



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?

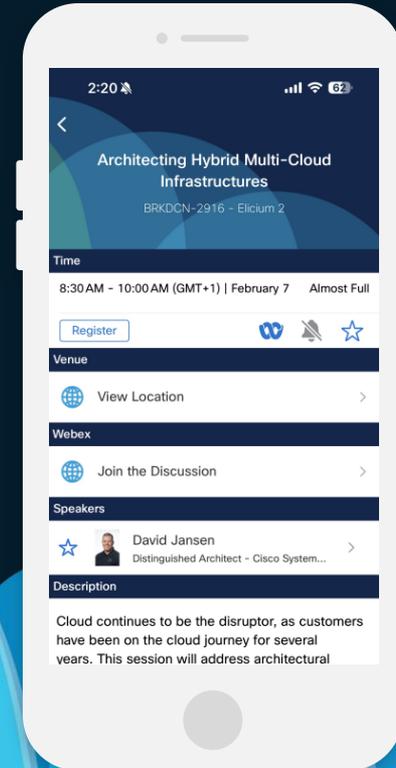
Use the Webex app to chat with the speaker after the session

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.

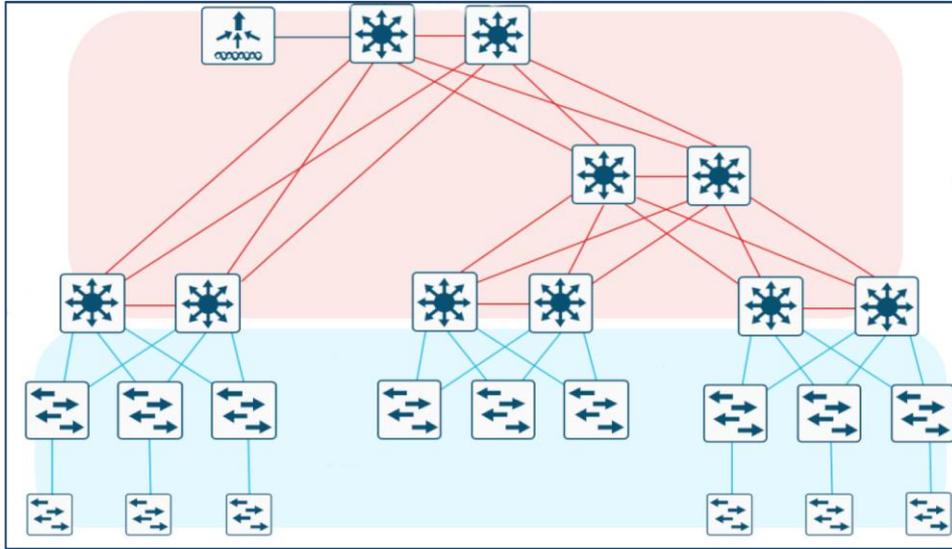
CISCO *Live!*



Navigating Amsterdam: A Biker's Journey



Navigating Brownfield: A Network Admin's Journey

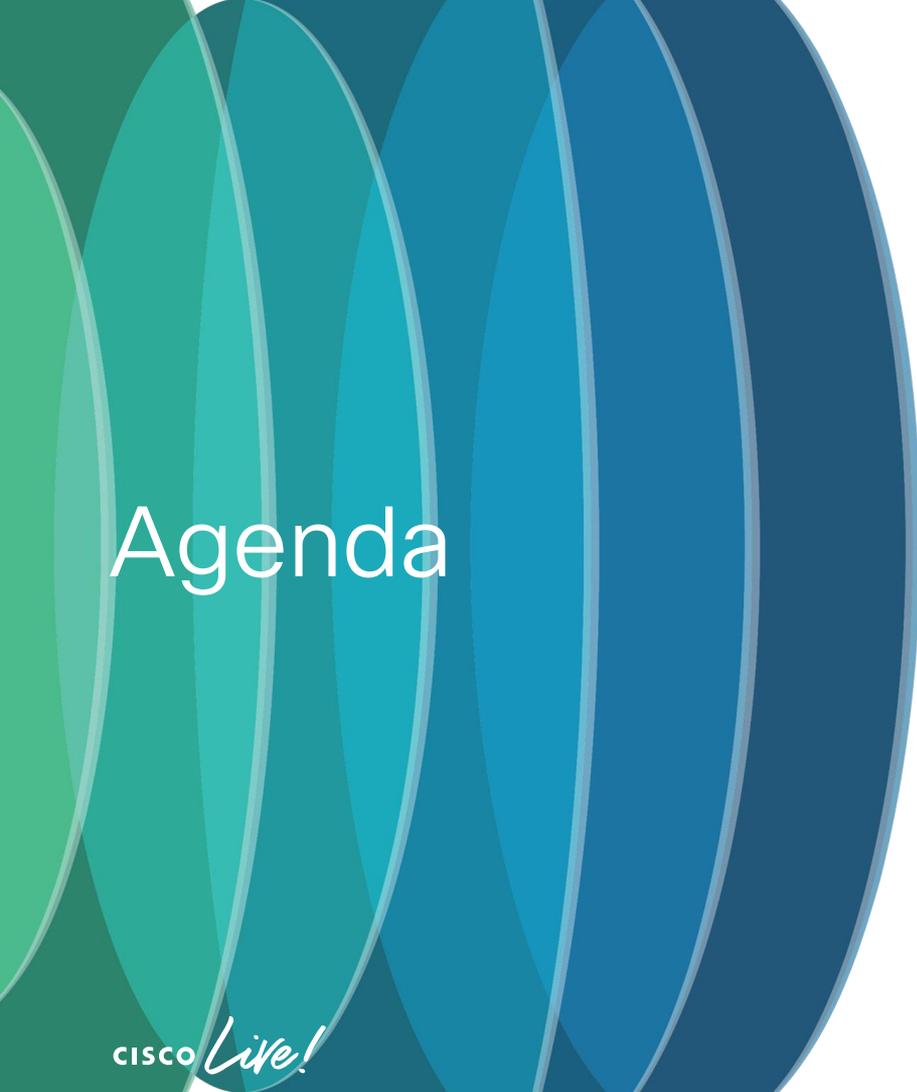


DOs



DON'Ts





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

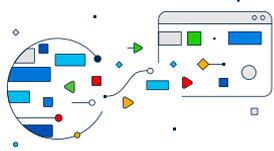
- Open the required ports/URLS
- Reachability between appliances and network devices

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

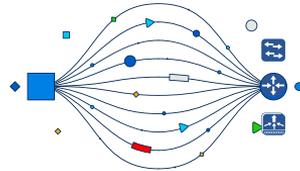
Onboarding & Inventory



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

Day-0

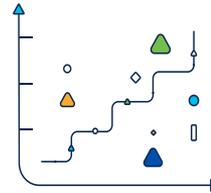
Network Configuration



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

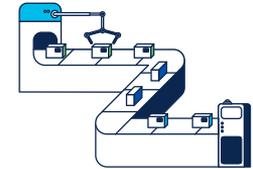
Day-1

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-N

Start your Journey

Cisco Catalyst Center

- Design
- Policy
- Provision
- Assurance
- Workflows
- Tools
- Platform
- Activities
- Reports
- System
- Explore**

Cisco Catalyst Center Explore

AIOps | **NetOps** | DevOps | SecOps

NetOps (13/20) As of: Jan 16, 2025 3:54 PM

NetOps

Simplified Onboarding

- 1 Network Discovery
- 2 Learn Device Config
- 3 Plug and Play
- 4 PnP Connect

Reporting, Compliance & Security

- 1 Generate Network Reports
- 2 Configuration Compliance
- 3 Security Advisories
- 4 Field Notices
- 5 Image Repository
- 6 Network Bug Identifier

Network Change Management

- 1 IP Address Manager (IPAM)
- 2 App Hosting for Switches
- 3 IoT Services
- 4 Application QoS
- 5 Network Profile
- 6 Device Replacement (RMA)
- 7 Network Profile

Application QoS

- 1 Application QoS

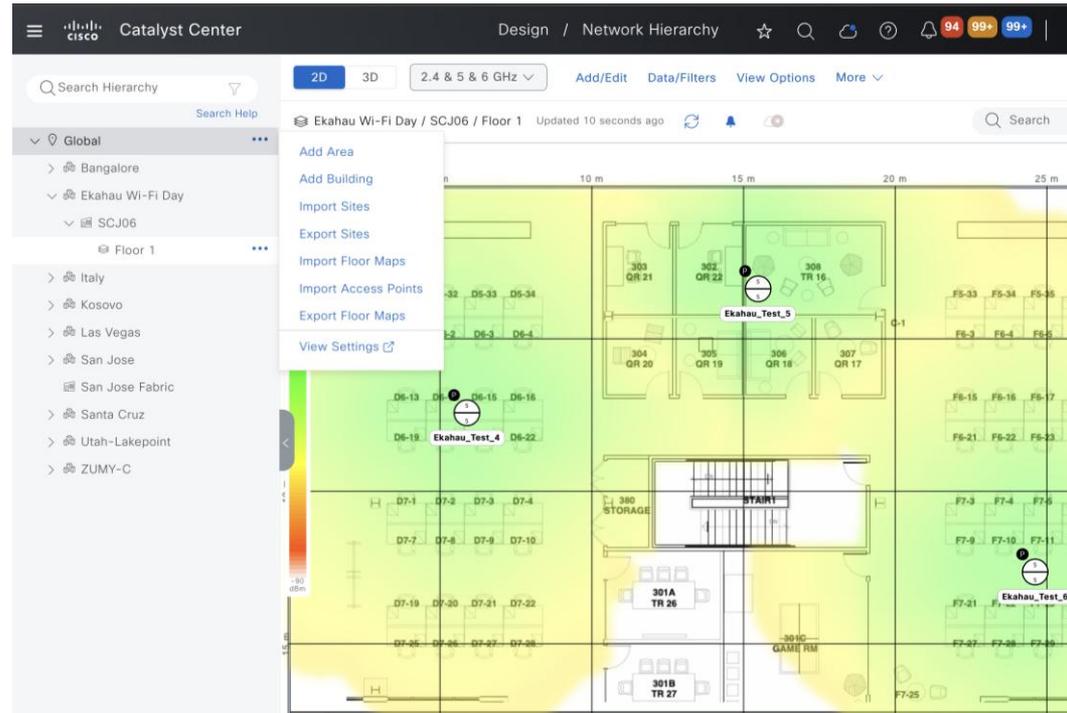
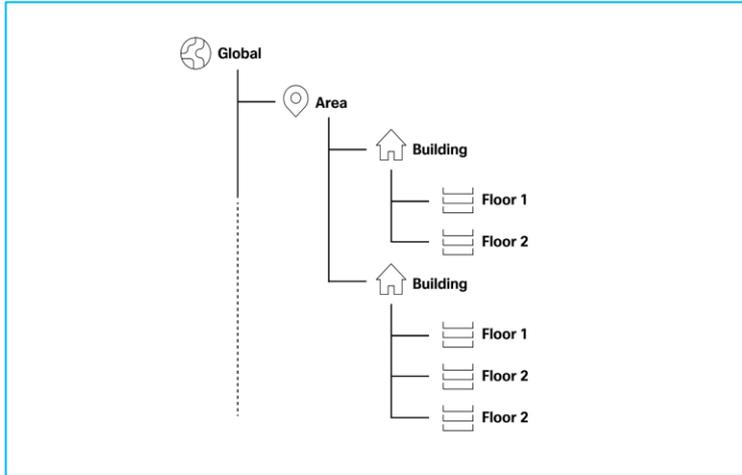
Completed Incomplete 13 of 20 steps completed

Pre-requisites to Onboard



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

The screenshot shows the Cisco Catalyst Center interface for configuring Device Credentials. The page title is "Design / Network Settings" and the user is logged in as "admin". The navigation menu includes Servers, Device Credentials (selected), IP Address Pools, Wireless, Telemetry, and Security and Trust. The main content area is titled "Create and configure the credentials used to access devices." and includes a note: "Assigned credentials aren't deployed automatically. To push a credential to your devices, click 'Manage Credentials' and choose the credential's Apply action in the Manage Credentials table." The configuration is organized into sections: "CLI" (with a red error icon), "SNMPv2c Read" (with a green success icon), and "SNMPv2c Write" (with a green success icon). The "CLI" section has a checkbox labeled "Assign a CLI credential" which is checked and highlighted with a green box. Below it is a dropdown menu for "Credential*" with a downward arrow. The "SNMPv2c Read" section has a checkbox labeled "Assign an SNMPv2c Read credential" which is checked. Below it is a dropdown menu for "Credential*" with the value "Read" selected. The "SNMPv2c Write" section has a checkbox labeled "Assign an SNMPv2c Write credential" which is unchecked. On the left side, there is a "Find Hierarchy" search bar and a tree view showing the hierarchy: Global (selected), Demo, India, US West, and Whynot. On the right side, there is a sidebar with a gear icon and a refresh icon.

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

The screenshot shows the Catalyst Center interface for configuring device credentials. The main panel is titled "Device Credentials" and contains a search bar, a hierarchy tree on the left, and a list of credential types on the right. The hierarchy tree shows "Global" expanded, with sub-items for "Andaman", "Chennai", "Demo", "India", "US West", and "Whynot". The credential types list includes "CLI", "SNMPv2c Read", and "SNMPv2c Write". Under "CLI", the "Assign a CLI credential" option is selected, and the credential name "ciscodna" is entered. Under "SNMPv2c Read", the "Assign an SNMPv2c Read credential" option is selected, and the credential name "read" is entered. Under "SNMPv2c Write", the "Assign an SNMPv2c Write credential" option is not selected. A right-hand panel titled "Apply 'ciscodna' (CLI)" shows a warning message: "The selected credential will only be applied to this site. To apply a credential to all applicable sites, choose 'Focus: System' in the Manage Credentials table." Below the warning, there are radio buttons for "Now" (selected) and "Later", and a text field for "Task Name*" containing "Apply CLI credentials for site Global". At the bottom of the right panel are "Close", "Back", and "Apply" buttons.

Designing Network Settings- Servers

The screenshot displays the Cisco configuration interface for Servers, organized into several sections:

- AAA:** Under the 'Client/Endpoint' tab, 'Add AAA servers' is checked. The 'Server Type' is set to 'ISE' (checked) and 'AAA' (unchecked). The 'Protocol' is set to 'RADIUS' (checked) and 'TACACS' (unchecked). The 'PAN*' is '172.100.1.99'. A 'Warning' icon is present next to the 'Add AAA servers' checkbox.
- DHCP:** 'Add DHCP servers' is checked. The 'IP Address*' is '192.168.4.1'. A 'Warning' icon is present next to the 'Add DHCP servers' checkbox.
- DNS:** 'Set a domain name' and 'Add DNS servers' are both checked. The 'Domain Name*' is 'tmelab.com'. The 'IP Address*' is '172.100.1.200'. A 'Warning' icon is present next to the 'Add DNS servers' checkbox.
- NTP:** 'Add NTP servers' is checked. The 'IP Address*' is '72.163.32.44'. A 'Warning' icon is present next to the 'Add NTP servers' checkbox.
- Stealthwatch Flow Destination:** 'Select from flow destinations configured in the Stealthwatch' is checked. The 'Select flow destination' is '172.100.1.97:2055 (FLOW_COLLEC...'. A 'Warning' icon is present next to the 'Add an external flow destination server' radio button.
- Time Zone:** 'GMT' is selected. A 'Warning' icon is present next to the 'Time Zone' dropdown.

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”

Wired Endpoint Data Collection

The primary function of this feature is to track the presence, location, and movement of wired endpoints in the network. Traffic received from endpoints is used to extract and store their identity information (MAC address and IP address). Other features, such as IEEE 802.1X, web authentication, Cisco Security Groups (formerly TrustSec), SD-Access, and Assurance, depend on this identity information to operate properly.

Wired Endpoint Data Collection enables Device Tracking policies on devices assigned to the Access role in Inventory.

- Enable Catalyst Center Wired Endpoint Data Collection At This Site
- Disable Catalyst Center Wired Endpoint Data Collection At This Site

Wireless Controller, Access Point and Wireless Clients Health

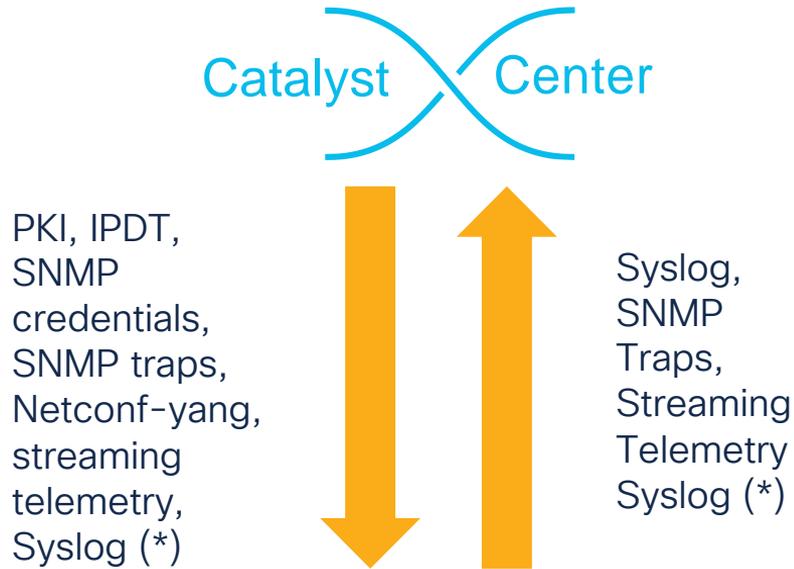
Enables Streaming Telemetry on your wireless controllers in order to determine the health of your wireless controller, access points and wireless clients.

- Enable Wireless Telemetry

The screenshot shows the Catalyst Center interface for configuring Telemetry settings. The breadcrumb navigation is 'Design / Network Settings'. The 'Telemetry' tab is selected in the top navigation bar. The main content area includes:

- A header section: 'Configure Syslog, Traps and NetFlow properties for your devices. The system will deploy these settings when devices are assigned to a site or provisioned.'
- A description: 'Catalyst Center is your default SNMP collector. It polls network devices to gather telemetry data. [View details](#) on the metrics gathered and the frequency with which they are collected.'
- A section for 'SNMP Traps' with a sub-header: 'Choose Catalyst Center to be your SNMP trap server, and/or add any external SNMP trap servers. These are the destination servers for SNMP traps and messages from network devices.' It contains two radio buttons: 'Use Catalyst Center as SNMP trap server' (checked) and 'Add an external SNMP trap server'.
- A section for 'Syslogs' with a sub-header: 'Choose Catalyst Center to be your syslog server, and/or add any external syslog servers. Devices will be provisioned with syslog severity level 6 (information messages) when they are assigned to a site and/or provisioned.' It contains two radio buttons: 'Use Catalyst Center as syslog server' (checked) and 'Add an external syslog server'.
- A section for 'Application Visibility' with a sub-header: 'When assigning Catalyst 9000 or Traffic Telemetry Appliance devices to the site, enable NetFlow Application Telemetry and Controller-Based Application Recognition by default.' It contains two radio buttons: 'Enable by default on supported wired access devices' (checked) and 'Use Catalyst Center as the Netflow Collector'.

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?

System / Settings

Device Controllability

Device Controllability is a system-level process on Catalyst Center that enforces state synchronization for some device-layer features. Its purpose is to aid in the deployment of required network settings that Catalyst Center needs to manage devices. Changes are made on network devices during discovery, when adding a device to Inventory, or when assigning a device to a site. If changes are made to any settings that are under the scope of this process, these changes are applied to the network devices during the Provision and Update Telemetry Settings operations, even if Device Controllability is disabled. The following device settings will be enabled as part of Device Controllability when devices are discovered:

- SNMP Credentials
- NETCONF Credentials

Subsequent to discovery, devices will be added to Inventory. The following device settings will be enabled when devices are added to inventory:

- Cisco TrustSec (CTS) Credentials

The following device settings will be enabled when devices are assigned to a site. Some of these settings can be defined at a site level under Design > Network Settings > Telemetry & Wireless.

- Wired Endpoint Data Collection Enablement
- Controller Certificates
- SNMP Trap Server Definitions
- Syslog Server Definitions
- Application Visibility
- Application QoS Policy
- Wireless Service Assurance (WSA)
- Wireless Telemetry
- DTLS Ciphersuite
- AP Impersonation

If Device Controllability is disabled, Catalyst Center does not configure any of the preceding credentials or settings on devices during discovery, at runtime, or during site assignment. However, the telemetry settings and related configuration are pushed when the device is provisioned or when the Update Telemetry Settings action is performed.

Enable Device Controllability

Configured during Discovery workflow

Configured during Site Assignment workflow

Autocorrect telemetry configuration

Catalyst Center identifies and automatically corrects the following telemetry configuration issues on the device:

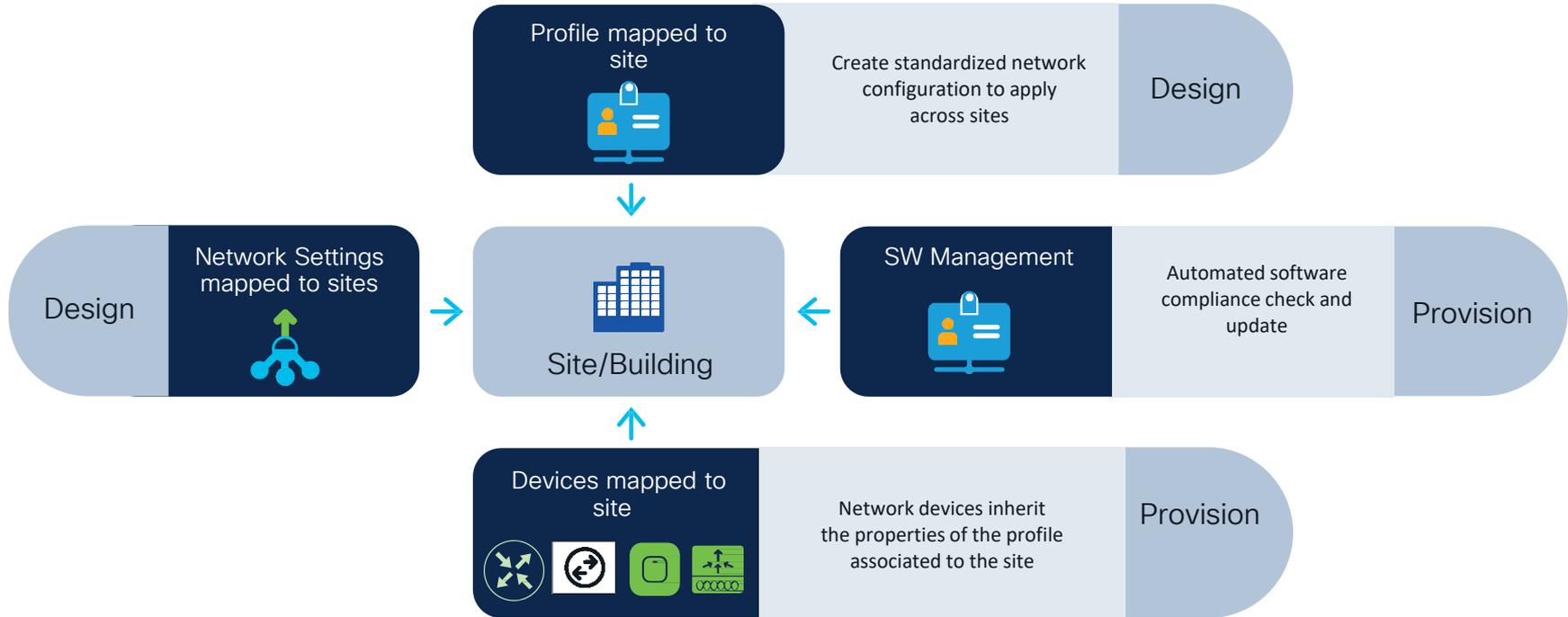
- SWIM certificate issue
- IOS WLC NA certificate issue
- PKCS12 certificate issue
- IOS telemetry configuration issue

The autocorrect telemetry config feature is supported only when Device Controllability is enabled.

Enable autocorrect telemetry config

Save

Site as a Focal Point in Catalyst Center



Pre-requisites before Onboarding devices



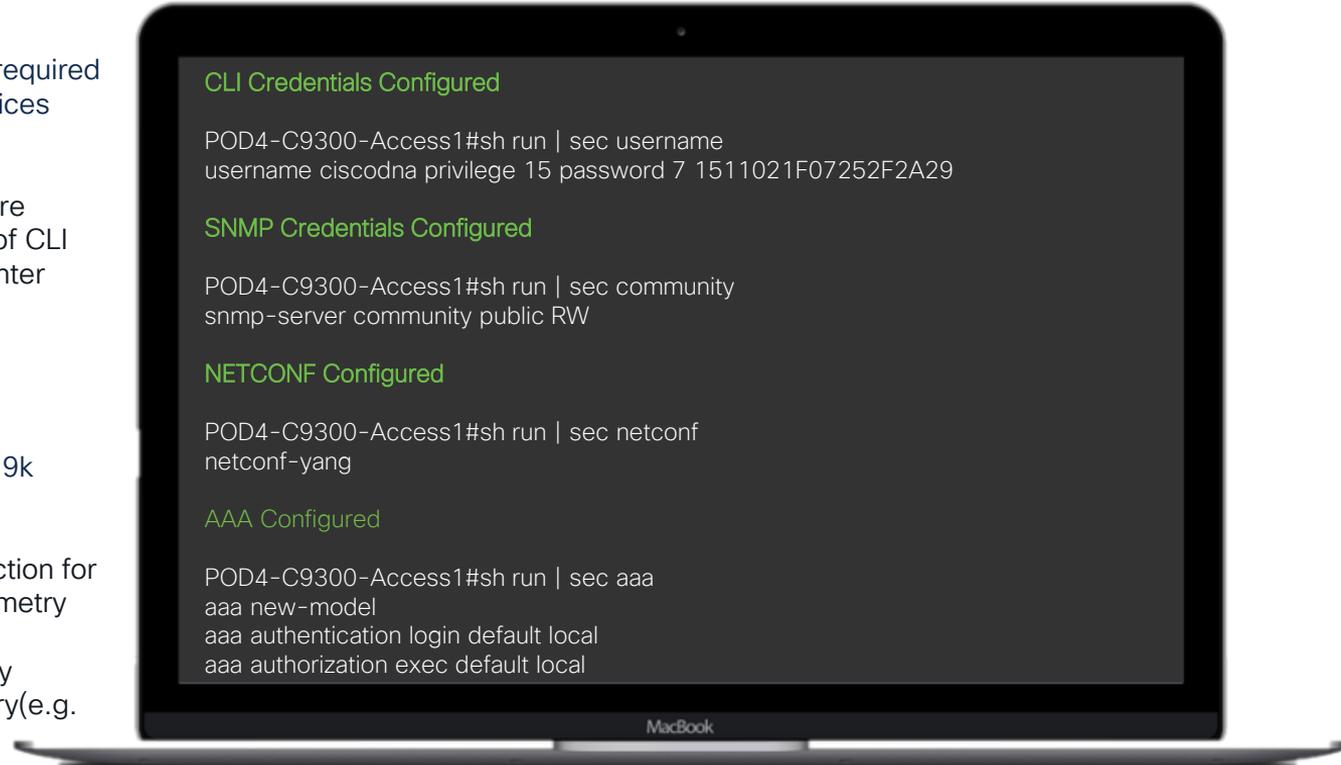
Minimal CLI and SNMP details are required for Catalyst Center to discover devices

- 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

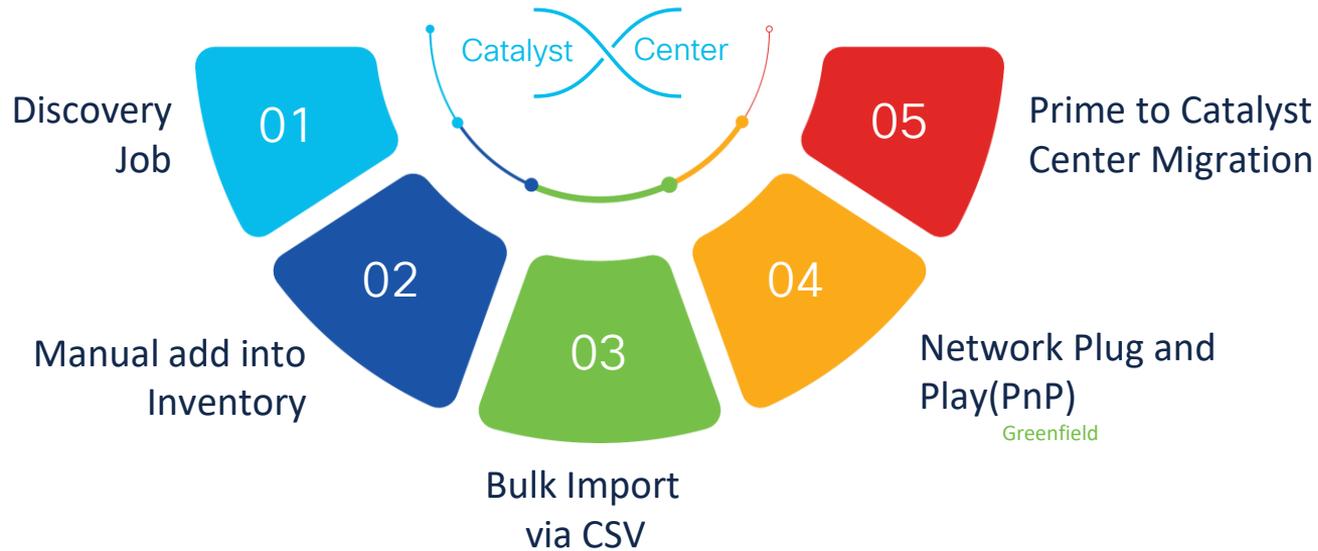
- The majority of data collection for WLC is via streaming telemetry
- Advanced features employ Netconf-yang for telemetry(e.g. POE status)



Device Onboarding Workflow

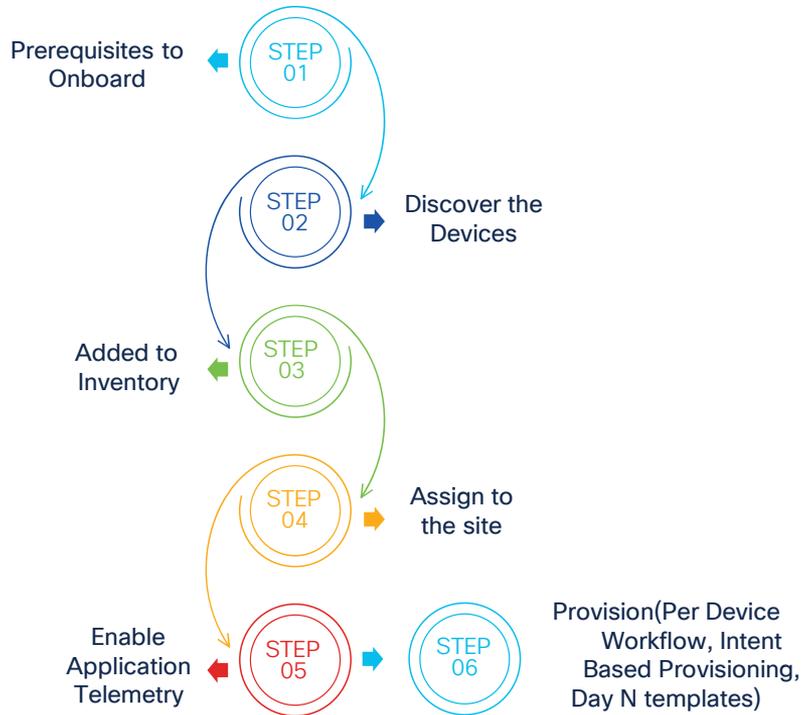


Various Ways To Onboard Devices Into Catalyst Center

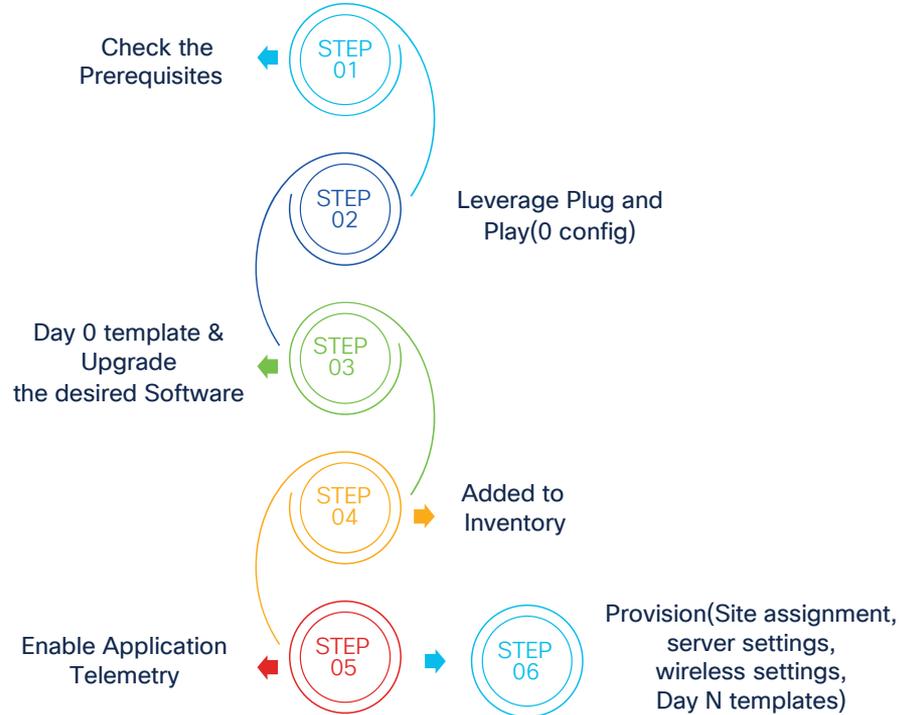


Brownfield vs Greenfield Device Onboarding

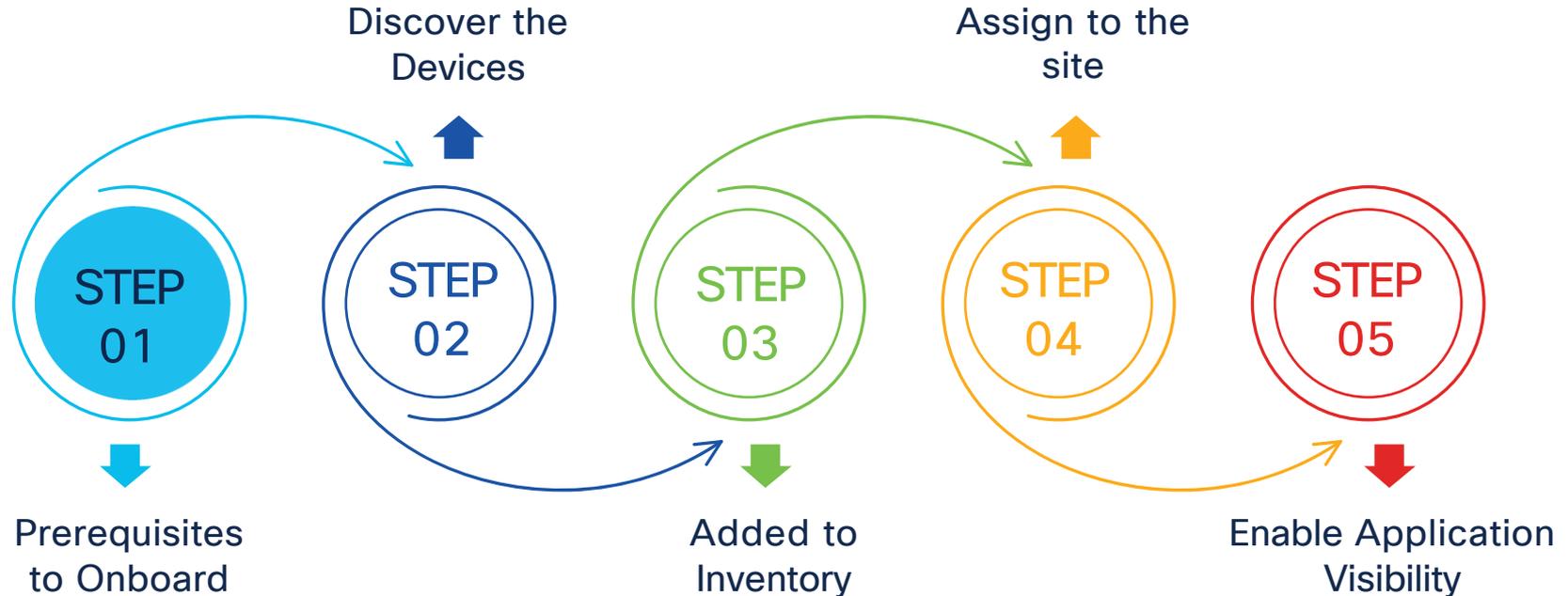
Brownfield Device Onboarding



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.

CLI (1)

SNMP

SNMPv2c Read (0)

SNMPv2c Write (0)

SNMPv3 (0)

NETCONF (0)

Advanced Settings

HTTP(S) Read (0)

HTTP(S) Write (0)

Protocol Order

SNMP Polling Properties

Select from existing credentials or add new ones. You can add either a job-specific credential or a global credential.

EXISTING GLOBAL SNMPV2C WRITE CREDENTIALS

SNMP RW Test ansible created snmp creds

[+ Add V2C Write Credentials](#)

Job specific

Global

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

CISCO *Live!*





Global

- ✓ 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 (0) Focus: Default ▾

[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: Feb 7, 2025 5:23 PM 🔄

<input type="checkbox"/>	Tags	Device Name ▾	IP Address	Device Family	MAC Address ⓘ
No devices available					

What If...? – Scenario-1

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.

Select from existing credentials or add new ones. You can add either a job-specific credential or a global credential.

EXISTING GLOBAL CLI CREDENTIALS

- ciscodna
- Test
- Test2
- Test3
- Test4
- Test5

[Add CLI Credentials](#)

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



Discovery Fails for the devices with Invalid Credentials

Reference / Discovery Details

All Discoveries

Invalid Credentials Date - Jan 19, 2025 2:58 PM (1) As of: Jan 19, 2025 3:16 PM

Completed Type: Range Retry Count: 3 Protocol Order: SSH Total Time: 0 minutes 25 seconds [View all details](#) [Re-discover](#)

DEVICE SUMMARY

1	0	1	0
Discovered	Successful	Failed	Discarded

Search Table

IP Address	Device Name	Status	ICMP	SNMP	CLI	HTTP(s)	NETCONF
192.168.4.4	NA	❌	✅	✅	❌	⊖	⊖

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 <ul style="list-style-type: none">• 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

The screenshot shows the Cisco Catalyst Center interface. The main panel displays a table of 12 devices in the 'Inventory' focus. The 'Add Device' button is highlighted with a green box. The modal form on the right is titled 'Add Device' and includes the following fields and options:

- Type: Network Device (with a hint)
- Device IP / DNS Name*
- Credentials: Validate (Note: CLI and SNMP credentials are mandatory. Please ensure authenticity of credentials. In case of invalid credentials, device will go into a collection failure state.)
- CLI*: Select global credential (selected) or Add device specific credential
- Credential* (dropdown)
- SNMP* (expandable)
- SNMP Retries and Timeout* (expandable)
- Device Controllability is Enabled. Config changes will be made on network devices during discovery/inventory or when device is associated to a site. [Learn more](#)
- Buttons: Cancel, Add

Tags	Device Name	IP Address
<input type="checkbox"/>	3850-access-Pod1	192.168.1.7
<input type="checkbox"/>	AP5CE1.7628.FE14	192.168.10.194
<input type="checkbox"/>	AP40CE.24A4.6F52	172.100.1.50
<input type="checkbox"/>	Branch-Switch.tmlab.com	192.168.10.5
<input type="checkbox"/>	C9300Access-2-POD1	192.168.1.4
<input type="checkbox"/>	C9800-vWLC	192.168.4.40
<input type="checkbox"/>	POD1-3850-Distr	192.168.1.2

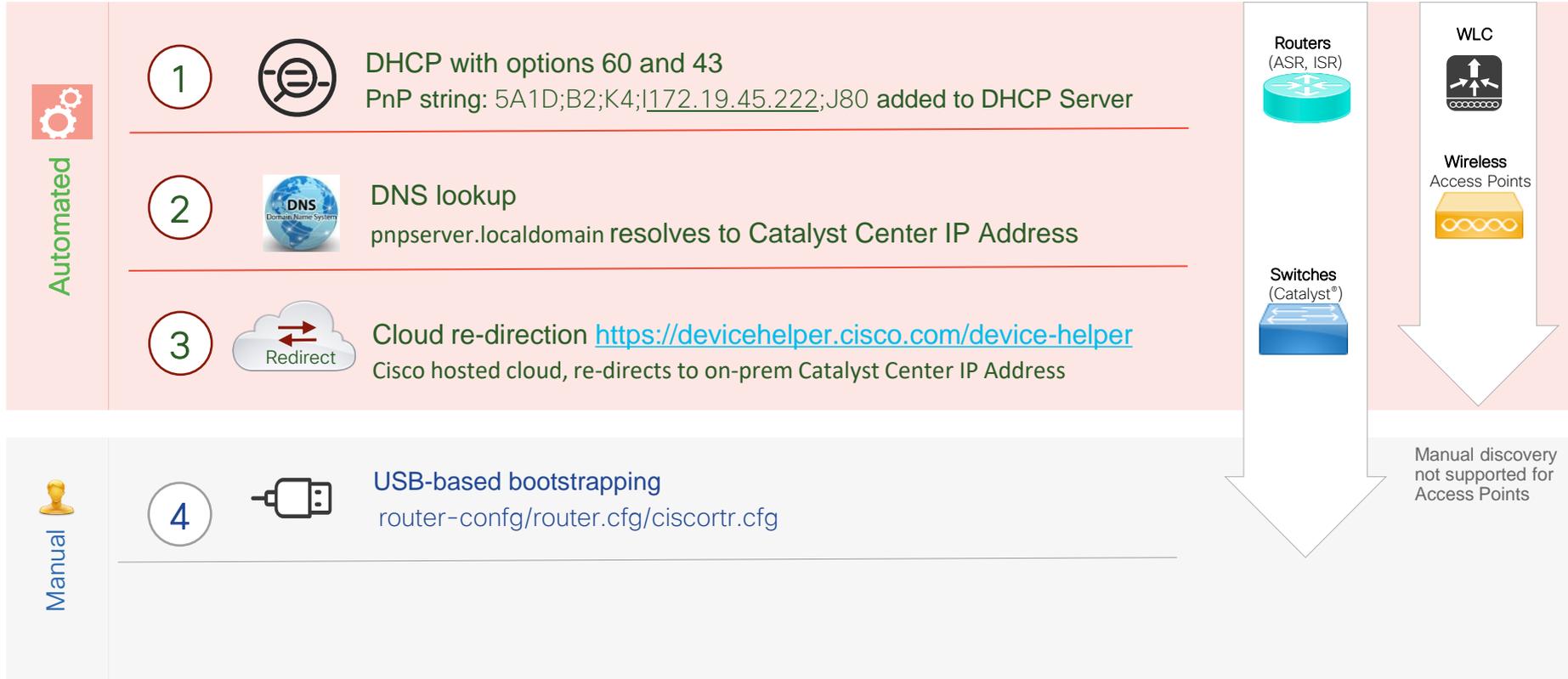
Devices in Inventory

Check [Device Roles](#) once devices are added into the inventory as some telemetry push depends on device role

The screenshot shows the Cisco Catalyst Center interface for the Provision / Inventory section. The page displays a table of 54 devices. A green box highlights the 'Device Role' column, which contains entries such as 'ACCESS', 'DISTRIBUTION', and 'BORDER ROUTER'. The table also includes columns for Tags, Device Name, IP Address, Vendor, Reachability, EoX Status, Manageability, and Compliance. The 'Device Role' column is highlighted with a green border.

Tags	Device Name	IP Address	Vendor	Reachability	EoX Status	Device Role	Manageability	Compliance
	BGL11_Floor3_AP1	192.168.4.17	NA	Reachable	Not Scanned	ACCESS	Managed	NA
	C9300-Edge-Pod2.tmelab.com	192.168.2.10	Cisco	Reachable	1 alert	ACCESS	Managed	Non-Compliant
	C9300-Pod2-Dist-2.tmelab.com	192.168.2.199	Cisco	Reachable	1 alert	DISTRIBUTION	Managed	Non-Compliant
	C9300Access-2-Pod2.tmelab.com	192.168.2.5	Cisco	Reachable	2 alerts	ACCESS	Managed	Non-Compliant
	C9800-Ent-2.tmelab.com	172.100.1.50	Cisco	Reachable	0 alerts	ACCESS	Managed	Compliant
	CE-1	172.100.1.20	Cisco	Unreachable	Not Scanned	BORDER ROUTER	Managed Device Unreachable	Non-Compliant
	CE-2	172.100.1.23	Cisco	Unreachable	Not Scanned	BORDER ROUTER	Managed Device Unreachable	Non-Compliant

Greenfield Device Onboarding- PnP Options



Demo

CISCO *Live!*



Welcome to Catalyst Center!

🖥️ [Explore](#)

⚠️ Some of your license compliance requirements have not been met. [Learn more.](#)

Cisco DNA Center is becoming Catalyst Center

As part of our vision to converge our products around an integrated platform, we are changing the name of Cisco DNA Center to Catalyst Center in the next release. The capability and functionality of Catalyst Center remains the same as Cisco DNA Center.

Assurance Summary

Health ⓘ

Healthy as of Feb 7, 2025 5:39 PM



Network Devices



Wireless Clients



Wired Clients

[View Details](#)

Critical Issues

Last 24 Hours



P1



P2

[View Details](#)

Trends and Insights

Last 30 Days



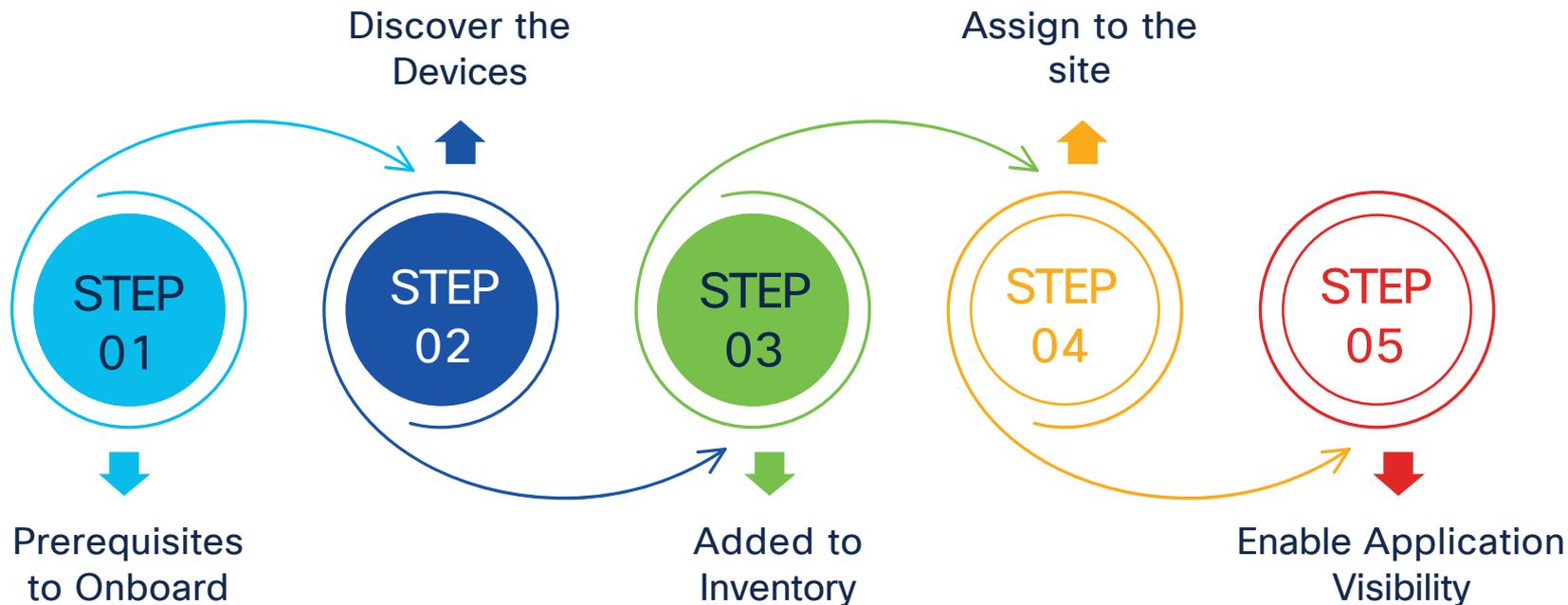
AP Performance Advisories



Trend Deviations

[View Details](#)

Brownfield Device Onboarding



Demo

CISCO *Live!*



Global

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 (8) 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: Feb 7, 2025 6:34 PM 🔄

<input type="checkbox"/>	Tags	Device Name	IP Address	Vendor	Reachability ⓘ	EoX Status ⓘ	Manageability ⓘ	Device Role	Compliance ⓘ	Site
<input type="checkbox"/>		AP01	172.16.19.10	NA	🟢 Reachable	🟡 Not Scanned	🟢 Managed	ACCESS	NA	Assign
<input type="checkbox"/>		AP02	172.16.19.12	NA	🟢 Reachable	🟡 Not Scanned	🟢 Managed	ACCESS	NA	Assign
<input type="checkbox"/>		Border.dcloud.cisco.com	172.16.10.104	Cisco	🟢 Reachable	🟡 Not Scanned	🟢 Managed	CORE	Non-Compliant	Assign
<input type="checkbox"/>		C9800-WLC	198.18.134.100	Cisco	🟢 Reachable	🟡 Not Scanned	🟢 Managed	CORE	Compliant	Assign
<input type="checkbox"/>		Edge1.dcloud.cisco.com	172.16.20.10	Cisco	🟢 Reachable	🟡 Not Scanned	🟢 Managed	ACCESS	Compliant	.../RTP/Bu

8 Record(s)

Show Records: 25 1 - 8 < ⓘ >

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
successfully
.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 source interface	Catalyst Center
logging host <>	<int with which device was	overwrites logging
logging trap 5	discovered>	source interface and
	logging host	trap level
	<catalyst center ip>	
	logging trap 6	

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
<pre>device-tracking policy POLICY1 trusted-port limit address-count 100 no protocol udp tracking enable interface GigabitEthernet1/0/1 device-tracking attach-policy POLICY1</pre>	<pre>device-tracking policy IPDT_POLICY no protocol udp tracking enable interface GigabitEthernet1/0/1 device-tracking attach-policy IPDT_POLICY</pre>	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

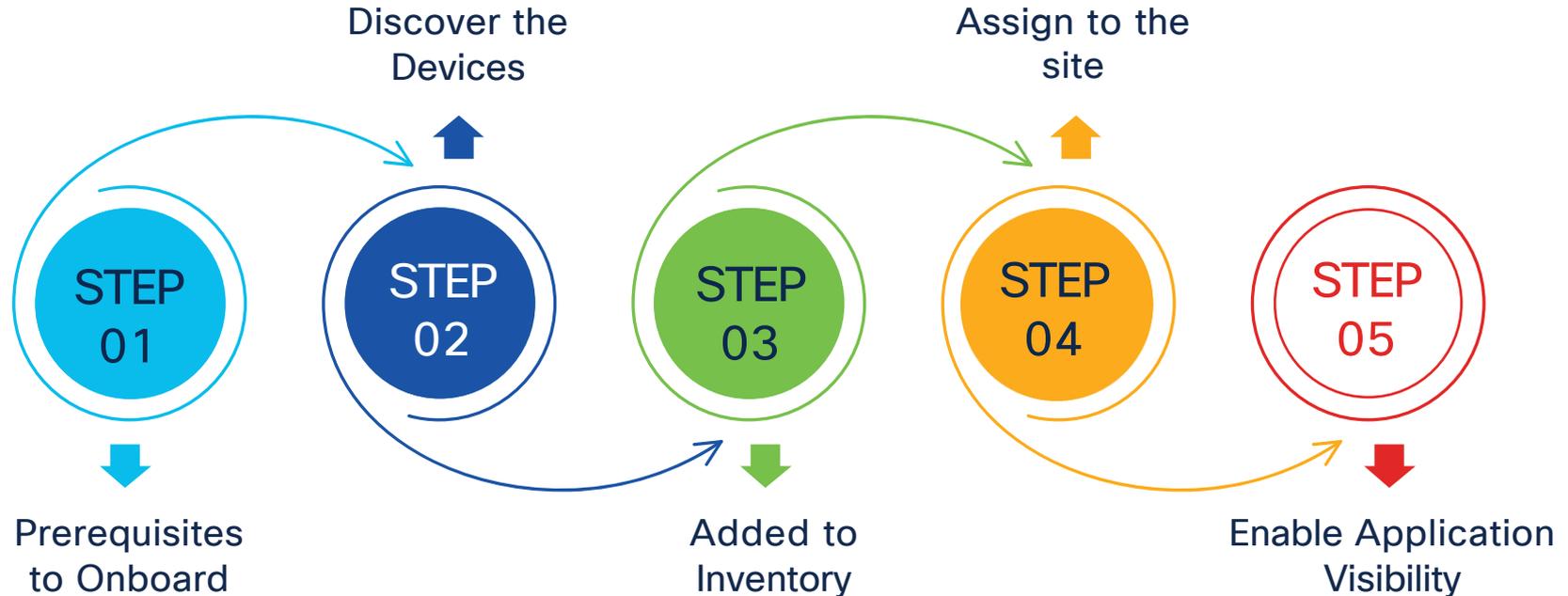
Brownfield
Configuration

```
Cat9300-Stack-Switch#sh
cts credentials
CTS password is defined in
keystore, device-id =
dummy
```

Catalyst Center
Device Controllability

If already present it
does not make any
changes

Brownfield Device Onboarding



Application Telemetry

Application Visibility (Application name & Throughput)

- IOS-XE Switches
- AireOS controllers - (Local Mode) or WSA(Flex/Fabric mode)

Application Experience (Latency, Jitter, and Packet Loss)

- Routers - Perfmon and ART Metrics
- 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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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

The screenshot shows the Cisco Catalyst Center interface. The top navigation bar includes 'Catalyst Center' and 'Provision / Inventory'. The main content area is titled 'Enable Application Telemetry'. It contains the following text:

You have chosen to enable Netflow with application telemetry on 1 wireless controllers.

By default, all non-guest WLANs on Wireless Controllers will be provisioned to send Netflow with Application telemetry. To override this default behavior, tag specific WLAN profile names with keyword "lan". Once specific WLANs are tagged, only those WLANs will be monitored.

For each wireless controller, select the AP modes where you would like to enable application telemetry.

- For Catalyst 9800 Series Wireless Controllers, the application telemetry source is always Netflow.
- For AireOS wireless controllers, the application telemetry source may be either Netflow or WSA (Wireless Service Assurance).

Warnings:

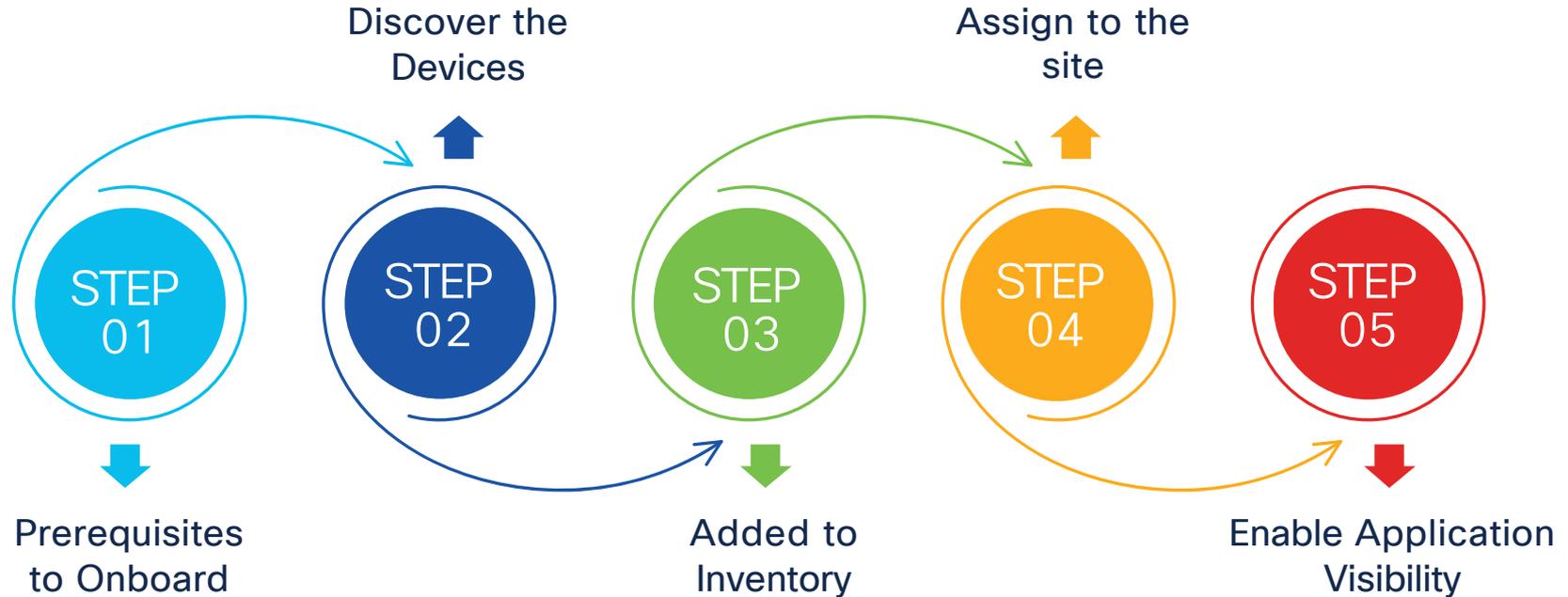
- Enabling or disabling application telemetry on the selected SSID types will cause a disruption in network services.
- Note: In order to update application telemetry configuration on the WLC, disable application telemetry first and then re-enable it. To do so, please use the Disable/Enable Application Telemetry buttons in the Actions menu.

Configuration for POD4-C9800-CL1:

- Local Flex/Fabric
- Include Guest SSIDs
- Telemetry Source: **NetFlow**

Buttons: Cancel, Enable

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

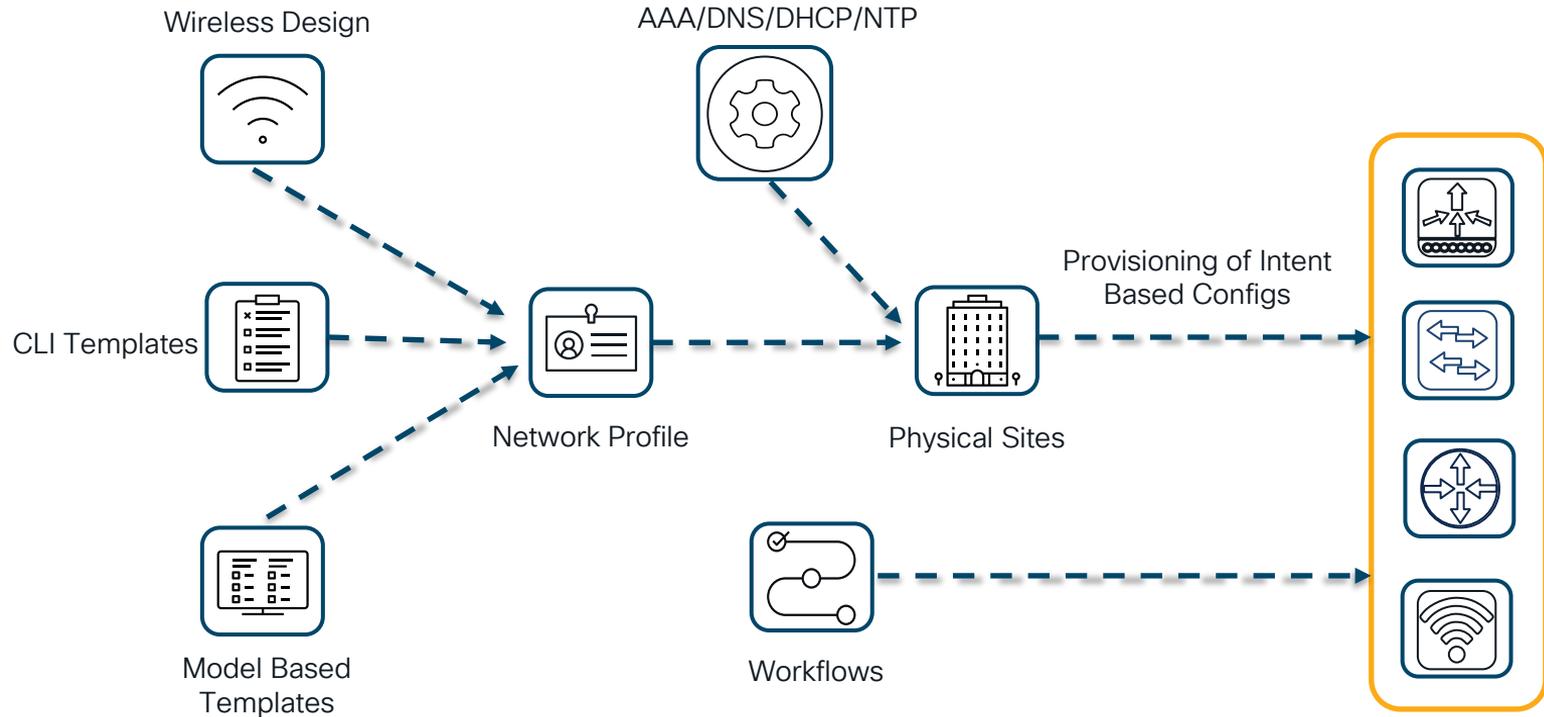
The screenshot shows the Catalyst Center interface. On the left, a list of devices is shown under 'Global'. The device 'POD4-C9300-Access1.tmelab.com' is selected. On the right, the 'Update Telemetry Settings' dialog is open. The 'Force Configuration Push' checkbox is checked and highlighted with a green box. Below it, a table lists various telemetry settings and their current values.

Setting	Value	
GLOBAL/INDIA/BANGALORE 1/FLOOR2	POD4-C9300-Access1.tmelab.com	
The following settings will be deployed during assignment to site.		
POD4-C9300-Access1.tmelab.com	Syslog Server	Catalyst Center
	Wired Endpoint Data Collection	Yes
	Cisco TrustSec (CTS) Credentials	No
	Streaming Telemetry	Yes
	Application Visibility	Enabled
	SNMP Trap Receiver	Catalyst Center
	Syslog Level	6 - Information Messages
	Controller Certificates	Yes (Expires on: Aug 6, 2025)

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

Managing Your Brownfield Deployment

Day-1 Configuration Changes – Provisioning

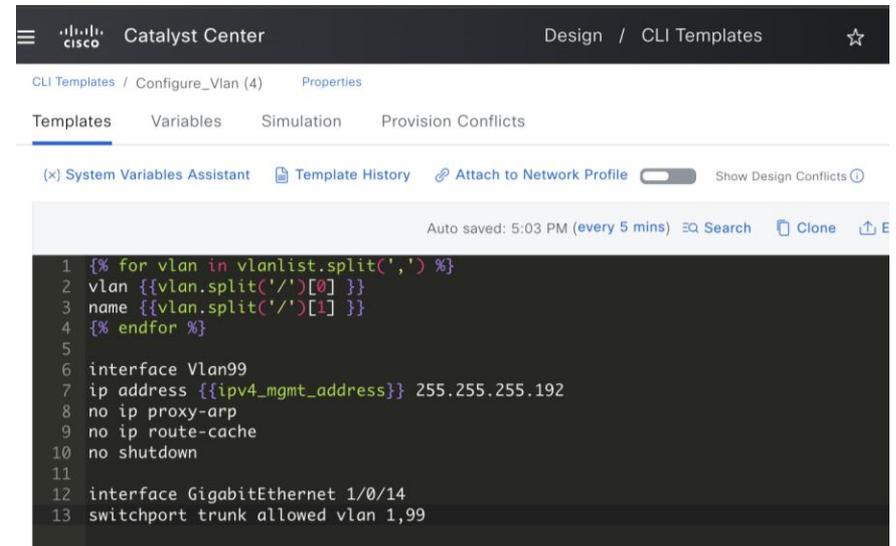


Scenario - Provisioning Workflow

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



The screenshot shows the Catalyst Center interface for editing a CLI template. The breadcrumb path is "CLI Templates / Configure_Vlan (4) Properties". The "Templates" tab is selected. The configuration content is as follows:

```
1 {% for vlan in vlanlist.split(',') %}
2 vlan {{vlan.split('/')[0] }}
3 name {{vlan.split('/')[1] }}
4 {% endfor %}
5
6 interface Vlan99
7 ip address {{ipv4_mgmt_address}} 255.255.255.192
8 no ip proxy-arp
9 no ip route-cache
10 no shutdown
11
12 interface GigabitEthernet 1/0/14
13 switchport trunk allowed vlan 1,99
```



CLI Templates



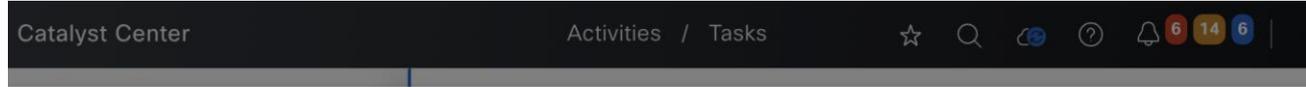
Network Profile



Physical Sites



Config Preview- Provisioning



Configurations - Side by side view

Device Name: POD4-C9300-Access1.tmelab.com
Configuration Source: All

Search configuration

Configuration to be Deployed ⓘ
62 Line(s)

```
1 ip radius source-interface vlan1
2 ip access-list extended ACL_WEBAUTH_REDIRECT
3 80 deny ip any host 172.100.1.99
4 500 permit tcp any any eq www
5 600 permit tcp any any eq 443
6 700 permit tcp any any eq 8443
7 800 deny udp any any eq domain
8 900 deny udp any any eq bootpc any eq bootps
9 exit
10 ip http server
11 ip http authentication local
12 ip http secure-server
13 aaa group server radius dnac-client-radius-group
14 server name dnac-radius 172.100.1.99
15 ip radius source-interface Vlan1
16 exit
17 aaa accounting identity default start-stop group dnac-client-radius-group
18 aaa accounting update newinfo periodic 2880
19 aaa authorization network default group dnac-client-radius-group
20 aaa authorization network dnac-cts-list group dnac-client-radius-group
21 aaa authentication dot1x default group dnac-client-radius-group
22 aaa authentication login dnac-cts-list group dnac-client-radius-group
23 radius server dnac-radius 172.100.1.99
24 address ipv4 172.100.1.99 auth-port 1812 acct-port 1813
25 pac key *****
26 retransmit 3
27 timeout 4
28 automate-tester username dummy ignore-acct-port probe-on
29 exit
30 radius-server vsa send authentication
31 radius-server vsa send accounting
32 radius-server dead-criteria time 5 tries 3
33 radius-server deadtime 3
34 radius-server attribute 31 send nas-port-detail mac-only
35 radius-server attribute 31 mac format ietf upper-case
36 radius-server attribute 8 include-in-access-req
```

Running Configuration ⓘ
1655 Line(s)

```
29 aaa new-model
30 !
31 !
32 aaa group server radius dnac-client-radius-group
33 server name dnac-radius 172.100.1.99
34 ip radius source-interface Vlan1
35 !
36 aaa authentication login default local
37 aaa authentication login dnac-cts-list group dnac-client-radius-group
38 aaa authentication dot1x default group dnac-client-radius-group
39 aaa authorization exec default local
40 aaa authorization network default group dnac-client-radius-group
41 aaa authorization network dnac-cts-list group dnac-client-radius-group
42 aaa accounting update newinfo periodic 2880
43 aaa accounting identity default start-stop group dnac-client-radius-group
44 !
45 !
46 aaa server radius dynamic-author
47 client 172.100.1.99 server-key 7 xxxxxxxx
48 !
49 aaa session-id common
50 switch 1 provision c9300-48u
51 !
52 !
53 !
54 !
55 !
56 !
57 !
58 !
59 !
60 ip name-server 172.100.1.200
61 ip domain lookup source-interface Vlan1
62 ip domain name tmelab.com
63 !
64 !
```



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
<pre>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</pre>	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.
<pre>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</pre>	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
<pre>aaa group server radius ise server name test ! aaa new-model aaa session-id common</pre>	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

The screenshot displays the Cisco Catalyst Center interface for device C9300-Pod2-Dist-2.tmelab.com. The top navigation bar shows the Cisco logo and 'Catalyst Center'. The device details include: Reachable, Managed, IP Address: 192.168.2.199, Device Model: Cisco Catalyst 9300 Switch, Device Role: DISTRIBUTION, and Uptime: 18 days 6 hrs 26 mins. The left sidebar contains sections for DETAILS, SECURITY, FIELD NOTICES, and COMPLIANCE. The main content area shows the 'Change History (Running Config)' for the device, with a 'Config Drift Date Range' from Nov 7, 2024, to Jan 21, 2025. A chart displays the number of lines of configuration drift over time, with a legend for In-band Config Drift (blue), Out-of-band Config Drift (purple), and Labelled Config (orange). Below the chart, two 'Running Config' versions are compared: 'Nov 12, 2024 02:03 PM' and 'Jan 07, 2025 06:50 PM'. The configurations are shown side-by-side, with line numbers 3 through 151. The 'Jan 07, 2025' version shows several changes, including a new 'hostname C9300-Pod2-Dist-2' and updated interface configurations for GigabitEthernet1/0/2 through 1/0/5.

Compliance

The screenshot displays the Cisco Catalyst Center interface for a specific device. The main content area shows a compliance check summary with the following categories and details:

- Network Settings:** 0 Open Violations. Compliant since Jan 24, 2025 2:12 AM. Compliance last run on: Feb 3, 2025 4:30 AM.
- EoX - End of Life:** Compliance last run on: Feb 6, 2025 3:11 AM. Software: Compliant, Hardware: Compliant, Module: Compliant.
- Startup vs Running Configuration:** 12 days since out of sync. Compliance last run on: Feb 3, 2025 4:30 AM. Lines added: 1, Lines removed: 0, Lines modified: 0.
- Network Profiles:** 2 Open Violations. Non-Compliant since Jan 24, 2025 4:02 PM. Compliance last run on: Feb 3, 2025 4:30 AM. CLI Template: 2.
- Application Visibility:** 0 Open Violations. Compliant since Feb 3, 2025 4:30 AM. Compliance last run on: Feb 3, 2025 4:30 AM.
- Software Image:** 17.09.06a Golden Image Version. Running Version: 17.9.2. Non-Compliant since Jan 23, 2025 8:57 PM. Compliance last run on: Feb 6, 2025 6:31 AM.
- Critical Security Advisories:** 1 violation. Non-Compliant since Jan 30, 2025 1:24 AM. Compliance last run on: Feb 6, 2025 1:24 AM.

Annotations with arrows point from green callout boxes to specific elements in the screenshot:

- Identifies devices with mismatch in configured Network settings on Catalyst Center:** Points to the Network Settings card.
- End of Sale & End of Life Alerts:** Points to the EoX - End of Life card.
- Identifies devices startup config does not match running config:** Points to the Startup vs Running Configuration card.
- Identifies devices with mismatch in configuration provisioned using Intent Workflow:** Points to the Network Profiles card.
- Identifies devices with mismatch in configuration provisioned using Application Visibility (CBAR) workflow:** Points to the Application Visibility card.
- Identify devices impacted with Critical Security Advisories:** Points to the Critical Security Advisories card.
- Helps Identify devices which are not running Golden Tag Images:** Points to the Software Image card.

Network Profile- Compliance Remediation

The screenshot displays the Cisco Catalyst Center interface for a device named 'POD4-C9300-Access1.tmelab.com'. The interface includes a navigation sidebar on the left with sections for DETAILS, SECURITY, FIELD NOTICES, and COMPLIANCE. The main content area shows a 'Compliance Summary' for 'Network Profiles' with a 'Fix All Configuration Compliance Issues' button. Below this, a table lists violations, with one entry for '9300_Day_N-EEM' highlighted. A 'Realize Template' window is open, showing the CLI configuration for this template. Green callout boxes provide annotations: 'Acknowledge config violations' points to the 'Acknowledge' button; 'Fix config violations by re-provisioning the intent' points to the 'Fix All Configuration Compliance Issues' button; 'Details of the intent config which is causing deviation/violation' points to the CLI configuration; and 'Which Network Intent config is in Non-compliance with the device config' points to the violation entry in the table.

DETAILS

- Summary
- System
- Interfaces
- Layer 2 Configuration *BETA*
- Browse Configurations
- User Defined Fields
- REP Rings
- Wireless Info

SECURITY

- Advisories

FIELD NOTICES

- Field Notices
- Potential Field Notices

COMPLIANCE

- Summary

You can now fix all configuration compliance issues on this device. You will be able to review before the fix is applied. [Fix All Configuration Compliance Issues](#)

Compliance Summary / Network Profiles [View Preference for Acknowledged Violations](#)

CLI Template (1)

CLI Deviations As of: Jan 24, 2025 4:04 PM

Search Table

Open Violations (1) Acknowledged Violations (0)

Template	Action
9300_Day_N-EEM	Acknowledge

1 Record(s) Show Records: 10 1 - 1

Realize Template: 9300_Day_N-EEM [View CLI Template Best Practices](#)

```
7 7 action 1.4 cli command "switchport access vlan90"
8 8 action 1.5 cli command "no shutdown"
9 9 action 1.6 cli command "end"
10 exit
```

Acknowledge config violations

Fix config violations by re-provisioning the intent

Details of the intent config which is causing deviation/violation

Which Network Intent config is in Non-compliance with the device config

Security Advisory- Compliance

Scan based on

- Hardware
- Software
- Running config – CX Cloud Integration
- Supports Regex based config scan

Fixed software version details to address the advisory

Shows all the critical advisories impacting the device

Advisory ID	Advisory Title	CVSS Score	Impact	Fixed Versions	CVE	Custom Match Pattern	Known Since	Last Updated
cisco-sa-iosxe-webui-privesc-j22SaA4z	Multiple Vulnerabilities in Cisco IOS XE Software Web UI Feature	10	Critical	17.3.8a	CVE-2023-20198 CVE-2023-20273	Add match pattern	Oct 16, 2023	Nov 1, 2023

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

CISCO *Live!*

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

Distribute

01

Copy of Images to flash via
HTTPS/SCP

03

ap image pre-download
(ewlc 9800)

Install add file <Image Name>

Activate

01

Install activate <image name>

02

Install Commit

02

SWIM- Workflow

Catalyst Center Design / Image Repository / Image Family

From Design > Image Repository, Select Device Family

Global

< Image Repository

Cisco Catalyst 9800-40 Wireless Controller

Images (6)

Filter Images

Image Name	Version	Devices	Image Status
C9800-40-universalk9_wlc.17.14.01.SPA.bin Verified	17.14.01.0.1391 Add On (N/A)	0	★

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

Device Name	IP Address	Inventory	Provision	Telemetry	Device Replacement	Switch Refresh	Compliance	More	ty	EoX Status	Manageability
D1-9500.pseudoco.com	10.4.15.2	Inventory	Provision	Telemetry	Device Replacement	Switch Refresh	Compliance	More			
AP6C71.0DE6.12F0	10.4.84.3	Software Image									
AP6C71.0DE6.1074	10.4.84.3										
AP0C75.BDB4.005C	10.4.84.3										
AD3-3850.pseudoco.com	10.4.95.5										
Refresh_9300.pseudoco.com	10.4.95.6										
SS-9800.pseudoco.com	10.4.174.10										

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



SWIM-C9800 Software Upgrade (ISSU)

Provision / Inventory ☆ 🔍 🔄 ? 🔔 2 14 2 | 👤 admin ▼

Device: 9800_SWIM (172.100.1.54)
Running Image: C9800-CL[17.06.03.0.3629]
Golden Image: C9800-CL-universalk9.17.09.06.SPA.bin
Reboot Required: Yes

Readiness Checks Results

[Re-Execute Checks](#)

[Export](#)

[As of: Feb 6, 2025 3:11 PM](#)

Check Type	Description	Status	Last Checked
Flash check	Flash check: SUCCESS Expected: 2662 MB Available Free space is: 10213 MB [Install mode needs free space to 2.2 times of Image size]	🟢	Feb 6, 2025 3:11 PM
Service Entitlement Check	Could not validate license service contract	🟡	Feb 6, 2025 3:11 PM
Startup config check	Startup configuration exist for this device	🟢	Feb 6, 2025 3:11 PM
Config register check	Config-register verified successfully Expected: 0x2102,0x102 Actual: 0x2102 Action: No action required	🟢	Feb 6, 2025 3:11 PM
File Transfer Check	HTTPS is NOT reachable / SCP is reachable Expected: Controller certificate has to be installed successfully and Device should be able to reach Catalyst Center (172.100.1.195) via HTTPS. Action: Reinstall the controller certificate, which is installed automatically on the device when it is assigned to a site. Please ensure that the device is assigned to a site for HTTPS transfer to work. Alternatively, the controller certificate (re)installation is attempted when HTTPS failure is detected during image transfer.	🟡	Feb 6, 2025 3:11 PM
ISSU Compatibility Check	ISSU Compatibility Check Successful.	🟢	Feb 6, 2025 3:11 PM
Image Version Support	The golden image is applicable to the device	🟢	Feb 6, 2025 3:11 PM

Executes various check before starting Image upgrade workflow

Checks include if Image can be upgraded using ISSU

SWIM- Flexible Device Ordering

The screenshot shows the Catalyst Center 'Image Update' page with the 'Device Activation Order' section set to 'Parallel'. The interface includes a search bar, a table of 5 selected devices, and 'Back' and 'Next' buttons. The table columns are: Device Name, IP Address, Site, Device Series, Device Role, Current Image, and Update Image. The selected devices are:

Device Name	IP Address	Site	Device Series	Device Role	Current Image	Update Image
C9300-Edge-Pod2.tmelab.com	192.168.2.10	.../US West/SJ1	Cisco Catalyst 9...	Access	cat9k_losxe_npe.1...	cat9k_losxe.1
C9300-Pod2-Dist-2.tmelab.com	192.168.2.199	.../US West/SJ1	Cisco Catalyst 9...	Distribution	CAT9K[17.03.05.0...	cat9k_losxe.1
C9300Access-2-Pod2.tmelab.com	192.168.2.5	.../Bangalore 1/floor2	Cisco Catalyst 9...	Access	CAT9K[17.12.03.0...	cat9k_losxe.1
Cell1-IE3000-1.tmelab.com	10.62.147.26	.../US West/Production-Line2	Cisco Catalyst IE...	Access	ie3x00-universalk9...	ie3x00-univer

The screenshot shows the Catalyst Center 'Image Update' page with the 'Device Activation Order' section set to 'Sequential'. The interface includes a search bar, a table of 4 selected devices, and 'Back' and 'Next' buttons. The table columns are: Device Name, IP Address, Site, Device Series, Device Role, Current Image, and Update Image. The selected devices are:

Device Name	IP Address	Site	Device Series	Device Role	Current Image	Update Image
C9300-Pod2-Dist-2.tmelab.com	192.168.2.199	.../US West/SJ1	Cisco Catalyst 9...	Distribution	CAT9K[17.03.05.0...	cat9k_losxe.1
C9300Access-2-Pod2.tmelab.com	192.168.2.5	.../Bangalore 1/floor2	Cisco Catalyst 9...	Access	CAT9K[17.12.03.0...	cat9k_losxe.1
C9300-Edge-Pod2.tmelab.com	192.168.2.10	.../US West/SJ1	Cisco Catalyst 9...	Access	cat9k_losxe_npe.1...	cat9k_losxe.1
Cell1-IE3000-1.tmelab.com	10.62.147.26	.../US West/Production-Line2	Cisco Catalyst IE...	Access	ie3x00-universalk9...	ie3x00-univer

- 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

CISCO Live!

SWIM- Device Activation Order

Device Activation Order

You can use filters to sort devices and order their activation in parallel or sequentially. After devices are sorted, you can reorder them sequentially.

Device in Parallel(1) [Edit Order](#)

Parallel Sequential

If software version supports ISSU, Software upgrade through ISSU can be enabled

Filter Devices

1 Selected [Move to Sequential Update Order](#) ISSU

Device Name	IP Address	Site	Device Series	Device Role	Current Image	Update Image	Comment
9800_SWIM ISSU	172.100.1.54	Unassigned	Cisco Catalyst 9800 ...	Access	C9800-CL[17.06.03.0.3...	C9800-CL-universalk9.1... ISSU	ISSU Validation Successful Update Readiness Report

If ISSU is grayed out, device will perform normal software activation

SWIM- Schedule Distribution & Activation

Schedule Task and Clean Up

You can schedule software distribution, activation, and cleanup of device memory.

The selected devices belong to different sites. Your time zone will be used as the default site time zone.

Software Distribution

Now Later

Start Date/Time

Jan 24, 2025

8:09 PM

Time Zone

Asia/Calcutta

Software Activation

After Distribution

Now Later

Start Date/Time

Jan 25, 2025

6:09 AM

Time Zone

Asia/Calcutta

INITIATE FLASH CLEANUP AFTER ACTIVATION

Flash clean up will store only the running image and remove all previous images saved on the device.

Initiate Flash Cleanup After Activation

Software Distribution

⚠ If the ITSM ServiceNow application is enabled, choose Later.

Now Later

Task Name*

Software Image Distribution

Start Date/Time

Jan 13, 2023

4:00 PM

Time Zone

America/Los_Angeles

Software Activation

ⓘ Activation is skipped for current Image Update workflow.

Audit Logs Tasks

Search by description

SUMMARY

Type (2)

- Task
- Work Item

OS UPDATE

admin

Software Image Distribution

Starts: Jan 13, 2023 4:00 PM

Status: Ticket Approved

SWIM- Staggered AP Upgrade

The screenshot displays the Cisco Catalyst Center Provisioning interface. The main header shows 'Catalyst Center' and 'Provision / Inventory'. A notification banner at the top states: 'To provision subscriptions on devices that have not been discovered with NETCONF'. The left sidebar shows 'Global' and 'Devices (6)' with a focus on 'Software Images'. A table lists several devices, including '9800_SWIM' with IP 172.100.1.54. The main content area shows a task titled '9800_SWIM (172.100.1.54) Image Update' with a progress bar at 82%. The 'Operations' tab is active, showing a sequence of steps: Distribution (17 minutes 57 seconds), Activation (22 minutes 46 seconds), Pre Activation Operation (1 second), Image Activation (22 minutes 14 seconds), and Staggered AP Upgrade (29 seconds). The 'Staggered AP Upgrade' step is highlighted with a green box and contains the following details:

Task Name	Staggered AP Upgrade
Task Status	In Progress (Staggered AP Upgrade Status : Completed, Total number of APs = 4, Upgraded = 0, In Progress = 1, Remaining = 3, APS not handled by Rolling AP Upgrade = 0)

Below the operations list, a green callout box contains the text: 'Staggered AP Upgrade based on'.

Switch Refresh

Catalyst Center Workflows

Maintain your network consistently with Workflows.

High end-to-end workflows tailored to make

Network Devices

- Replace Device (Wired, Wireless)
- Switch Refresh (Wired)**
- Access Point Refresh (Wireless)
- Configure REP Ring (Non-Fabric)
- Configure REP Ring (Fabric)
- Configure Access Points (Wireless)

Prerequisites

Complete the following task(s) before you refresh a switch.

Mark a Golden Image

For the new device series being on-boarded, please ensure you have a golden image marked for the device series. You can complete this action from the image repository page. [Image Repository](#)

Old device auth type and golden image

If the old device is configured with MDS and the golden image for new device is higher than 17.14.1, the new device will be configured with SHA.



Select Devices

Select the devices that you want to refresh.

Note: Switch Refresh is currently limited to 3650 and 3850 device series running on IOS-XE, New device for refresh is limited to 9300 device series with same number of ports as Old Device.

Search Hierarchy

- Global
- Demo
- India
- US West
- Whynot

Switches (2)

Device Name	IP Address	Refresh Status	Serial Number
<input checked="" type="checkbox"/> POD2-3850-Distr	192.168.2.2	<input checked="" type="radio"/> Marked for Refresh	FCW2050C16T
<input type="checkbox"/> POD4-3850-Distribution	192.168.4.2	<input checked="" type="radio"/> Marked for Refresh	FCW2126F1CA

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.

Old Devices			New Devices	
Old Device Name	Platform Series	Site	New Device Name*	Platform
POD2-3850-Distr 192.168.2.2 FCW2050C16T	WS-C3850-24XU-S Cisco Catalyst 385...	..Global/US ...	POD2-9300-Distr	C9300-48U

Refresh AP

Cisco Catalyst Center Workflows

Maintain your network consistently with Workflows.

High end-to-end workflows tailored to make

Network Devices

- Replace Device: Replace your device in a few quick easy steps. (Wired, Wireless)
- Access Point Refresh: Replace Your Access Points with New ones. (Wireless)**
- Smart License Compliance: Explore capabilities for Smart License Enabled devices.
- Configure REP Ring (Fabric): Configure a REP Ring to enable
- Configure Access Points: Configure AP and Radio
- Provision Template: Provision templates directly to devices

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

Catalyst Center Access Point Refresh ☆ 🔍 🔄 ?

Assign New APs to Old APs

You have selected 1 Old APs for refresh. Assign New AP for each Old one. If New AP(s) is already connected, it will be detected in Catalyst Center either through WLC inventory or PnP based on the existing configuration. If New AP is not yet connected, provide the Serial Number of those New APs against each Old AP.

You can also download the Old APs list in CSV format, provide the details of the New AP against each Old AP and Upload it.

Would you like to auto detect your APs based on Switch Port NEW ⓘ

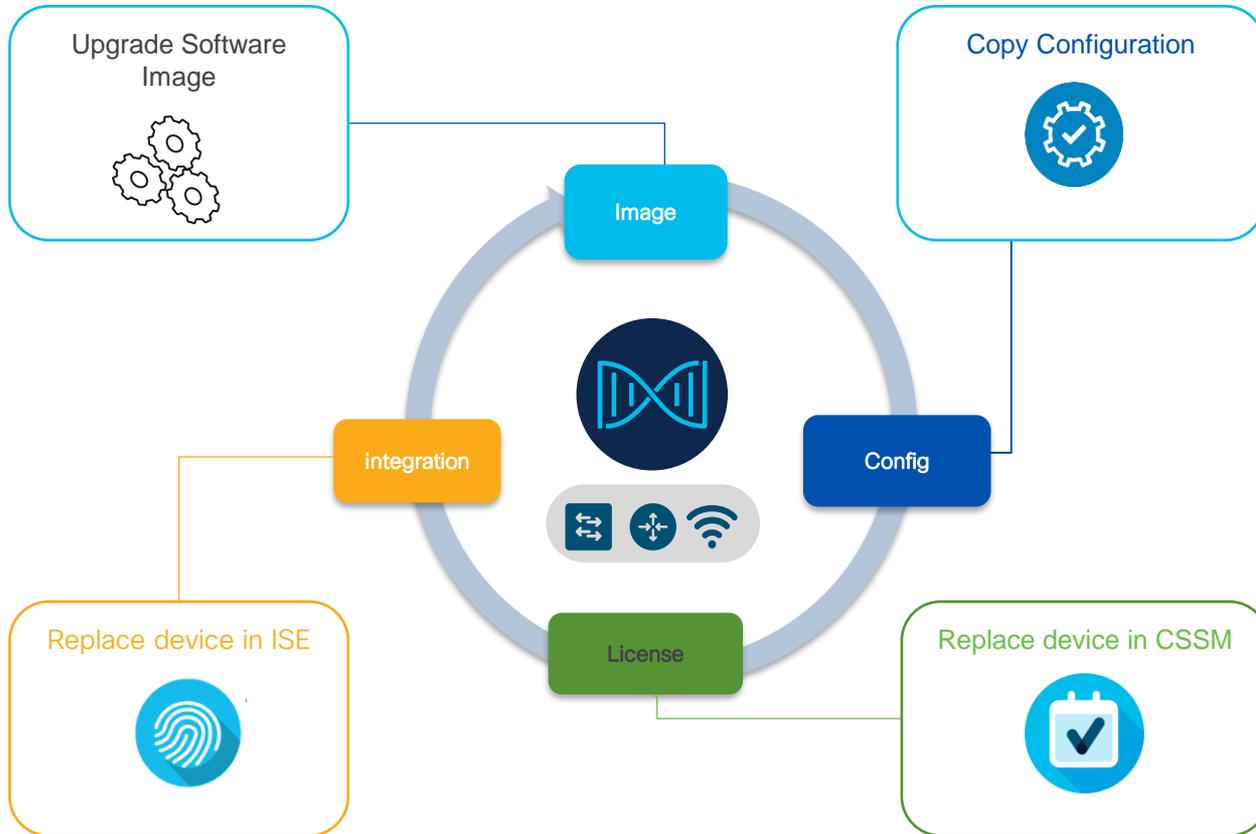
ACCESS POINTS (1)

🔍 Search Table

[↑ Upload CSV](#) [↓ Download CSV](#) 1 Selected [Delete](#)

Old Devices			New Devices				
<input checked="" type="checkbox"/>	Device Name	Platform	Site	Edit	Device Name*	Platform	Serial Number* ⓘ
<input checked="" type="checkbox"/>	POD4-AP3 192.168.4.74 FGL2245A8EK	AIR-AP4800-D-K9 Cisco 4800 SeriesIndia/Bengaluru	✎	POD4-AP3	C9115AXI-D	abc

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

Inventory

Delete Device (1)

Device Name	IP Address	Device Family	Comments
Switch.tmelab.com	192.168.1.11	Switches and Hubs	Device is eligible for deletion to proceed

1 Record(s) Show Records: 25 1 - 1

Clean Up Configuration

Selecting the clean up configuration option attempts to remove device settings that are configured as part of addition of device to inventory and site assignment

[View the list of configurations that will be deleted from the device](#)

The following settings configured during assignment of device to site will be deleted.

- DHCP Server
- AAA Server
- Wireless Service Assurance (WSA)
- AP Impersonation
- Controller CA Certificates
- Wired Endpoint Data Collection Enablement
- Syslog Server Definitions
- DNS Server
- HTTP Configuration
- Telemetry Certificates
- Wireless Telemetry
- PKCS12 Certificates
- SNMP Trap Server Definitions
- NetFlow Server Definitions

Only after a successful clean up, Catalyst Center will proceed with deleting the device(s)

Cancel Delete

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

LABOPS-1399 Walk in Lab

Exploring AI Ops: AI's Potential in Network Operations

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

CSSSENT-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



○ BU-led sessions

CISCO Live!

Webex App

Questions?

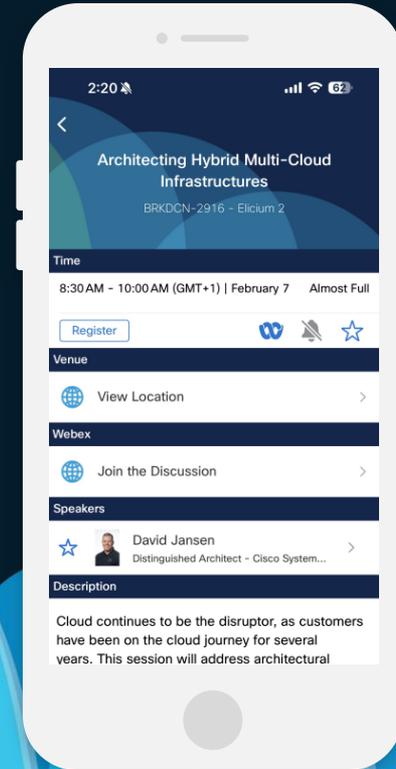
Use the Webex app to chat with the speaker after the session

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.

CISCO *Live!*



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

A series of overlapping, vertically-oriented ovals in various shades of blue, ranging from light to dark, positioned on the right side of the image. The ovals are layered, with some appearing in front of others, creating a sense of depth and movement.