The bridge to possible

Discovering and Managing Brownfield Deployment with Cisco Catalyst Center (formerly Cisco DNA Center)

Sneha Amarapuram
Customer Success Specialist

BRKOPS- 1461

Cisco Webex App

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKOPS-1461

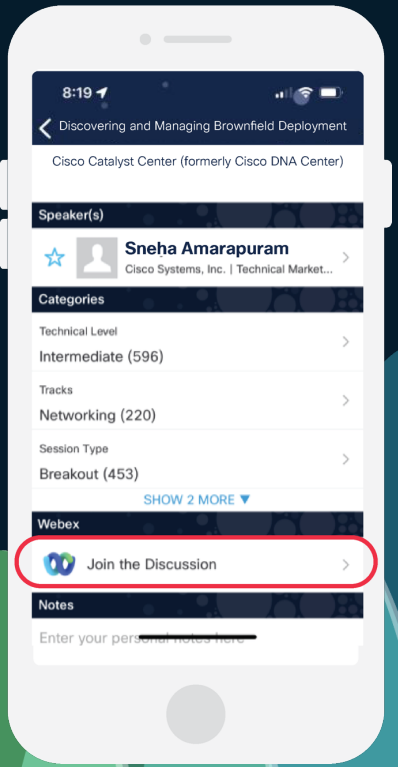
Questions?

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

How

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

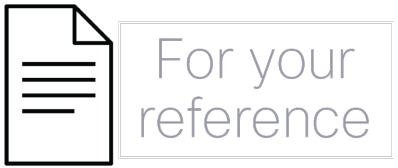
Webex spaces will be moderated by the speaker until June 7, 2024.



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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"



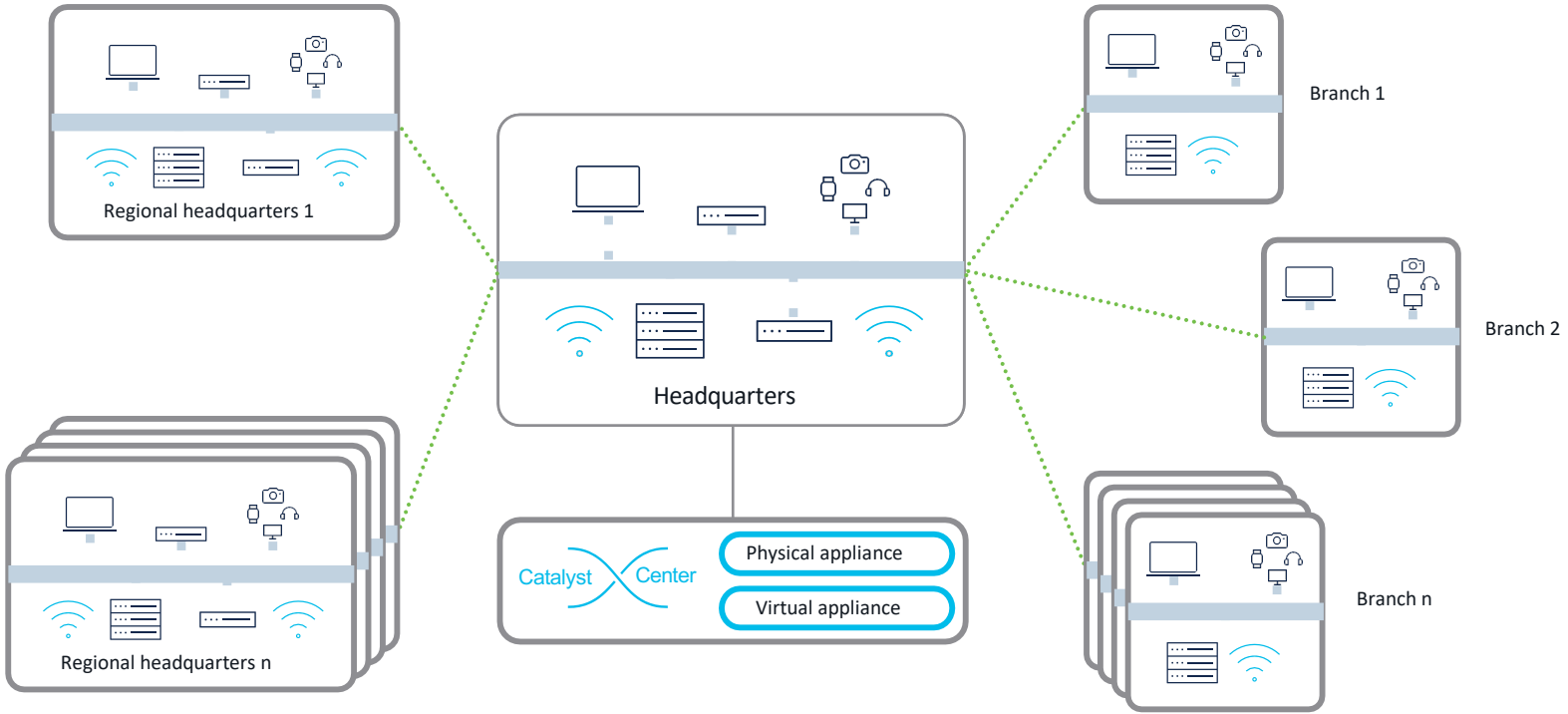
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Agenda

- Introduction to Catalyst Center
- Greenfield vs Brownfield Onboarding
- Device Onboarding into Catalyst Center
- Managing your brownfield deployment

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Single Management Console For The Campus



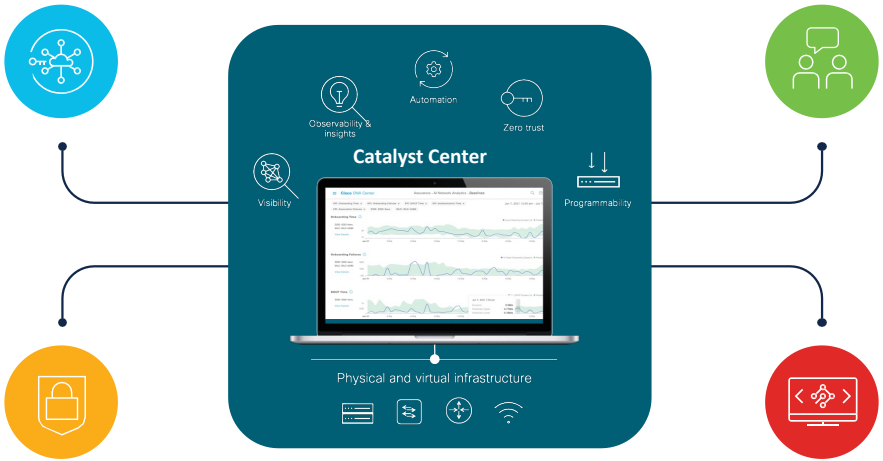
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Driving Business Outcomes

Achieve your long-term IT business goals – Today

NetOps

Automation and workflows simplify building and maintaining large scale networks. AI/MR streamlines and simplifies complex tasks



AIOps

AI/ML and predictive insights for proactive optimization to ensure consistent performance and reliability and the optimal user experience

SecOps

AI/ML and DPI Identify and classify endpoints, enforce security policies and mitigate threats for a complete workplace zero trust solution

DevOps

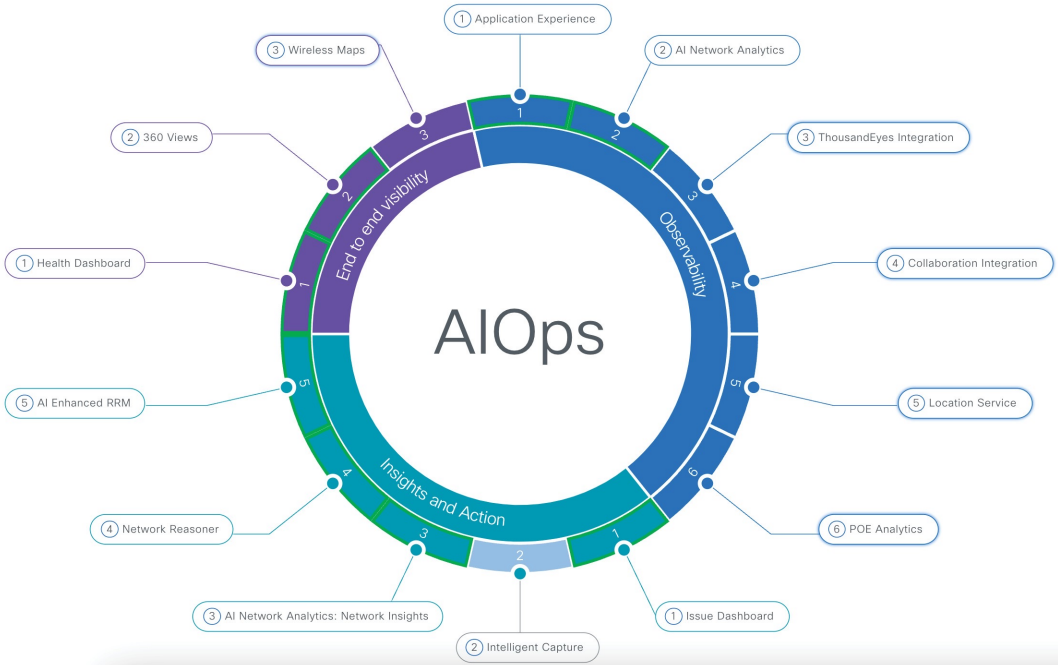
Mature APIs, SDKs, and closed-loop integrations, untangle the complexities of interconnecting third party systems

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Know Your Utilization

AIOps | NetOps | DevOps | SecOps

AIOps (8/14)



Catalyst Center
-> Explore

Completed | Incomplete | 8 of 14 steps completed

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

For your reference

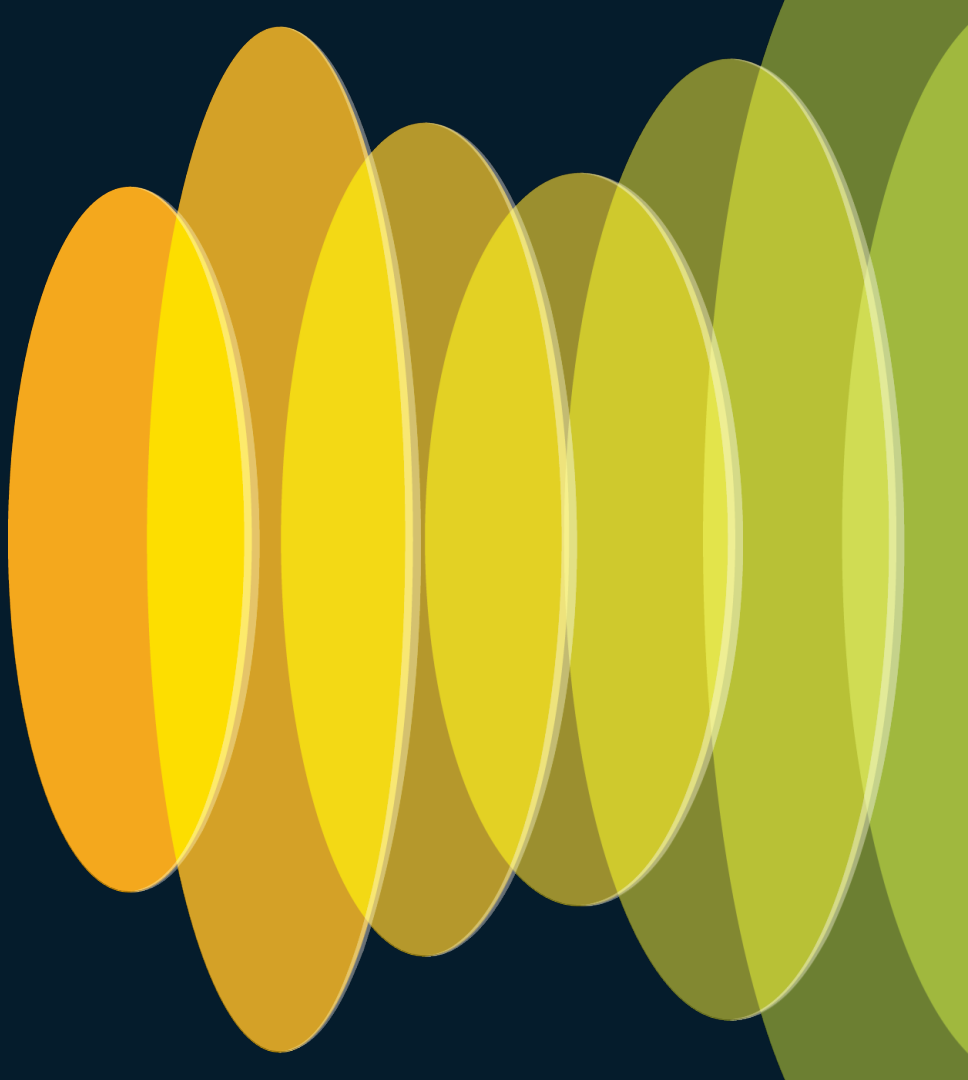
Prime Use Case Parity

	Catalyst Center 2.3.7
Reporting	
• Automation Reports	95%
• Assurance Reports	95%
Compliance	
• Compliance Visibility	95%
• Compliance remediation	80%
Maps	
• 2D Maps	100%
Assurance	
• Wired Visibility	95%
• Wireless Visibility	100%
• Issue Troubleshooting	100%

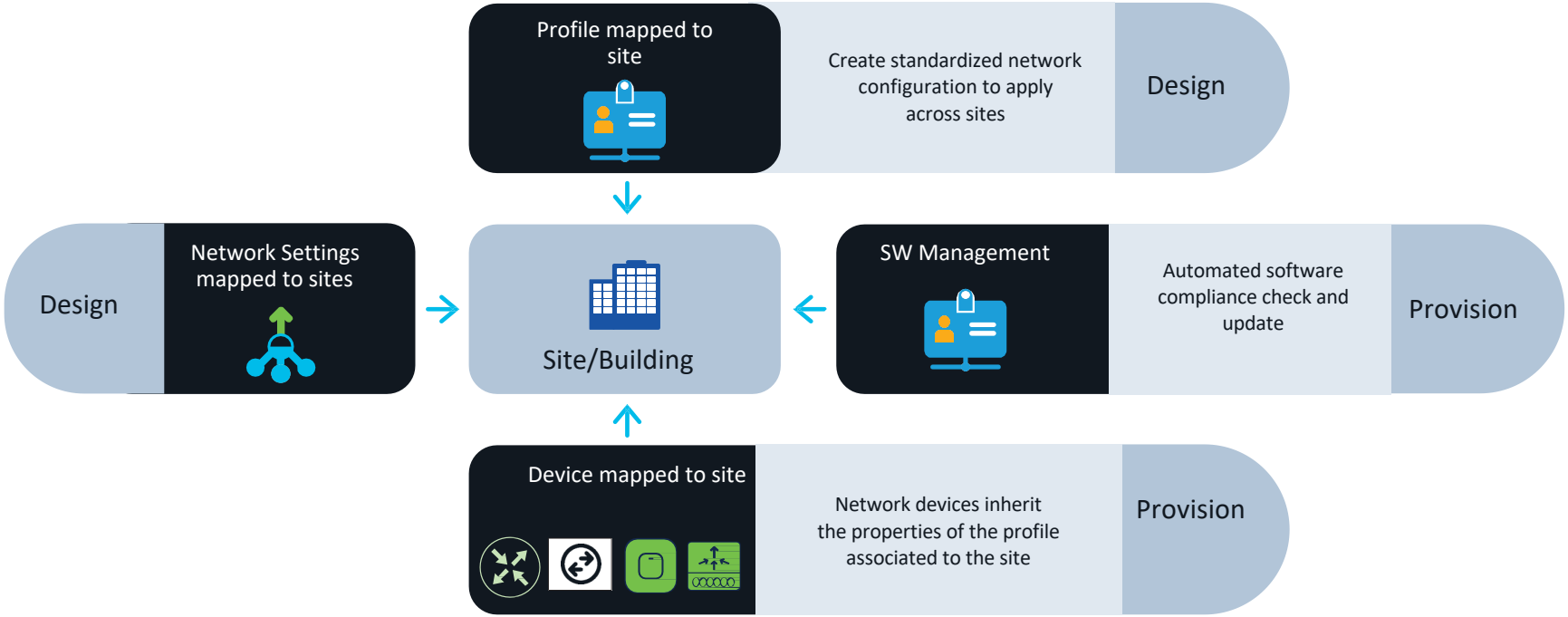
	Catalyst Center 2.3.7
Inventory	
• EoX, PSIRT	100%
Automation	
• WLAN Mgmt	95%
• AP Mgmt	95%
SWIM	
• Software Image Management	100%
Security	
• Rogue/ aWIPS Mgmt	95%

© 2024 Cisco and/or its affiliates. All rights reserved.

Greenfield vs Brownfield Onboarding

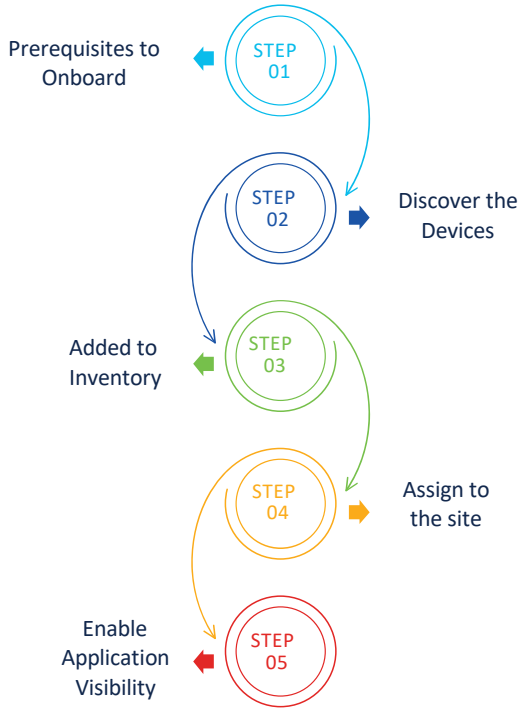


Site as a Focal Point in Catalyst Center

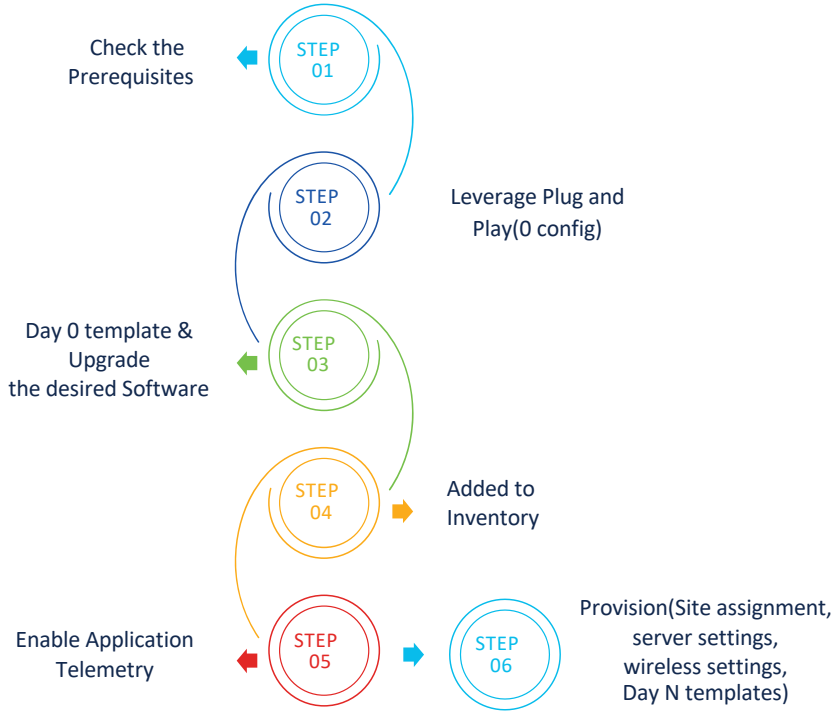


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Brownfield Device Onboarding



Greenfield Device Onboarding



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

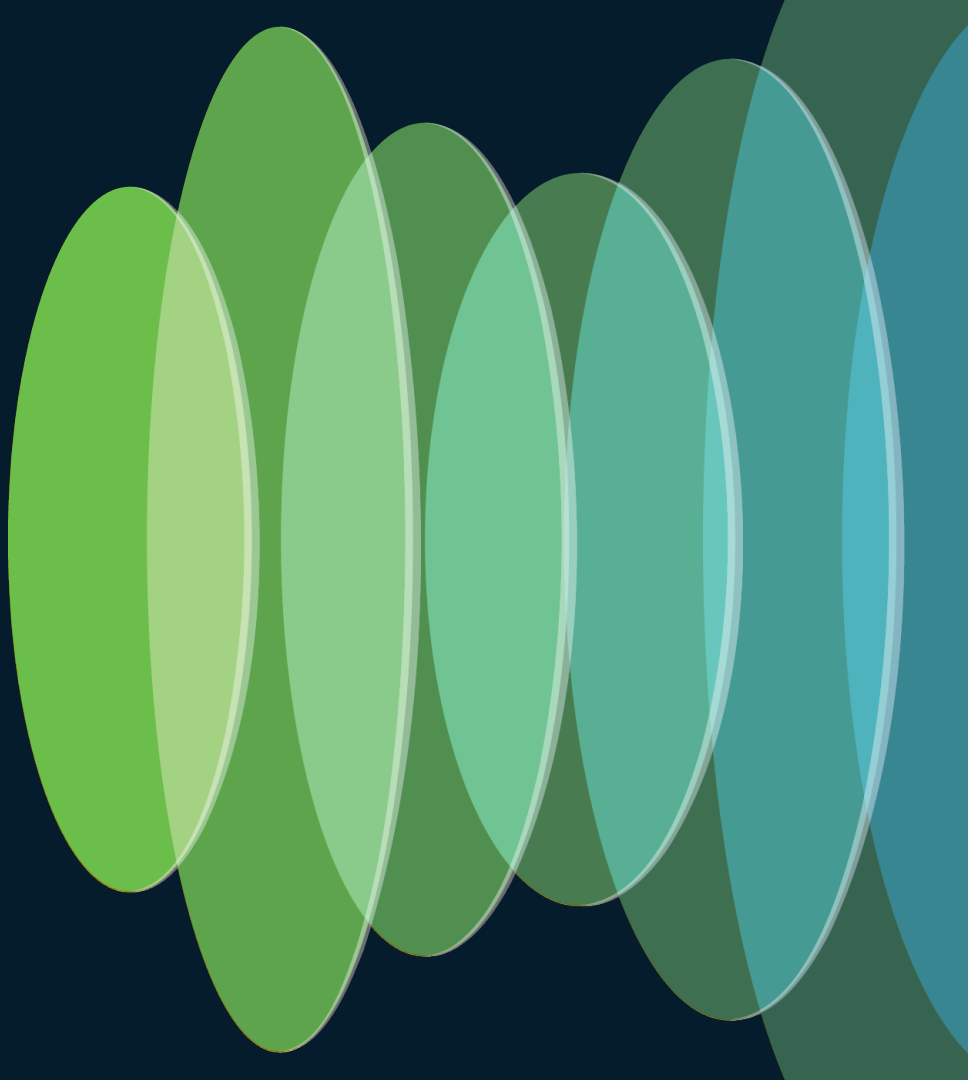
9800 WLC - Provisioned vs Non-Provisioned with Catalyst Center

For your reference

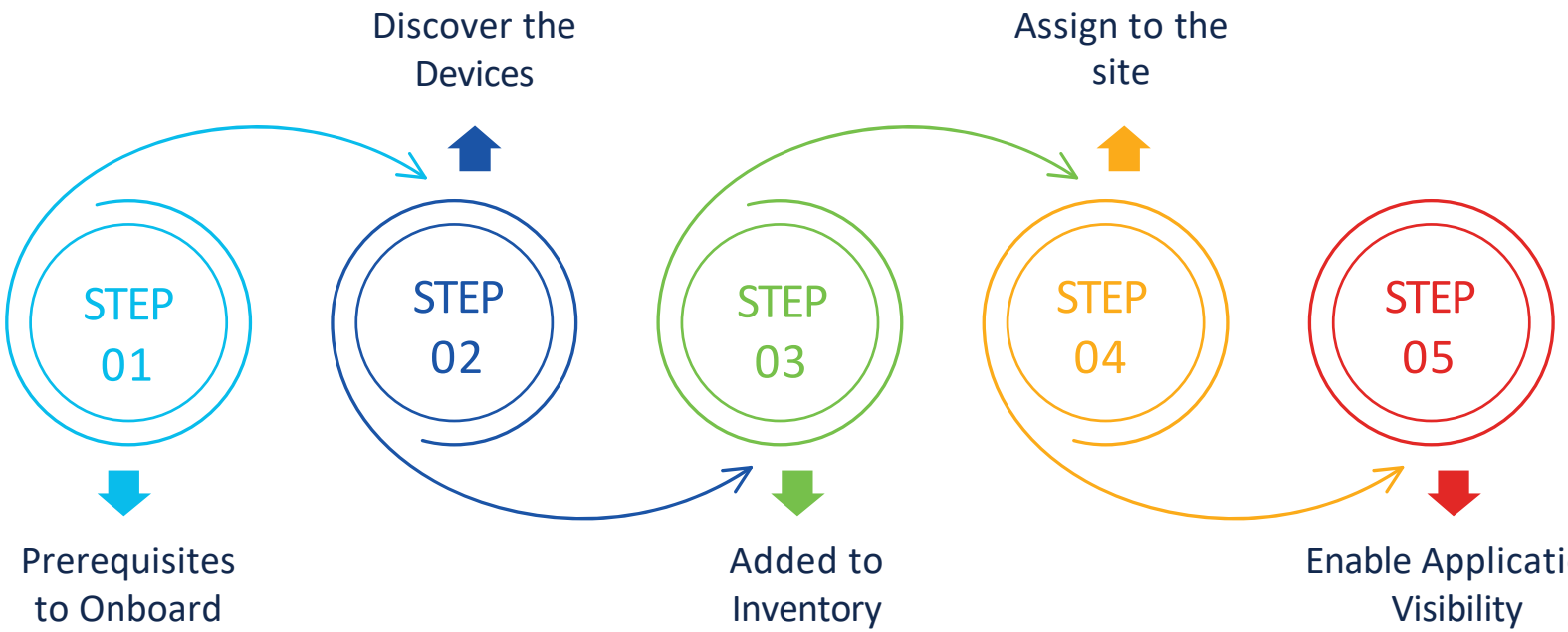
Features	Not Provisioned	Provisioned
Assurance Health	Yes	Yes
AI Network Analytics	Yes	Yes
Intelligent Capture	Yes	Yes
Rogue and aWIPS	Yes	Yes
Application Experience	Yes	Yes
Configure AP Workflow	Yes	Yes
Device Replacement Workflow	Yes	Yes
Enable CBAR	No	Yes
AP Refresh Workflow	Yes(2.3.7)	Yes
Configure RLAN Workflow	No	Yes
AI Endpoint Analytics	No	Yes
AI - RRM	Yes (2.3.7)	Yes

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Brownfield Device Onboarding



Brownfield Device Onboarding



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

1. 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

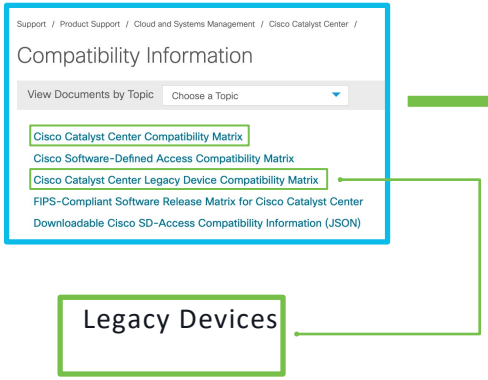
Prime Migration or Start Fresh

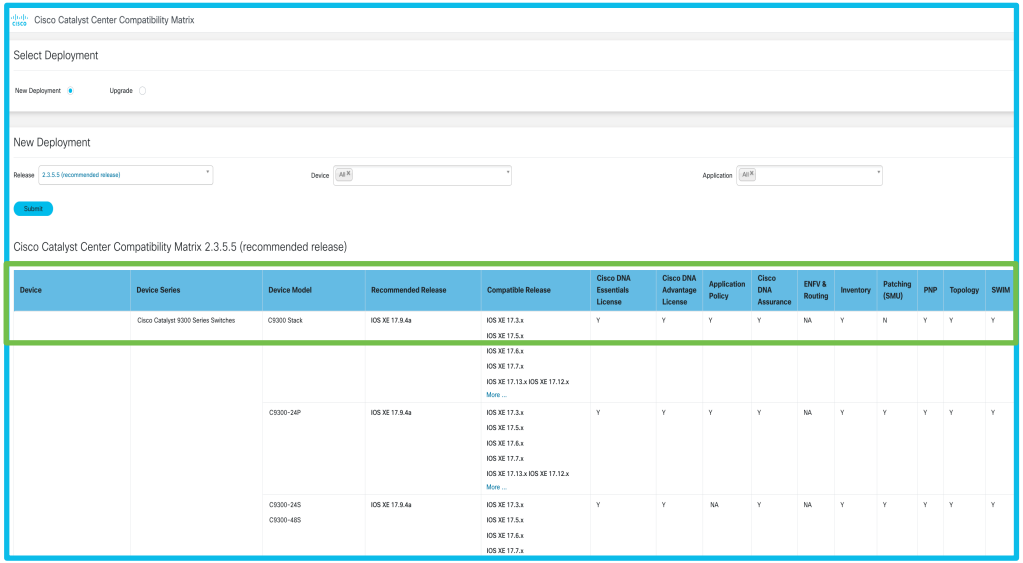
- Start from scratch on Catalyst Center or migrate from Prime (Prime Data Migration Tool makes it hassle free)

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

2. Check Catalyst Center and Network Devices Compatibility

Hardware/Software/License/Applications Compatibility





© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Device Support Types

For your reference

1) Supported

The device profile has been tested for all applications on Catalyst Center

3) Third Party Support

- Non-Cisco devices that support MIB-II/SNMP (RFC1213) 2.3.7.x
- No need of License
- Add device using SNMP v2/v3 credentials
- Exception - C1K device family classified as 3rd party
- Adding 3rd Party Device : Provision -> Inventory -> Add Device -> Third Party Device(Type)
- Third Party Support -
  - Discovery & Inventory
  - Device Uptime
  - Topology (Limited View)
  - Interface Status
  - Vendor Names (e.g., Palo Alto, HP)
  - Device 360 (Limited View)

2) Limited Support

- 541 legacy devices added – 2.3.5
- Limited Support –
  - Discovery
  - Topology
  - Device Reachability
  - Config Change Audit
  - Inventory
  - Software Image Management (Software images may not be available for EOL devices on cisco.com. Not recommended for EOL devices.)
  - Template Provisioning (Applicable only for switches.)

4) Unsupported

The device profile has not been tested with Catalyst Center.
You can try various features on the device only as best effort.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

3. Preferred latency -100ms to 200ms

4. A full list of URLs, FQDNs - Catalyst Center Security Best Practices/ Installation Guide

Some Important Ports

Ping	SSH	SNMP Poll	SNMP Trap	Syslog	NetFlow	HTTP/HTTPS	Netconf	Streaming Telemetry	Intelligent Capture(AP)
ICMP echo and reply	TCP 22	UDP 161	UDP 162	UDP 514	UDP 6007	TCP/80,443	TCP 830	25103	32626

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

5. 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

6. NETCONF for Cat9800 WLC & Cat 9k switches

- 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)

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

NETCONF Requirement

- Discover cat 9800, cat 9k with Netconf port enabled. Port 830 is recommended. Do not use standard ports like 22, 80, 8080
- NETCONF uses SSH credentials and it has to be admin privilege
- If aaa new-model is enabled,

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

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

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

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

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

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

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

7. Configuring Catalyst Center Before Onboarding Devices

Network Hierarchy-
Sites (Areas, buildings(physical address) & Floors) Create/ Import(.csv)/ Migrate from Cisco Prime

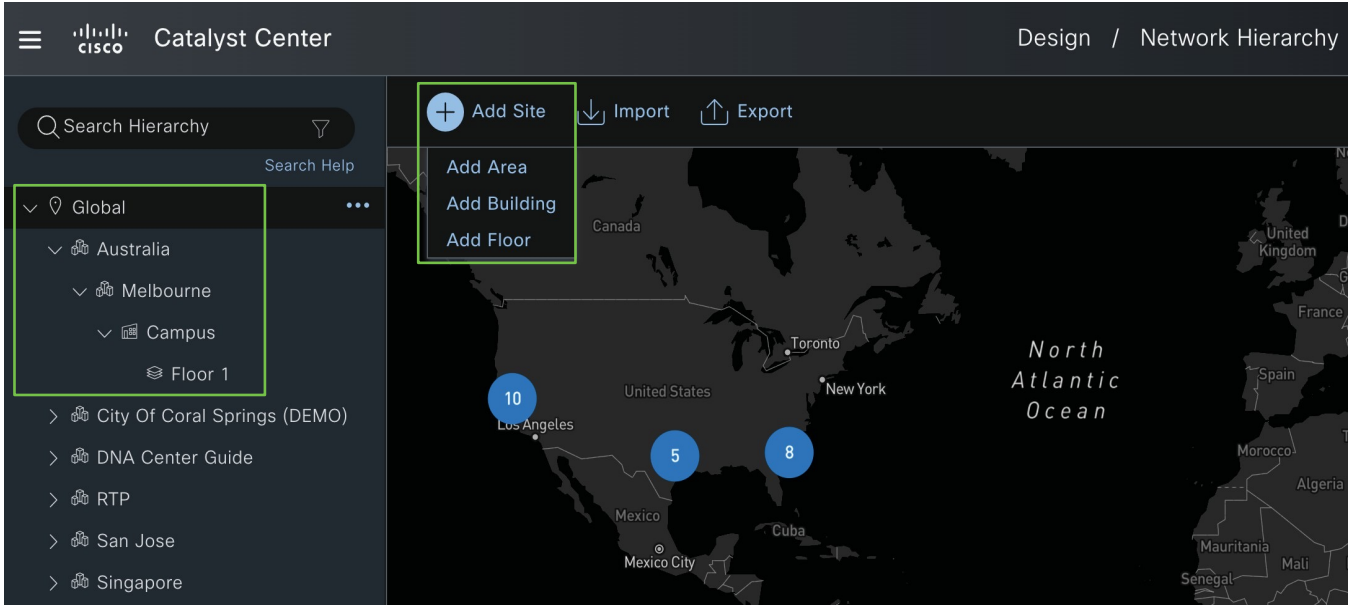
Floor Maps-
Upload(DXF, DWG, JPG, GIF, PNG, PDF)/ Import from Prime Maps(.gz,.tgz)/ Ekahau(.esx)/ Migrate from Prime

Network Settings-
Servers, Device Credentials, Telemetry

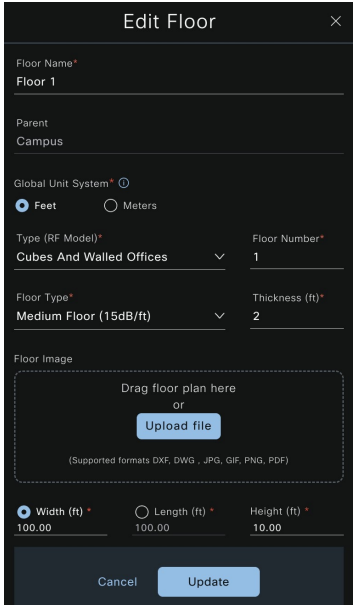
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Sites & Floor Maps

Create Sites(Add Area, Building, Floor)



Upload Floor Image

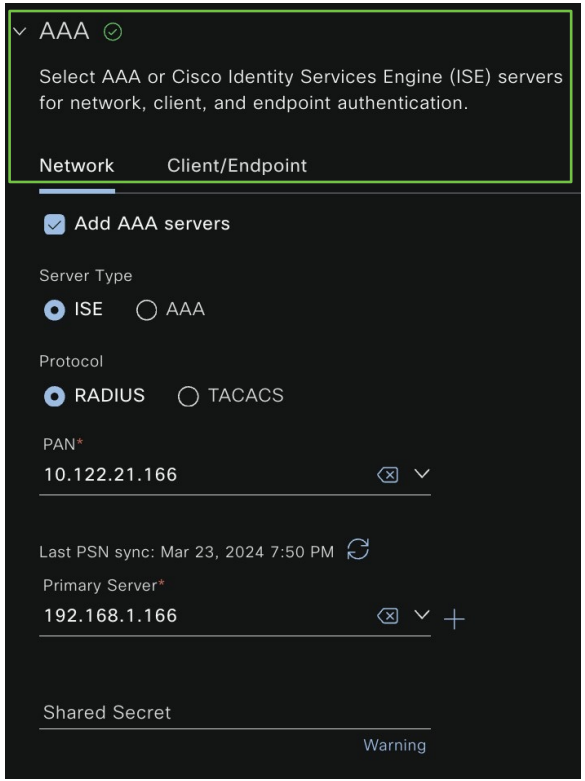


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Servers

- AAA
- DHCP
- DNS
- Stealthwatch Flow Destination
- Image Distribution
- NTP
- Time Zone
- Message of the Day

Design –> Network Settings -> Servers



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Device AAA and Site AAA Interaction

For your reference

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

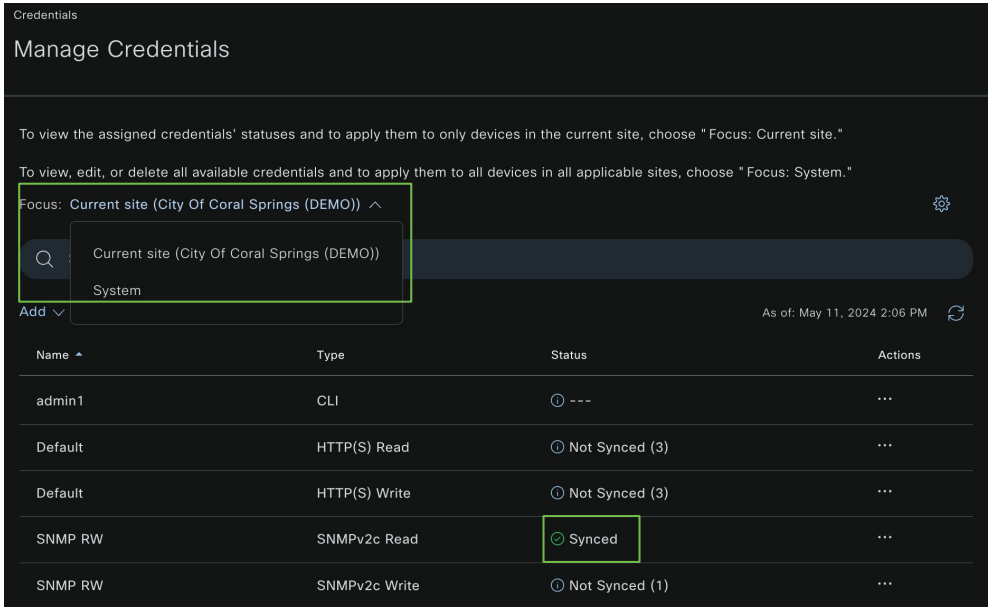
Note: If just client/device AAA, then all will work.
Network AAA is the issue - due to lockout concerns (NAD entry in ISE)
For Brownfield, you can skip configuring AAA under network settings if you want to provision the device.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Global Device Credentials

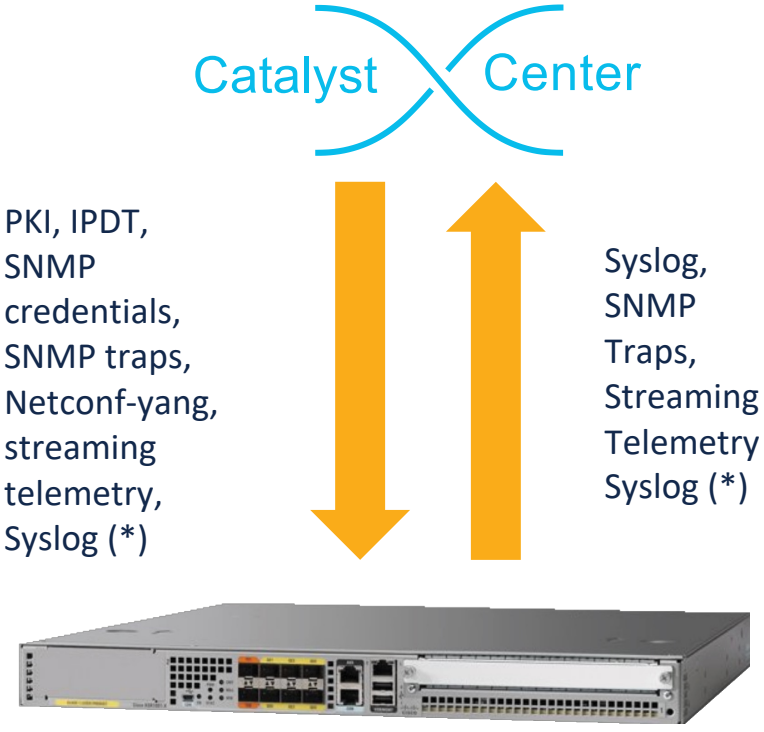
- Define common CLI/HTTP(S), SNMP for device authentication.
- Assignable globally or to specific sites.
- **Update Credentials**: Push credentials to devices with "Apply" action or individually in inventory Actions-> Inventory -> Edit
- Cisco DNA Center does not remove credentials from devices.
- **AAA Configuration**:
  - Ensure CLI credentials match those on the AAA server.
  - CLI changes cannot be applied if the site is configured with AAA.

Design –> Network Settings -> Device Credentials



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Why We Need Telemetry?



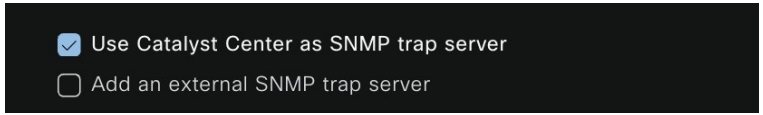
1. Network and Client Health
2. Application Health
3. Network Services (AAA, DHCP, DNS)
4. View and Manage Issues
5. Visibility into Wi-Fi 6/6E Readiness
6. Monitor Power over Ethernet
7. EoX Insights
8. Inventory Insights
9. Network Trends and Insights

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

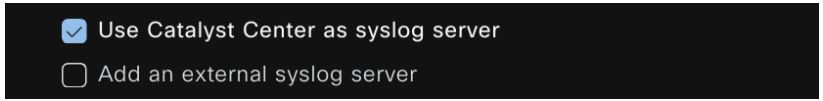
Enable Telemetry

- Design - > Network Settings -> Telemetry
- Catalyst Center is default SNMP collector

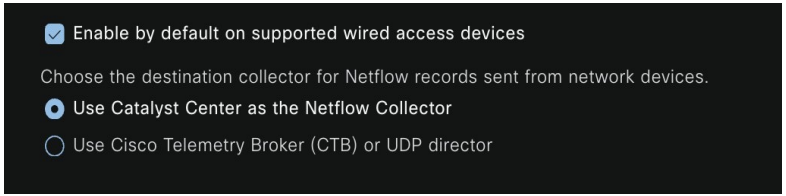
SNMP Traps



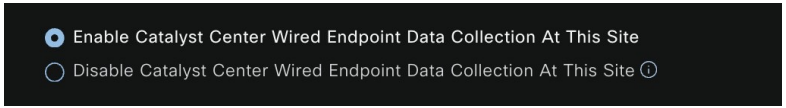
Syslogs



Application Visibility



Wired Endpoint Data Collection

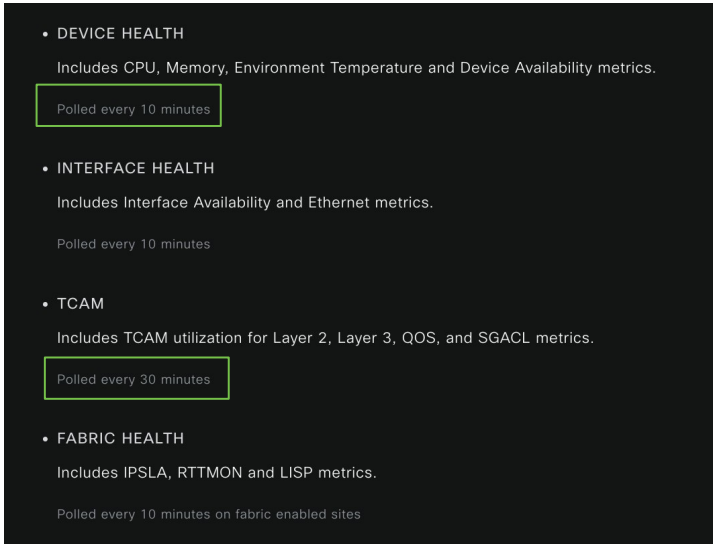


Wireless Controller, Access Point and Wireless Clients Health

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Global Device Credentials

- Default SNMP polling is 10minutes
- Polling interval can be modified System - > Data Platform -> Collectors -> COLLECTOR SNMP
- It does not cause any change on network devices



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Device Controllability – What is it ?

During Discovery –

- SNMP Credentials
- NETCONF Credentials

Added to Inventory –

- Cisco TrustSec(CTS) Credentials

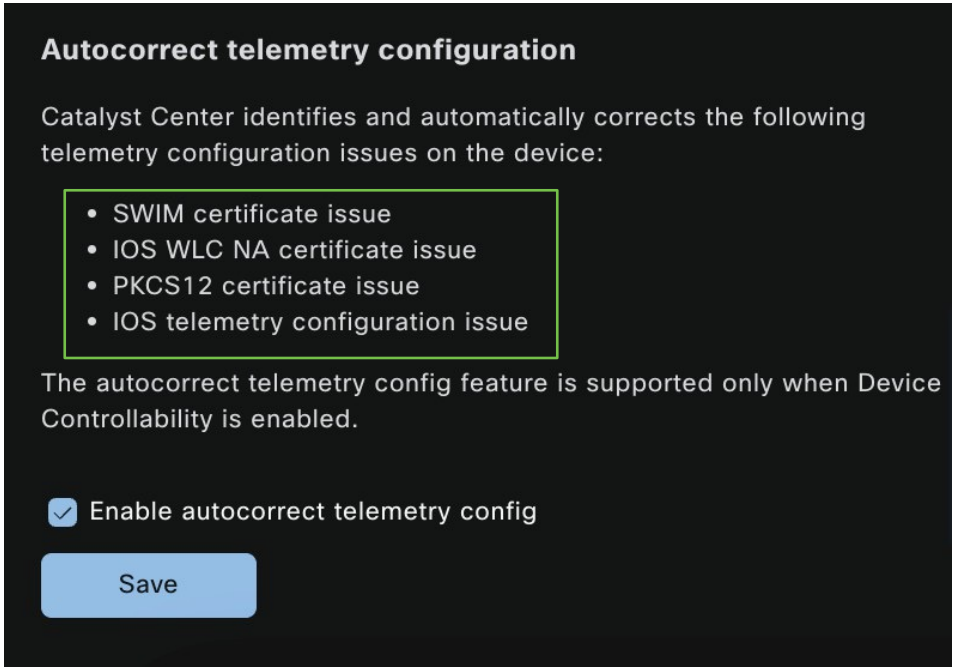
Assigned to Site –

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

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

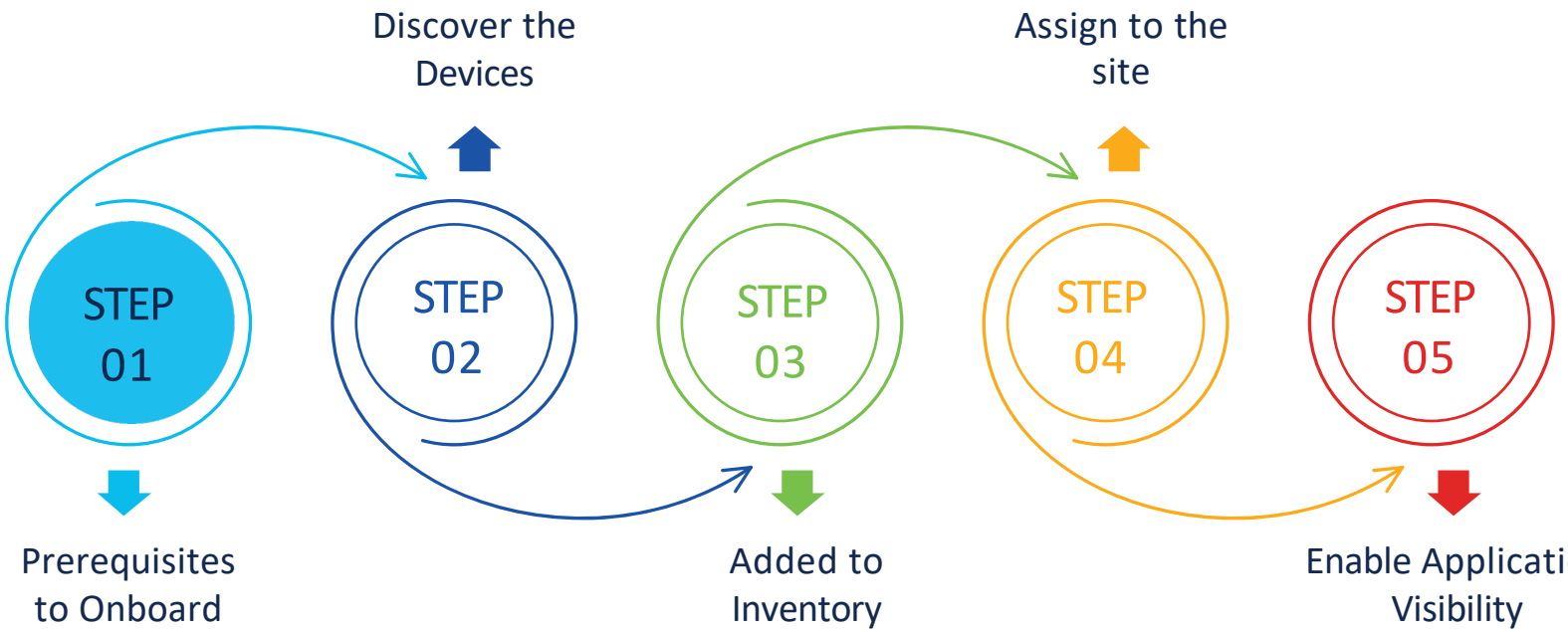
Device Controllability

- Autocorrects telemetry configuration issues on the devices



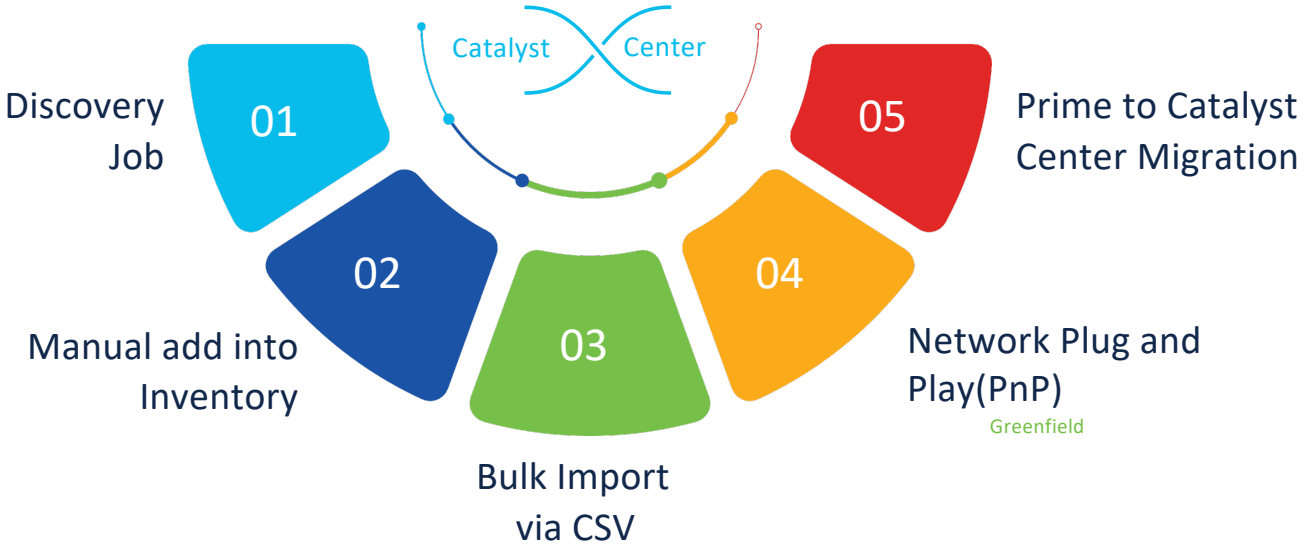
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Brownfield Device Onboarding



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Various Ways To Onboard Devices Into Catalyst Center



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

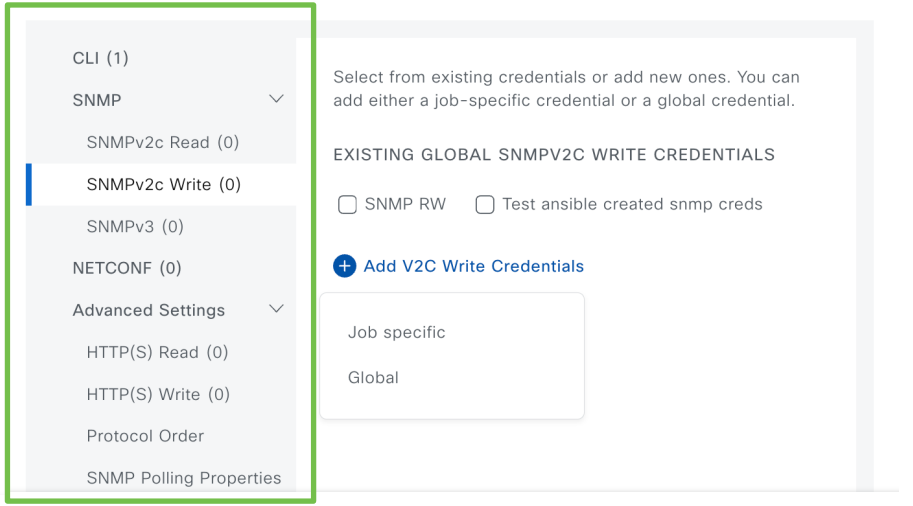
PREFERRED MANAGEMENT IP ADDRESS

(•) 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.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

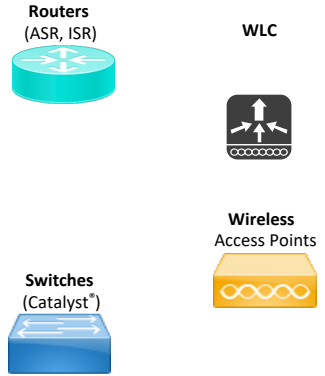
PnP Server Options

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 Cisco DNA Center IP Address

3. Cloud re-direction https://devicehelper.cisco.com/device-helper
   Cisco hosted cloud, re-directs to on-prem Cisco DNA Center IP Address



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

What Happens When a Device Is Discovered

- Cisco Catalyst Center validates the device's CLI credentials against the credentials configured on Cisco Catalyst Center. If successful, SNMP credentials are validated
- Cisco Catalyst Center checks if device is configured with SNMP/Netconf config
- If not present, Cisco Catalyst Center provisions the respective Netconf and SNMP credentials to make the discovery successful

Greenfield

```
snmp-server community public ro
snmp-server community public rw
netconf-yang
```

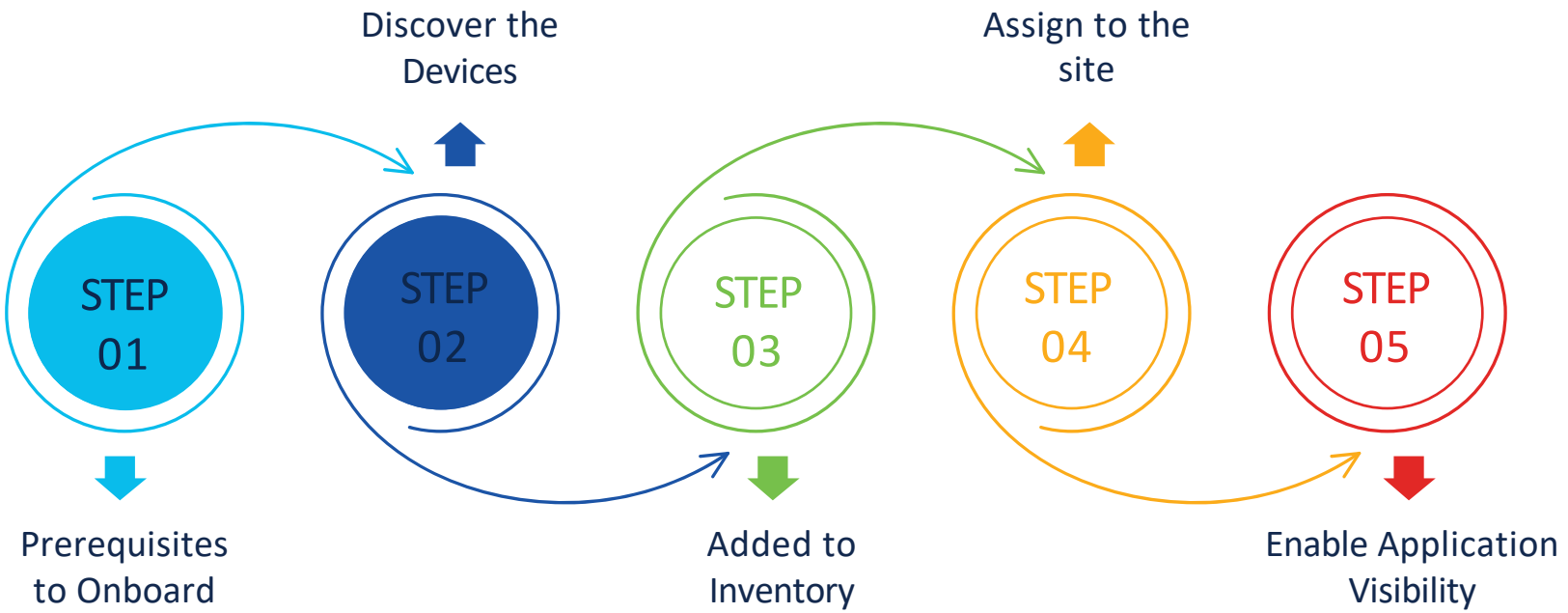
Brownfield

Brownfield Configuration	Catalyst Center Device Controllability	Result	Mitigation Action
snmp-server community public RO 20	Snmp-server community public RO	Catalyst Center overwrites any SNMP community with ACL's	Use CLI templates to append ACL string to SNMP. No impact to the managed network devices

Note: This is applicable for Switches, WLAN & Routers

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

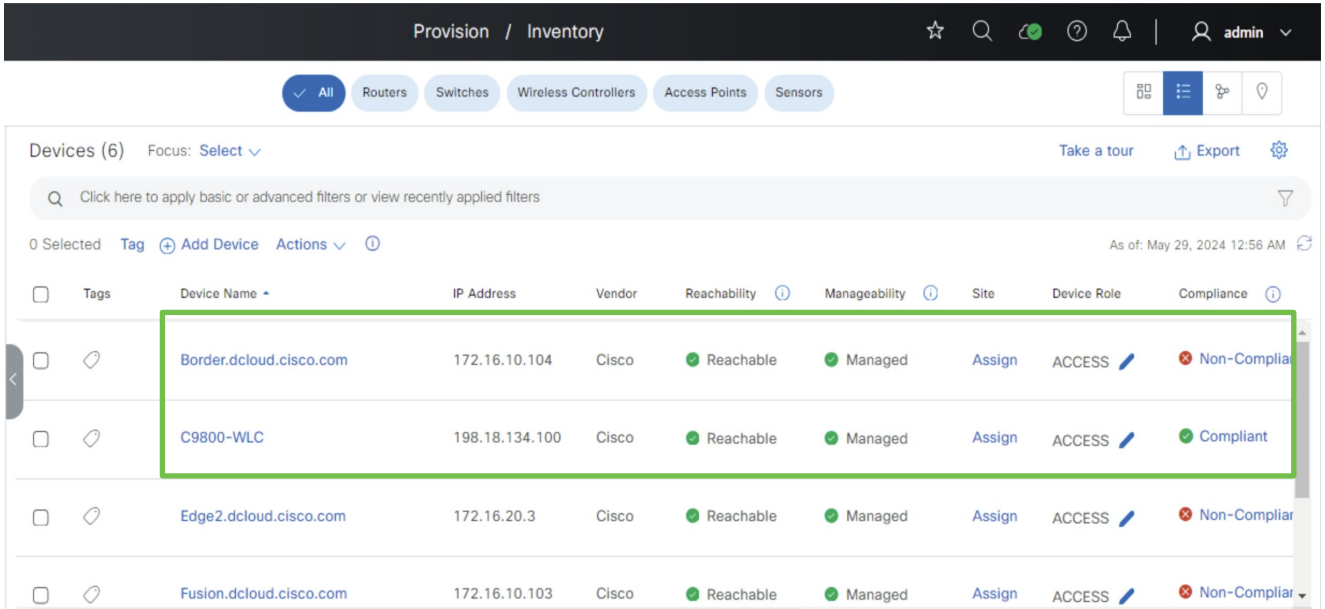
Brownfield Device Onboarding



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

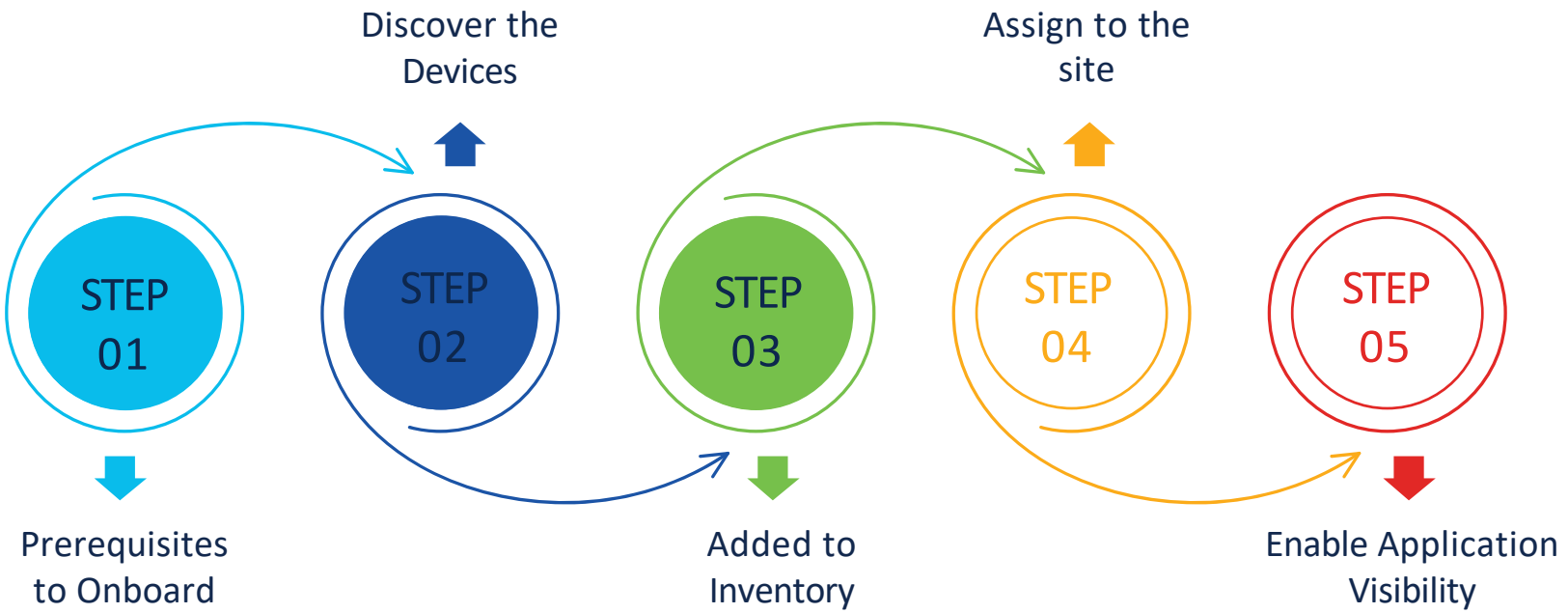
Devices in Inventory

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



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

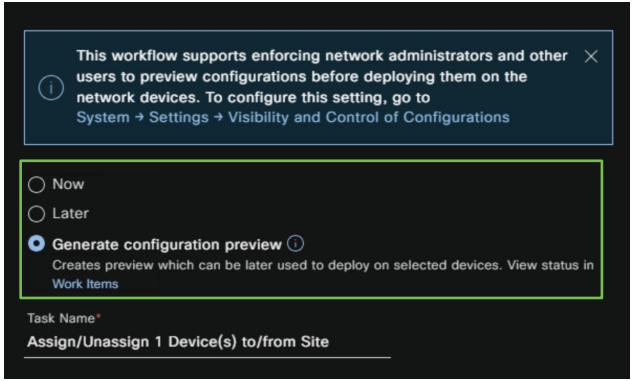
Brownfield Device Onboarding



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

What Happens When a Device Is Assigned To The Site

- Telemetry settings at site level are pushed to the device
- Configuration preview is available which can be sent for approval to ITSM
- Site assignment directly or as part of provisioning
- Source interfaces for telemetry would be the management interface with which device was discovered



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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 AAA servers are configured to the network settings, CTS credentials are not provisioned
- CTS credentials that are pushed by Catalyst Center are usually the devices' SN and hence unique to each device

Greenfield

cts credentials id FCW2333D0TT password FCW233D0TT

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

Note: This is applicable for Switches, WLAN & Routers

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

IP Device tracking

- IPDT tracks connected hosts by linking MAC to IP addresses. Its purpose is to help the switch maintain a list of IP-connected devices
- To do this IPDT sends unicast Address Resolution Protocol (ARP) probes with a default interval of 30 seconds to the connected hosts
- IPDT is pushed to only access switch access role when it is enabled on Catalyst Center.
- For brownfield –
  - If IPDT is already enabled, no need to enable it on catalyst center to get visibility to connected hosts.
  - If DHCP snooping is enabled on a vlan and that vlan is part of a trunk interface, there is programmatic IPDT that is already enabled on the trunk interface . So, please review the configuration before enabling IPDT on catalyst center to not have burst of ARP traffic both on trunk and access ports.

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	Cisco DNAC overwrites the existing IPDT config.	Use Cisco DNAC CLI template to append commands like trusted-port.

Syslog

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

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Snippets Of Configuration Pushed During Site Assignment

For your reference

- Based on the platform, all applicable traps are configured

```
snmp-server community public RO
snmp-server community private RW
snmp-server community cisco RO
snmp-server trap-source Vlan120
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps flowmon
snmp-server enable traps entity-perf throughput-notif
snmp-server enable traps call-home message-send-fail server-fail
snmp-server enable traps tty
snmp-server enable traps eigrp
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
```

```
snmp-server host 198.18.129.100 version 2c cisco
```

- Catalyst Center certificates pushed to the devices to help them to trust Catalyst Center

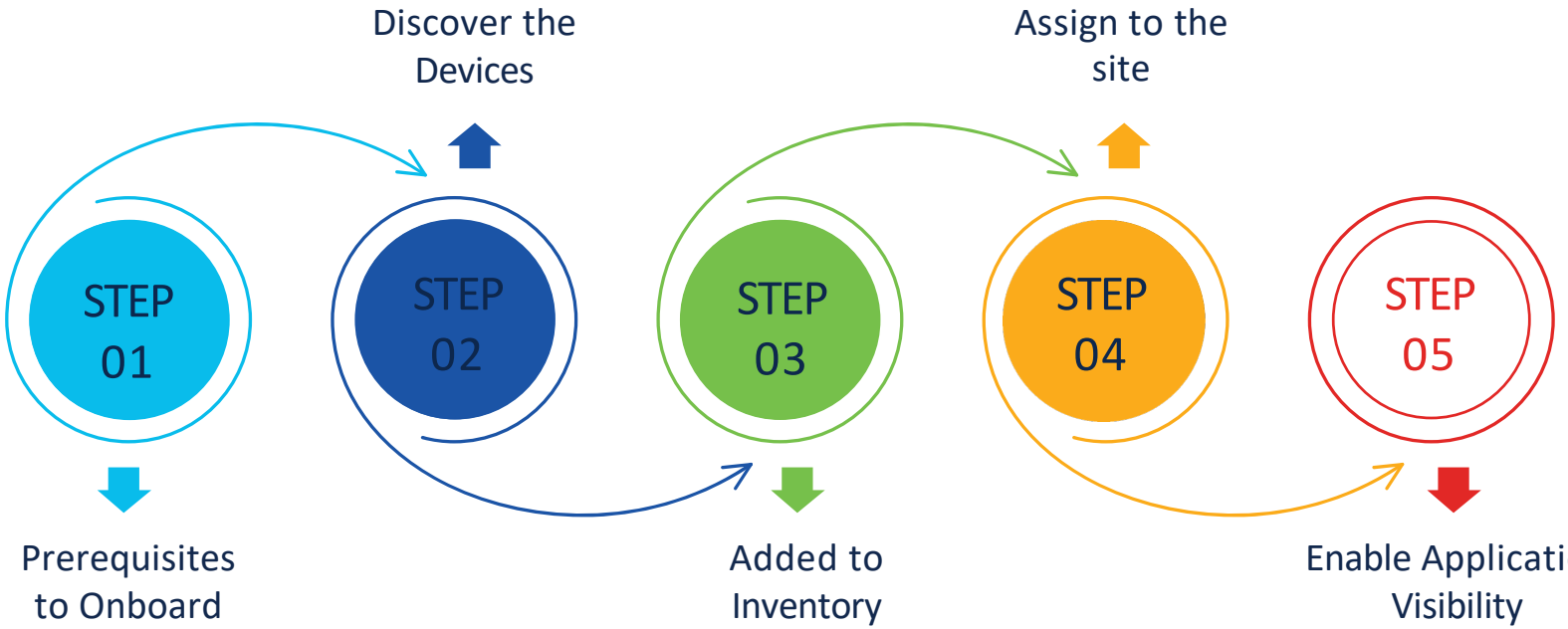
```
crypto pki trustpoint sdn-network-infra-iwan
 enrollment url http://198.18.129.100:80/ejbca/publicweb/apply/scep/sdnscep
 fqdn Edge2.dcloud.cisco.com
 subject-name CN=C9300-24P_FJC2327S02P_sdn-network-infra-iwan
 subject-alt-name Edge2.dcloud.cisco.com
 revocation-check crl
 source interface Vlan120
 rsakeypair sdn-network-infra-iwan
 auto-enroll 80 regenerate
```

- Telemetry Subscriptions

```
telemetry ietf subscription 8882
 encoding encode-tdl
 filter tdl-transform trustSecCounterDelta
 receiver-type protocol
 source-address 172.16.20.3
 stream native
 update-policy periodic 90000
 receiver name DNAC_ASSURANCE_RECEIVER
telemetry receiver protocol DNAC_ASSURANCE_RECEIVER
 host ip-address 198.18.129.100 25103
 protocol tls-native profile sdn-network-infra-iwan
```


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Brownfield Device Onboarding



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Application Telemetry

- Quantitative(Application Visibility) – Application name & Throughput
  - IOS-XE Switches - NetFlow
  - AireOS controllers – NetFlow(Local Mode) or WSA(Flex/Fabric mode)
- Qualitative(Application Experience) - DSCP Markings and Performance Metrics (Latency, Jitter, and Packet Loss)
  - Routers - Cisco Performance Monitor (PerfMon) feature and the Cisco Application Response Time (ART) metrics.
  - 9800 WLC – NetFlow
- Put “lan” keyword in the description of the interface/WLAN profile name to override the automatic selection algorithm for Application telemetry provision

  Switches – all access interfaces

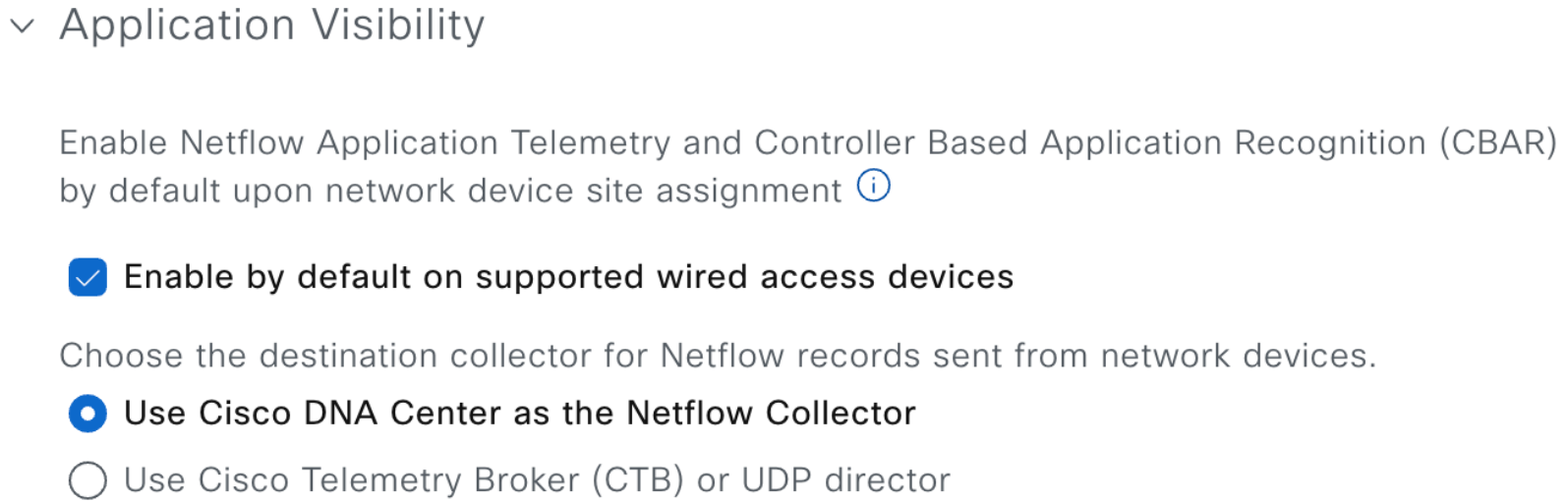
  Routers – all LAN-facing interfaces

  WLC - all non-guest WLANs
- 9800 WLC - Before enabling application telemetry in Catalyst Center, delete any existing flow monitors configured manually from Configuration > Services > Application Visibility > Flow Monitors through 9800 WLC GUI. Recommended to do after hours.
- NBAR(Network based application recognition) to recognize applications
- CBAR(Controller based application algorithm) to enhance the NBAR function for protocol pack upgrades, enhanced visibility for unknown applications, etc.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

1)Configure Destination Collector

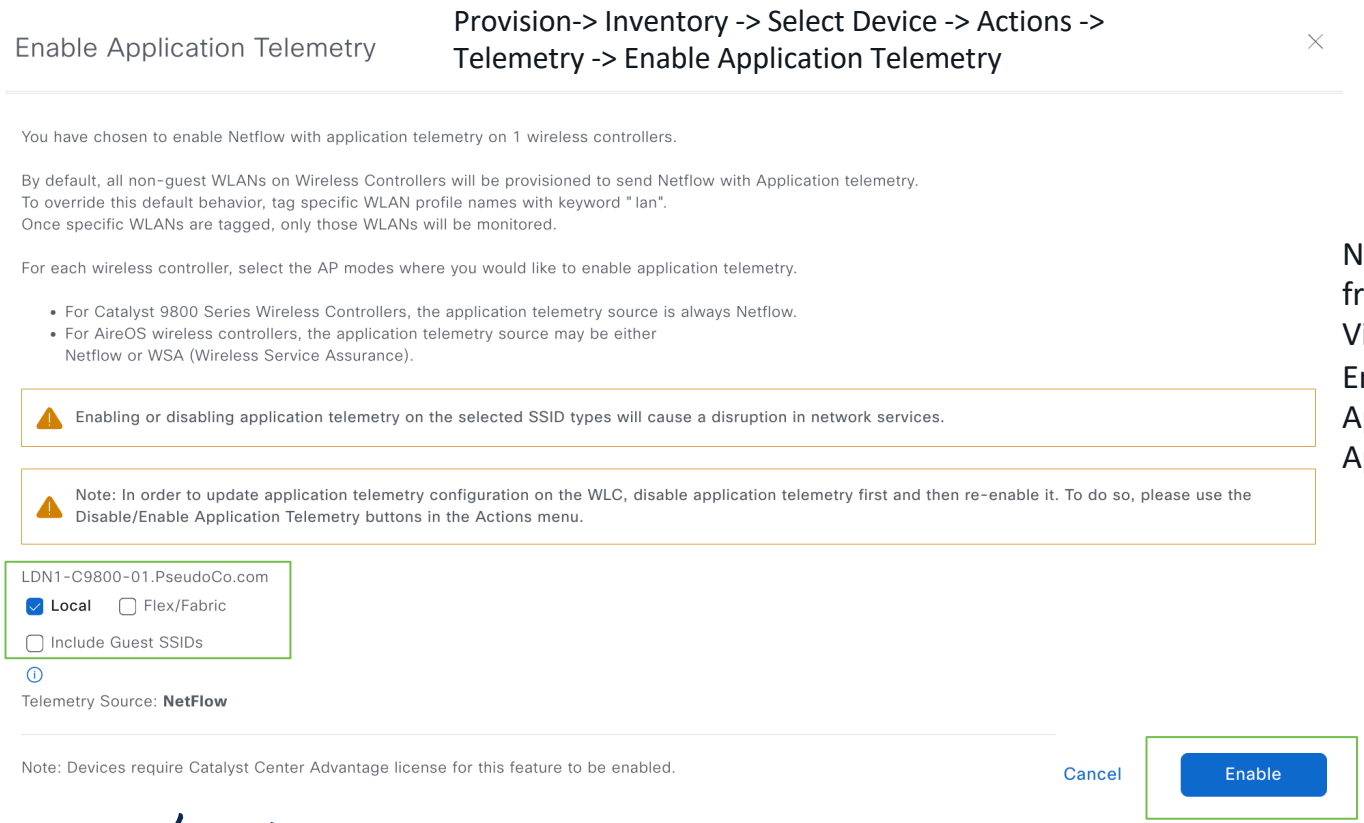
Design -> Network Settings -> Telemetry



Note : Catalyst Center should be separately configured as a NetFlow destination in the CTB/UDP Director if 2nd option is selected

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

2)Enabling Application Telemetry after site assignment

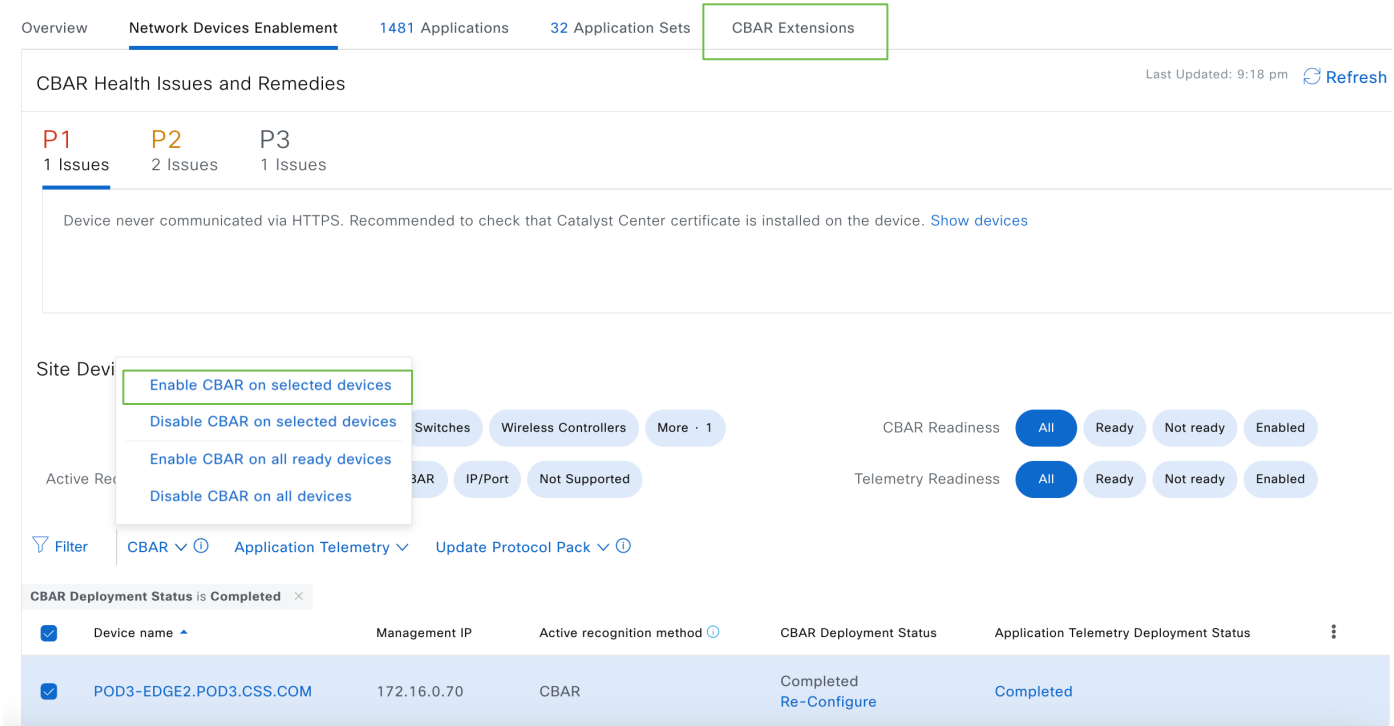


Note: Same can also be enabled from – Provision->Application Visibility->Network Devices Enablement->select device-Application Telemetry-> Enable Application Telemetry

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

3)Enabling CBAR after application telemetry has been enabled

Provision->Application Visibility Setup->Network Devices Enablement->select device->CBAR->Enable CBAR on selected devices



Note: Enable CBAR cloud prior to enabling application telemetry under CBAR Extensions

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Platform Support for Application Experience and Application Visibility in Catalyst Center

For your reference

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.

Also Check Monitor Application Health - > Application Health Prerequisites Under Catalyst Assurance Guide

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Criteria for Enabling Application Telemetry on Devices

For your reference

Platform	Conventional Tagging-Based Algorithm	Automatic Selection Algorithm

Router	• Interface description has the **lan** keyword.[1,2]
	• Interface has an IP address other than the management IP address.
		• Interface has an IP address other than the management IP address.
		• Interface is not any of the following:
		  • WAN
		  Note An interface is treated as a WAN-facing interface if it has a public IP address, and if there is a route rule with a public IP address that routes through the interface.
		  In this context, a public IP address is not in a private range (for example, not in 192.168.x.x, 172.16.y.y, 10.z.z.z), or is an IP address that is not in the system's IP pools.
		  Route rules can be dynamically learned. In this context, the **show ip route** command does not show a route to a public IP address that goes through this interface.
		  • Loopback.
		  • Management interface: GIGABITETHERNET0, GIGABITETHERNET0/0, MGMT0, FASTETHERNET0, or FASTETHERNET1.

Switch	• Interface description has the **lan** keyword.[1,2]
	• Switch port is configured as an access port.
	• Switch port is configured with the **switch-mode access** command.
		• Interface is a physical interface.
		• Access port does not have neighbors.
		• Interface is not any of the following:
		  • Management interface: FASTETHERNET0, FASTETHERNET1, GIGABITETHERNET0/0, or MGMT0
		  • LOOPBACK0, Bluetooth, App Gigabit, WPAN, Cellular, or Async
		  • VSL interface.

Cisco AireOS Controller	WLAN profile name is tagged with the **lan** keyword.[1,2]	If the SSIDs are mixed, that is Local mode, Flex mode, and Fabric mode, Wireless Service Assurance (WSA) processing is enabled. If all the SSIDs are in Local mode, NetFlow is enabled.
Cisco Catalyst 9800 Series Wireless Controller with Optimized Application Performance Monitoring (APM) profile and IOS 16.12.1 and later.	WLAN profile name is tagged with the **lan** keyword.[1,2]	If the SSIDs are mixed—that is, central switching, Flex mode, and Fabric mode—the Cisco Application Visibility and Control (AVC) basic record is configured. If all the SSIDs use central switching, the Optimized APM record is configured. For Cisco Catalyst 9800 Series Wireless Controllers with IOS 17.10 and later, Catalyst Center pushes the APM profile, not the AVC basic profile, for flex and fabric SSIDs.
	Note If you want to update the telemetry configuration, you must disable telemetry and then enable it after making the configuration changes.	
Catalyst Center Traffic Telemetry Appliance with Optimized APM profile and IOS 17.3 and later.	• Interface description has the **lan** keyword.[1,2] • Interface is a physical interface.	• Interface is a physical interface. • Interface is not a management interface: GIGABITETHERNET0, GIGABITETHERNET0/0, MGMT0, FASTETHERNET0, and FASTETHERNET1.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Snippets of NetFlow Configuration pushed on switch for Application Visibility

For your reference

```
!
flow record dnacrecord
 match ipv4 version
 match ipv4 protocol
 match application name
 match connection client ipv4 address
 match connection server ipv4 address
 match connection server transport port
 match flow observation point
 collect timestamp absolute first
 collect timestamp absolute last
 collect flow direction
 collect connection initiator
 collect connection client counter packets long
 collect connection client counter bytes network long
 collect connection server counter packets long
 collect connection server counter bytes network long
 collect connection new-connections
 collect datalink mac source address input
!
```

```
flow exporter dnacexporter
 destination 198.18.129.100
 source Vlan120
 transport udp 6007
 export-protocol ipfix
 option interface-table timeout 300
 option vrf-table timeout 300
 option sampler-table
 option application-table timeout 300
 option application-attributes timeout 300
```

```
flow monitor dnacmonitor
 exporter dnacexporter
 cache timeout inactive 10
 cache timeout active 60
 record dnacrecord
```

```
interface TenGigabitEthernet1/1/7
 device-tracking attach-policy IPDT_POLICY
 ip flow monitor dnacmonitor input
 ip flow monitor dnacmonitor_dns input
 ip flow monitor dnacmonitor output
 ip flow monitor dnacmonitor_dns output
 ipv6 flow monitor dnacmonitor_v6 input
 ipv6 flow monitor dnacmonitor_dns_v6 input
 ipv6 flow monitor dnacmonitor_v6 output
 ipv6 flow monitor dnacmonitor_dns_v6 output
 ip nbar protocol-discovery
```


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Snippet of CBAR configuration

For your reference

```
avc sd-service
 segment AppRecognition
 controller
  address 198.18.129.100
  destination-ports sensor-exporter 21730
  dscp 16
  source-interface Vlan120
  transport application-updates https url-prefix sdavc
```


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Snippets of NetFlow Configuration pushed to 9800 WLC

For your reference

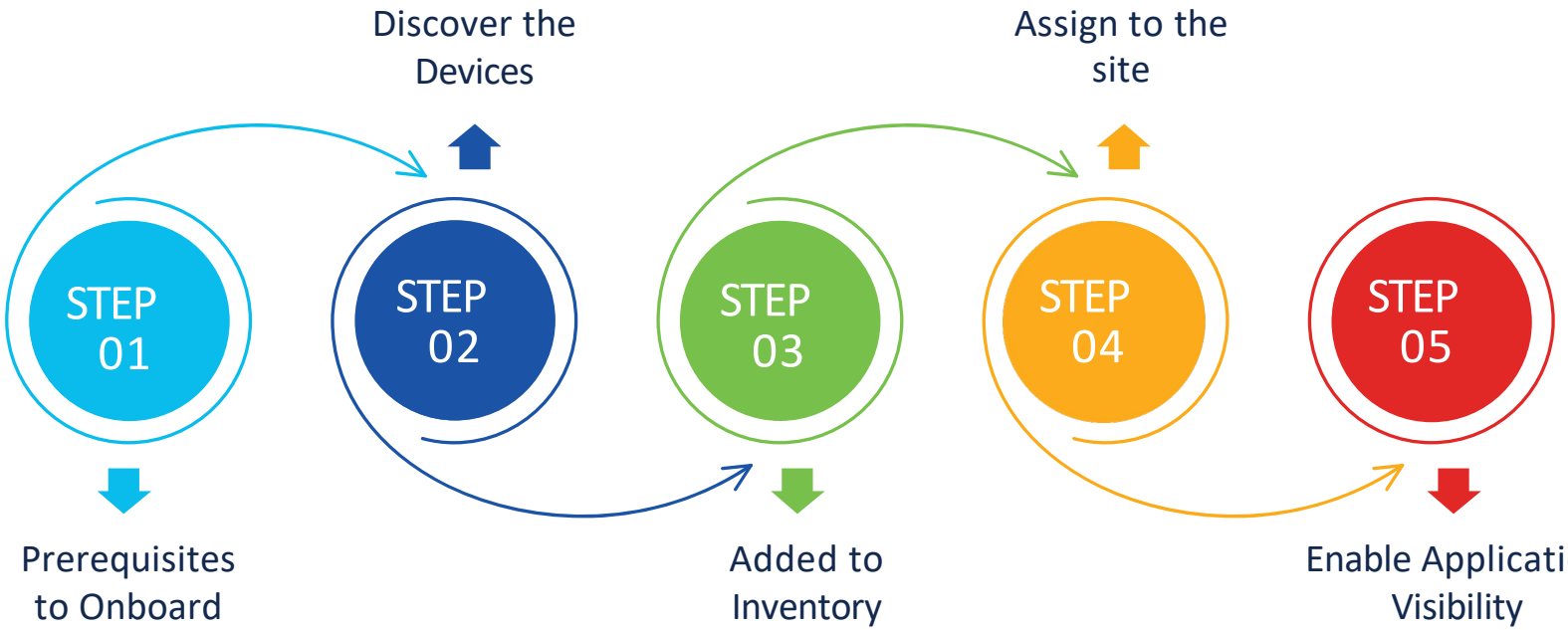
```
TNT-9800-Lab-1#show run | b flow exporter avc_exporter
flow exporter avc_exporter
 destination 10.200.6.40
 source Vlan201
 transport udp 6007
 export-protocol ipfix
 option vrf-table timeout 300
 option ssid-table timeout 300
 option application-table timeout 300
 option application-attributes timeout 300
!
!
flow exporter avc_local_exporter
 destination local wlc
!
!
flow monitor avc_ipv4_assurance
 exporter avc_exporter
 exporter avc_local_exporter
 cache timeout active 60
 record wireless avc ipv4 assurance
!
```

```
!
flow monitor avc_ipv6_assurance
 exporter avc_exporter
 exporter avc_local_exporter
 cache timeout active 60
 record wireless avc ipv6 assurance
!
!
flow monitor avc_ipv4_assurance_rtp
 exporter avc_exporter
 cache timeout active 60
 record wireless avc ipv4 assurance-rtp
!
!
flow monitor avc_ipv6_assurance_rtp
 exporter avc_exporter
 cache timeout active 60
 record wireless avc ipv6 assurance-rtp
!
!
flow monitor avc_ipv4_assurance_dns
 exporter avc_exporter
 cache timeout active 60
 record wireless avc ipv4 assurance-dns
!
!
flow monitor avc_ipv6_assurance_dns
 exporter avc_exporter
 cache timeout active 60
 record wireless avc ipv6 assurance-dns
!
multilink bundle-name authenticated
```

```
TNT-9800-Lab-1#sh run | s wireless profile policy Lab_PSK
wireless profile policy Lab_PSK
 dhcp-tlv-caching
 http-tlv-caching
 idle-timeout 3600
 ipv4 arp-proxy
 ipv4 flow monitor avc_ipv4_assurance input
 ipv4 flow monitor avc_ipv4_assurance_dns input
 ipv4 flow monitor avc_ipv4_assurance_rtp input
 ipv4 flow monitor avc_ipv4_assurance output
 ipv4 flow monitor avc_ipv4_assurance_dns output
 ipv4 flow monitor avc_ipv4_assurance_rtp output
 ipv6 flow monitor avc_ipv6_assurance input
 ipv6 flow monitor avc_ipv6_assurance_dns input
 ipv6 flow monitor avc_ipv6_assurance_rtp input
 ipv6 flow monitor avc_ipv6_assurance output
 ipv6 flow monitor avc_ipv6_assurance_dns output
 ipv6 flow monitor avc_ipv6_assurance_rtp output
 radius-profiling
 session-timeout 86400
 vlan Lab_PSK
 wgb broadcast-tagging
 wgb vlan
 no shutdown
TNT-9800-Lab-1#
```


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Brownfield Device Onboarding

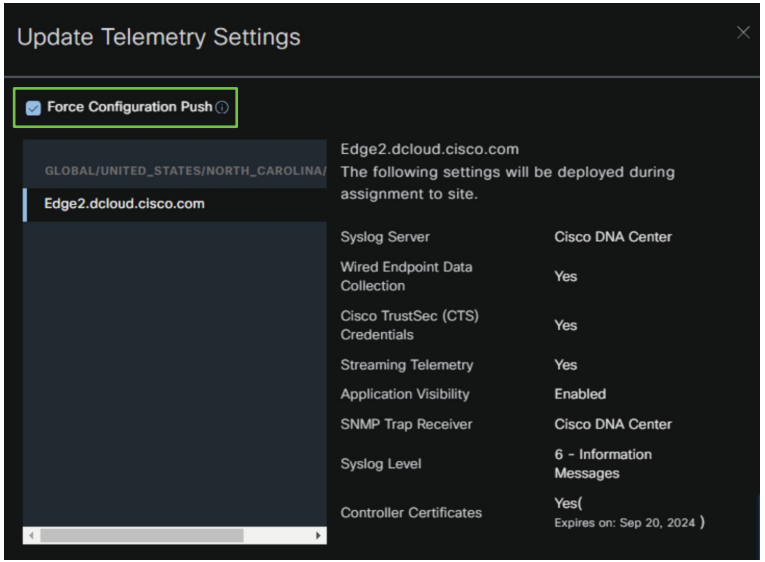


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Not Comfortable With Configuration Being Pushed While Device Onboarding?

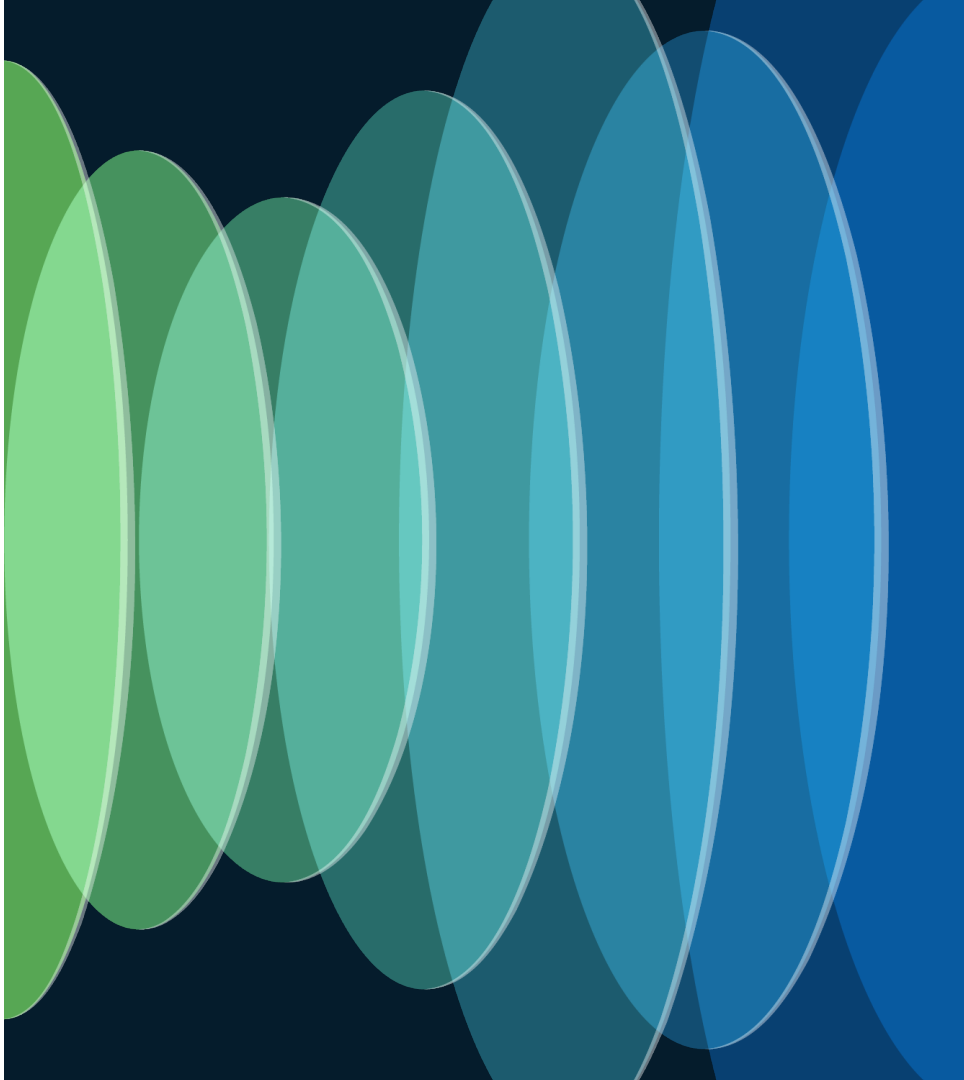
- You can disable Device Controllability which is enabled by default
- You can push the telemetry settings later to network devices to get real time insights
- Telemetry settings can be customized at site level under Design->Network Settings->Telemetry

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

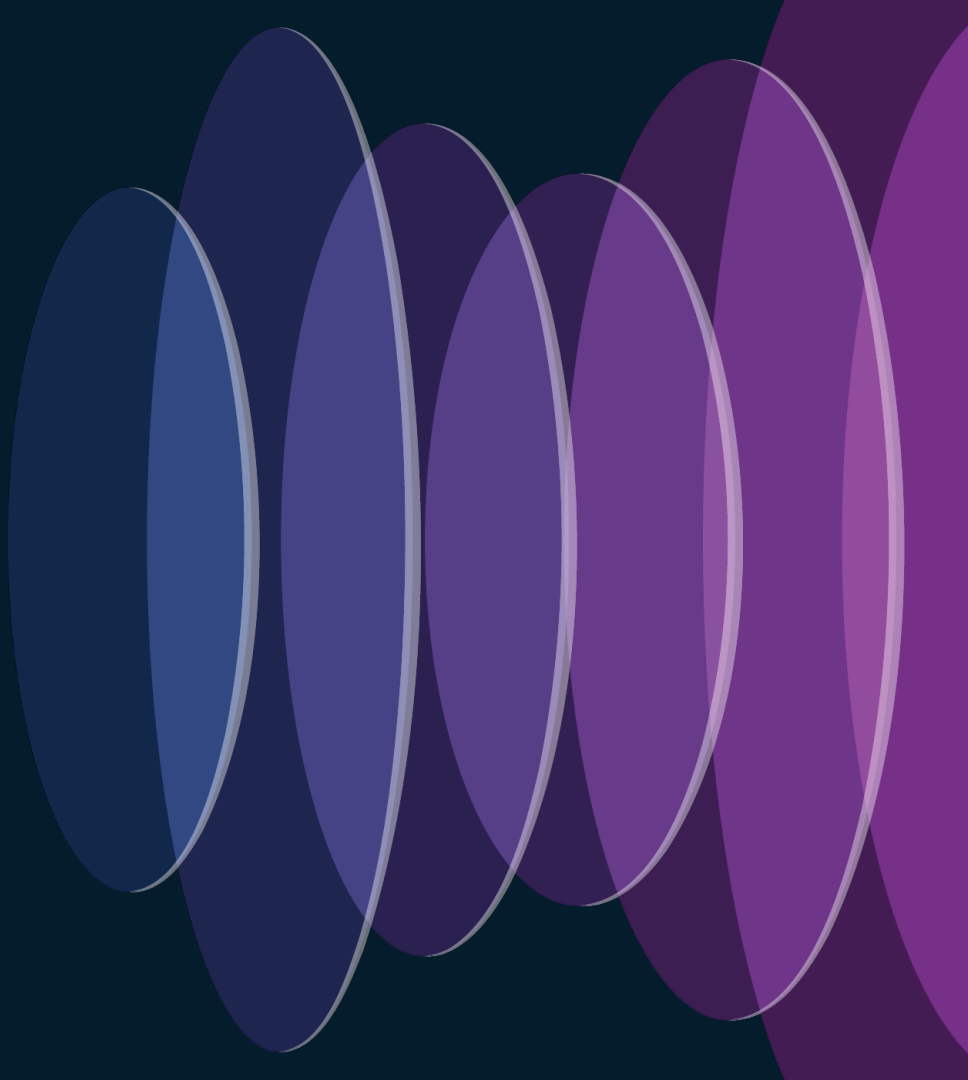


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Let’s see how to discover devices



Managing Your Brownfield Deployment

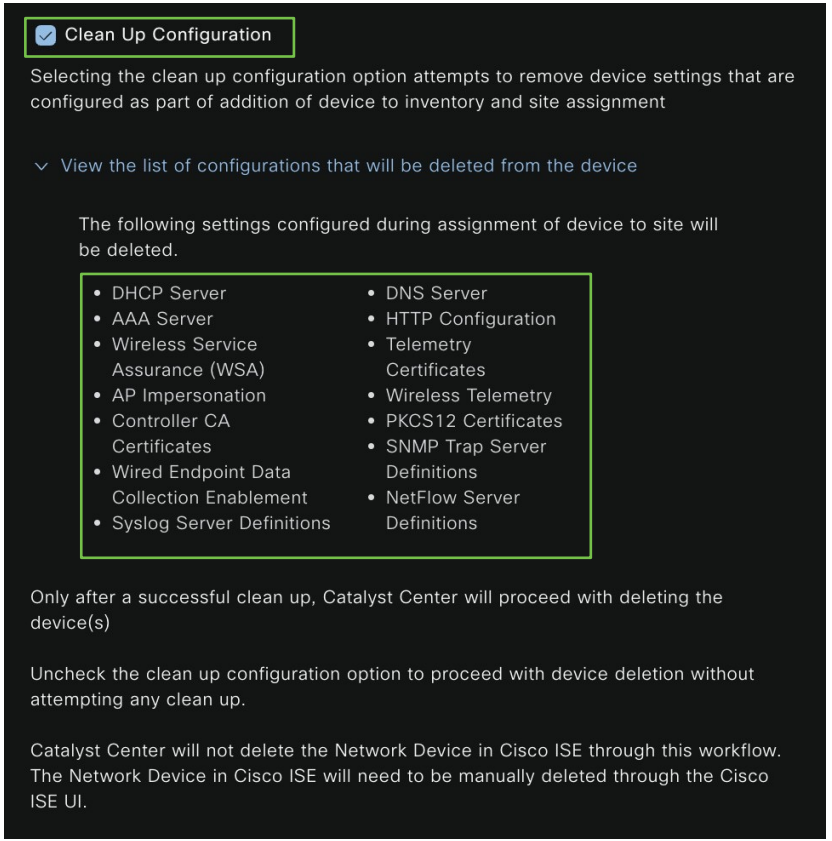


- Deleting Device from Inventory
- Replace a faulty device(RMA)
- Device Refresh
- Simplified View and Edit of Switch Configuration
- Simplified Config Learning and Provisioning for Catalyst 9800 WLC
- Configuration Archive
- Visibility and Control of Configurations
- Inventory Insights
- Software Image Management(SWIM)
- CLI Templates
- Compliance Audit for the device

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Deleting Device

- 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

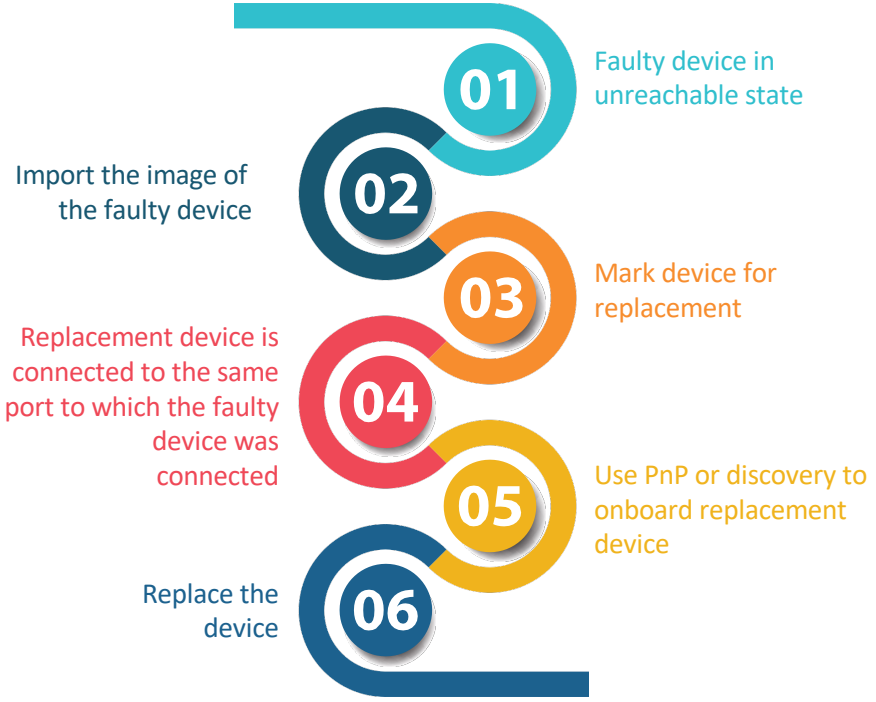


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Replace A Faulty Device

RMA Workflow to replace routers, switches & APs

- Like to Like device replacement
- Switches/Routers - Software, configuration, license are restored
- Full stack replacement supported. Member replacement is handled directly by active switch(no separate procedure in Catalyst Center)
- Replacement APs automatically assigned to the same site and settings:
  - Provisioned with primary WLC
  - RF profile and AP group settings maintained
  - Placed in the same floor map location as failed AP



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

RMA - Behind the Scenes

- Running readiness checks for device replacement.
- Claim the (PnP) replacement device.
- Distribute and activate the software image to the replacement device.
- Deploy licenses.
- Provision VLAN configurations.
- Provision startup configurations.
- Reload the replacement device.
- Check for reachability of the replacement device.
- Deploy SNMPv3 credentials to the replacement device.
- Synchronize the replacement device.
- Remove the faulty device from CSSM.
- Add the replacement device to CSSM.
- Revoke and create the PKI certificate.
- Update Cisco ISE.
- Delete the faulty device.

RMA - Technical Considerations

- Configuration Replacement
  - RMA applies latest config archive to the replacement device
  - Automatic config archive happens every 24 hours and based on Events/Traps.
- The replacement device must use a different IP address than the faulty device.
- The replacement AP must have joined the same Cisco Wireless Controller as the faulty AP.
- DNA Center does not support legacy license deployment.
- Switch stacks (SVL stacking), embedded wireless controller not supported
- The replacement device must not be in a provisioning state while triggering the RMA workflow.

For your reference

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

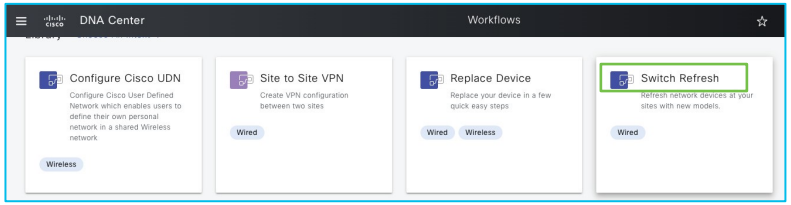
Switch Refresh

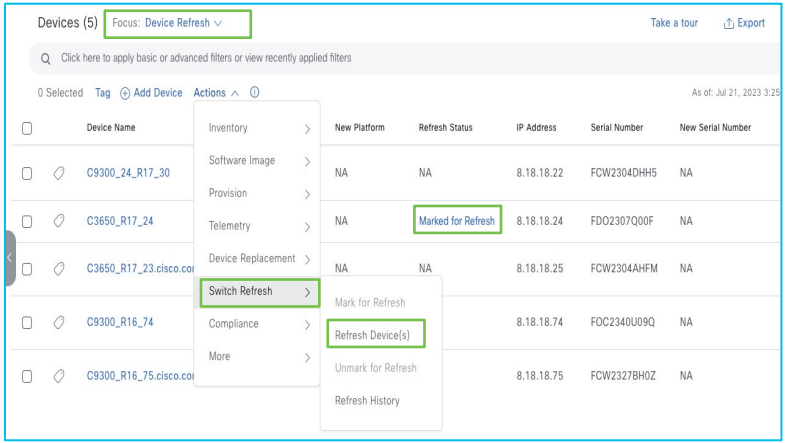
Challenges

- Replacing end-of-life devices
- Ensuring configurations and license accuracy
- Streamlining upgrade processes

Features

- Guided workflow for seamless IOS XE to IOS XE switch refresh
- Flexible addition methods: Discovery or PnP
- Supports refresh from C3650 & C3850 to Catalyst 9300
- Requires identical port configurations
- IOS to IOS XE – in roadmap





© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

AP Refresh

For your reference

Replace older model APs with new

Automation Use Case	Assurance Use Case
WLC and APs are provisioned through Catalyst Center with network intent configuration	WLC and APs are not provisioned via Catalyst Center and used mainly for assurance
The old AP site must be provisioned as a managed AP location for the wireless controller to which the new AP is associated	New AP must join the same wireless controller where the old AP was previously associated.
You must connect the new AP to a wireless controller. The new AP must either be available in the Catalyst Center inventory or be able to contact Catalyst Center through Plug and Play (PnP). It must be in the Reachable state.	You must connect the new AP to a wireless controller. The new AP must be available in the Catalyst Center inventory.

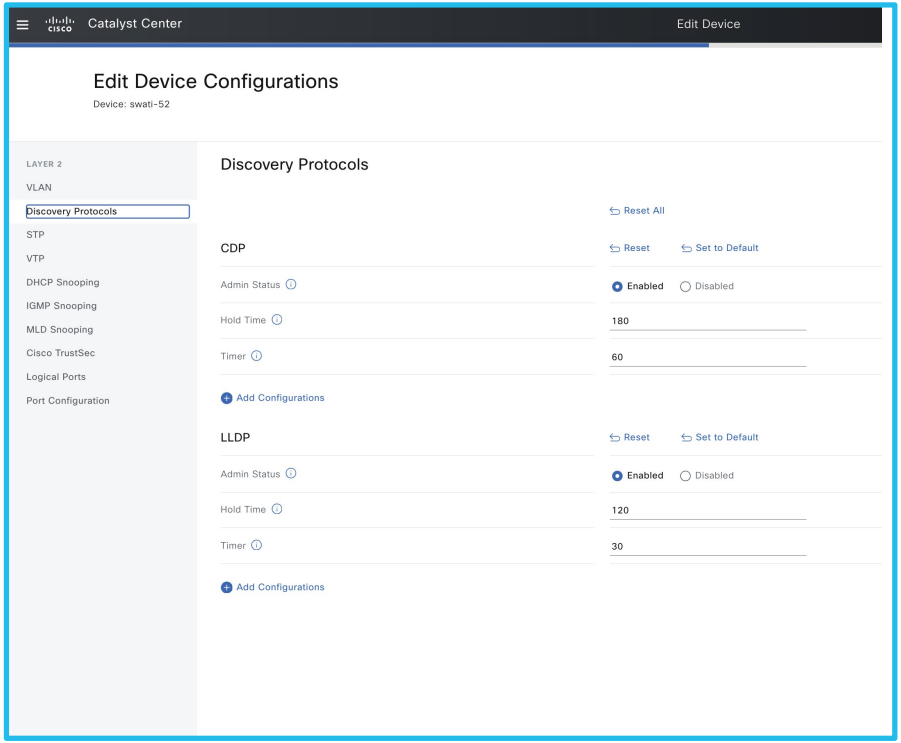
Workflows -> Access Point Refresh

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Simplified View and Edit of Switch Configuration

Beta
2.3.7
Cat 9k
Only L2

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

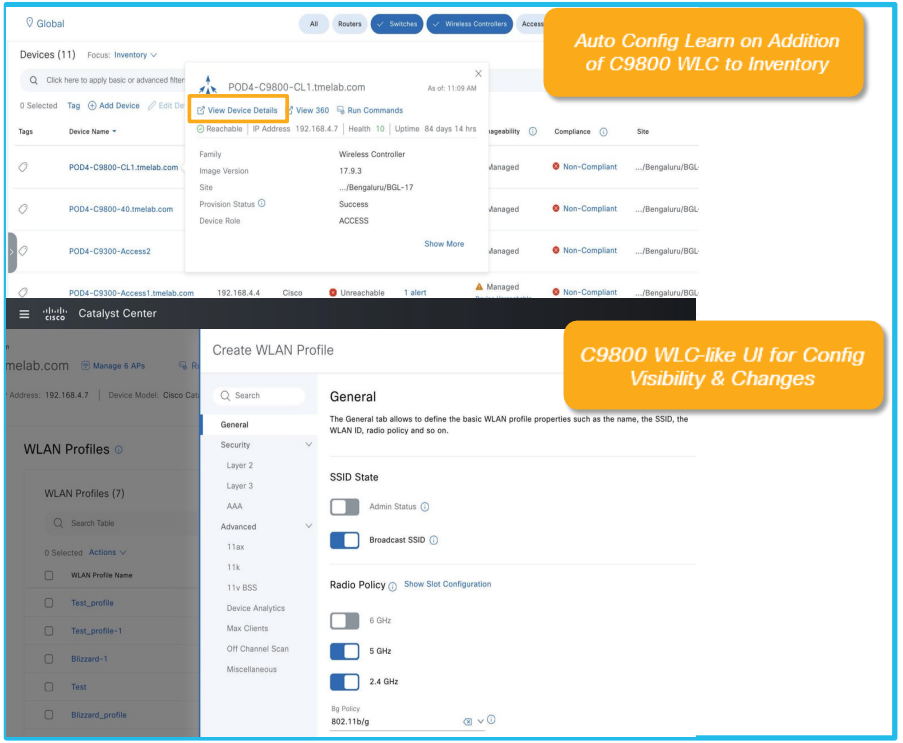


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Simplified Config Learning and Provisioning for Catalyst 9800 WLC

Beta
2.3.7

- Simplified Config Learning for Brownfield 9800s
- Aiming to achieve Configuration Parity with Prime & C9800 WebUI
- Improved Automation with Config Visibility and Network Stability
- Increased Feature Velocity on Catalyst Center



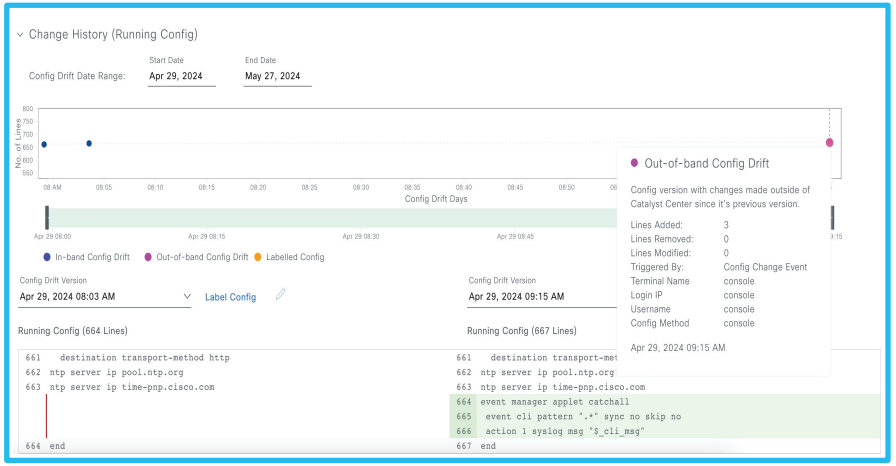
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Configuration Archive

Periodic backup of devices running configuration

Use Case

- Compare the configuration changes on the devices against a standard configuration



Feature Details

- 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

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

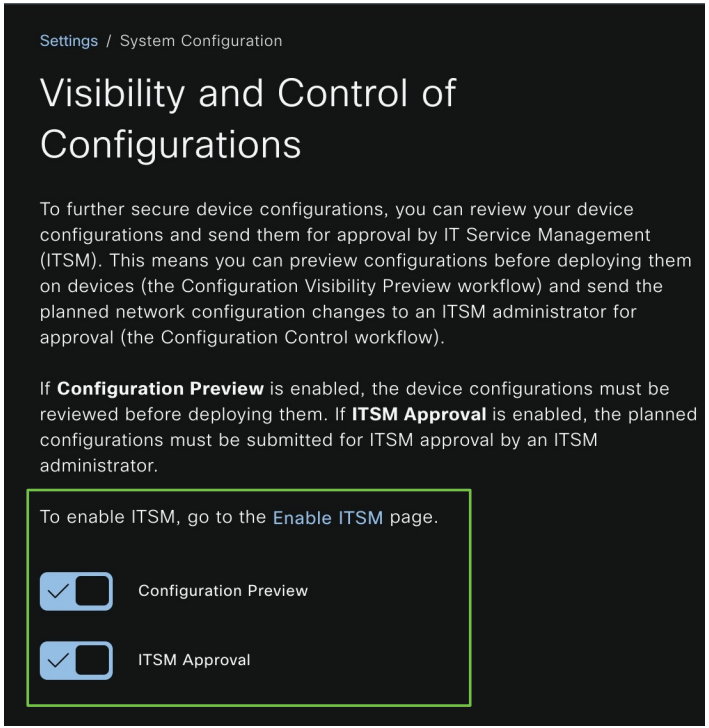
Visibility and Control of Configurations

Challenge

- Visualization/validating and approving the configuration changes made by Cisco Catalyst Center

Feature Capability

- Approval can be sent to ITSM for Config Preview for CLI template, provisioning



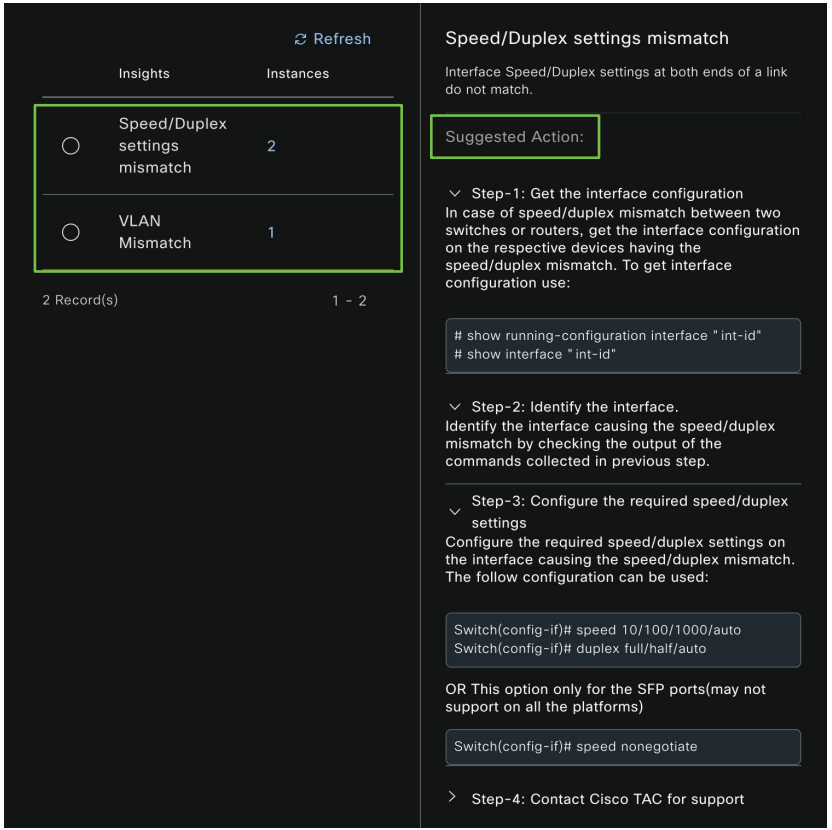
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Inventory Insights

Speed & Duplex mismatch

Use Case

- Finding configuration inconstancies/ misconfigurations and giving suggested actions



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

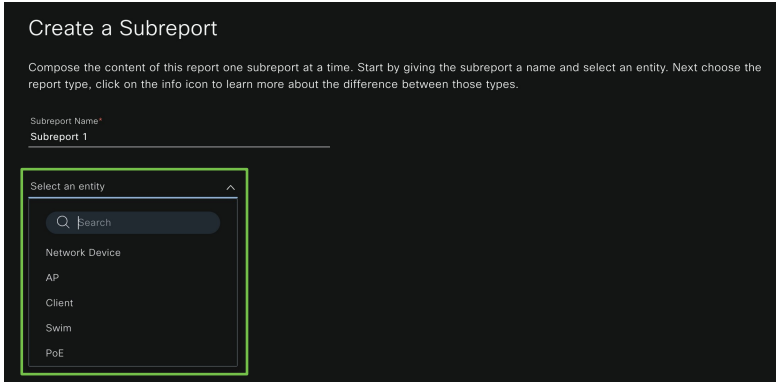
Flexible Reports

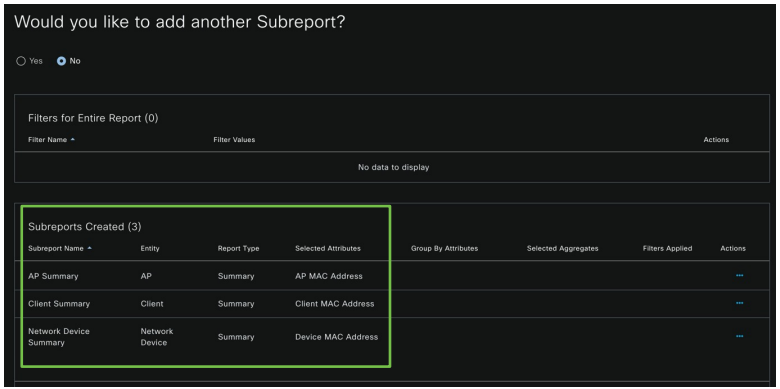
Use Case

- Generate detailed reports from multiple data sources, tailored to include every possible data combination.

Features

- Flexible Report Generation: Create reports with sub-reports for various entities like Clients, Network Devices, APs, SWIM, and PoE.
- Customizable Data Presentation: Include trends, summaries, top performers, and distributions.
- Dynamic Data Handling: Options to group, aggregate, filter, and sort data.
- Versatile Reporting Schedules: Generate reports on-demand or schedule them regularly.
- Export Options: Reports available in CSV format for easy integration with external platforms.





© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

What you need to know about Software Image Management (SWIM)

Intent Based Network Upgrades

Golden-image driven to automate process and drive consistency

Trustworthiness Integration

Assures that device images are not compromised in any way

Common Workflow

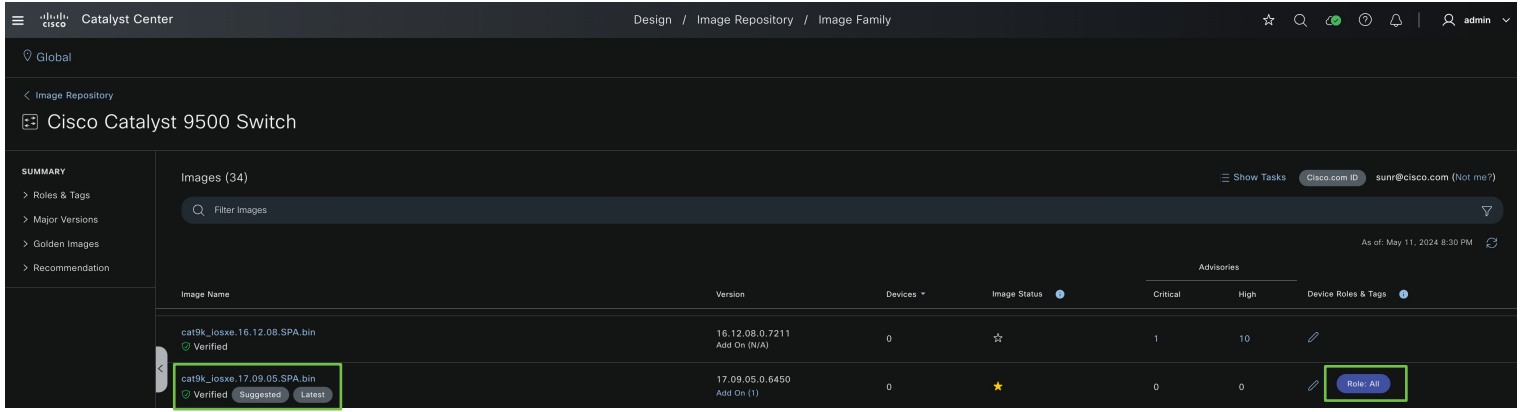
Upgrade base image, patches, ROMMON in one single flow. ISSU supported

Upgrade Checks

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

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Intent-based Network Upgrades Using “Golden Image”



Device family

- Golden image per device family (includes router, switches, and WLC).

Device role & Tag

- Devices in the same family classified by role & tag
- Ex: CAT9300 as an access switch vs distribution switch, lab device given a tag
- Tag has precedence over role

Site mapping

- Site hierarchy provides an override of the golden image set at a higher level

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Image Distribution and Activation

Schedule Task and Clean Up

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

The time zone of the site to which the device belongs will be used as the default site time zone.

Software Distribution

Now Later

Start Date/Time

Jun 3, 2024

10:52 AM

Time Zone

America/Chicago

Software Activation

After Distribution

Now Later

Start Date/Time

Jun 3, 2024

8:52 PM

Time Zone

America/Chicago

INITIATE FLASH CLEANUP AFTER ACTIVATION

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

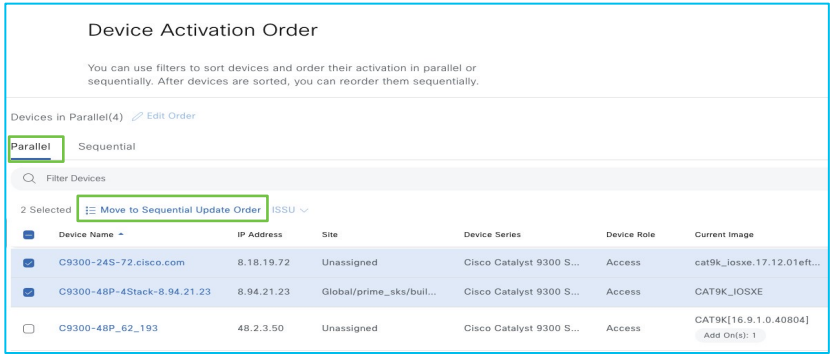
Initiate Flash Cleanup After Activation

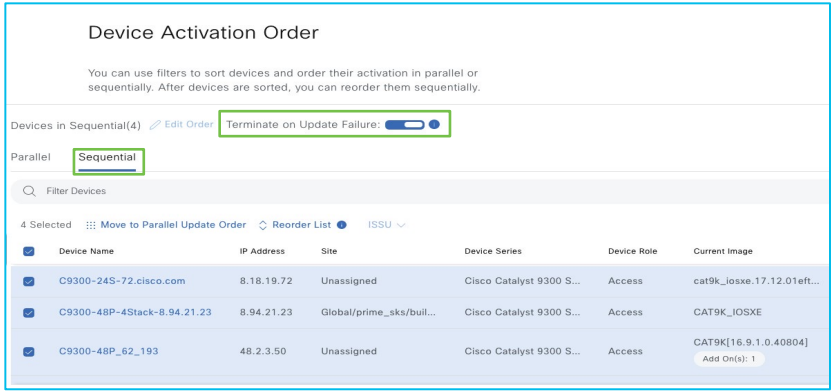
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Flexible device ordering during SWIM upgrade

Use Case

- 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





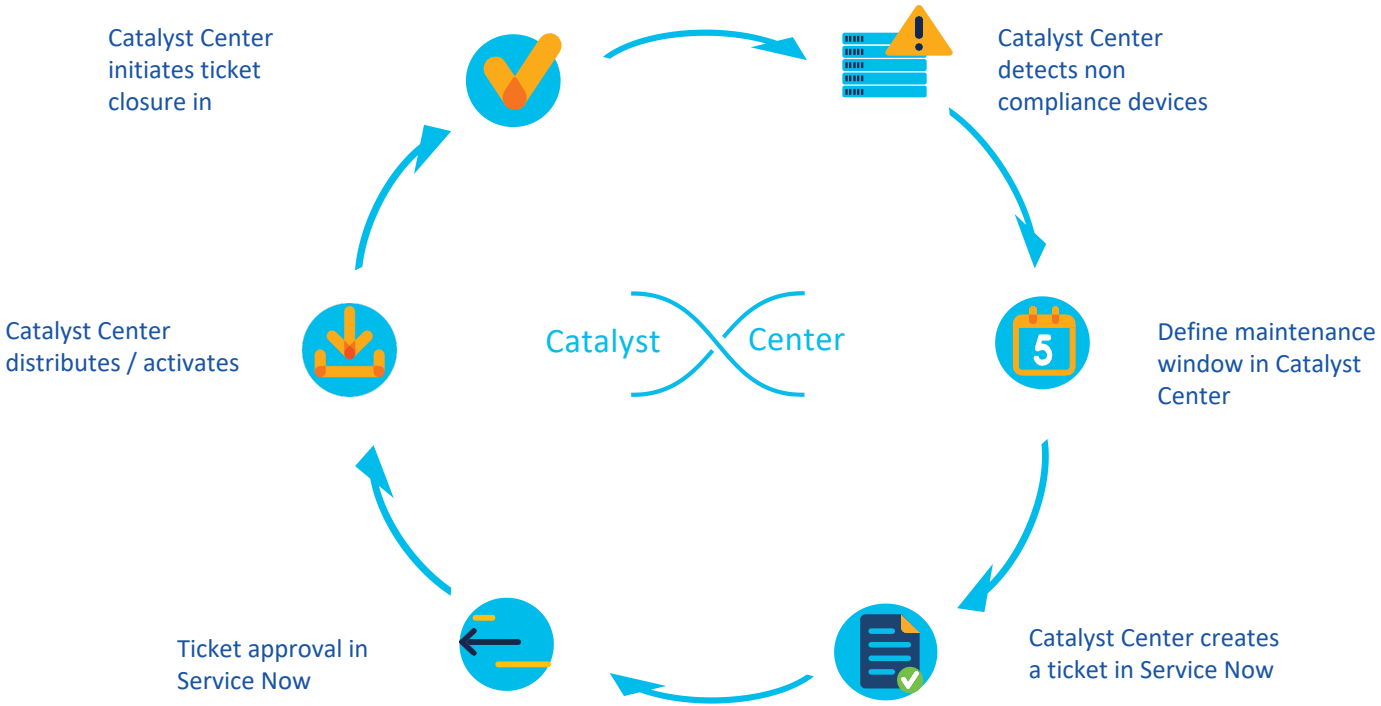
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

In-Service Software Upgrade(ISSU)

- ISSU supports both wired & wireless devices
- ISSU requires controllers in HA SSO
- ISSU together with AP Pre-Image Download and Rolling AP Upgrade helps reduce network downtime

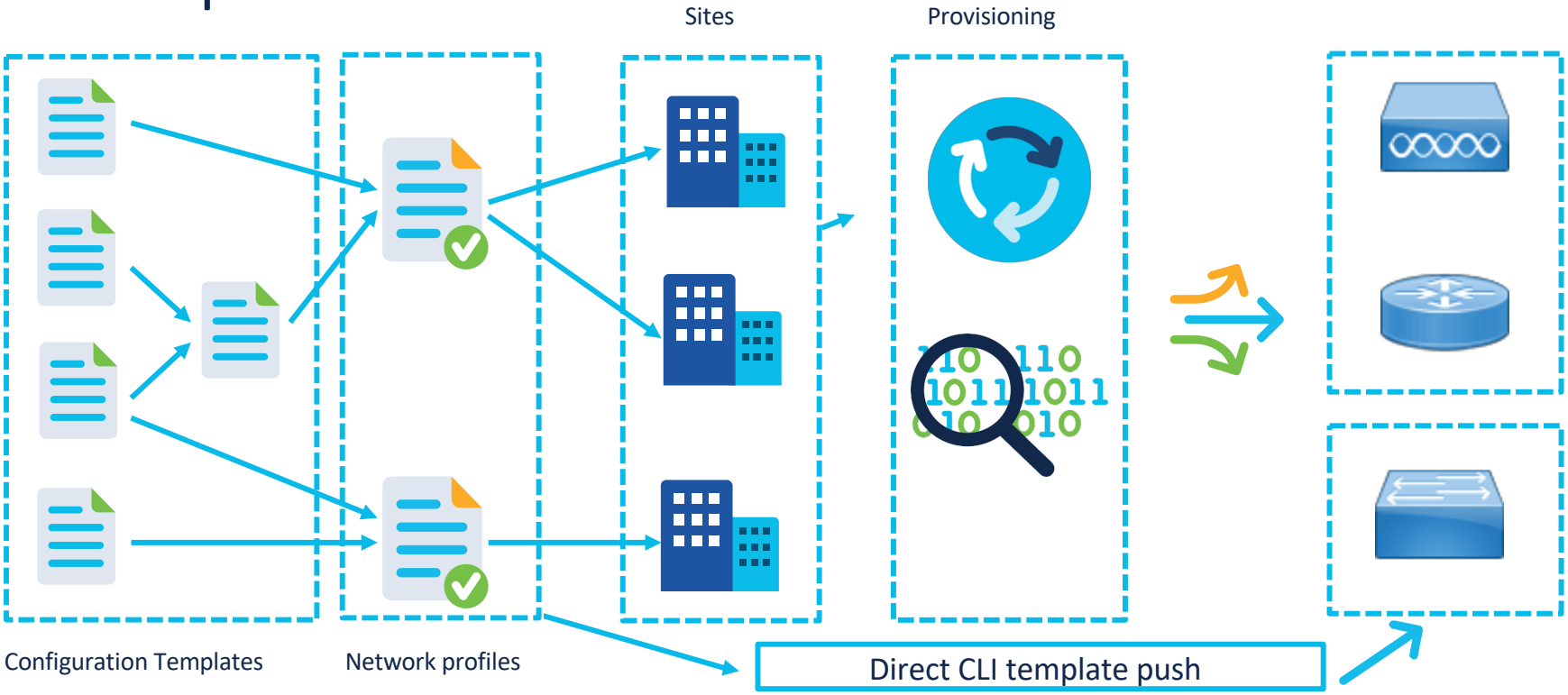
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Closed-loop Automation Via ITSM Integration



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

CLI Templates



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Templates Overview

- Onboarding Template(Day 0 template) vs Day N Template
- Day 0 – all at once. Day N – line by line
- Language Options – Velocity or Jinja
- All commands in the config t mode
- Variables, Bind to source, Implicit variables
- Detecting Conflicts – Design & Run-Time conflict

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Special Keywords

- #MODE_ENABLE <<commands>> #MODE_END_ENABLE

- #INTERACTIVE no crypto pki trustpoint server-

  CA<IQ>yes/no<R>yes #ENDS_INTERACTIVE

- <MLTCMD>first line of multiline command
  second line of multiline command ... ... last line of multiline command</MLTCMD>

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

For your reference

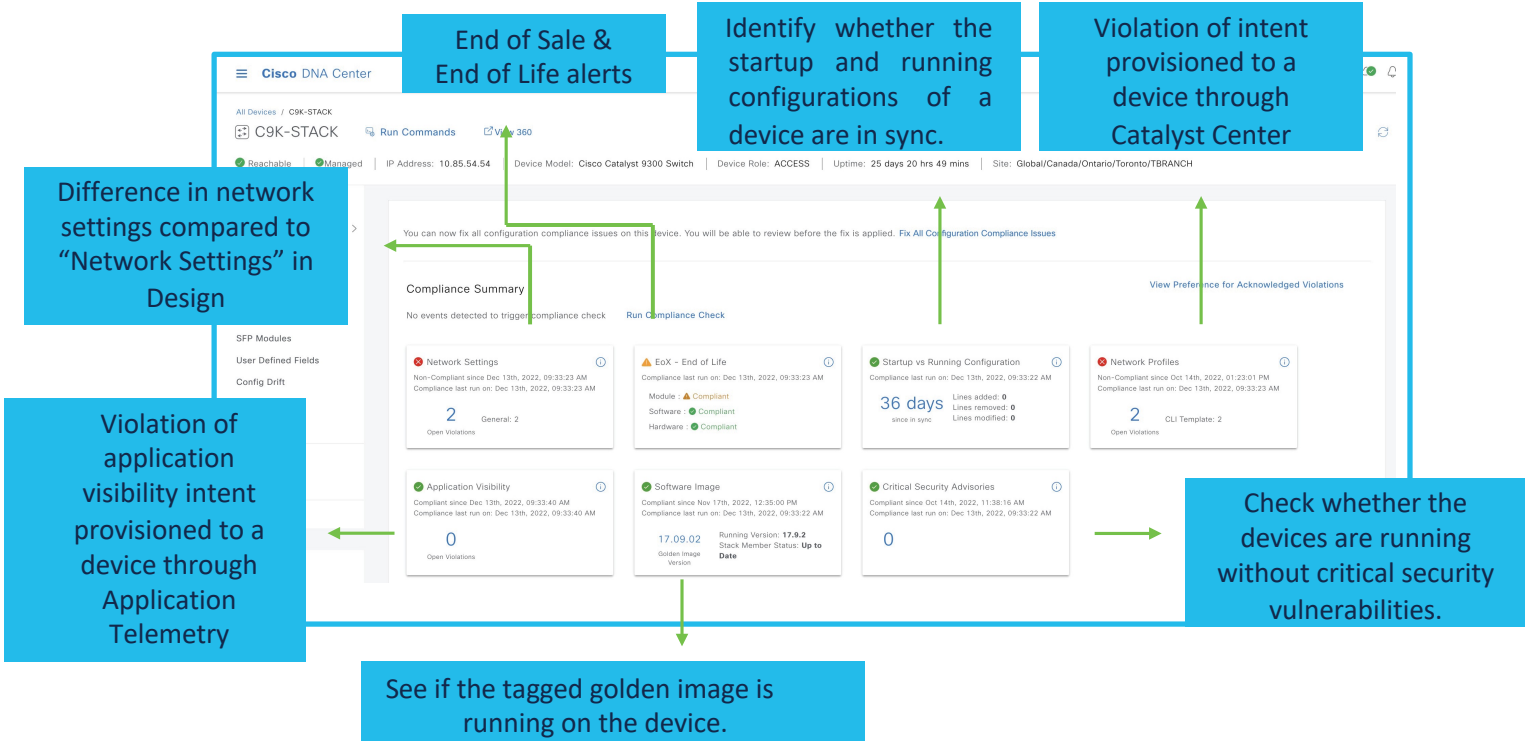
CLI Templates

Velocity vs Jinja

	Velocity	jinja
variable reference	`$loopback`	`{{loopback}}`
assignment	`#set ($loopback = "10.10.10.1")`	`{% set loopback = "10.10.10.1" %}`
conditional	`#if ($hostname == "border01") foo #end`	`{% if hostname == "border01" %} foo {% endif %}`
loop	`#foreach ($number in [0..3]) int gig1/${number}/24 shutdown #end`	`{% for number in range(3) %} int gig1/{{ number }}/24 shutdown {% endfor %}`
implicit variables	`#foreach ($interface in __interfaces)`	`{% for interface in __interface %}`

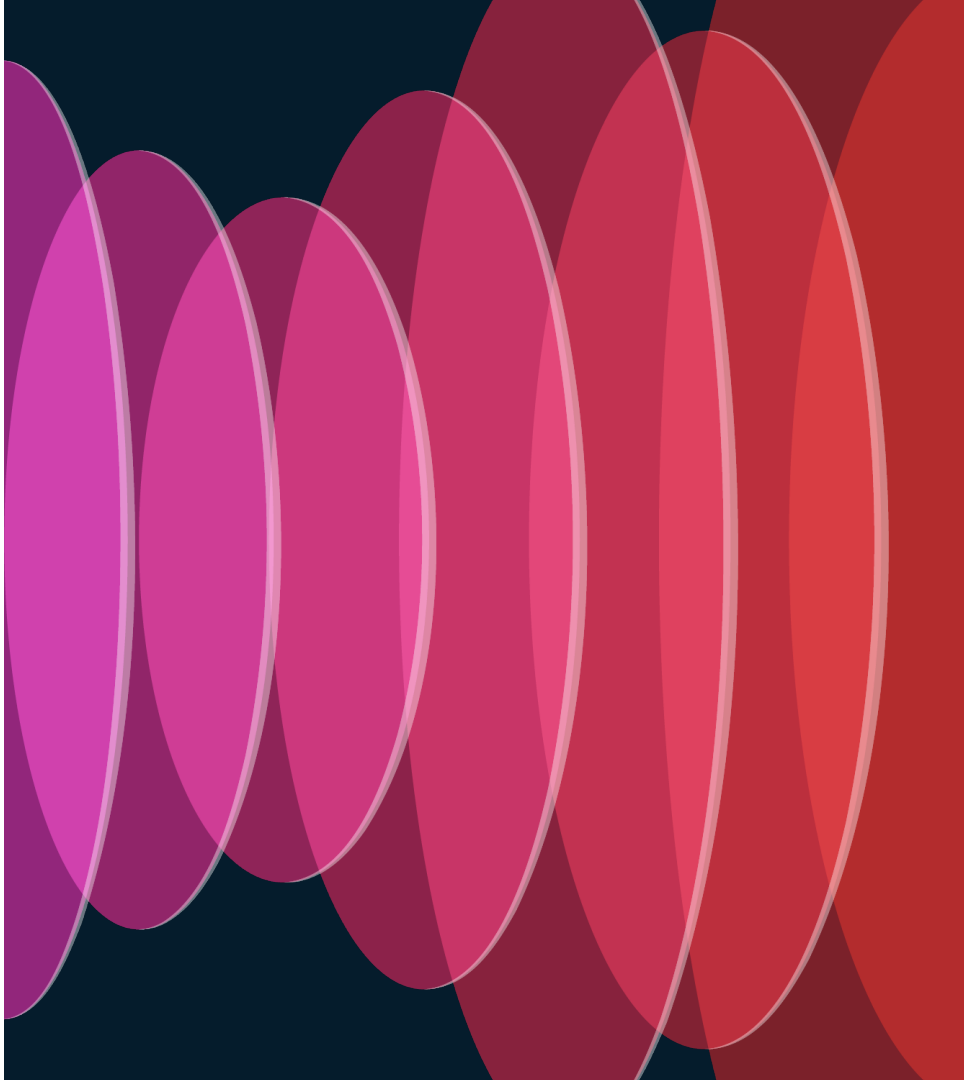
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Compliance Audit for Network Devices



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Demo



Cisco Live US Catalyst Center Learning Map

Sunday—2nd

- LTRENS-2890 9AM
  Deploying and Operating Cisco SD-Access with Pub-Sub using Cisco Catalyst Center
- TECOPS-2001 2PM
  The Ultimate Guide to Install, Onboard, Operate your Campus Network with Catalyst Center
- LTRSEC-2005 2PM
  Building Cisco SD-Access with Cisco Catalyst Center and ISE
- TECENS-2349 2PM
  Software-Defined Access for Industry Verticals

Monday—3rd

- BRKOPS-2548 8AM
  Network Troubleshooting Using Cisco Catalyst Center APIs
- BRKEWN-2029 9:30AM
  7 Ways to Optimize User Experience using Catalyst Center Wireless AIOps and Assurance
- BRKOPS-2416 10:30AM
  7 Habits for Success with Cisco Catalyst Center
- DEVWKS-1004 11AM
  Deploy Cisco Catalyst Center with Rest-APIs in Seconds
- IBOOPS-2882 1PM
  Let's Talk about Catalyst Center Integrations
- BRKOPS-2596 1PM
  Revolutionize Your Network Management with Catalyst Center: Physical or Virtual on AWS or VMware ESXi
- BRKOPS-1461 1PM
  Discovering and Managing Brownfield Deployment with Cisco Catalyst Center
- BRKIOT-2016 2:30PM
  Automating OT Services with Cisco Catalyst Center Best Practices

Tuesday—4th

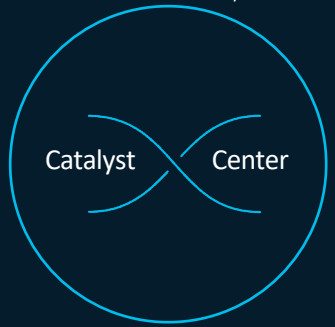
- BRKOPS-2208 10:30AM
  Discovering the Secrets of AI/ML in Cisco Catalyst Center
- DEVNET-1087 12PM
  Cisco Catalyst Center Platform: APIs, Event Notifications, Integrations, and DevOps Resources
- BRKCOC-2041 1PM
  Catalyst Center Automation and Use Cases in Cisco IT
- BRKOPS-2402 3PM
  Automate the Deployment of a Wireless Network with the Help of Cisco Catalyst Center

Wednesday—5th

- BRKOPS-2032 10:30AM
  3 Catalyst Center and ITSM Workflows: CMDB, Incident Management, and SWIM
- BRKENS-1601 10:30AM
  Catalyst Center and Meraki Cloud: The Right Choice for your Catalyst 9000 Switch Management!
- BRKGRN-1012 10:30AM
  Fostering Sustainable Campus Communities: Cisco Catalyst Center and Smart Buildings
- IBOENS-2600 10:30AM
  Revolutionizing Campus Networks: The Power of Automation with Catalyst Center
- DEVWKS-2041 2PM
  Cisco Catalyst Center and Targeting Event Notifications via Webex Messaging
- TACENT-2011 2:45PM
  Unlocking the troubleshooting power of Cisco Catalyst Center
- DEVNET-3000 3PM
  Chatbot for Catalyst Center—on Open Source AI-based Bot

Thursday—6th

- BRKOPS-2343 8:30AM
  Decoding Site Reliability Engineering Through Catalyst Center
- BRKENS-1851 8:30AM
  Zero Trust: Secure the Workplace with Cisco Software-Defined Access
- SKILLS-1660 9AM
  Introduction to Catalyst Center
- SKILLS-1661 10AM
  Introduction to Catalyst Center Platform
- BRKEWN-2306 1PM
  Wireless Network Automation and Assurance with Cisco Catalyst Center
- BRKXAR-3001
  End-to-End Visibility and Actionable Insights Using Catalyst Center, ISE, Catalyst SD-WAN and ThousandEyes



BU-led sessions

cisco Live!

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Live US EN Programmability Learning Map

Sunday—2nd

LTRCRT-1100 9AM
A Hands-On Preparation for the DevNet Associate Exam (Palmer/Quinn/Kareem)

Monday—3rd

BRKOPS-2548 8AM
Network Troubleshooting Using Catalyst Center APIs (Gabi)

DEVWKS 1004 11AM
Deploy Cisco Catalyst Center with Rest-API's in Seconds (Keith)
)

BOOPS-2882 1PM
Let's Talk about Catalyst Center Integrations (Gabi)

DEVNET-1283 1PM
Programmability, Automation Model Driven Telemetry on Cisco IOS XE with a dash of YANG Suite (Story)

DEVWKS-2031 4PM
Test Automation with Cisco Catalyst 9000 Virtual Switch (Jeremy)

Tuesday—4th

SKILLS-1110 10AM
Configure IOS XE using CLI (Jeremy & Story)

SKILLS-1111 11AM
Configure IOS XE using Automation (Jeremy & Story)

DEVNET-1087 12PM
Catalyst Center Platform: APIs, Event Notifications, Integrations, and DevOps Resources (Gabi)

BRKDEV-2017 2:30PM
Oh My! An Enterprise Network Automation Journey (Jeremy)

BRKDEV-2017 4PM
Test Automation with Cisco Catalyst 9000 Virtual Switch (Jeremy)

Wednesday—5th

BRKOPS-2032 10:30AM
3 Catalyst Center and ITSM Workflows: CMDB, Incident Management, and SWIM (Gabi)

DEVWKS-2042 1PM
Becoming a Cisco Catalyst IOS XE Terraform Expert

DEVNET-3000 3PM
Chatbot for Catalyst Center—on Open Source AI-based Bot (gabi)

SKILLS-1110 3PM
Configure IOS XE using CLI (Jeremy & Story)

SKILLS-1111 4PM
Configure IOS XE using Automation (Jeremy & Story)

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to win 1 of 5 full conference passes to Cisco Live 2025.

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

Level up and earn exclusive prizes!

Complete your surveys in the Cisco Live mobile app.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Continue your education

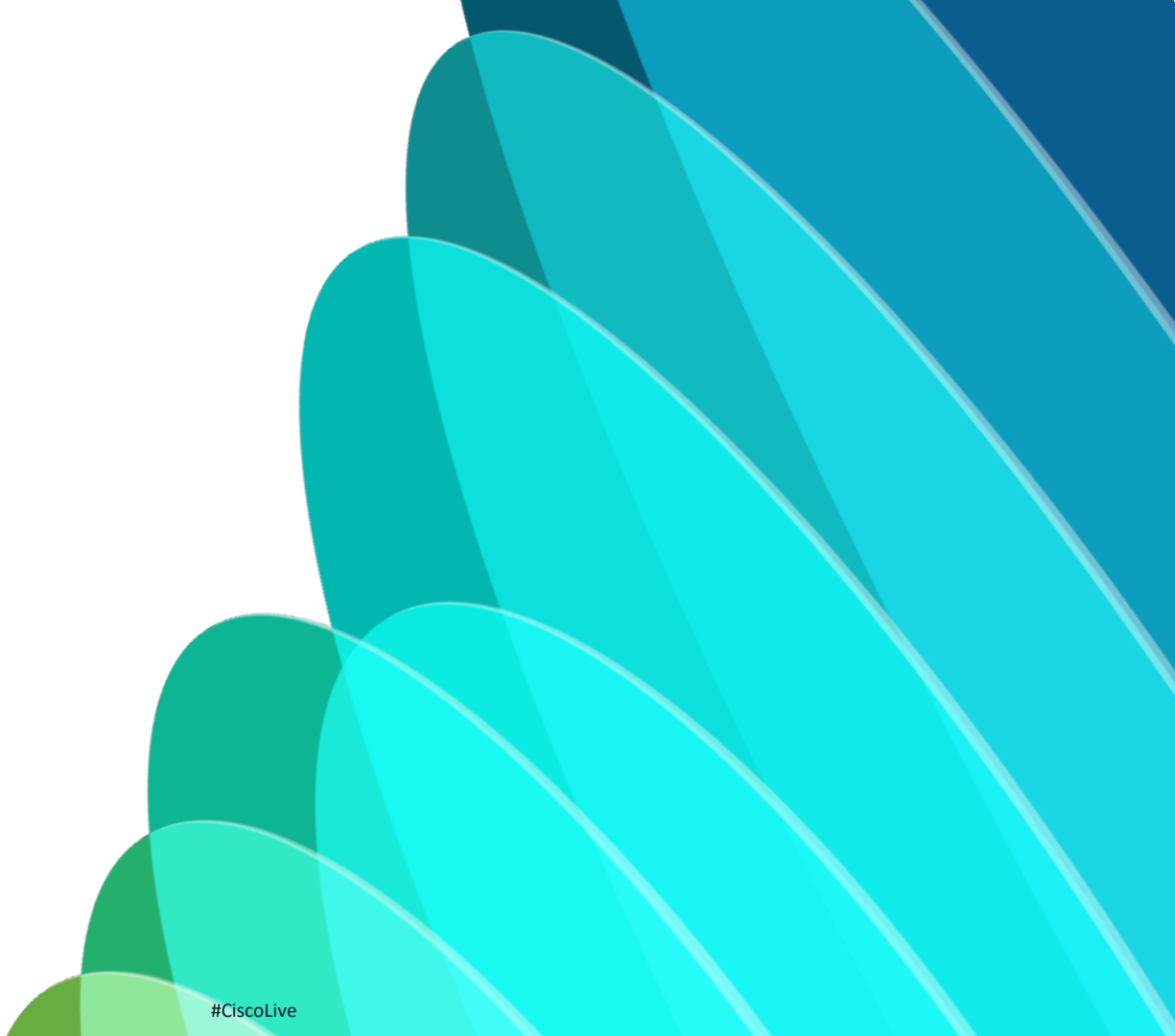
- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact me at:
www.linkedin.com/in/snehaamarapuram
or samarapu@cisco.com

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

The bridge to possible

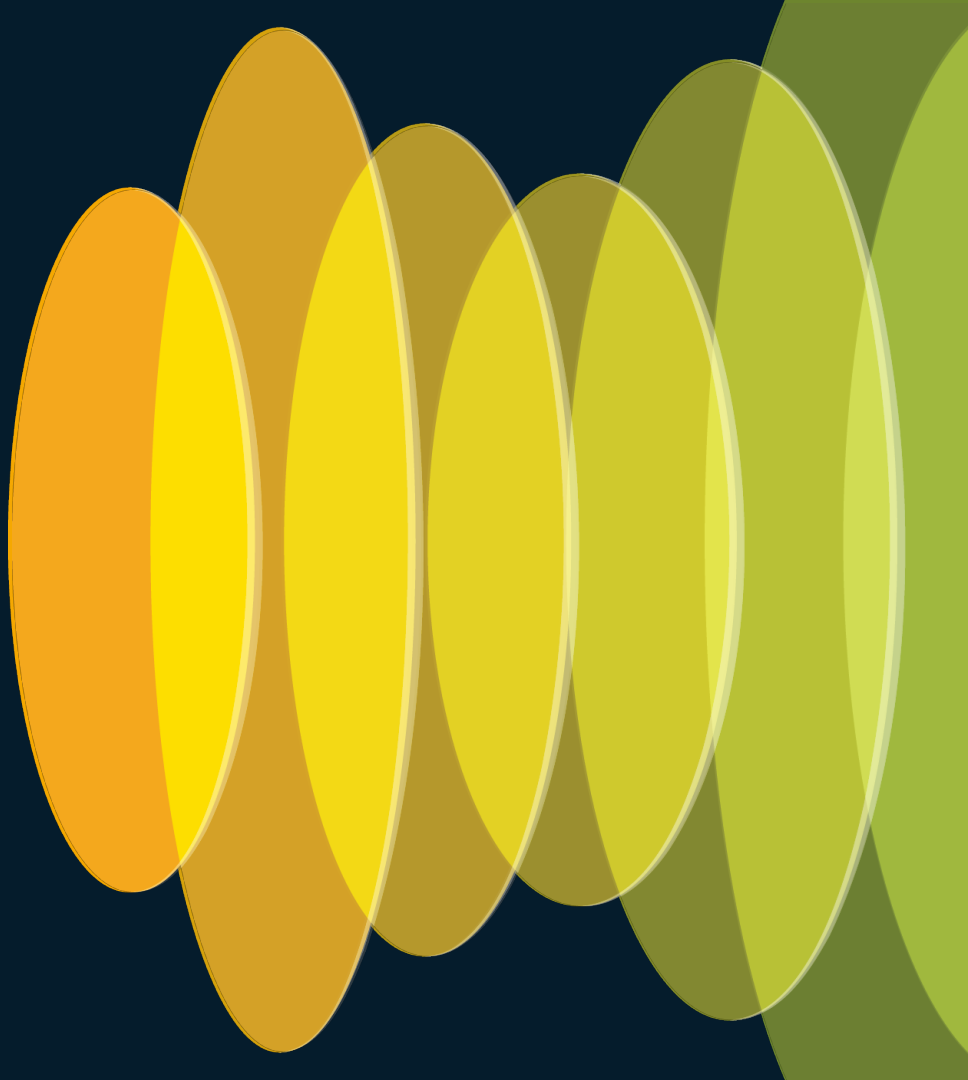
Thank you



cisco Live!

#CiscoLive

Appendix



Resources

- https://www.cisco.com/site/us/en/products/networking/catalyst-center/index.html
- https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/series.html
- https://www.cisco.com/c/dam/en/us/td/docs/Website/enterprise/catalyst_center_compatibility_matrix/index.html
- https://developer.cisco.com/catalyst-center/
- https://blogs.cisco.com/networking/dnatemplatesgetstarted01
- https://github.com/kebaldwi/DNAC-TEMPLATES
- https://velocity.apache.org/engine/devel/vtl-reference.html
- https://palletsprojects.com/p/jinja/

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Logging All CLI Commands with EEM Applet

```
conf t
event manager applet catchall
event cli pattern ".*" sync no skip no
action 1 syslog msg "$_cli_msg"
```

Note: You can use this to view the configuration changes done by Catalyst Center

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public