Managed with Errors” state



Devices in Inventory

Check Device Roles once devices are added into the inventory as some telemetry push depends on device role



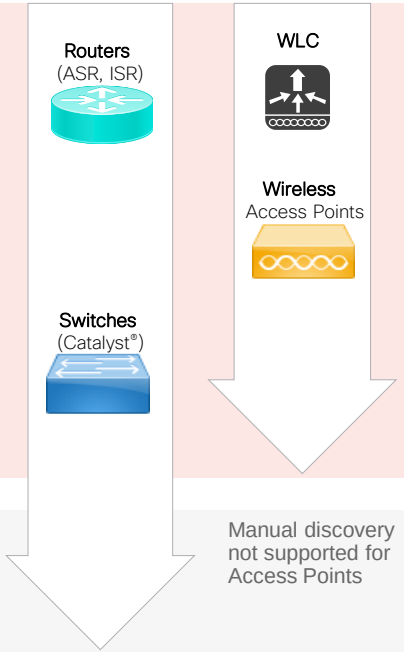
Greenfield Device Onboarding- PnP Options

Automated

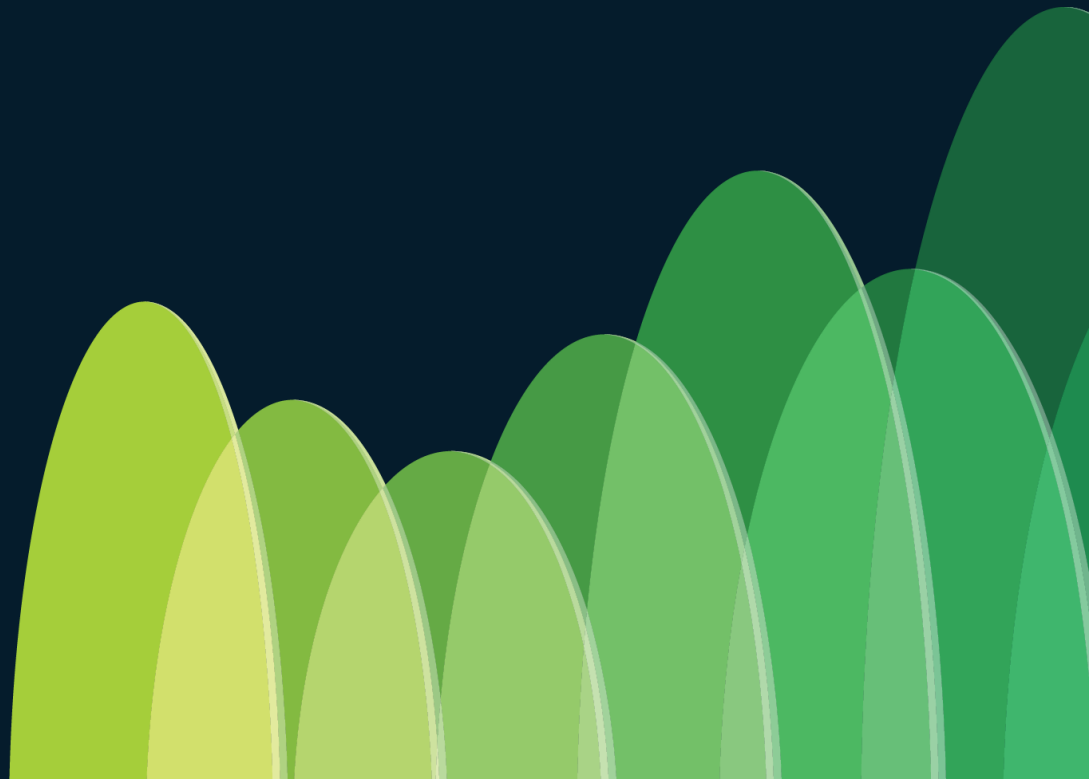
1. DHCP with options 60 and 43
   PnP string: 5A1D;B2;K4;I172.19.45.222;J80 added to DHCP Server
2. DNS lookup
   pnpserver.localdomain resolves to Catalyst Center IP Address
3. Cloud re-direction https://devicehelper.cisco.com/device-helper
   Cisco hosted cloud, re-directs to on-prem Catalyst Center IP Address

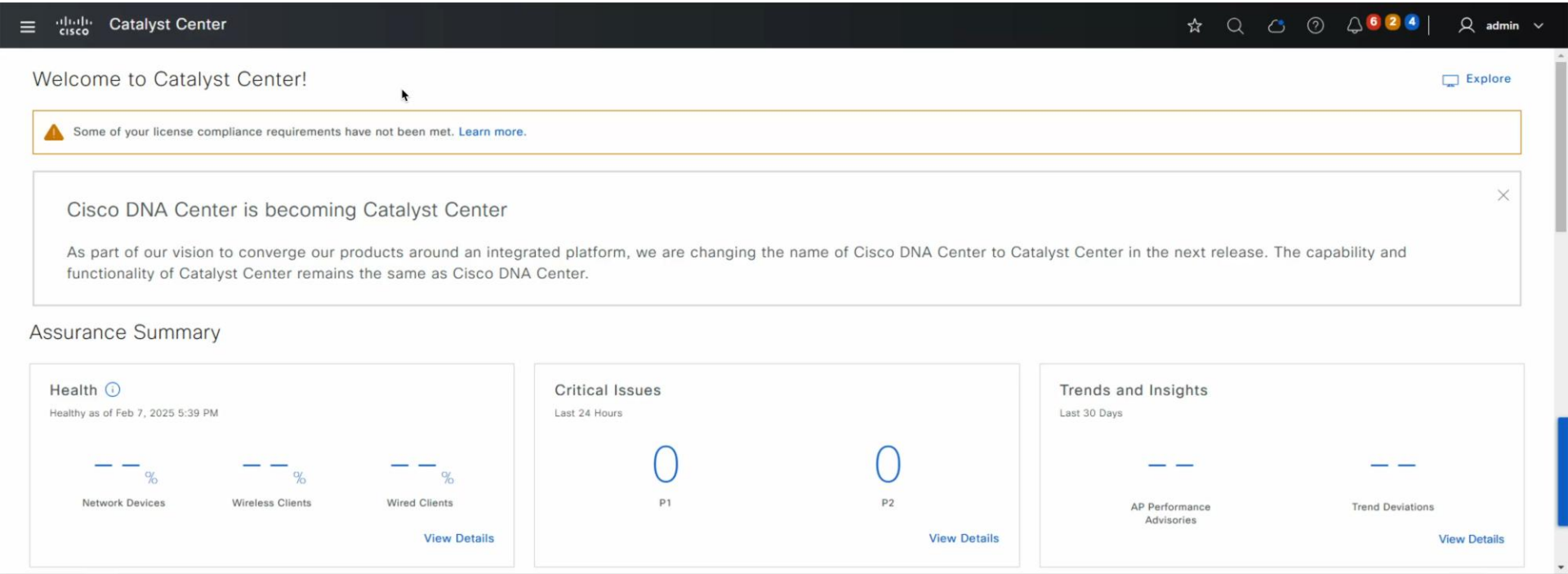
Manual

4. USB-based bootstrapping
   router-confg/router.cfg/ciscortr.cfg

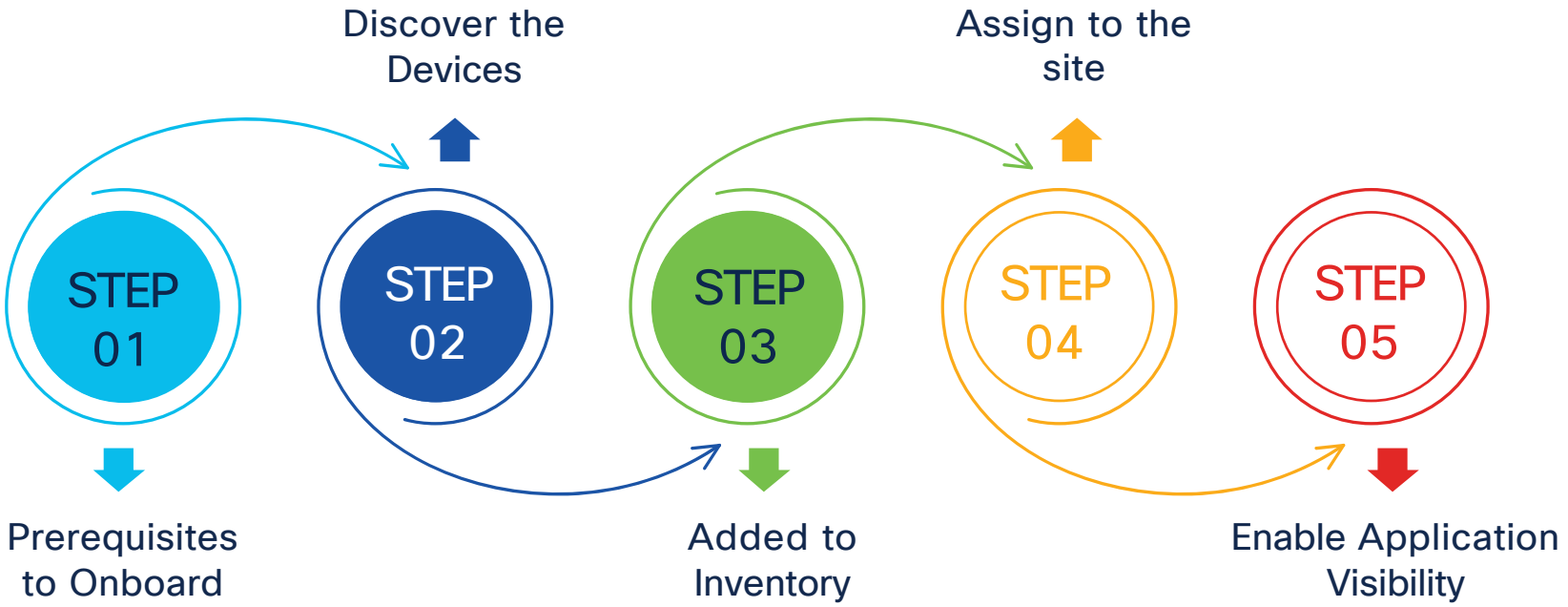


Demo

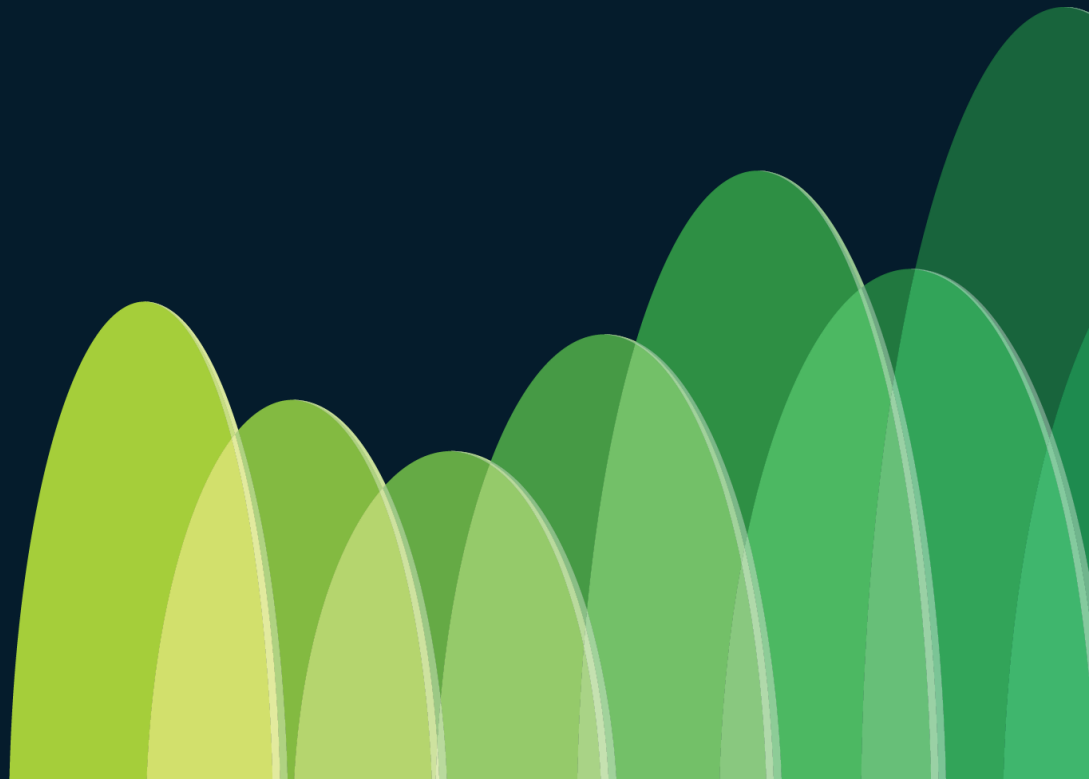


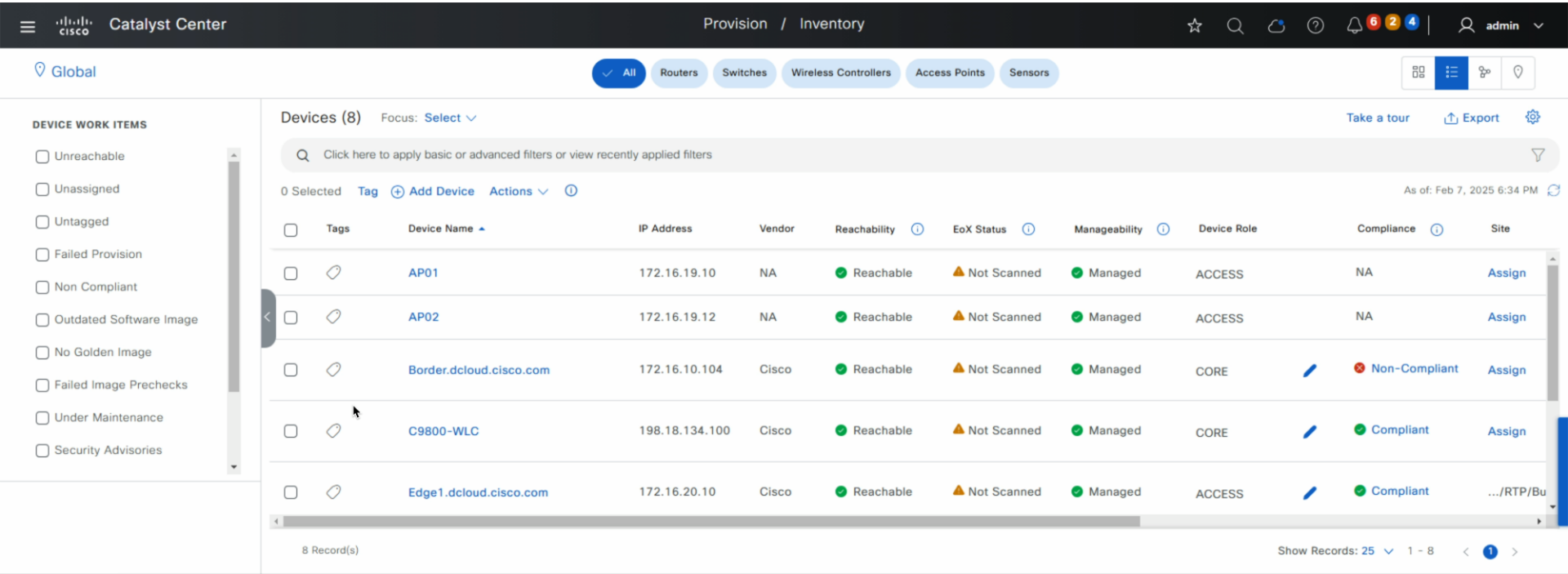


Brownfield Device Onboarding



Demo





Snippets Of Configuration Pushed During Site Assignment


```
.Jan 20 15:49:20.713: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: ciscodna]
[Source: 172.100.1.195] [localport: 22] at 15:49:20 UTC Mon Jan 20 2025
.Jan 20 15:49:20.818: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host
172.100.1.195 port 0 CLI Request Triggered
.Jan 20 15:49:20.820: %HA_EM-6-LOG: CLI_CAPTURE: logging host 172.100.1.195
transport udp port 514
.Jan 20 15:49:20.821: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host
172.100.1.195 port 514 started - CLI initiated
.Jan 20 15:49:20.839: %HA_EM-6-LOG: CLI_CAPTURE: logging source-interface Vlan1
.Jan 20 15:49:20.844: %HA_EM-6-LOG: CLI_CAPTURE: logging trap 6
```

```
ip http client source-interface Vlan1
.Jan 20 15:49:34.884: %HA_EM-6-LOG: CLI_CAPTURE: ip ssh source-interface Vlan1
.Jan 20 15:49:34.901: %HA_EM-6-LOG: CLI_CAPTURE: ip ssh version 2
.Jan 20 15:49:34.924: %HA_EM-6-LOG: CLI_CAPTURE: ip domain lookup
.Jan 20 15:49:34.953: %PKI-6-TRUSTPOINT_CREATE: Trustpoint: DNAC-CA created
succesfully
.Jan 20 15:49:34.955: %HA_EM-6-LOG: CLI_CAPTURE: crypto pki trustpoint DNAC-CA
.Jan 20 15:49:34.977: %HA_EM-6-LOG: CLI_CAPTURE: source interface Vlan1
.Jan 20 15:49:34.994: %HA_EM-6-LOG: CLI_CAPTURE: enrollment mode ra
.Jan 20 15:49:35.009: %HA_EM-6-LOG: CLI_CAPTURE: enrollment terminal
.Jan 20 15:49:35.020: %HA_EM-6-LOG: CLI_CAPTURE: usage ssl-client
.Jan 20 15:49:35.042: %HA_EM-6-LOG: CLI_CAPTURE: revocation-check crl none
.Jan 20 15:49:35.045: %HA_EM-6-LOG: CLI_CAPTURE: exit
.Jan 20 15:49:35.081: %HA_EM-6-LOG: CLI_CAPTURE: crypto pki authenticate DNAC-CA
```

```
.Jan 20 15:50:19.979: %HA_EM-6-LOG: CLI_CAPTURE: do-exec cts credentials
id 779df3a306b64f57bcc4b981556acaf1 password 779df3a306b64f57
.Jan 20 15:50:19.980: %HA_EM-6-LOG: CLI_CAPTURE: cts credentials id
779df3a306b64f57bcc4b981556acaf1 password 779df3a306b64f57
```

```
snmp-server enable traps
.Jan 20 15:49:25.226: %HA_EM-6-LOG: CLI_CAPTURE: show running-config
brief
.Jan 20 15:49:25.538: %HA_EM-6-LOG: CLI_CAPTURE: snmp-server host
172.100.1.195 traps version 2c public udp-port 162
.Jan 20 15:49:25.636: %HA_EM-6-LOG: CLI_CAPTURE: snmp-server source-
interface traps Vlan1
```

```
telemetry ietf subscription 501
 encoding encode-tdl
 filter tdl-uri /services;serviceName=ios_oper/poe_module
 receiver-type protocol
 source-address 192.168.4.4
 stream native
 update-policy periodic 60000
 receiver name DNAC_ASSURANCE_RECEIVER
```

Syslog, HTTPS & SSH

Greenfield

logging source interface <int with which device was discovered>
logging host <catalyst center ip>
logging trap 6

Brownfield

Brownfield Configuration	Catalyst Center Device Controllability	Result
logging source interface <> logging host <> logging trap 5	logging source interface <int with which device was discovered> logging host <catalyst center ip> logging trap 6	Catalyst Center overwrites logging source interface and trap level

http configuration

ip http server
ip http authentication local
ip http secure-server
ip http max-connections 16
ip http client source-interface Vlan120

ssh configuration

ip ssh source-interface Vlan120
ip ssh version 2

IP Device tracking

Greenfield

device-tracking policy IPDT_POLICY
no protocol udp tracking enable
For each interface:
interface $physicalInterface
device-tracking attach-policy IPDT_POLICY

Brownfield

Brownfield Configuration	Catalyst Center Device Controllability	Result	Mitigation Action
device-tracking policy POLICY1 trusted-port limit address-count 100 no protocol udp tracking enable interface GigabitEthernet1/0/1 device-tracking attach-policy POLICY1	device-tracking policy IPDT_POLICY no protocol udp tracking enable interface GigabitEthernet1/0/1 device-tracking attach-policy IPDT_POLICY	Catalyst Center overwrites the existing IPDT config.	Use CLI template to append any additional commands like trusted-port.

CTS Credentials

- Cisco TrustSec (CTS) Credentials are pushed during inventory only if the Global site is configured with Cisco ISE as AAA. Otherwise, CTS is pushed to devices during " Assign to Site" when the site is configured with Cisco ISE as AAA
- When no ISE servers are configured to the network settings, CTS credentials are not provisioned
- CTS credentials that are pushed by Catalyst Center are unique ID's generated for each device.

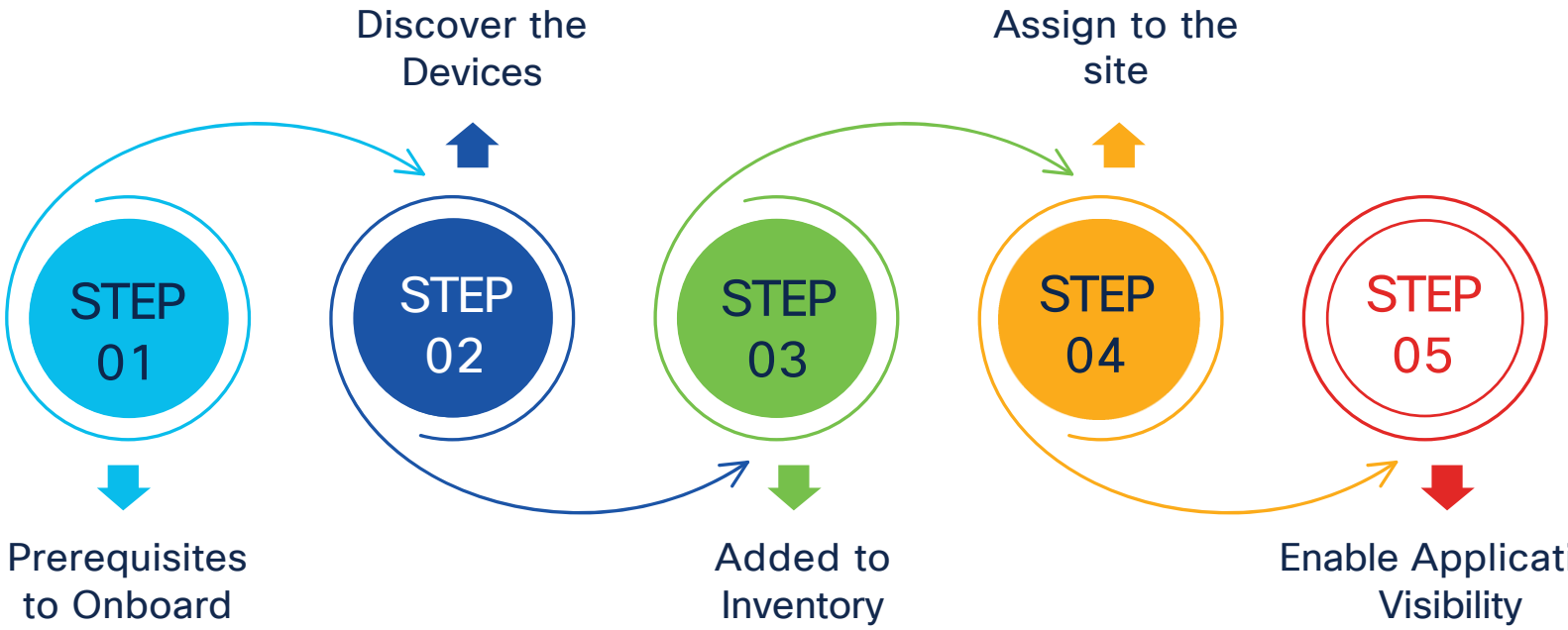
Greenfield

cts credentials id 779df3a306b64f57bcc4b981556acaf1 password 779df3a306b64f57

Brownfield

Brownfield Configuration	Catalyst Center Device Controllability
Cat9300-Stack-Switch#sh cts credentials CTS password is defined in keystore, device-id = dummy	If already present it does not make any changes

Brownfield Device Onboarding



Application Telemetry

Application Visibility (Application name & Throughput)	Application Experience (Latency, Jitter, and Packet Loss)
• IOS-XE Switches	• Routers – Perfmon and ART Metrics
• AireOS controllers – (Local Mode) or WSA(Flex/Fabric mode)	• 9800 WLC – Local, Flex/Fabric

Automatic Algorithm Selection

- Switches – All Access interfaces
- Routers – All LAN-Facing interfaces
- WLC - all non-guest WLANs

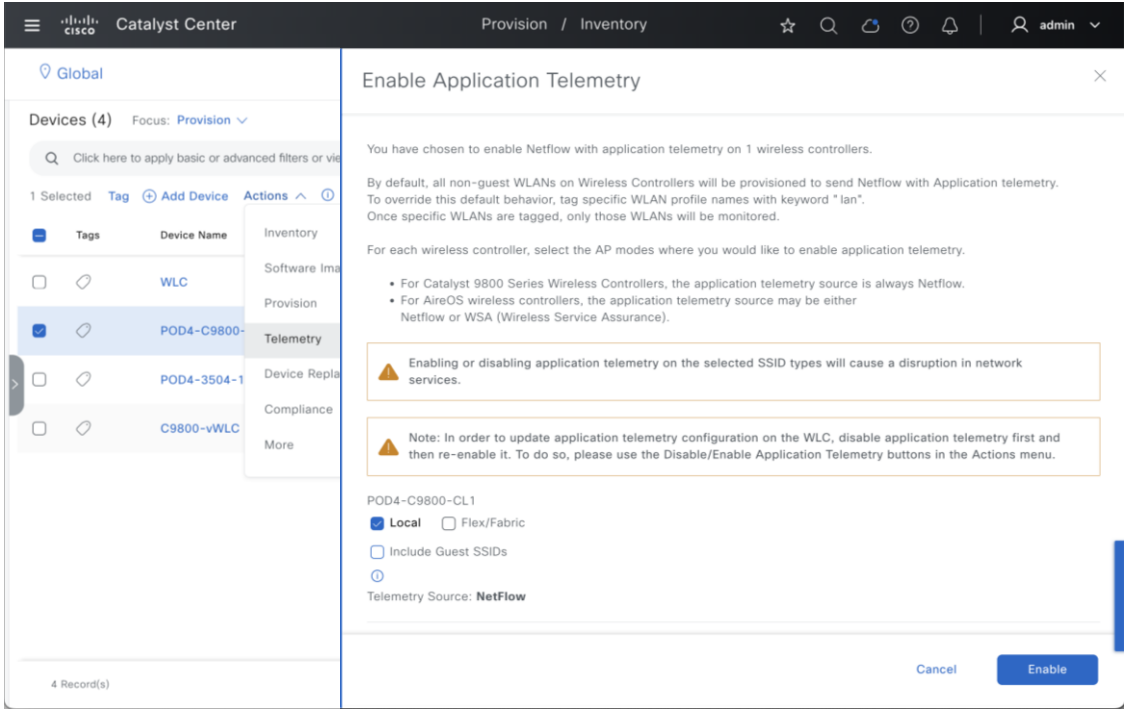
Use “LAN” keyword to override automatic algorithm.

Platform	Data Collection	Notes
Cisco IOS XE Routers	Application Experience data collection.	• Requires an active NBAR2 license. • Cisco IOS XE 16.3 minimum software version. • For Optimized APM: Cisco IOS XE 17.3 minimum software version.
Catalyst 9000 Series Switches	Application Visibility data collection for 9200, 9300, 9400.	• Requires an Advantage license. • Cisco IOS XE 16.10.1 minimum software version. • IP routing must be enabled.
Cisco AireOS Wireless Controllers	Application Visibility data collection.	• Requires an Advantage license. • Requires 8.8 MR2 software version 8.8.114.130 or later.
Cisco 9800 Series Wireless Controller	Application Visibility data collection for Flex/Fabric SSIDs. Application Experience data collection for central switching/local SSIDs, and Flex/Fabric SSIDs.	• Application Visibility for Optimized APM: Cisco IOS XE 16.12.1 minimum software version. • Application Experience for local mode: Cisco IOS XE 16.12.1 minimum software version. For flex/fabric mode: Cisco IOS XE 17.10.1 minimum software version.
Catalyst Center Traffic Telemetry Appliance	Application Experience data collection.	• Requires an Advantage license. • For Optimized APM: Cisco IOS XE 17.3 minimum software version.

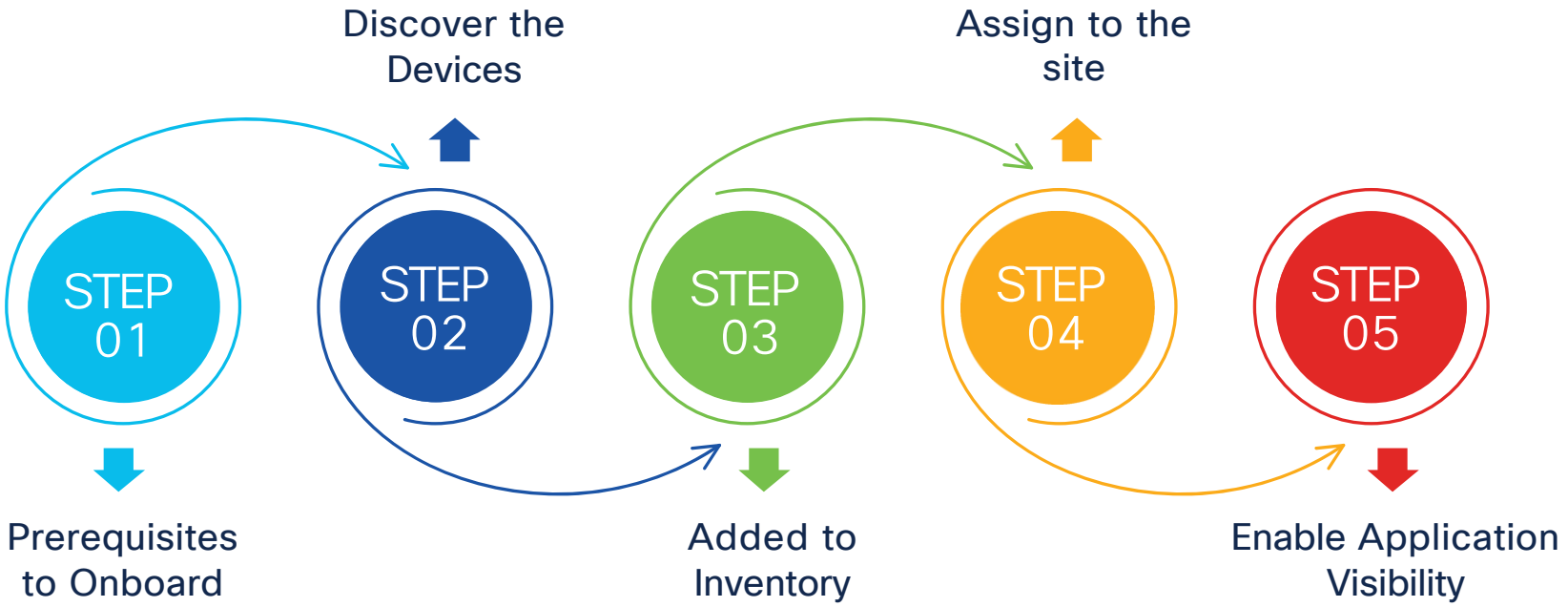
Application Telemetry

Application Telemetry enables DNS Service monitoring (local mode)
17.10 and above for both IPv4 and IPv6

- Enable Application Telemetry from Provision > Actions > Telemetry > Enable Application Telemetry
- WLC need not be provisioned for enabling Application telemetry
- Ensure manually created flow monitor configurations are removed before enabling Application Telemetry
- Enable/Disable Application Telemetry temporarily Disables Policy profiles

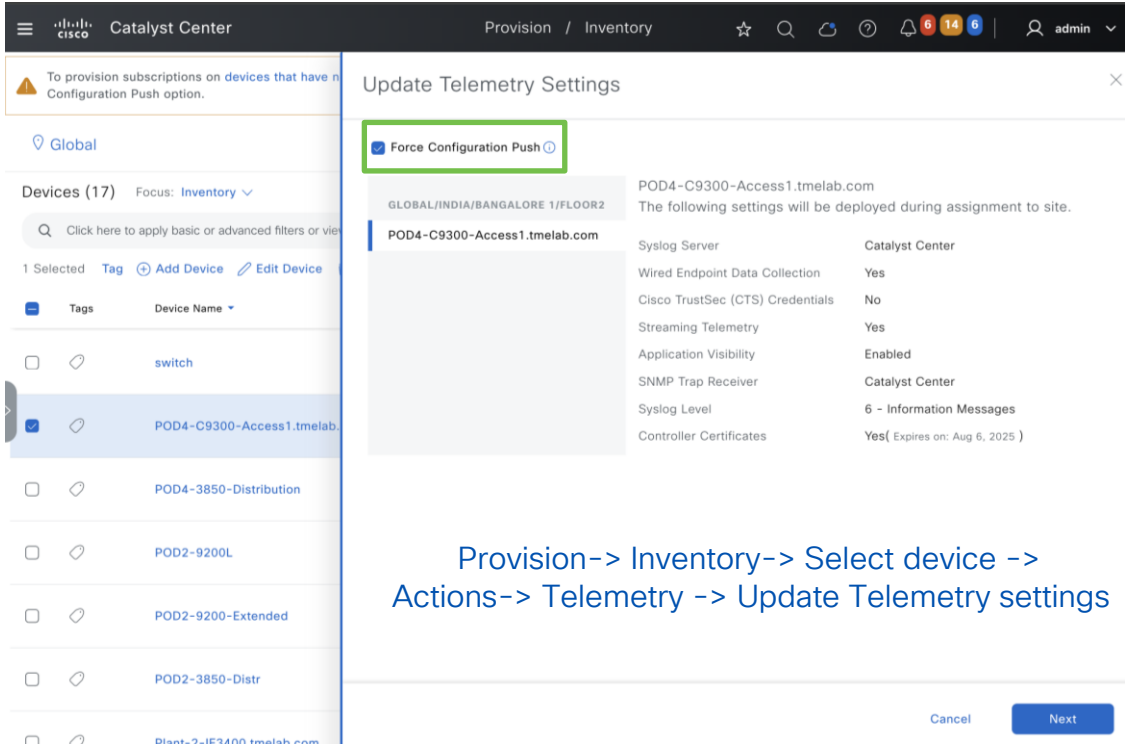


Brownfield Device Onboarding



Not Comfortable With Configuration Being Pushed While Device Onboarding?

- You can disable Device Controllability which is enabled by default
- You can push the telemetry settings later to network devices to get real time insights
- Telemetry settings can be customized at site level under Design->Network Settings->Telemetry

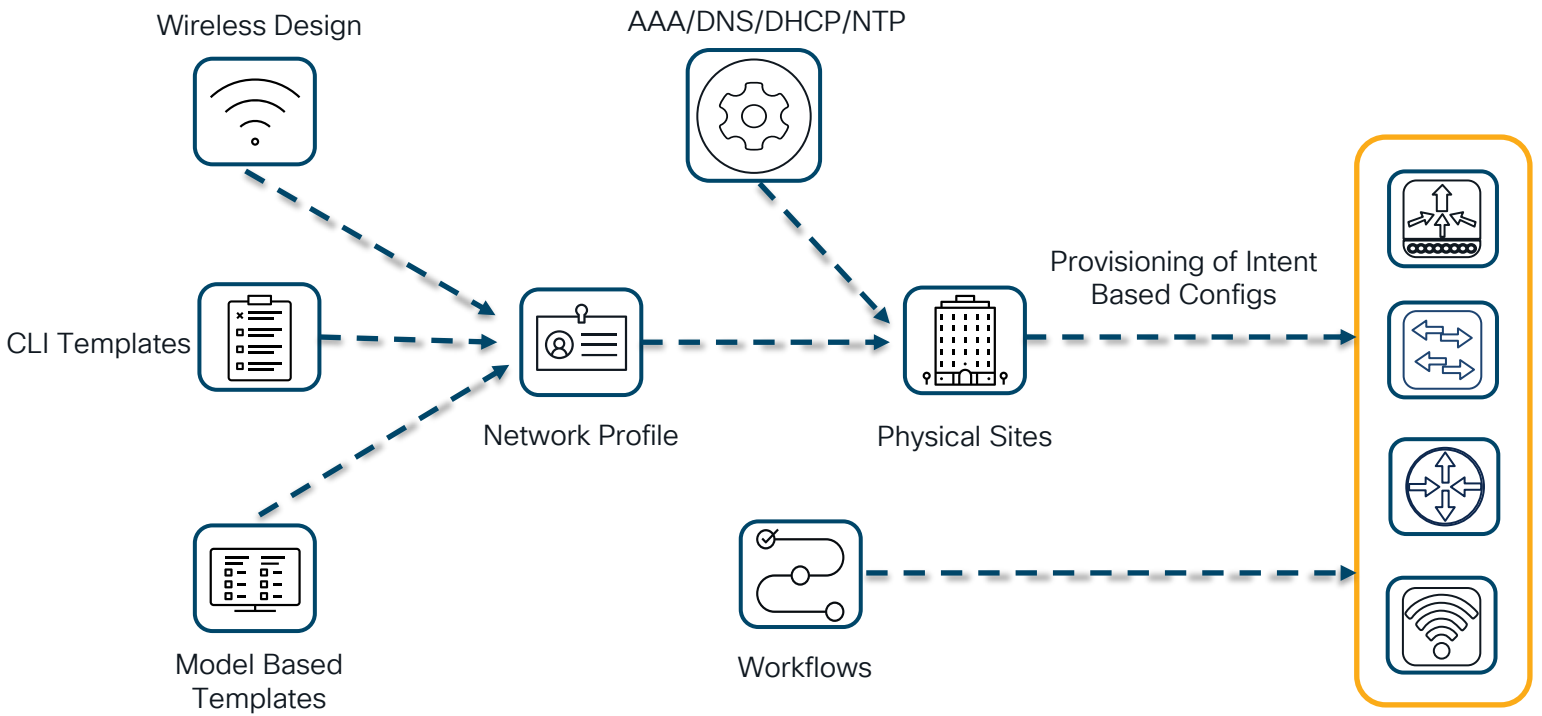


Provision-> Inventory-> Select device -> Actions-> Telemetry -> Update Telemetry settings

Managing Your Brownfield Deployment

cisco Live!

Day-1 Configuration Changes – Provisioning

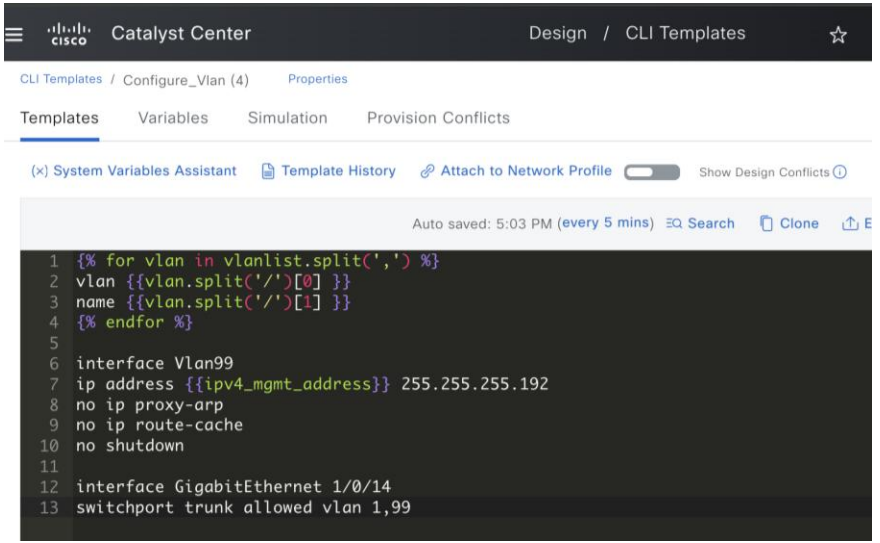


Scenario – Provisioning Workflow

Brownfield Config on a Switch

```
interface GigabitEthernet1/0/12
 description "dot 1x client"
 switchport mode access
 ip access-group ACL-DEFAULT in
 logging event bundle-status
 shutdown
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 authentication timer reauthenticate server
 mab
 snmp trap mac-notification change added
 snmp trap mac-notification change removed
 dot1x pae authenticator
!
interface GigabitEthernet1/0/13
 spanning-tree portfast
!
interface GigabitEthernet1/0/14
 description "connection to Uplink Switch trunk"
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/15
 switchport mode access
 switchport voice vlan 10
 ip access-group ACL-DEFAULT in
 logging event bundle-status
 duplex full
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order mab
 authentication priority mab
 authentication port-control auto
 authentication timer reauthenticate server
 mab
 spanning-tree portfast
```

Additional config to be deployed on the switch using Catalyst Center



CLI Templates

Network Profile

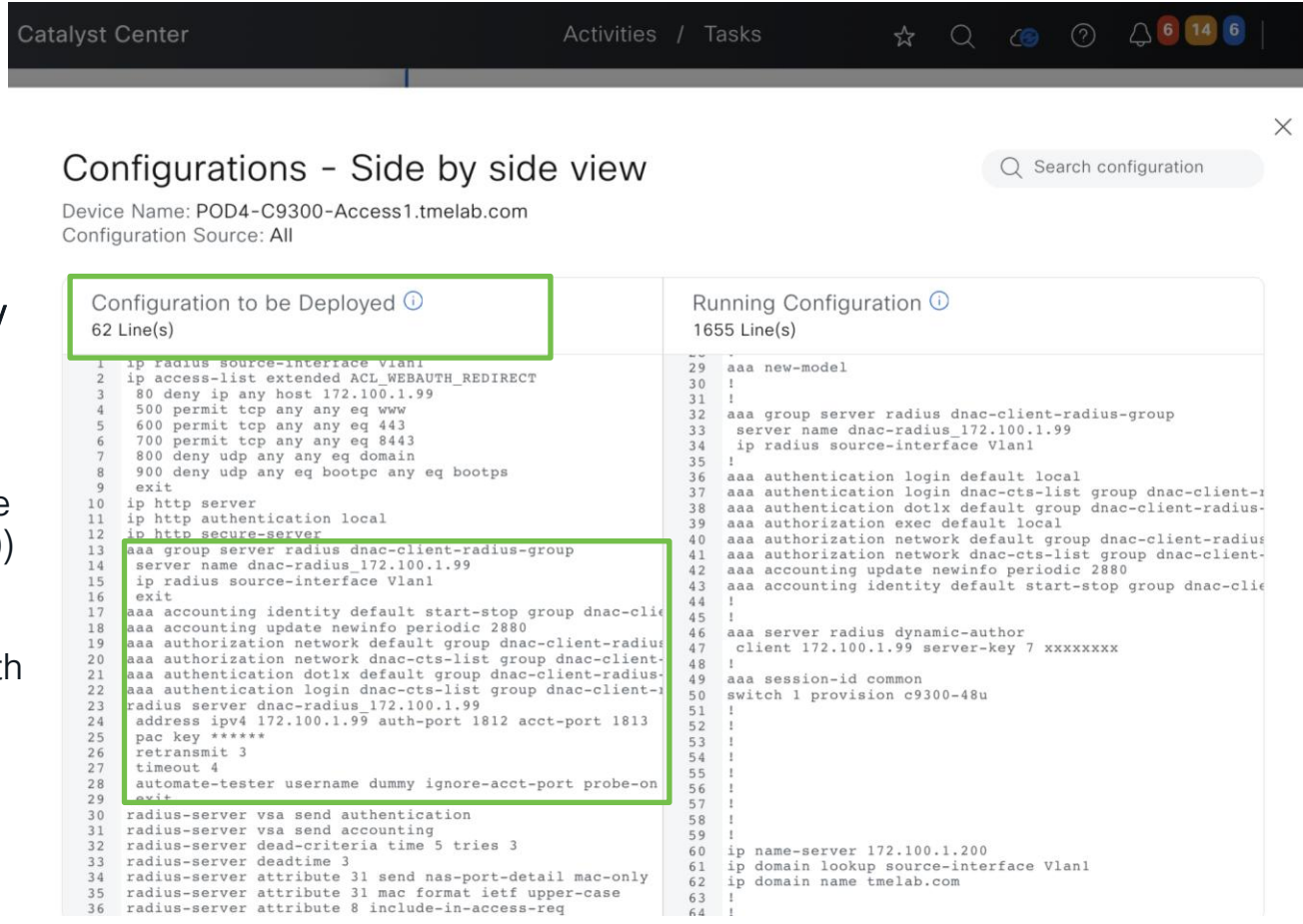
Physical Sites

Config Preview- Provisioning

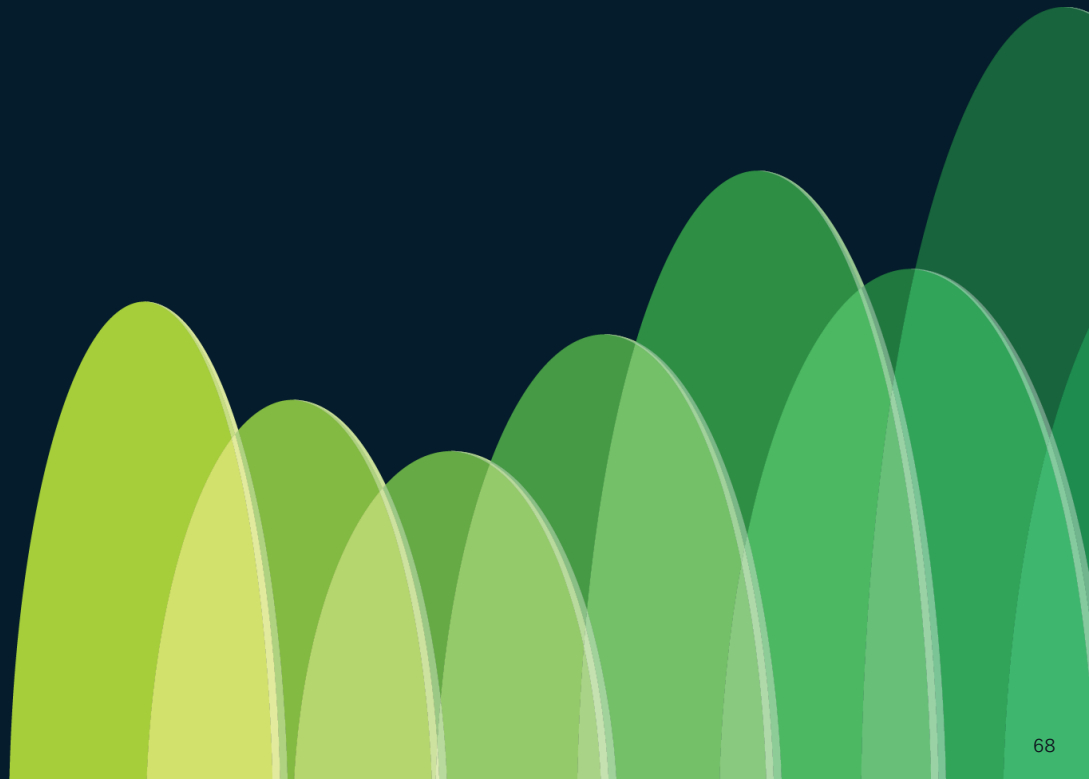
For better control, ‘Configuration Preview’ is enabled by default under **System > Settings > Visibility and Control**

Starting IOS-XE 17.13 and above, Configurations can be viewed in CLI format (C9800)

Running config compared with CLI generated



Demo

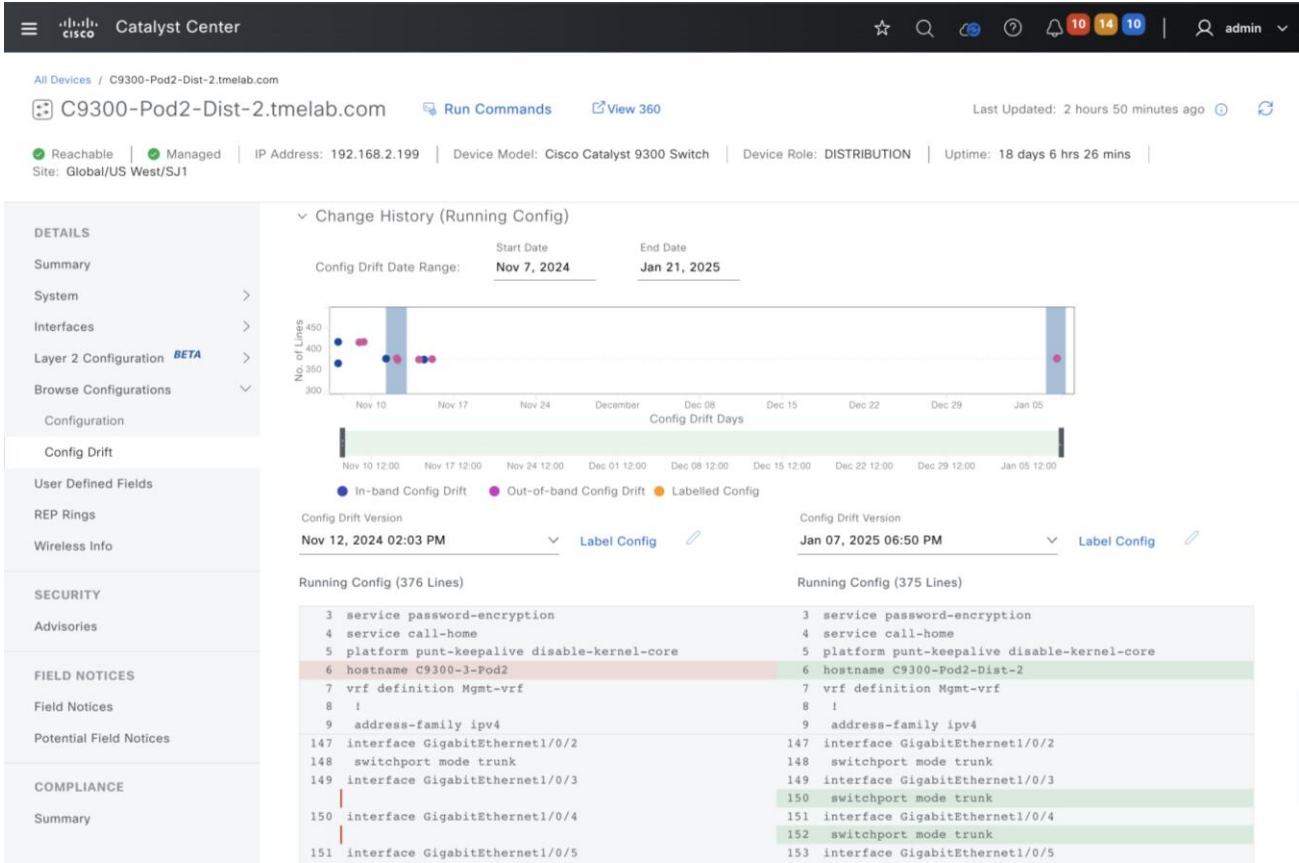


Decoding AAA Provisioning Failures and Overwrites – ISE Integrated Use cases

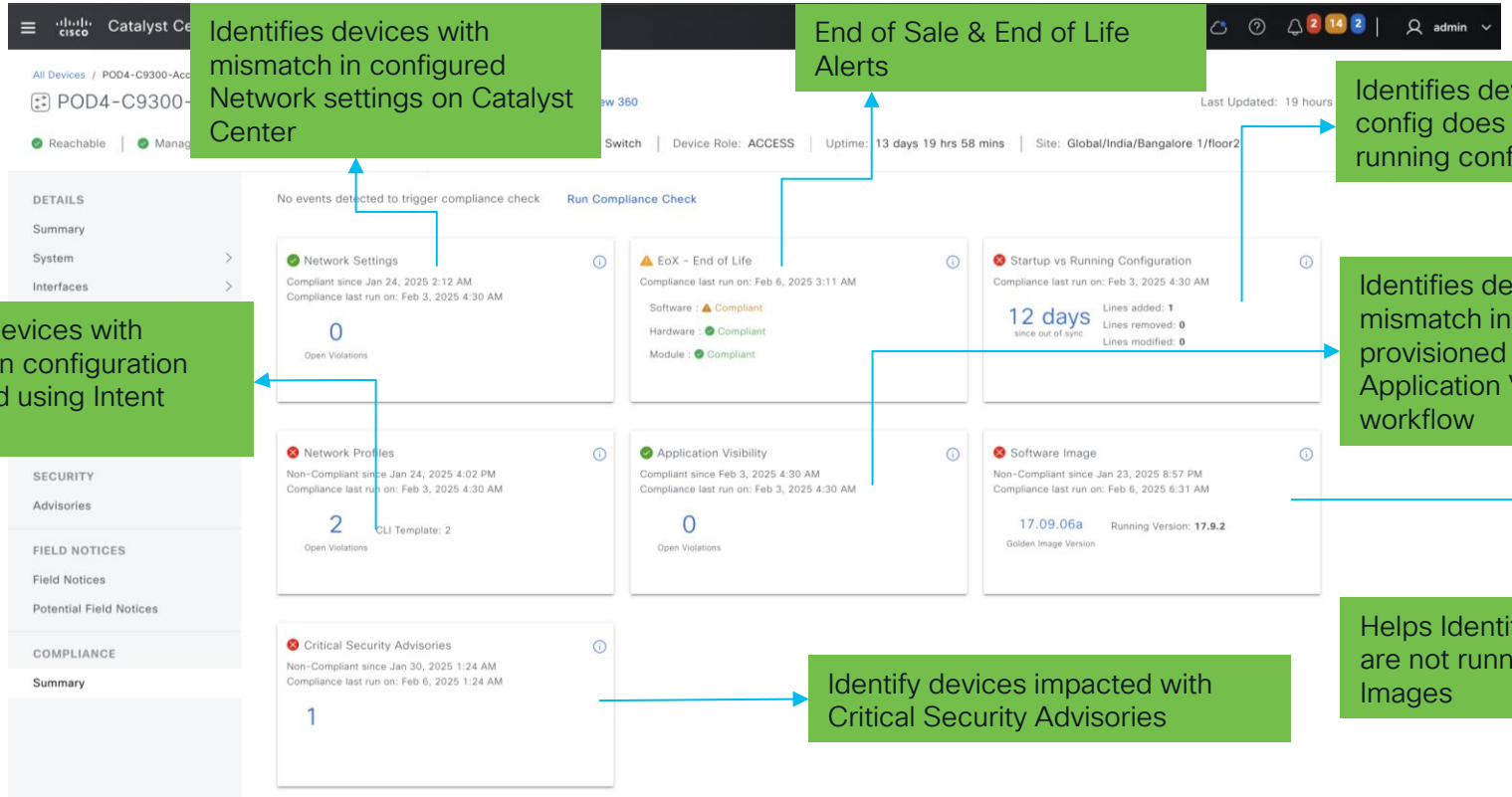
AAA Manual Config on devices	Scenario	Provisioning Workflow Result	Failure Reason
C9300-Access#sh run aaa ! aaa authentication login default local aaa authentication dot1x default group ise aaa authorization exec default local aaa authorization network default group ise aaa accounting system default start-stop group ise aaa accounting Identity default start-stop group ise aaa server radius dynamic-author client 10.106.142.176 server-key 7 14141B180F0B7B7977 ! radius server test address ipv4 172.100.1.16 auth-port 1812 acct-port 1813 key 7 05080F1C22431F5B4A ! aaa group server radius ise server name test ! aaa new-model aaa session-id common	Same/Different PSN IP on Catalyst Center Network Settings	Provisioning pre-validation failed. No configuration deployed	AAA CLI(s) are already present on the device POD4-C9300-Access1: aaa server radius dynamic-author, aaa accounting settings. Remove the CLIs, resync the device and retry.
	Same PSN IP on Network Device and Catalyst Center Network Settings	Provisioning Failure	Failure Reason: Unable to push to device 192.168.4.4 using protocol ssh2 the CLI address ipv4 172.100.1.99 auth-port 1812 acct-port 1813
	Different PSN IP on Network Device and Catalyst Center Network Settings	Provisioning Success and AAA config Overwritten on the device	
	Modify CC deployed AAA method list to custom method list manually	Catalyst Center 2.3.5.6 or 2.3.7.x, Provisioning any intent will not overwrite the modified AAA method list Unless AAA Network Settings are modified in Catalyst Center	

Config Drift

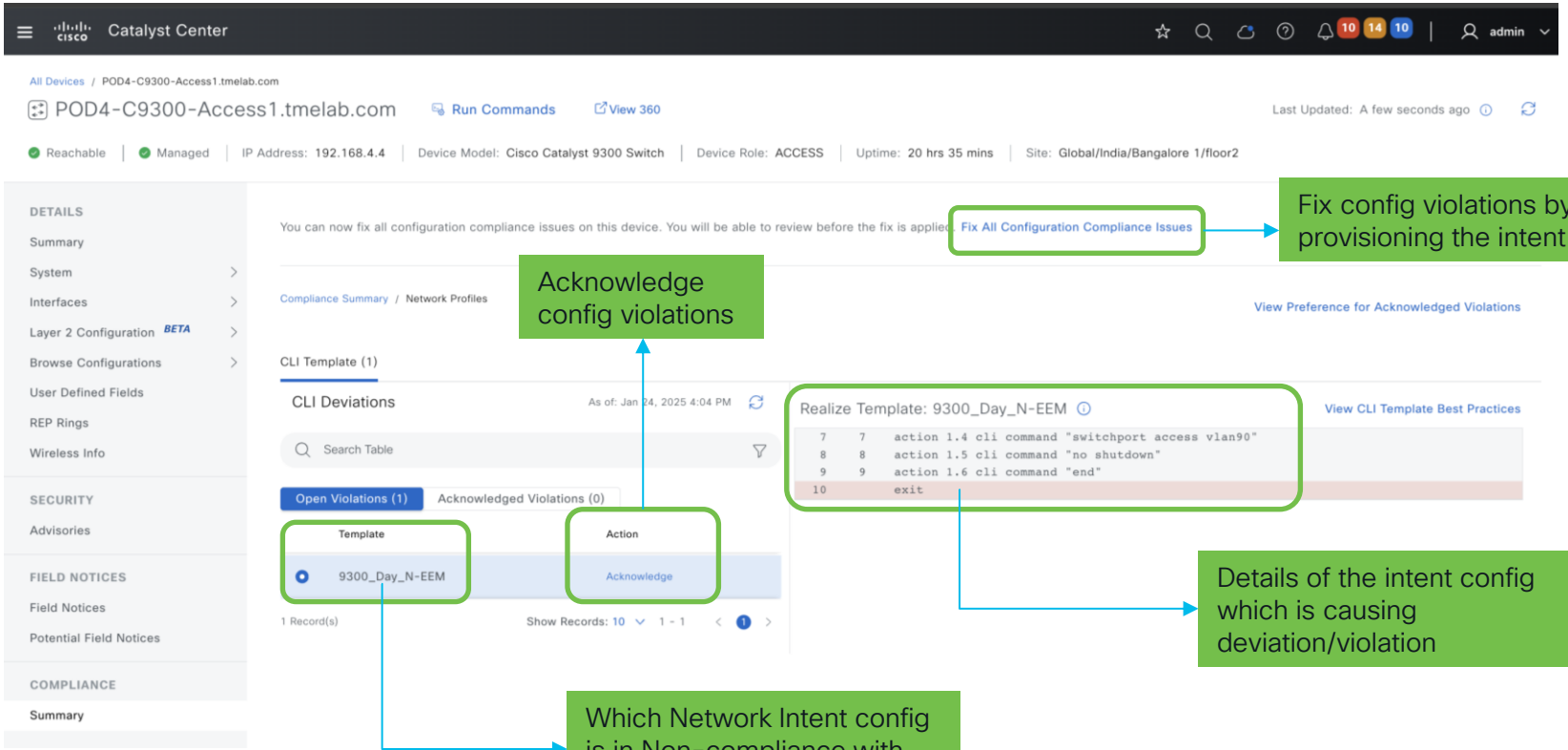
- Compare the configuration changes on the devices against a standard configuration
- Archiving can be done internally(max 50 config drifts) or on external SFTP server. System -> Settings -> Configuration Archive Internal.
- Config drift is saved when device is initially added or when there is a change in the configuration(tracked with syslog events) or when device is backed up. Limit is 50 drifts
- Configuration drifts can be viewed and compared
- A drift can be labeled which will not get deleted until unlabeled



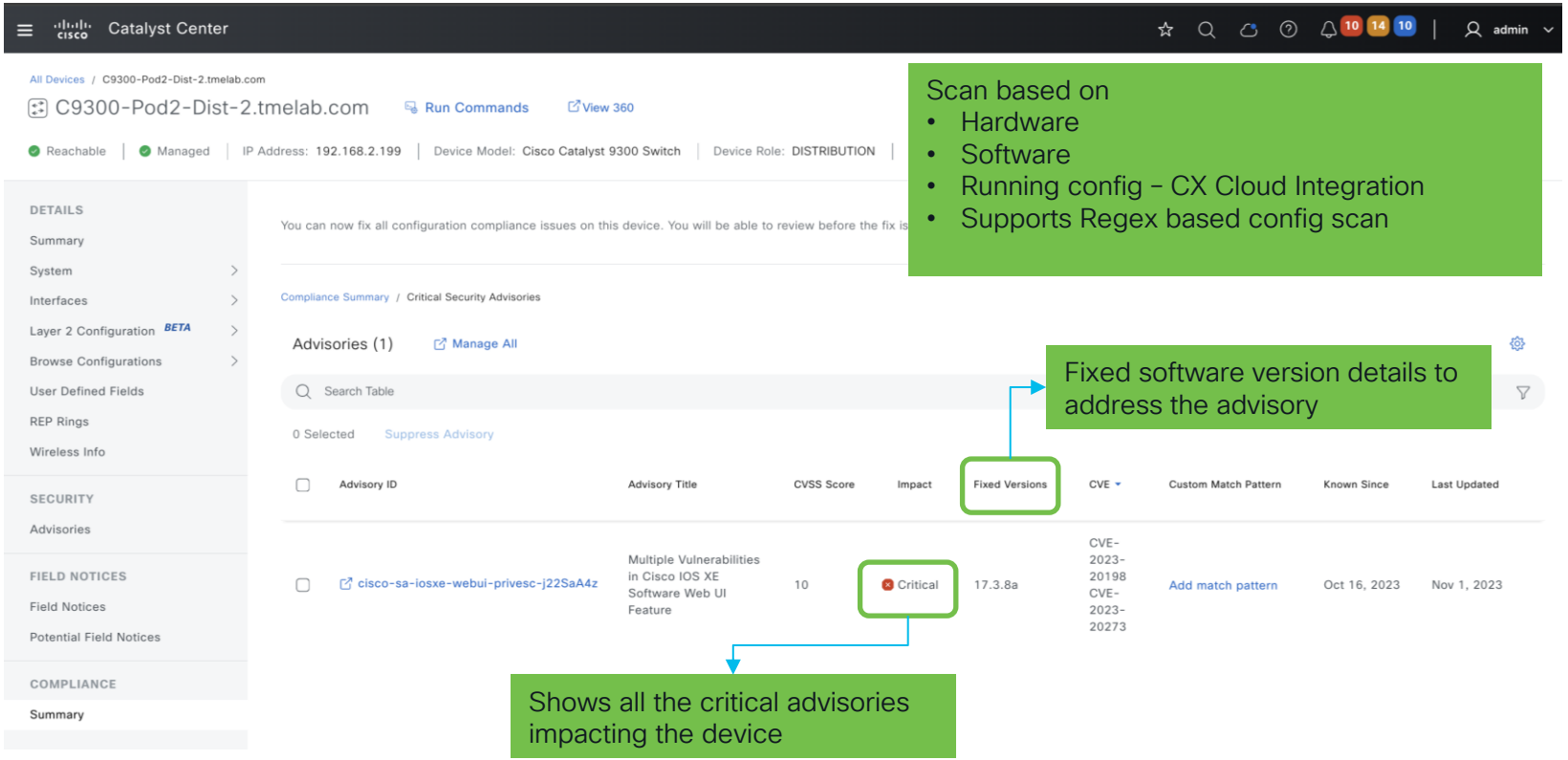
Compliance



Network Profile- Compliance Remediation

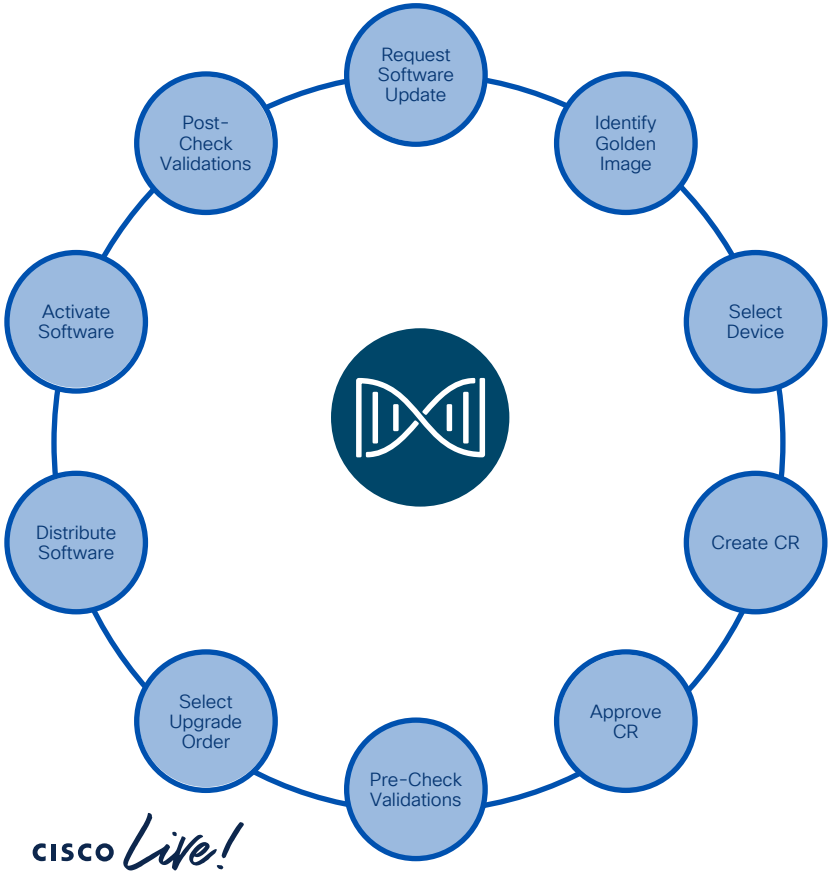


Security Advisory- Compliance



Catalyst Center – SWIM

Easily identify out-of-date software images and simplify image update process (SWIM)



Intent-Based Network Upgrades

Captures your upgrade intent to automate process and drive consistency

Streamlined Upgrade Process

Upgrade base image, patches, and other add-ons in one single flow

Trustworthiness Integration

Assures that device images are not compromised in any way.

Patching Support

Pre/Post check ensures updates do not have adverse effects on network

SWIM- Tips & Tricks

First Distribute and Schedule Activate

- Always plan to Distribute First
- Schedule the Activation during Maintenance Windows.
- Use Custom Pre/post checks to your advantage

Consider External File Server

- Use external file servers for remote locations

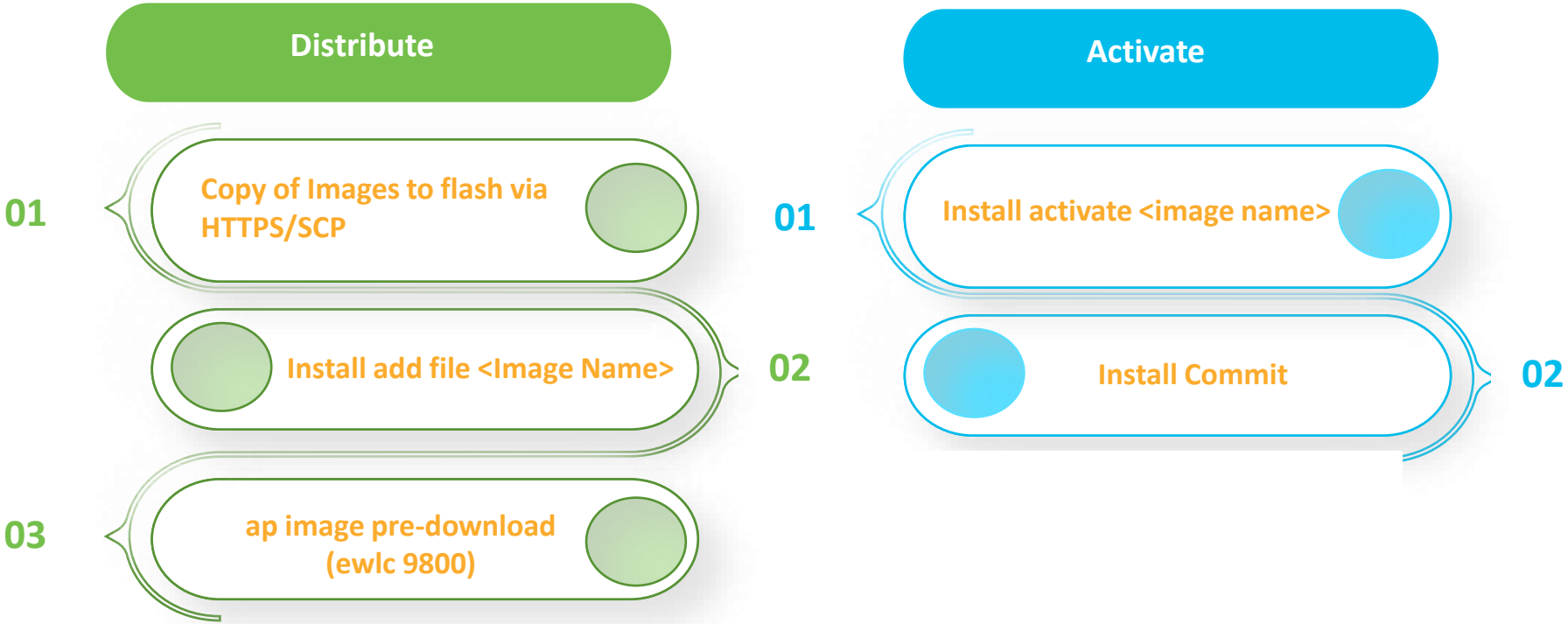
Wireless

- Start with ISSU, AP Pre-Image Download is in works.
- Use Rolling AP upgrades where ISSU is not available

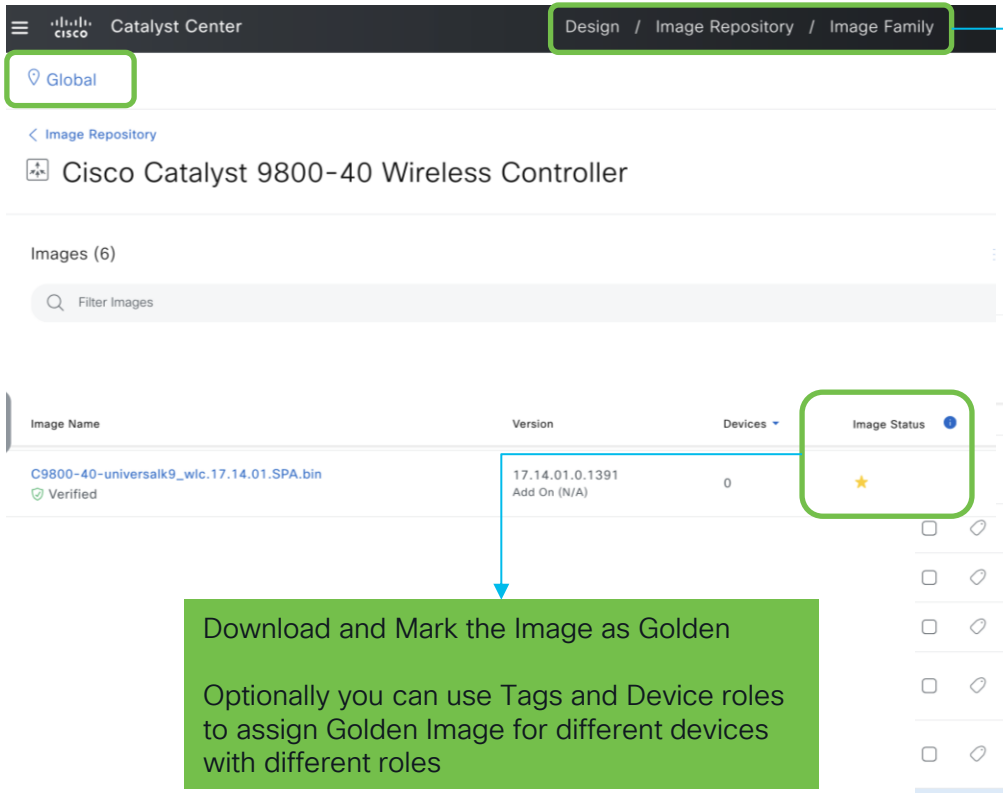
SMU/Patch Management

- Patch fixes for PSIRTS
- Image Recommendations based on PSIRTS*

Image Upgrade Workflow

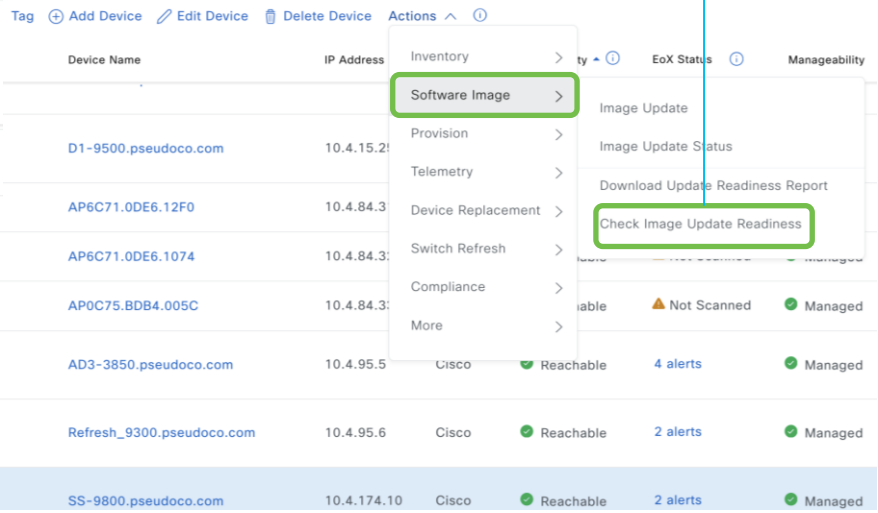


SWIM- Workflow



From Design > Image Repository, Select Device Family

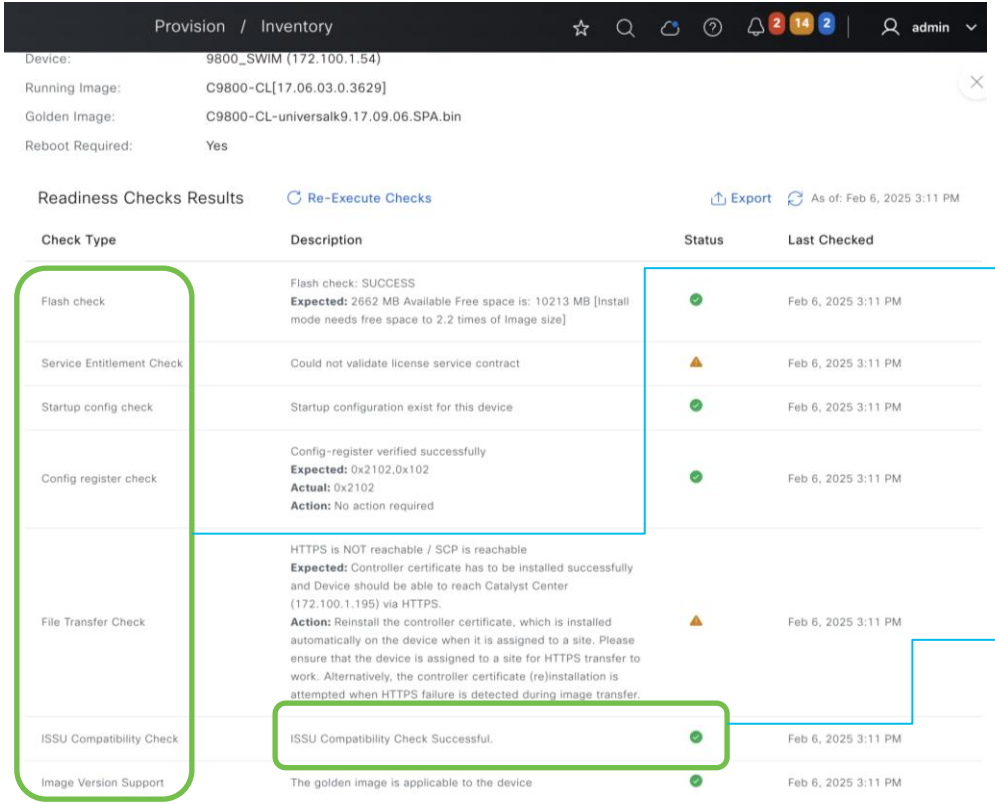
From Provision > Inventory, Select device and run Image Update Readiness Check



Download and Mark the Image as Golden

Optionally you can use Tags and Device roles to assign Golden Image for different devices with different roles

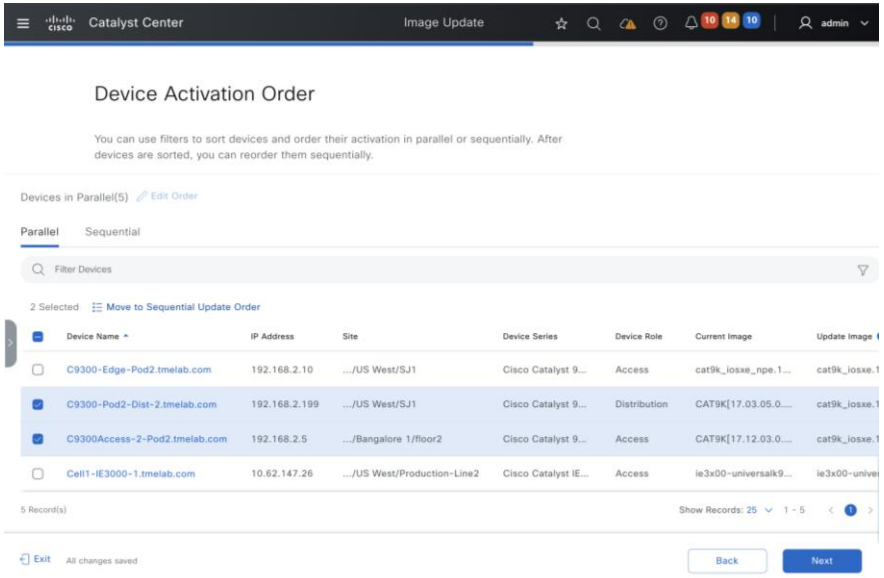
SWIM-C9800 Software Upgrade (ISSU)

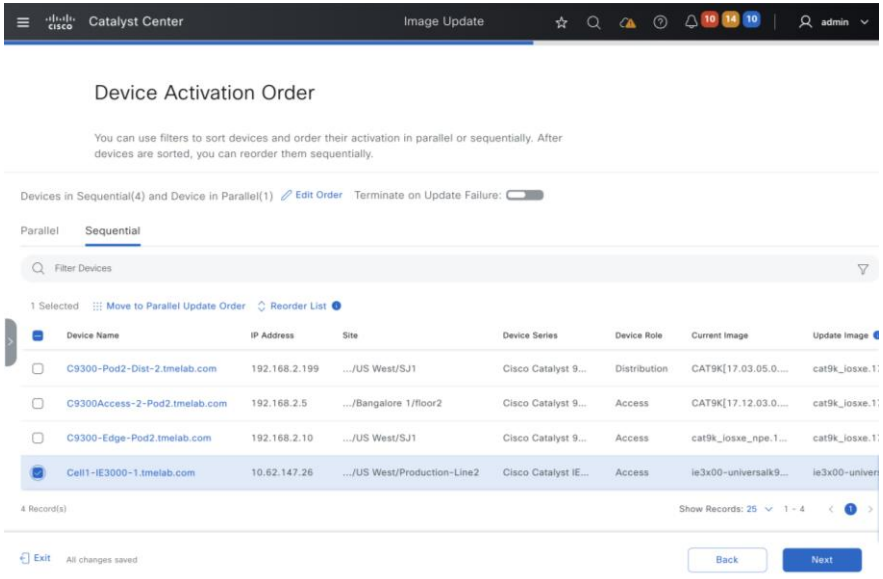


Executes various check before starting Image upgrade workflow

Checks include if Image can be upgraded using ISSU

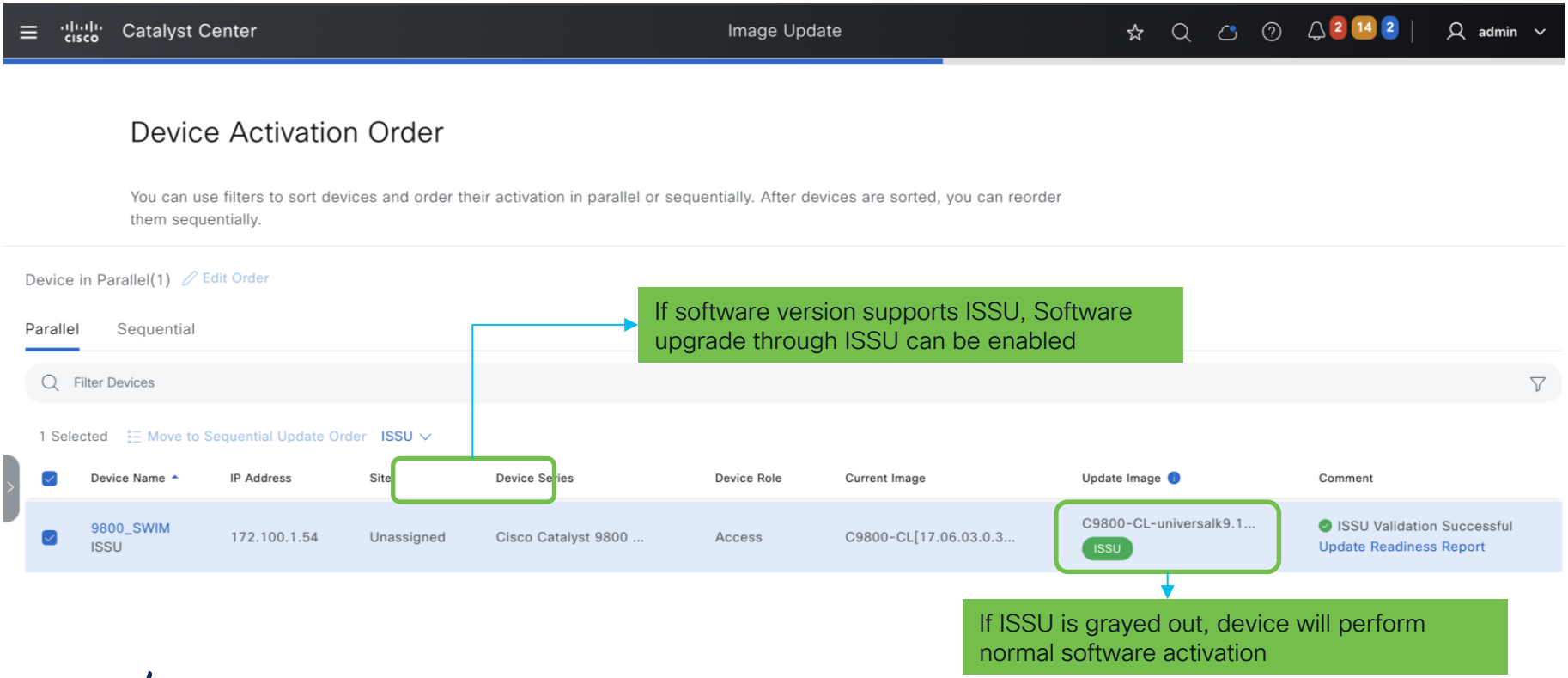
SWIM- Flexible Device Ordering



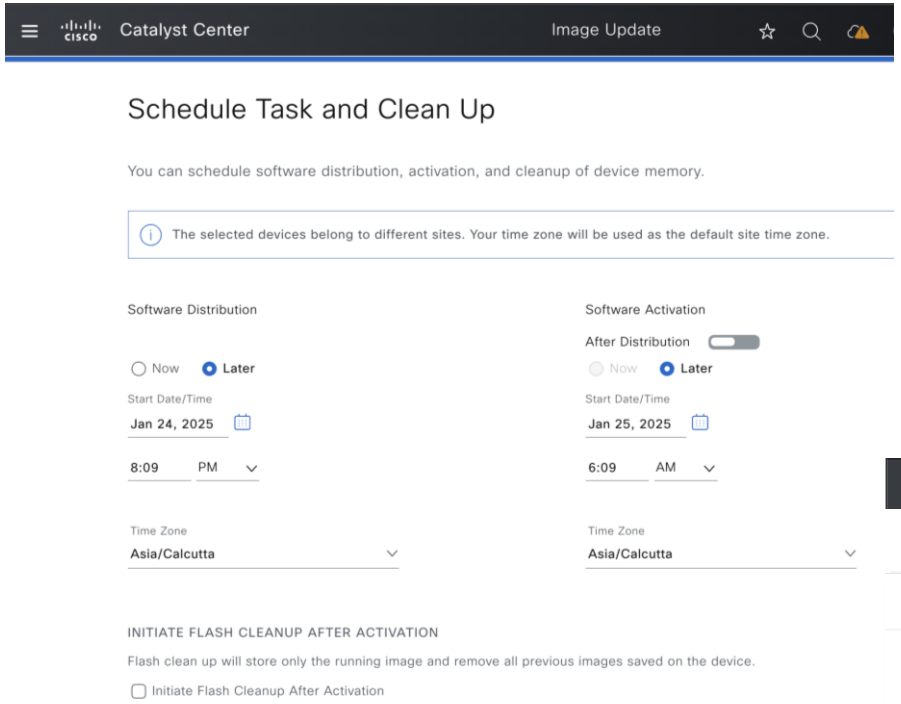


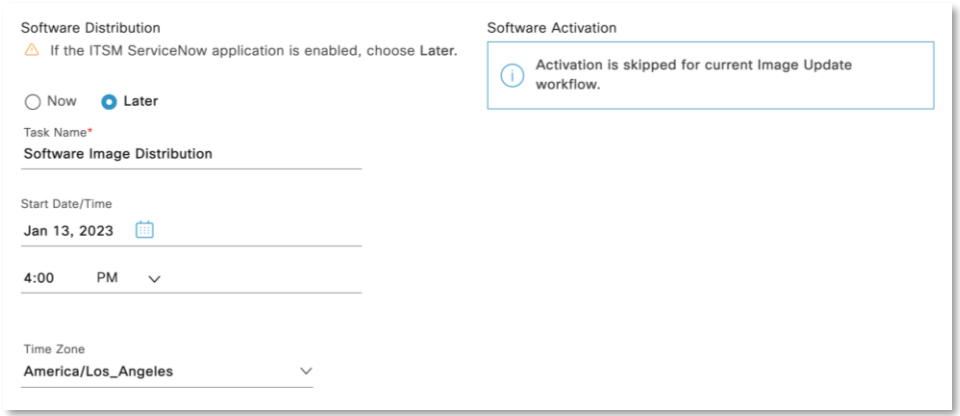
- Flexibility to upgrade devices either sequentially or in parallel when upgrading multiple devices across core, distribution and access layers
- Decide the order of device upgrades
- Need to be able to abort image upgrades in failure scenarios

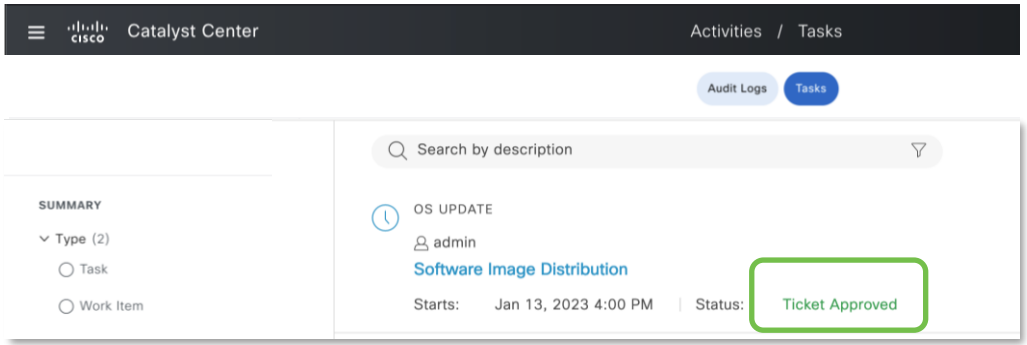
SWIM- Device Activation Order



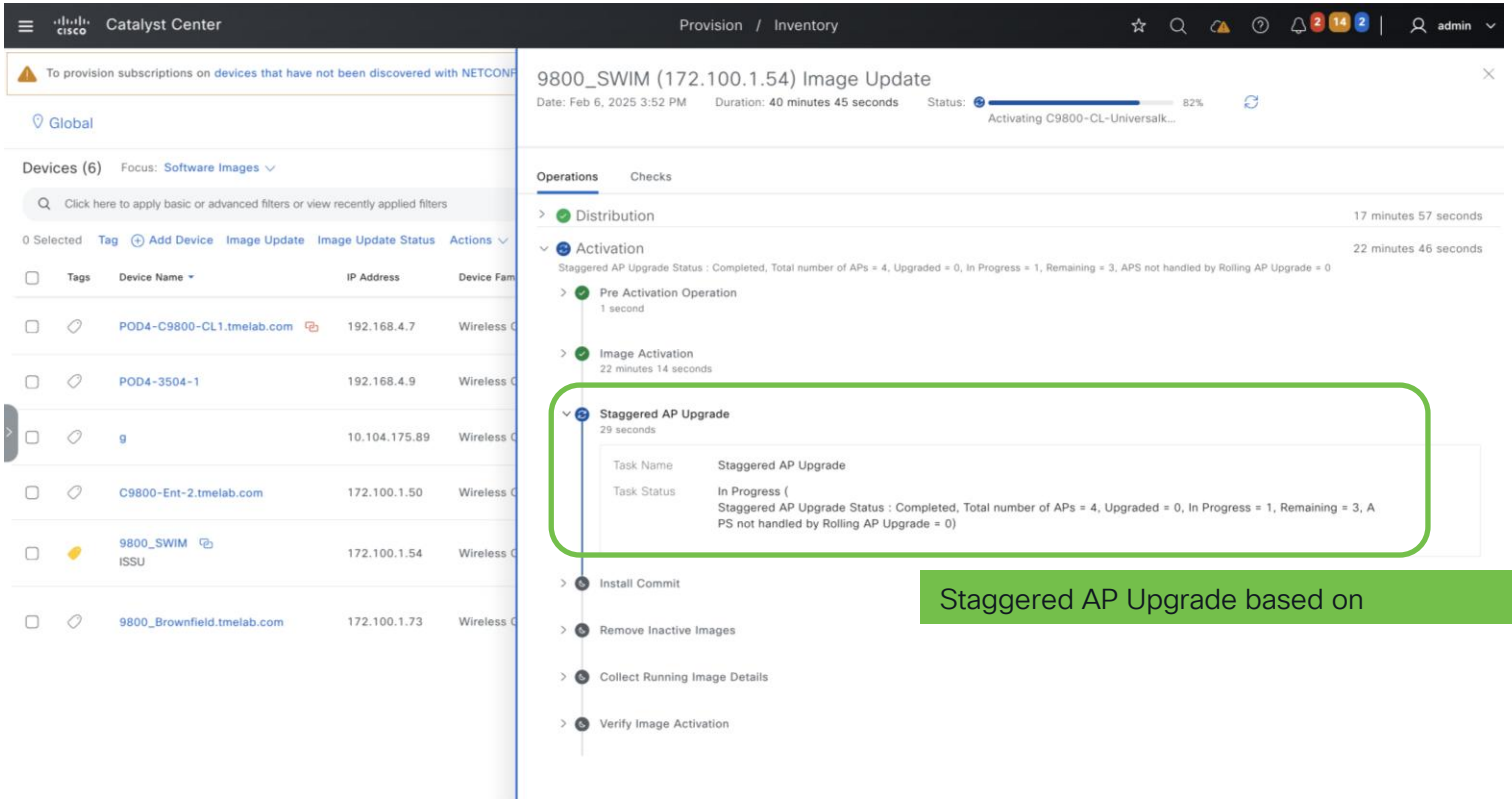
SWIM- Schedule Distribution & Activation





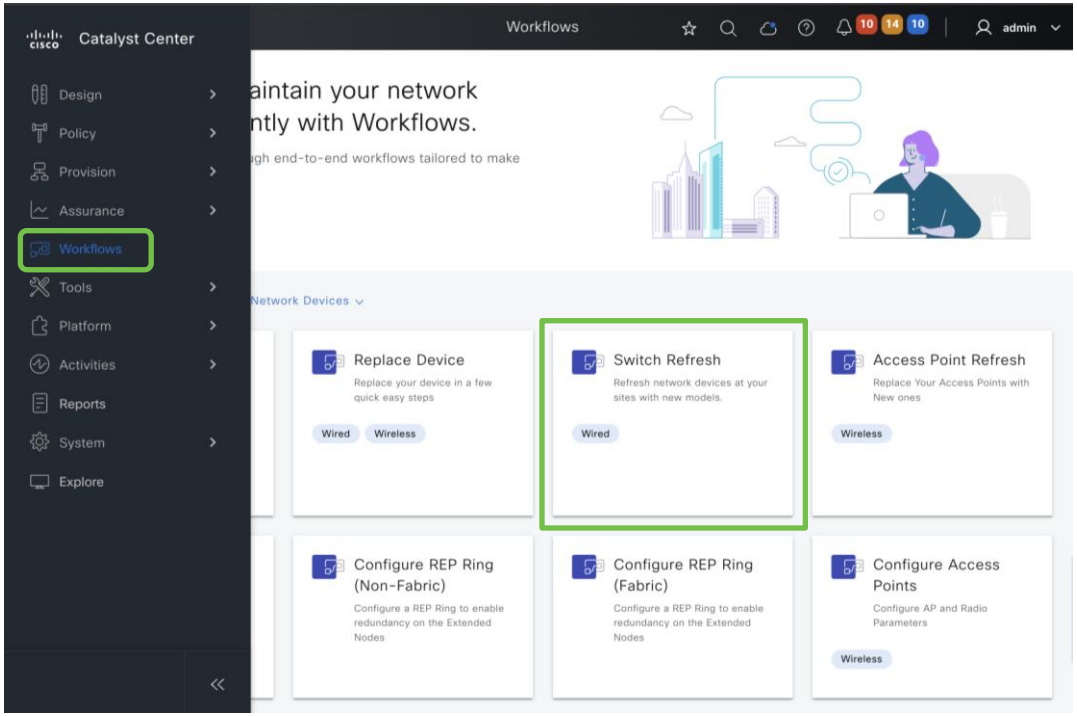


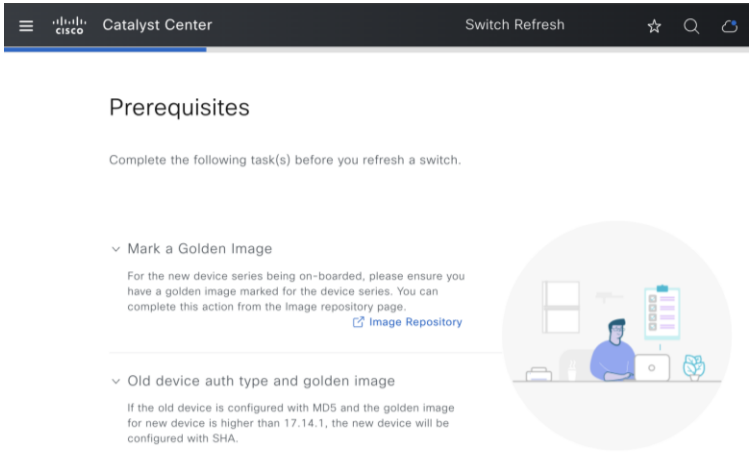
SWIM- Staggered AP Upgrade

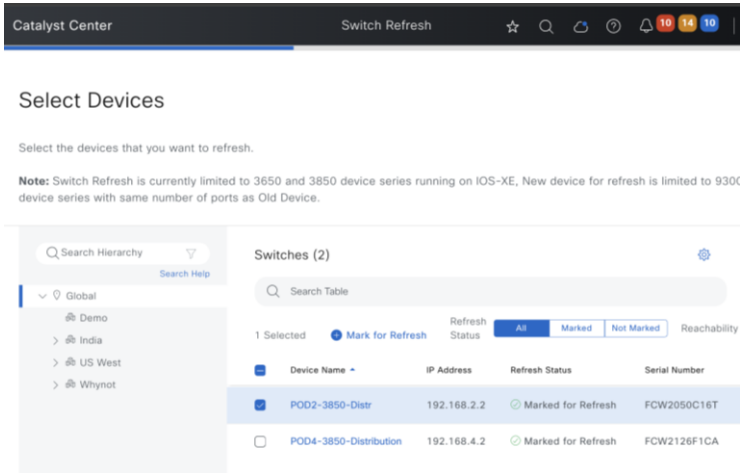


Staggered AP Upgrade based on

Switch Refresh

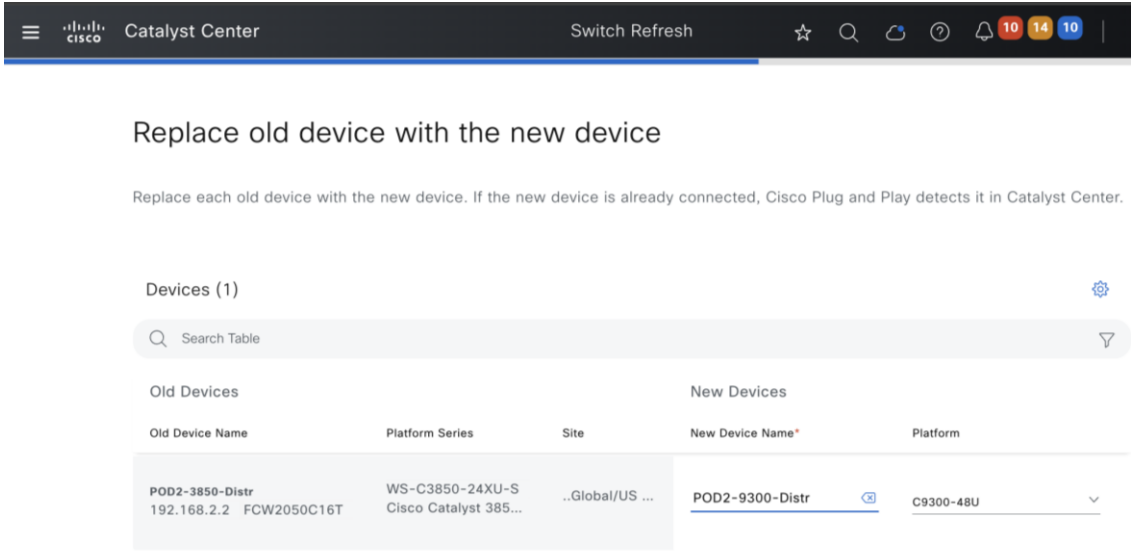




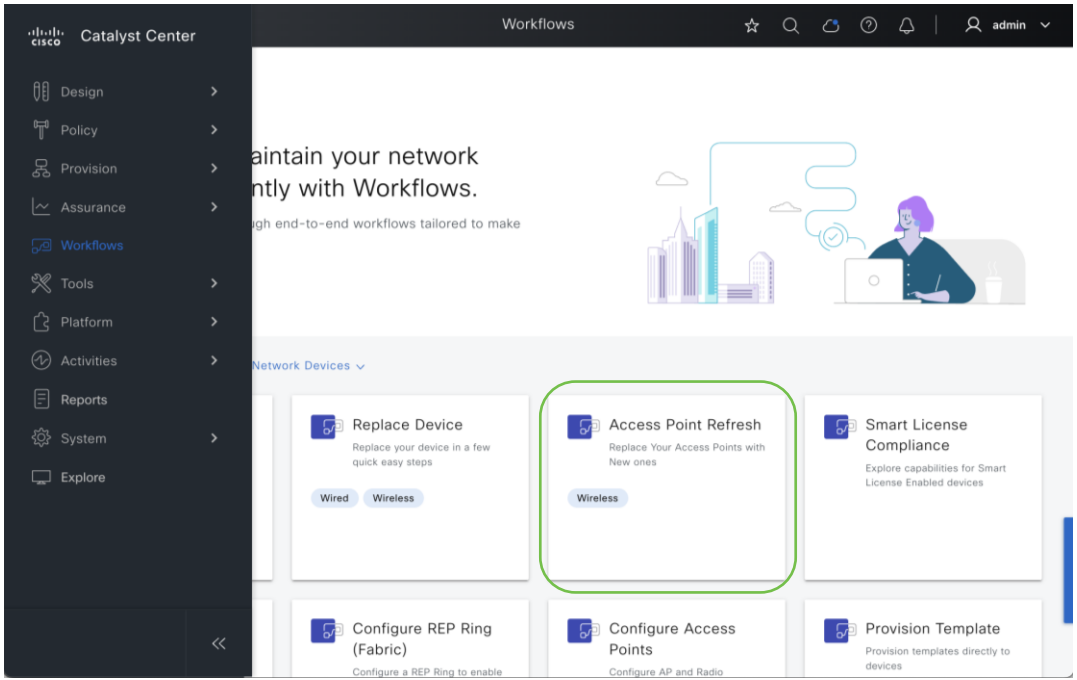


Switch Refresh

- Current support C3650/C3850 to C9300 switches
- Its mandatory to have a golden image tagged for new device family
- For Pre-staging, Old device need not be in unreachable state for completing the workflow
- Workflow ensures that all configurations, licensing and integration with ISE are taken care.



Refresh AP



Assurance Usecase

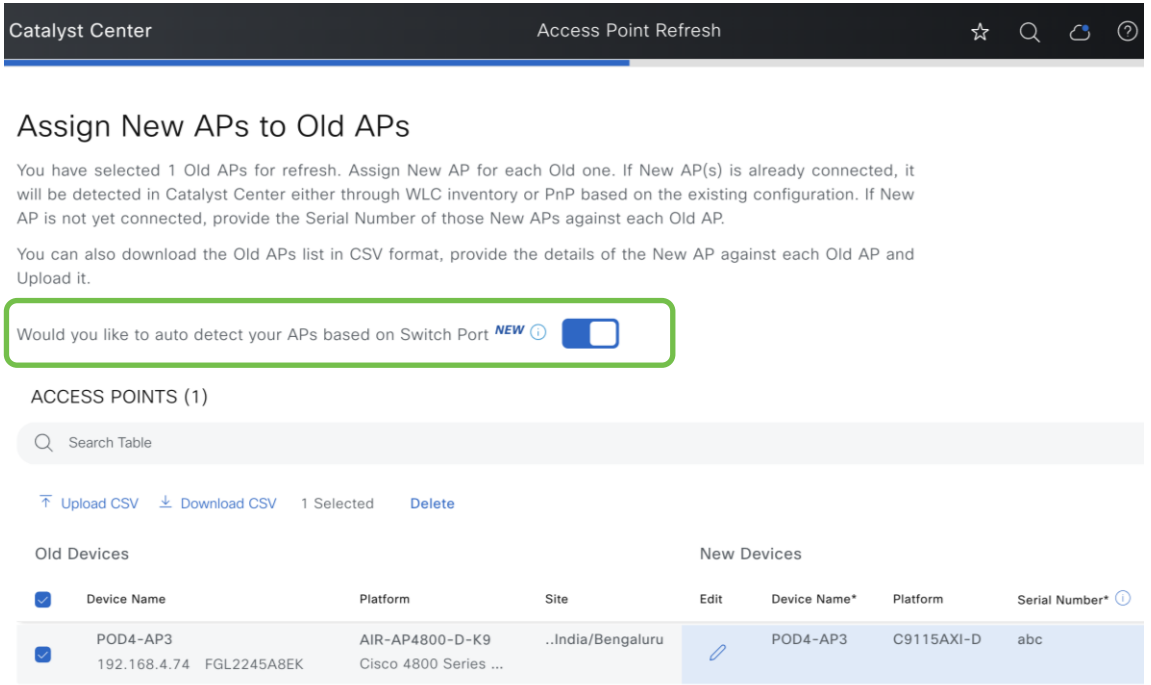
AP will not be provisioned in this scenario and only old configuration will be copied

Automation Usecase

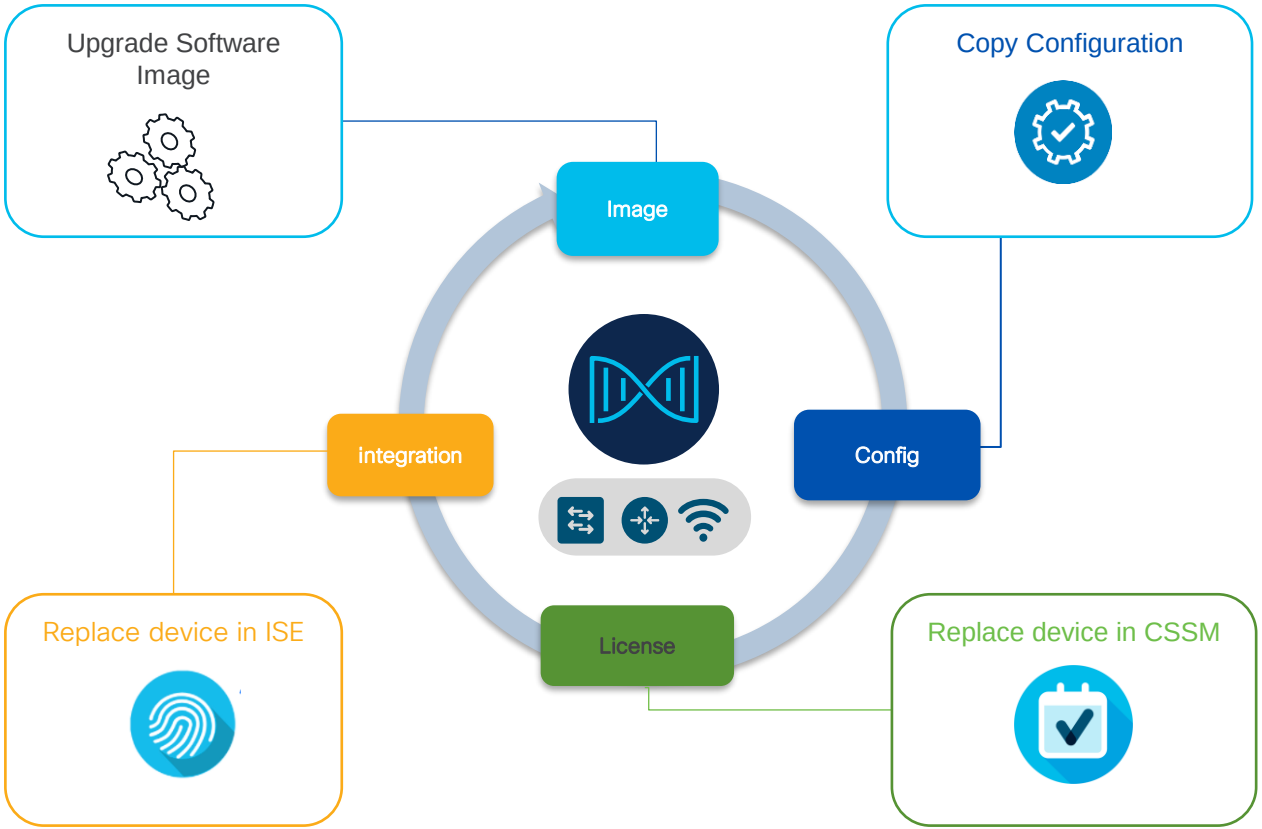
AP will be provisioned in this scenario

Refresh APs- Tips & Tricks

- Old AP **needs to be** Assigned to Site
- New AP **should not** be Assigned to Sites
- For Pre-staging, Old AP need not be in unreachable state for completing the workflow
- If new AP is connected to same switch port, workflow will auto detect new AP



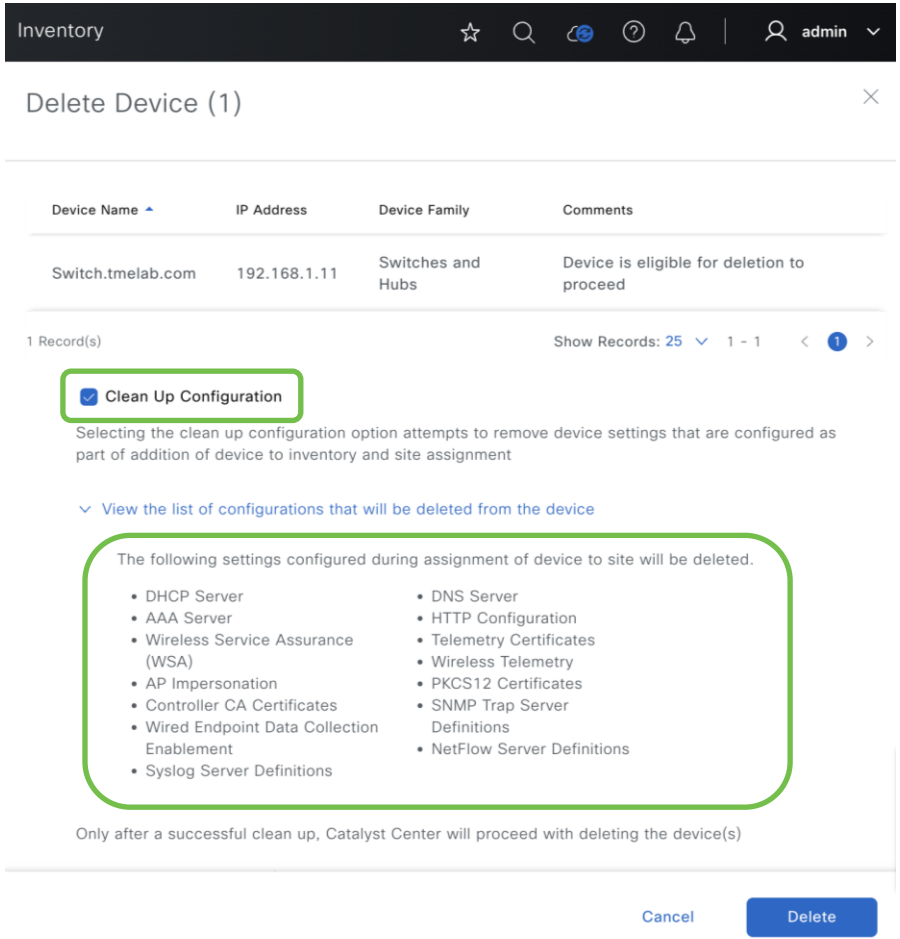
RMA Workflow



- SMU/Sub-Package Activation on Replacement device
- Full Stack Replacement
- RMA Retry Option
- License update in CSSM
- Support for IE Extended Nodes
- Zero Touch Fabric RMA
- Support for External SCEP broker configured PKI Certificate
- RMA support for full stack replacement
- Readiness check for RMA workflow
- RMA support for Authenticated Extended Node

Deleting Devices

- Selecting Clean up configuration deletes the configuration pushed by Catalyst Center to Network Devices
- Provision - > Inventory -> Select Device -> Delete Device
- If a device is provisioned, deleting from inventory is the only way to reassign it to a different site



Cisco Live EMEA Catalyst Center Learning Map

Sunday–9th

LTRENS-2890 7:45AM
ThousandEyes Network Agent Deployment on Cisco Catalyst 9000 Series Through Cisco Catalyst Center

LABENT-1809 7:45AM
Cisco Catalyst Center Monitoring and Troubleshooting

LABDEV-3752 8:30AM
Building Cisco SD-Access with Cisco Catalyst Center and ISE

LABOPS-1470 9:15AM
Click Once, Configure Everything with Cisco Catalyst Center using Configuration Templates

LABEWN-2697 10:45AM
Configure and Monitor AI-RRM with Cisco Catalyst Center

LABOPS-2779 10:45AM
Deploying Cisco Catalyst Center Virtual Appliance in AWS

TECOPS-1111 1:30PM
Let's Onboard, Configure and Optimize the brownfield Cisco Catalyst Wireless Infrastructure using NetOps and AIOps capabilities of Cisco Catalyst Center

TECOPS-2158 1:30PM
Cisco Catalyst Center Out-of-the-Box and Custom Integrations

TECOPS-2501 1:45PM
Mastering Catalyst Center: Troubleshooting Tips for Network automation and management

Monday–10th

TECOPS-2002 8:30AM
How to leverage Cisco Catalyst Center to build a Zero Trust Campus Network

TECOPS-2823 8:45AM
How to Leverage Cisco Catalyst Center to its Greatest Potential

TECOPS-2113 8:45AM
Building Custom Apps with Splunk Add-On Builder to Enhance Cross-Technology Operations with Cisco Catalyst Center and Splunk

BRKOPS-2402 4:00PM
Automate the Deployment of a Wireless Network with the Help of Cisco Catalyst Center

Tuesday–11th

BRKCOC-2483 8:00AM
Cisco IT: Streamlining Network Management and Decisions with Catalyst Center Automation and Splunk

BRKOPS-1894 8:00AM
Cisco Meraki Dashboard Meets Cisco Catalyst Center – Better Together!

BRKIPV-1007 8:00AM
Deploying Catalyst Center for IPv6 Networks

LTROPS-2341 8:30AM
Build a Flexible Network Automation Workflow with GitLab CI/CD, Catalyst Center, NetBox, and Ansible

BRKOPS-2464 12:00PM
Understanding and Troubleshooting the Cisco Catalyst Center

BRKOPS-2038 12:00PM
The Flow of Things: Navigating and Properly Enabling NetFlow-based Solutions through Cisco Catalyst Center

DEVNET-3000 3:00PM
Open-Source GenAI Bot for Catalyst Center

Wednesday–12th

DEVNET-1087 9:30AM
Cisco Catalyst Center Platform: APIs, Event Notifications, Integrations, and DevOps Resources

CSSENT-1144 11:00AM
Driving IT/OT Excellence with AI-Powered Cisco Catalyst Center at the Worldwide Vehicle Industry

BRKOPS-2416 1:15PM
7 Habits for Optimizing Your Cisco Catalyst Center Environment

LTRENS-3751 2:00PM
SD-Access as Code with Cisco Catalyst Center and ISE Automation

BRKOPS-2442 3:15PM
Leveraging Digital Twin Technology for Advanced Network Management with Cisco Catalyst Center

IBOOPS-2882 4:00PM
Let's Talk about Cisco Catalyst Center Integrations

BRKIOT-2362 5:00PM
Converge IT and OT Networks with Cisco Catalyst Center: In-Depth look into Industrial Networks

Thursday–13th

BRKOPS-1461 8:30AM
Discovering and Managing Brownfield Deployment with Cisco Catalyst Center

IBOOPS-2391 8:30AM
AI/ML in Cisco Catalyst Center: Transforming Network Operations

BRKOPS-2596 10:30AM
Revolutionize Your Network Management with Cisco Catalyst Center: Physical or Virtual on AWS or VMware

BRKOPS-3429 10:30AM
Simplify Network Management using GenAI and Cisco Catalyst Center APIs

BRKEWN-2667 1:00PM
Cisco Wireless Supercharged by Catalyst Center: The Ultimate Guide

BRKOPS-2608 2:15PM
Architecting your Cisco Catalyst Center for Resiliency and Business Continuity -

BRKTRS-3821 2:15PM
Mastering Troubleshooting with Cisco Catalyst Center & SD-Access

Catalyst Center

LABOPS-1399 Walk in Lab
Exploring AI Ops:
AI's Potential in Network Operations

BU-led sessions

cisco Live!

BRKOPS-1461

Webex App

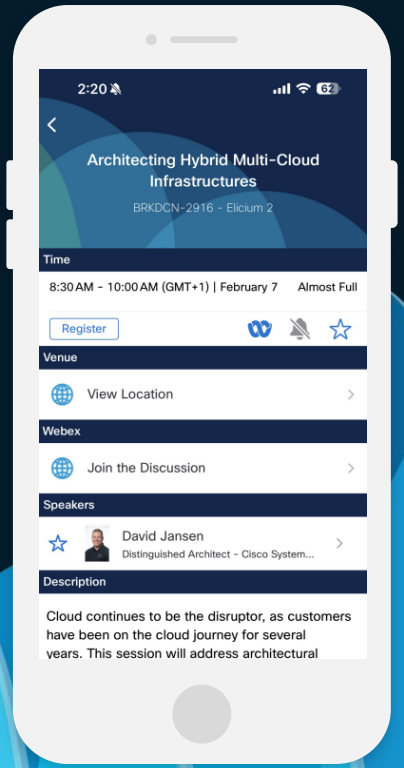
Questions?

Use the Webex app to chat with the speaker after the session

How

1. Find this session in the Cisco Events 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 February 28, 2025.



Fill Out Your Session Surveys

Participants who fill out a minimum of 4 session surveys and the overall event survey will get a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)

All surveys can be taken in the Cisco Events mobile app or by logging in to the Session Catalog and clicking the ‘Participant Dashboard’

Content Catalog

Continue your education

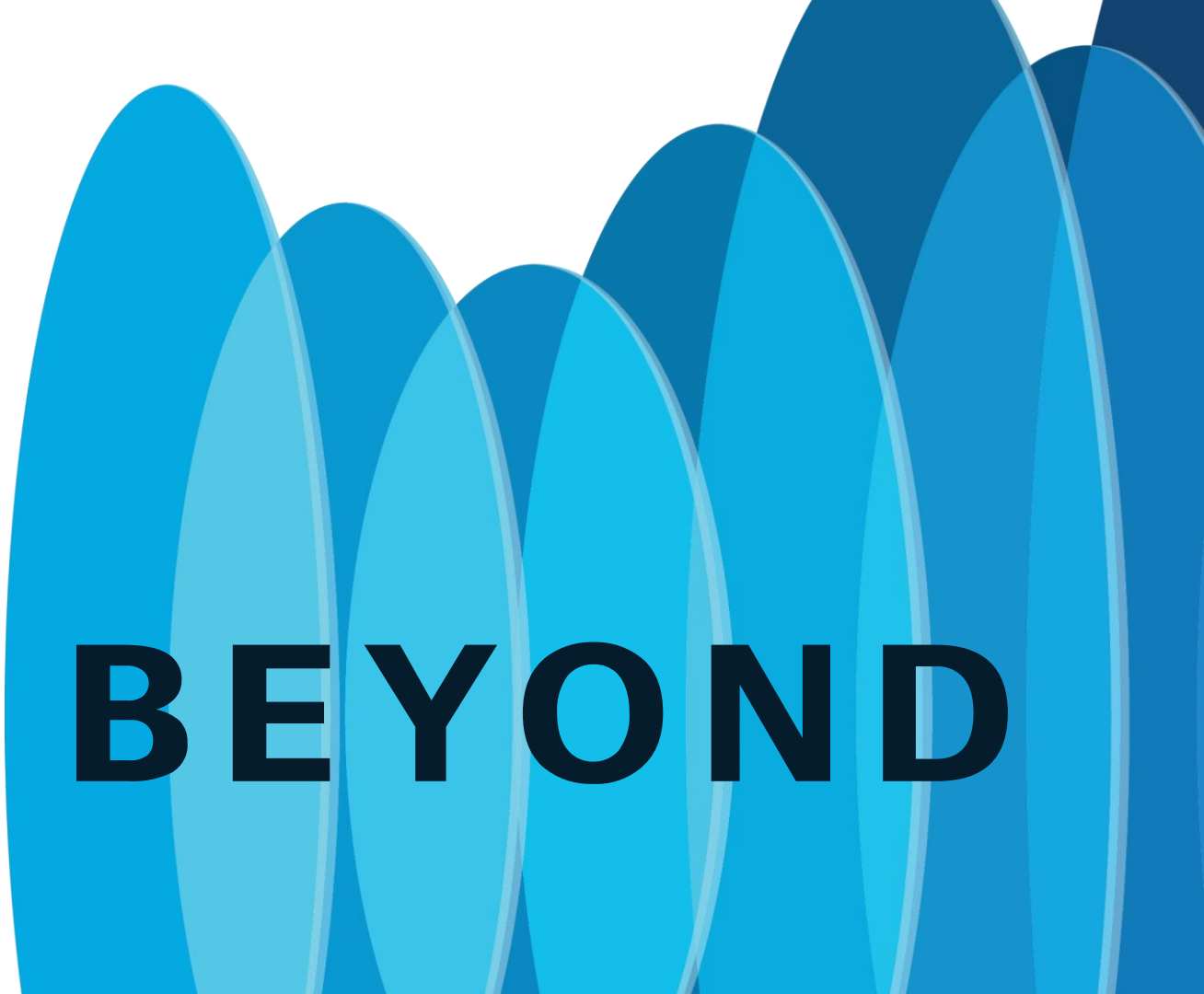
- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at ciscolive.com/on-demand. Sessions from this event will be available from March 3.

Contact me at:
www.linkedin.com/in/snehaamarapuram
www.linkedin.com/in/ramkumarchellappa

Thank you

cisco Live!

cisco Live!



GO BEYOND