



TURN IT UP

CISCO *Live!*

#CiscoLive



The bridge to possible

Cisco DNA Center – Device Controllability under the covers



Adam Radford – Distinguished Architect – @adamradford123

Lila Rousseaux – Technical Solutions Architect – @lila_rousseaux

BRKEMT-2003

CISCO *Live!*

#CiscoLive



Agenda

- Why “Device Controllability”
- What happens when we add a device in DNA Center
- What happens when we change user credentials
- Common objections on “Device Controllability”
- Conclusion

Why “Device Controllability”



Device Controllability

Monitoring

Settings

Telemetry

Trust

reallylongName2.adamlab.cisco.com

Management IP 10.10.10.146
Device Type Cisco Catalyst 9800-CL Wireless Controller for Cloud
Device Role ACCESS

Deployment of syslog setting
• Deployment of syslog setting initiated
• COMPLETED: Configuring new Syslog Server Configurations Settings IP: [10.10.10.144] on the device: 10.10.10.146 completed successfully.

SUCCESS

Deployment of snmp setting
• Deployment of snmp setting initiated
• COMPLETED: Configuring new SNMP Trap Server Configurations Settings IP: [10.10.10.144] on the device: 10.10.10.146 completed successfully.

SUCCESS

Deployment of dns setting
• DNS Configurations pushed successfully
• Process success on all devices.

SUCCESS

Deployment of netflow setting
• Deployment of netflow setting initiated
• COMPLETED: Configuring new Netflow Collector Server Configuration Settings IP: [10.10.10.144] and Port: [6007] on the device: 10.10.10.146 completed successfully.

SUCCESS

Application telemetry
• Configuration of application telemetry is only applicable upon enable/disable application telemetry action, so no operation was performed

SUCCESS

Install of Swim Certificate
• SWIM Certificate was pushed successfully

SUCCESS

Deployment of WSA certificate
• ICAP port and Assurance WSA Configuration pushed successfully
• WSA Certificate was pushed successfully

SUCCESS

Deployment of Wireless AP Join Certificate

- Certificate already exists on the device.
- Deployment of Wireless AP Join Certificate setting initiated

SUCCESS

Deployment of PKCS12 certificate

- Started process: Pkcs12 Internal Certificate Configure
- Reachable DNAC IP:10.10.10.144
- PKI Configurations pushed successfully
- PKCS12 Certificate was pushed successfully

SUCCESS

Deployment of IOS WLC NA Certificate configuration

- Setting does not apply to device, so no operation was performed

SUCCESS

Deployment of IOS Telemetry Subscriptions configuration

- Configuring Assurance Telemetry Receiver Information
- Configuring Assurance Telemetry Subscriptions
- Configured Telemetry Subscription Receiver on the device with Receiver as 10.10.10.144
- Assurance Telemetry Subscriptions Configuration Success
- App Based Telemetry Subscriptions Configuration Success
- Telemetry Subscriptions was pushed successfully
- App Based Telemetry Subscriptions Configuration Success

SUCCESS

Deployment of AP Impersonation configuration

- AP Impersonation pushed successfully
- Deployment of AP Impersonation setting initiated

SUCCESS

Deployment of Terminal Width

- Setting does not apply to device, so no operation was performed

SUCCESS

Deployment of IPDT

- Cannot push IPDT Configuration on the device with IpAddress: 10.10.10.146 for Product Family: wireless controller (Not Applicable)

SUCCESS

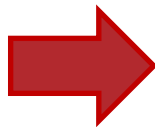
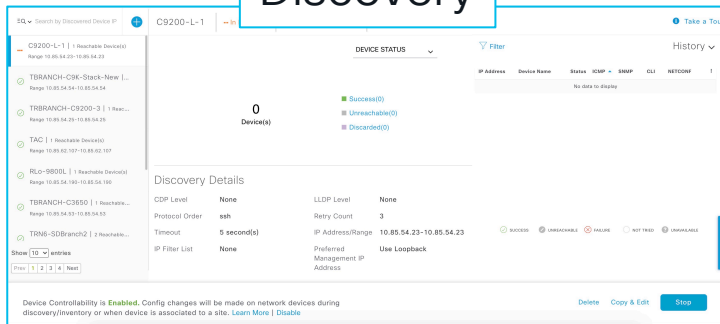
What happens
when we add a
device in DNA
Center



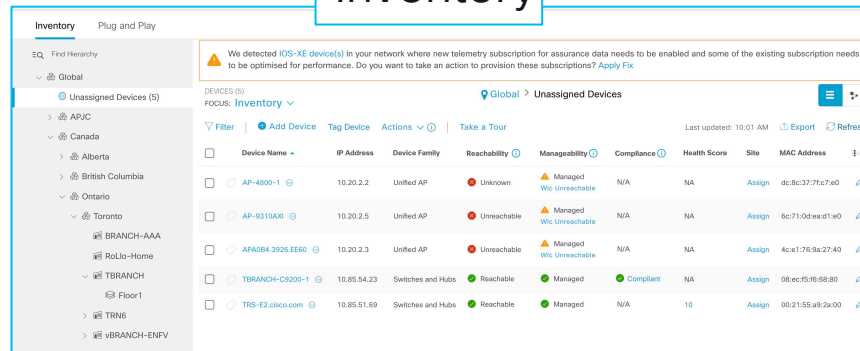
What happens when a device is added to DNAC?

- Inventory Collection
- Configuration pushed to devices to allow DNAC manageability
- Establish Streaming Telemetry over secure connection

Discovery

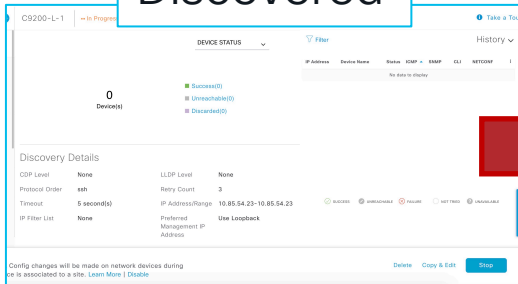


Inventory

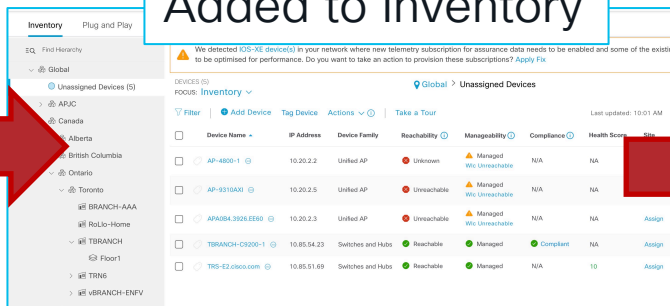


Full device on-boarding process into DNA Center

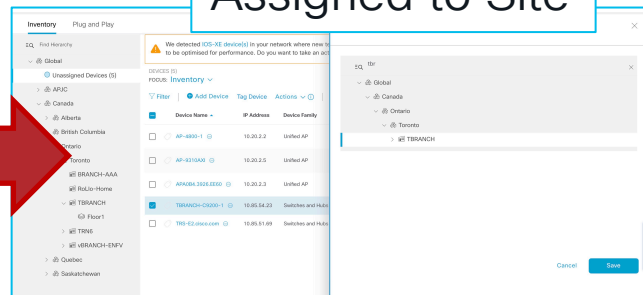
Discovered



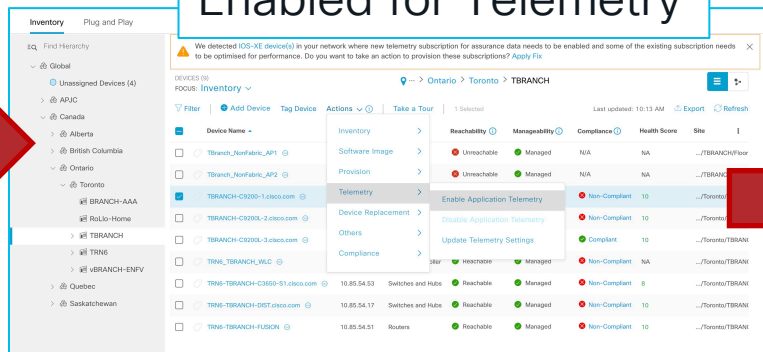
Added to Inventory



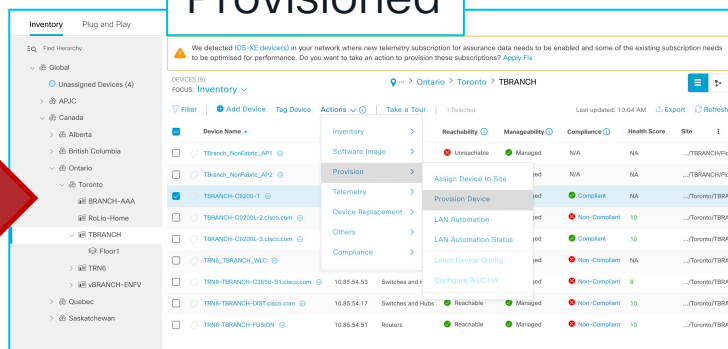
Assigned to Site



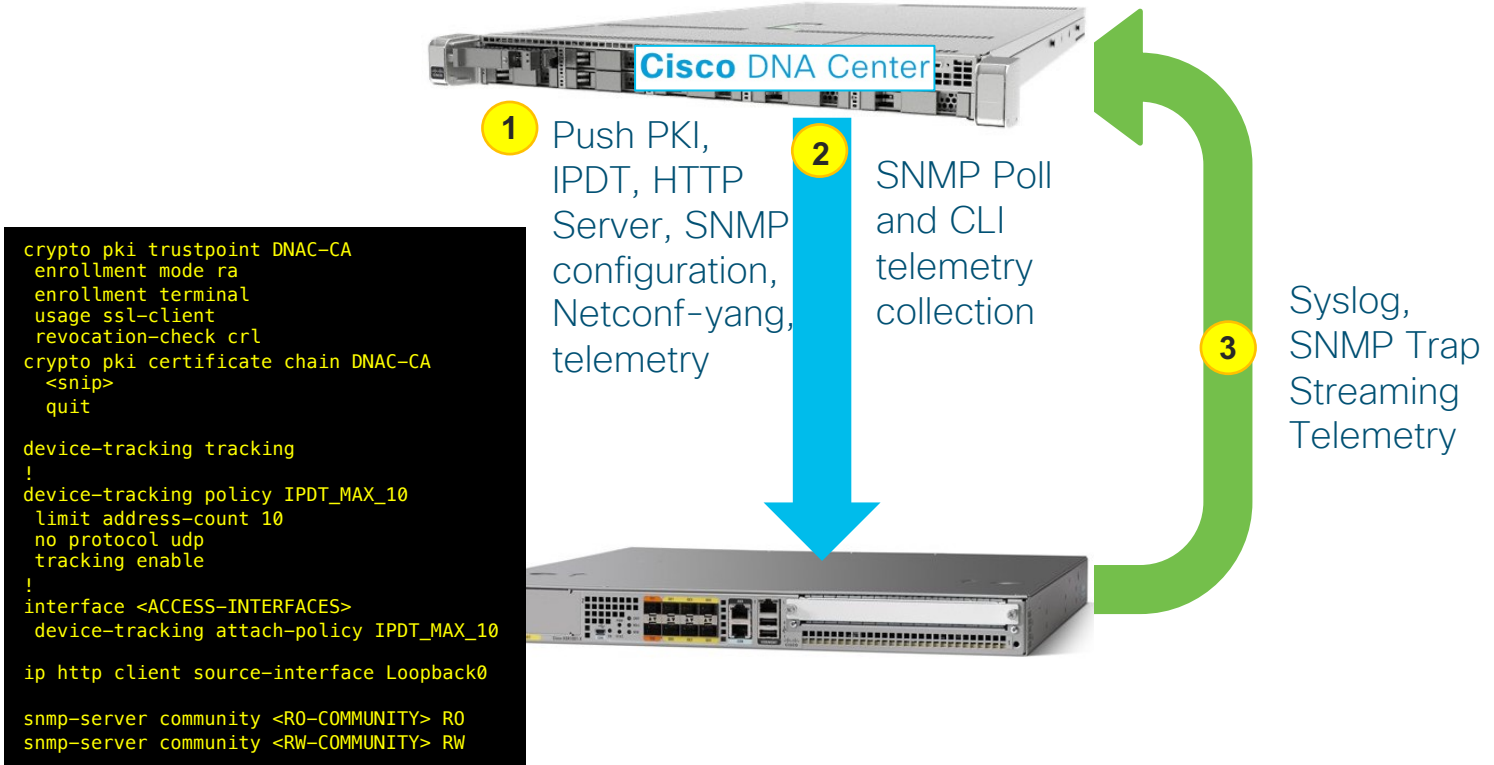
Enabled for Telemetry



Provisioned



What happens when a C9K switch is added to Cisco DNA Center?



Changes in the right direction: more visibility and control of required configuration

DNA Center 1.x

Device Added to DNA Center inventory the following are configured

- SNMP/CLI credentials
- Syslog to DNAC
- Traps to DNAC
- Netflow to DNAC
- IPDT for wired clients
- WSA/TDL for Wireless telemetry
- Cisco trustsec credentials
- Cisco controller certs

DNA Center 2.x

Device Added to DNA Center inventory the following is configured

- SNMP/CLI credentials

Adding device to a site (site level customization of what to enable):

- Syslog to DNAC
- Traps to DNAC
- Netflow to DNAC
- IPDT for wired clients (2.2.1)
- WSA/TDL for Wireless telemetry
- Cisco trustsec credentials
- Cisco controller certificates

Adding a switch to DNA Center – Discovery

The screenshot shows the Cisco DNA Center Discovery interface. At the top, a search bar contains 'C9200-L-1' and shows '1 Reachable Device(s)' with a timer at '00h:00m:00s'. Below the search bar, a list of discovered devices is shown on the left, including 'C9200-L-1', 'TBRANCH-C9K-Stack-New', 'TBRANCH-C9200-3', 'TAC', 'RLO-9800L', 'TBRANCH-C3650', and 'TRN6-SDBranch2'. The main area displays '0 Device(s)' with a 'DEVICE STATUS' dropdown and a 'Filter' button. Below this, a 'Discovery Details' section shows various parameters: CDP Level (None), LLD Level (None), Protocol Order (ssh), Retry Count (3), Timeout (5 second(s)), IP Address/Range (10.85.54.23-10.85.54.23), IP Filter List (None), Preferred Management IP Address (Use Loopback), and a legend for SUCCESS, UNREACHABLE, FAILURE, NOT TRIED, and UNAVAILABLE.

```
com over ssh. External groups: PRIV15
TBRANCH-C9200-1#
*Feb  5 14:57:35.950: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: netadmin] [Source: 10.85.54.180] [localport: 22] at 14:57:35 UTC Fri Feb 5 2021
*Feb  5 14:57:36.168: %SYS-5-CONFIG_I: Configured from console by netadmin on vty1 (10.85.54.180)
TBRANCH-C9200-1#
*Feb  5 14:57:40.568: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: netadmin] [Source: 10.85.54.180] [localport: 22] at 14:57:40 UTC Fri Feb 5 2021
TBRANCH-C9200-1#
*Feb  5 14:57:40.654: %SYS-6-LOGOUT: User netadmin has exited tty session 4(10.85.54.180)
TBRANCH-C9200-1#
*Feb  5 14:57:41.348: %DMI-5-AUTH_PASSED: Switch 1 R0/0: dmiauthd: User 'netadmin' authenticated successfully from 10.85.54.180:60713 and was authorized for net
conf over ssh. External groups: PRIV15
*Feb  5 14:57:42.683: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: netadmin] [Source: 10.85.54.180] [localport: 22] at 14:57:42 UTC Fri Feb 5 2021
TBRANCH-C9200-1#
*Feb  5 14:57:44.155: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: netadmin] [Source: 10.85.54.180] [localport: 22] at 14:57:44 UTC Fri Feb 5 2021
TBRANCH-C9200-1#
*Feb  5 14:57:50.054: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: netadmin] [Source: 10.85.54.180] [localport: 22] at 14:57:50 UTC Fri Feb 5 2021
TBRANCH-C9200-1#
```

Adding a switch to DNA Center – Discovery

The screenshot shows the Cisco DNA Center Inventory page. The left sidebar contains a navigation menu with 'Unassigned Devices (5)' highlighted. The main content area displays a table of unassigned devices. The table has columns for Device Name, IP Address, Device Family, Reachability, Manageability, Compliance, Health Score, Site, and MAC Address. The device 'TBRANCH-C9200-1' is highlighted with a red box, showing it is a 'Switches and Hubs' device with a 'Reachable' status and 'Compliant' health score.

Inventory Plug and Play

Find Hierarchy

Global

Unassigned Devices (5)

APJC

Canada

Alberta

British Columbia

Ontario

Toronto

BRANCH-AAA

RoLlo-Home

TBRANCH

Floor1

TRN6

vBRANCH-ENFV

DEVICES (5)
FOCUS: Inventory

Global > Unassigned Devices

Filter Add Device Tag Device Actions Take a Tour

Last updated: 10:01 AM Export Refresh

	Device Name	IP Address	Device Family	Reachability	Manageability	Compliance	Health Score	Site	MAC Address	
<input type="checkbox"/>	AP-4800-1	10.20.2.2	Unified AP	Unknown	Managed Wlc Unreachable	N/A	NA	Assign	dc:8c:37:7f:c7:e0	
<input type="checkbox"/>	AP-9310AXI	10.20.2.5	Unified AP	Unreachable	Managed Wlc Unreachable	N/A	NA	Assign	6c:71:0d:ea:d1:e0	
<input type="checkbox"/>	APA0B4.3926.EE60	10.20.2.3	Unified AP	Unreachable	Managed Wlc Unreachable	N/A	NA	Assign	4c:e1:76:9a:27:40	
<input type="checkbox"/>	TBRANCH-C9200-1	10.85.54.23	Switches and Hubs	Reachable	Managed	Compliant	NA	Assign	08:ec:f5:f6:68:80	
<input type="checkbox"/>	TRS-E2.cisco.com	10.85.51.69	Switches and Hubs	Reachable	Managed	N/A	10	Assign	00:21:55:a9:2a:00	

Adding a switch to DNA Center – Discovery

C9200L-24T-4G
IOS-XE: 17.03.01

```
device-tracking tracking
!
device-tracking policy IPDT_POLICY
  no protocol udp
  tracking enable
!
<snip>
!
interface GigabitEthernet1/0/2
  device-tracking attach-policy IPDT_POLICY
!
interface GigabitEthernet1/0/3
  device-tracking attach-policy IPDT_POLICY
!
interface GigabitEthernet1/0/4
  device-tracking attach-policy IPDT_POLICY
!
interface GigabitEthernet1/0/5
  device-tracking attach-policy IPDT_POLICY
!
<snip>
```

```
<snip>
!
snmp-server community ro RO
!
<snip>
!
netconf-yang
!
```

Adding a switch to DNA Center – Assign to Site

The screenshot displays the Cisco DNA Center interface. The main header shows 'Cisco DNA Center' and 'Provision - Network Devices - Inventory'. The left sidebar contains navigation options: 'Inventory' (selected), 'Plug and Play', 'Find Hierarchy', 'Global', 'Unassigned Devices (5)', 'APJC', and 'Canada'. The main content area shows a list of devices with columns for 'Device Name', 'IP Address', and 'Reachability'. A modal window titled 'Choose a site' is open on the right, showing a search bar with 'aaa' and a list of sites: 'Global', 'Canada', 'Ontario', and 'Toronto'. The 'BRANCH-AAA' site is highlighted in the search results. A red box highlights the 'BRANCH-AAA' site in the search results. A 'Cancel' button and a 'Save' button are at the bottom right of the modal.

Inventory Plug and Play

Find Hierarchy

Global

Unassigned Devices (5)

APJC

Canada

We detected IOS-XE device(s) in your network where new te to be optimised for performance. Do you want to take an act

DEVICES (5)
FOCUS: Inventory

Filter Add Device Tag Device Actions

Device Name	IP Address	Reachability
AP-4800-1	10.20.2.2	Un
AP-9310AXI	10.20.2.5	Un
APA0B4.3926.EE60	10.20.2.3	Un
TBRANCH-C9200-1	10.85.54.23	Re
TRS-E2.cisco.com	10.85.51.69	Re

Choose a site

aaa

Global

Canada

Ontario

Toronto

BRANCH-AAA

Cancel Save

Adding a switch to DNA Center – Assign to Site

The screenshot displays the Cisco DNA Center interface. On the left, the 'Inventory' tab is active, showing a list of devices. A warning message at the top states: 'We detected IOS-XE device(s) in your network where new to be optimised for performance. Do you want to take an act'. The device list includes:

Device Name	IP Address	Reachability
AP-4800-1	10.20.2.2	Unreachable
AP-9310AXI	10.20.2.5	Unreachable
APA0B4.3926.EE60	10.20.2.3	Unreachable
TBRANCH-C9200-1	10.85.54.23	Reachable
TRS-E2.cisco.com	10.85.51.69	Reachable

The 'TBRANCH-C9200-1' device is selected. The 'Assign Device to Site' dialog box is open, showing the following settings:

Setting	Value
Syslog Server	Cisco DNA Center
Netflow Collector	Cisco DNA Center
SNMP Trap Receiver	Cisco DNA Center, 10.10.10.10
Syslog Level	6 - Information Messages
Cisco TrustSec (CTS) Credentials	Yes
Controller Certificates	Yes

At the bottom of the dialog, a red box highlights the text: 'Device Controllability is **Enabled**. [Learn More](#) | [Disable](#)'. The 'Assign' button is highlighted in blue.

Adding a switch to DNA Center – Assign to Site

The screenshot displays the Cisco DNA Center interface. On the left is a navigation pane with a tree structure: Global (expanded) > Unassigned Devices (4) > APJC > Canada > Alberta > British Columbia > Ontario (expanded) > Toronto (expanded) > BRANCH-AAA (highlighted with a red box). The main content area shows the 'DEVICES (1)' page for the 'BRANCH-AAA' site. The breadcrumb path is 'Ontario > Toronto > BRANCH-AAA'. The 'FOCUS' is set to 'Inventory'. Below the breadcrumb, there are links for 'Filter', 'Add Device', 'Tag Device', 'Actions', and 'Take a Tour'. The table below lists the device details, with the first row highlighted by a red box:

<input type="checkbox"/>	Device Name	IP Address	Reachability	Manageability	Compliance	Health Score	Site	Last Updated	Platform	Support
<input type="checkbox"/>	TBRANCH-C9200-1.cisco.com	10.85.54.23	Reachable	Managed	Compliant	8	.../Toronto/BRANCH-AAA	2 hours ago	C9200L-24T-4G	Supported

Adding a switch to DNA Center – Assign to Site – Part 1

Cisco DNA Center

Version 2.1.2.3

[Release Notes](#)

[> Packages](#)

C9200L-24T-4G
IOS-XE: 17.03.01

```
!  
flow exporter 10.85.54.177  
  destination 10.85.54.177  
  transport udp 6007  
!  
<snip>  
!  
crypto pki trustpoint DNAC-CA  
  enrollment mode ra  
  enrollment terminal  
  usage ssl-client  
  revocation-check crl none  
!  
crypto pki trustpoint sdn-network-infra-iwan  
  enrollment url  
http://10.85.54.177:80/ejbca/publicweb/apply/scep/sdnscep  
  fqdn TBRANCH-C9200-1  
  subject-name CN=C9200L-24T-4G_JAE22501JXT_sdn-network-infra-  
iwan  
  revocation-check crl  
  source interface Vlan419  
  rsakeypair sdn-network-infra-iwan  
  auto-enroll 80 regenerate
```

```
!  
crypto pki certificate chain DNAC-CA  
  certificate ca 00B8550967690FF9AC  
!  
<snip>  
!  
crypto pki certificate chain sdn-network-  
infra-iwan  
  certificate 6692DA412BE64785  
  <snip>  
  certificate ca 4259D7BFCB7B5B46  
    30820323 3082020B A0030201 02020842  
!  
<snip>  
!  
logging source-interface Vlan419  
logging host 10.85.54.177  
!  
<snip>  
!
```

Adding a switch to DNA Center – Assign to Site – Part 2

```
<snip>
snmp-server enable traps tty
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
!
<snip>
snmp-server enable traps eigrp
!
<snip>
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps license
!
<snip>
!
snmp-server enable traps cpu threshold
snmp-server enable traps memory bufferpeak
snmp-server enable traps stackwise
snmp-server enable traps udd status-change
snmp-server enable traps fru-ctrl
snmp-server enable traps flash insertion removal lowspace
```

```
<snip>
snmp-server enable traps power-ethernet police
snmp-server enable traps entity
snmp-server enable traps envmon
!
<snip>
snmp-server enable traps config-copy
snmp-server enable traps config
!
<snip>
snmp-server enable traps syslog
snmp-server enable traps ipsla
snmp-server enable traps mac-notification change move threshold
snmp-server host 10.85.54.177 version 2c ro
!
<snip>
```

C9200L-24T-4G
IOS-XE: 17.03.01

Adding a switch to DNA Center – Assign to Site – Part 3

C9200L-24T-4G
IOS-XE: 17.03.01

```
telemetry ietf subscription 550
  encoding encode-tdl
  filter tdl-uri /services;serviceName=smevent/sessionevent
  source-address 10.85.54.23
  stream native
  update-policy on-change
  receiver ip address 10.85.54.177 25103 protocol tls-native profile sdn-network-infra-iwan
telemetry ietf subscription 551
  encoding encode-tdl
  filter tdl-uri /services;serviceName=sessmgr_oper/session_context_data
  source-address 10.85.54.23
  stream native
  update-policy periodic 360000
  receiver ip address 10.85.54.177 25103 protocol tls-native profile sdn-network-infra-iwan
telemetry ietf subscription 552
  encoding encode-tdl
  filter tdl-uri /services;serviceName=iosevent/sisf_mac_oper_state
  source-address 10.85.54.23
  stream native
  update-policy on-change
  receiver ip address 10.85.54.177 25103 protocol tls-native profile sdn-network-infra-iwan
!
<snip>
```

Adding a switch to DNA Center – Telemetry

The screenshot displays the Cisco DNA Center web interface. On the left is a navigation pane with a tree structure: 'Unassigned Devices (4)' is expanded, showing 'APJC', 'Canada', 'Alberta', 'British Columbia', 'Ontario', and 'Toronto'. Under 'Toronto', several locations are listed, including 'BRANCH-AAA', 'BRANCH-NORTH-YOR', 'RoLlo-Home', 'TBRANCH', and 'TRN6'. The main content area is titled 'DEVICES (1)' with a 'FOCUS: Inventory' dropdown. Breadcrumbs at the top right show the path: '... > Ontario > Toronto > BRANCH-AAA'. A table lists the device 'TBRANCH-C9200-1' with IP address '10.85.54.1'. An 'Actions' dropdown menu is open for this device, listing options like 'Inventory', 'Software Image', 'Provision', 'Telemetry', 'Device Replacement', 'Others', and 'Compliance'. The 'Telemetry' option is selected, opening a sub-menu where 'Enable Application Telemetry' is highlighted with a red rectangle. Other options in the sub-menu include 'Disable Application Telemetry' and 'Update Telemetry Settings'. The table also shows columns for 'Manageability', 'Site', 'Last Updated', 'Provision Status', and 'Application Telemetry'.

Device Name	IP Address	Manageability	Site	Last Updated	Provision Status	Application Telemetry
TBRANCH-C9200-1	10.85.54.1	Managed	.../Toronto/BRANCH-AAA	2 minutes ago	Success See Details	Not Provisioned

Adding a switch to DNA Center – Telemetry – Part 1

Cisco DNA Center

Version 2.1.2.3

[Release Notes](#)

[> Packages](#)

C9200L-24T-4G
IOS-XE: 17.03.01

```
!  
!  
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  
!
```

```
!  
flow exporter dnacexporter  
  destination 10.85.54.177  
  source Vlan419  
  transport udp 6007  
  export-protocol ipfix  
  option interface-table timeout 10  
  option vrf-table timeout 10  
  option sampler-table  
  option application-table timeout 10  
  option application-attributes timeout 10  
!  
!  
flow monitor dnacmonitor  
  exporter dnacexporter  
  cache timeout inactive 10  
  cache timeout active 60  
  record dnacrecord
```

Adding a switch to DNA Center – Telemetry – Part 2

C9200L-24T-4G
IOS-XE: 17.03.01

```
<snip>
!
interface GigabitEthernet1/0/14
  device-tracking attach-policy IPDT_POLICY
  ip flow monitor dnacmonitor input
  ip flow monitor dnacmonitor output
!
interface GigabitEthernet1/0/15
  device-tracking attach-policy IPDT_POLICY
  ip flow monitor dnacmonitor input
  ip flow monitor dnacmonitor output
!
!
interface GigabitEthernet1/0/16
  device-tracking attach-policy IPDT_POLICY
  ip flow monitor dnacmonitor input
  ip flow monitor dnacmonitor output
!
<snip>
```

Adding a switch to DNA Center – Telemetry

Application Telemetry Field

DEVICES (1)
FOCUS: Provision ▾

... > Ontario > Toronto > BRANCH-AAA

Filter | + Add Device Tag Device Actions ▾ ① | Take a Tour

Last updated: 1:57 PM Export Refresh

Device Name ▴	IP Address	Site	Reachability ①	Provision Status	Credential Status	Last Provisioned	Device Role	Manageability ①	Application Telemetry
TBRANCH-C9200-1.cisco.com	10.85.54.23	.../Toronto/BRANCH-AAA	Reachable	Configuring See Details	Not Provisioned	a few seconds ago	ACCESS	Managed	Not Provisioned

DEVICES (1)
FOCUS: Provision ▾

... > Ontario > Toronto > BRANCH-AAA

Filter | + Add Device Tag Device Actions ▾ ① | Take a Tour

Last updated: 1:58 PM Export Refresh

Device Name ▴	IP Address	Site	Reachability ①	Provision Status	Credential Status	Last Provisioned	Device Role	Manageability ①	Application Telemetry
TBRANCH-C9200-1.cisco.com	10.85.54.23	.../Toronto/BRANCH-AAA	Reachable	Success See Details	Not Provisioned	a minute ago	ACCESS	Managed	Enabled

Adding a switch to DNA Center – Provision

The image displays two screenshots of the Cisco DNA Center web interface, illustrating the process of adding a switch to the network.

Left Screenshot: AAA Server Configuration

- Navigation Pane:** The left-hand navigation pane shows the hierarchy: Global > APJC > Canada > Alberta > British Columbia > Ontario > Toronto > **BRANCH-AAA** (highlighted with a red box).
- Configuration Page:** The main configuration area is titled "Configure AAA, NTP, and Image Distribution (SFTP) servers using the 'Add Servers' link. Once devices are discovered, DNA Center will deploy using these settings." The "Add Servers" button is visible in the top right.
- AAA Server Settings:** The "AAA Server" section is active. The "Network" checkbox is selected. The "Servers" section shows "ISE" selected. The "Protocol" section shows "RADIUS" selected. The "Network" section shows "10.85.54.185" as the IP Address (Primary).
- DHCP Server:** The "DHCP Server" section shows "10.85.48.7" as the DHCP address.
- DNS Server:** The "DNS Server" section shows "cisco.com" as the Domain Name.

Right Screenshot: NTP Server Configuration

- Navigation Pane:** The left-hand navigation pane shows the hierarchy: Global > APJC > Canada > Alberta > British Columbia > Ontario > Toronto > **BRANCH-AAA** (highlighted with a red box).
- Configuration Page:** The main configuration area is titled "Configure AAA, NTP, and Image Distribution (SFTP) servers using the 'Add Servers' link. Once devices are discovered, DNA Center will deploy using these settings." The "Add Servers" button is visible in the top right.
- NTP Server Settings:** The "NTP Server" section is active. The "NTP" checkbox is selected. The "Primary" section shows "64.102.6.247" as the Primary NTP address and "173.37.137.85" as the Secondary NTP address. The "Additional NTP" section shows "10.81.254.131" as the Additional NTP address.
- Time Zone:** The "Time Zone" section shows "US/Eastern (UTC)" as the selected time zone.
- Message of the day:** The "Message of the day" section shows a message: "Welcome to C9200L-1 - From Branch-AAA - Provisioned by DNAC".

Adding a switch to DNA Center – Provision

DEVICES (1)
FOCUS: **Inventory** ▾

Filter | + Add Device | Tag Device | Actions ▾ ① | Take a Tour | 1 Selected | Last updated: 10:37 AM | Export | Refresh

Device Name	IP	Manageability	Compliance	Health Score	Site	Last Updated	Platform	Support
<input checked="" type="checkbox"/> TBRANCH-C9200-1.cisco.com	10...	<input checked="" type="checkbox"/> Managed	<input checked="" type="checkbox"/> Compliant	8	.../Toronto/BRANCH-AAA	2 hours ago	C9200L-24T-4G	Supported

Actions menu options:

- Inventory
- Software Image
- Provision (highlighted)
 - Assign Device to Site
 - Provision Device (highlighted)
 - LAN Automation
 - LAN Automation Status
 - Learn Device Config
 - Configure WLC HA
- Telemetry
- Device Replacement
- Others
- Compliance

Adding a switch to DNA Center – Provision

1 Assign Site

2 Advanced Configuration

3 Summary

TBRANCH-C9200-1.cisco.com

Device Details

Device Name: TBRANCH-C9200-1.cisco.com

Platform Id: C9200L-24T-4G

Device IP: 10.85.54.23

Device Location: Global/Canada/Ontario/Toronto/BRANCH-AAA

Network Settings

NTP Server: 10.81.254.131 , 10.81.254.202

AAA Network ISE Server: 10.85.54.185

AAA Network Primary Server: 10.85.54.185

WARNING: Do not use "admin" as the username for your device CLI credentials, if you are using ISE as your AAA server. If you do, this can result in you not being able to login to your devices.

DHCP Server: 10.85.48.7

DNS Domain Name: cisco.com

DNS Primary Server: 64.102.6.247

DNS Secondary Server: 173.37.137.85

Syslog Server: Cisco DNA Center

Netflow Collector: Cisco DNA Center

SNMP Trap Receiver: Cisco DNA Center, 10.10.10.10

Syslog Level: 6 - Information Messages

Cisco TrustSec (CTS) Credentials: Yes

Controller Certificates: Yes

Advanced Configuration

Template Name: PDESCRIPTION,VLAN419

Cancel

Deploy

Adding a switch to DNA Center – Provision

Inventory > Provision Devices

1 Assign Site 2 Advanced Configuration 3 Summary

TBRANCH-C9200-
1.cisco.com

Device Details

Device Name:

TBRANCH-C9200-1.cisco.com

Cisco DNA Center

Activity - Work Items

PROVISION

Provision Device - Configuration preview

Feb 5, 2021 10:10 AM | Status: Success | Last updated: 10:11:30 AM | Refresh

DEVICES
10.85.54.23

Configuration Preview

Device Name : TBRANCH-C9200-1

```
ntp server 10.81.254.202
ntp server 10.81.254.131
ip domain lookup
ip name-server 64.102.6.247
ip name-server 173.37.137.85
ip domain name cisco.com
service password-encryption
interface GigabitEthernet1/0/15
switchport access vlan 419
switchport mode access
interface GigabitEthernet1/0/16
switchport access vlan 419
switchport mode access

interface GigabitEthernet1/0/15
description Description pushed by DNAC Template -- lan
interface GigabitEthernet1/0/16
description Description pushed by DNAC Template -- lan

alias exec showntp show ntp status
```

EXIT Deploy

Provision Device

☐ Now

☐ Later

☒ Generate configuration preview

Creates preview which can be later used to deploy on selected devices. If Site assignment is invoked during configuration preview, Device controllability configuration will be pushed to corresponding device(s).

Task Name*

Provision Device - Configuration preview

Cancel

Apply

CISCO Live!

#CiscoLive

BRKEMT-2003

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

29

Adding a switch to DNA Center – Provision

Part 1

C9200L-24T-4G
IOS-XE: 17.03.01

```
!  
aaa new-model  
!  
!  
aaa group server radius dnac-network-radius-group  
  server name dnac-radius_10.85.54.185  
  ip radius source-interface Loopback0  
!  
aaa authentication login default local  
aaa authentication login VTY_authen group dnac-network-  
radius-group local  
aaa authorization exec default local  
aaa authorization exec VTY_author group dnac-network-  
radius-group local if-authenticated  
aaa accounting update newinfo periodic 2880  
aaa accounting exec default start-stop group dnac-network-  
radius-group  
!  
!  
!  
aaa session-id common
```

```
<snip>  
!  
ip radius source-interface Loopback0  
!  
radius-server attribute 6 on-for-login-auth  
radius-server attribute 6 support-multiple  
radius-server attribute 8 include-in-access-req  
radius-server attribute 25 access-request include  
radius-server attribute 31 mac format ietf upper-case  
radius-server attribute 31 send nas-port-detail mac-only  
radius-server dead-criteria time 5 tries 3  
radius-server deadtime 3  
!  
radius server dnac-radius_10.85.54.185  
  address ipv4 10.85.54.185 auth-port 1812 acct-port 1813  
  timeout 2  
  retransmit 1  
  pac key 7 123A54041104282A0B6A  
!
```

Adding a switch to DNA Center – Provision

Part 2

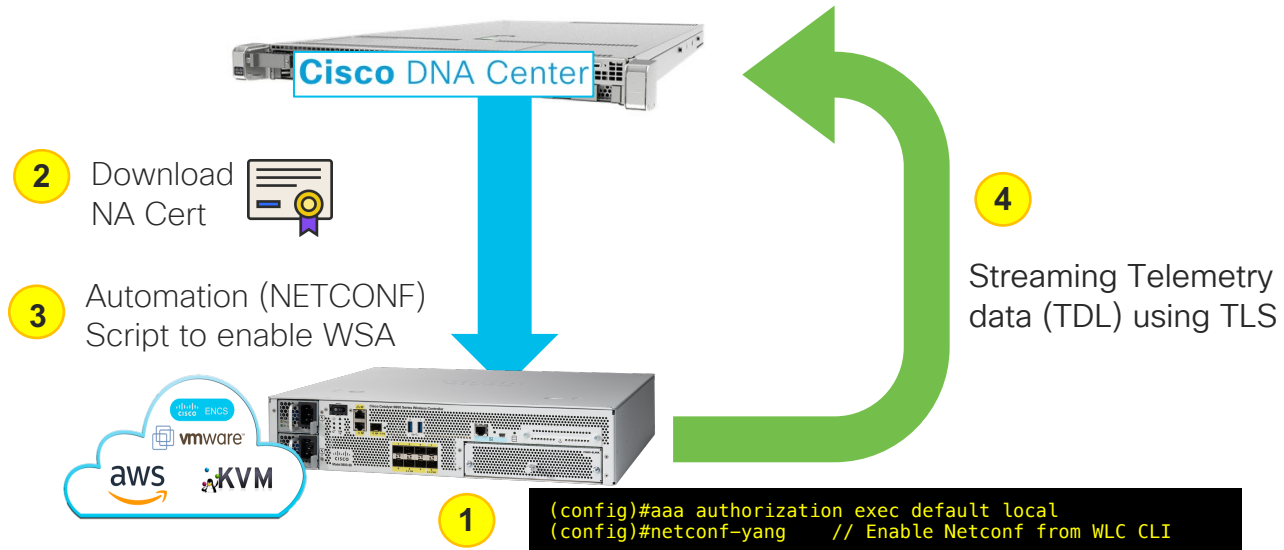
C9200L-24T-4G
IOS-XE: 17.03.01

```
!  
ip name-server 64.102.6.247 173.37.137.85  
ip domain name cisco.com  
!  
access-session mac-move deny  
!  
<snip>  
!  
interface GigabitEthernet1/0/15  
  description Description pushed by DNAC Template -- lan  
  switchport access vlan 419  
  switchport mode access  
  device-tracking attach-policy IPDT_POLICY  
!  
interface GigabitEthernet1/0/16  
  description Description pushed by DNAC Template -- lan  
  switchport access vlan 419  
  switchport mode access  
  device-tracking attach-policy IPDT_POLICY  
!
```

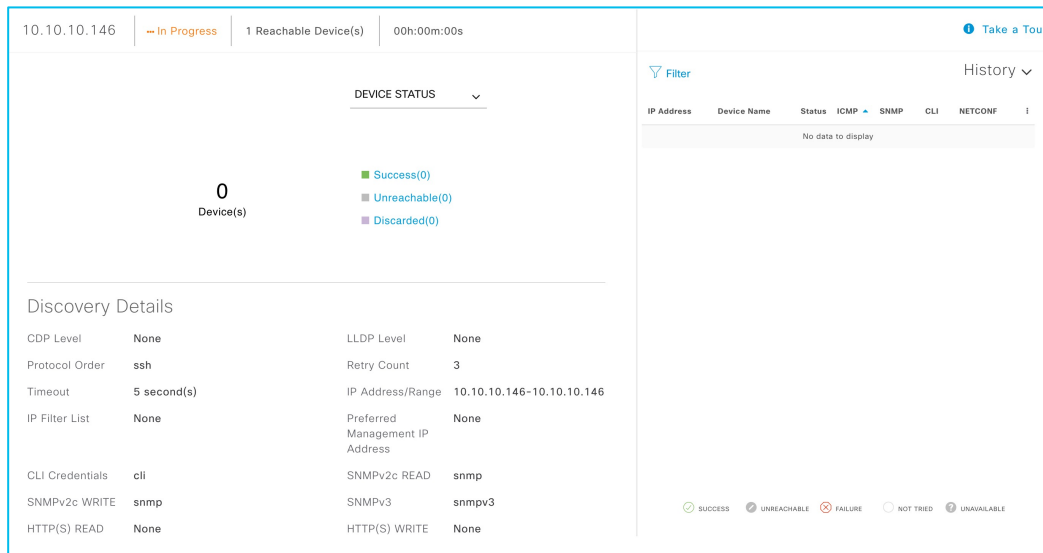
```
!  
<snip>  
!  
banner motd ^C***** Welcome to TBRANCH-AAA  
device managed by Cisco DNAC ***** ^C  
!  
<snip>  
alias exec showntp show nto status  
!  
!  
<snip>  
ntp server 10.81.254.202  
ntp server 10.81.254.131
```

What happens when an IOS-XE C9800 WLC is added to Cisco DNA Center?

- Cisco DNAC pushes automated scripts to enable telemetry
 - Prerequisite – Enable Netconf-yang from Cat9800 CLI
 - Install DNAC Certificate for https setup with Cisco DNAC
 - Configure and Enable streaming telemetry (TDL) using NETCONF to Cisco DNAC



Adding a C9800 WLC to DNA Center – Discovery



```
Feb 10 05:28:22.900: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: sdn] [Source: 10.10.10.144] [localport: 22] at 05:28:22 UTC Wed Feb 10 2021
Feb 10 05:28:23.964: %SYS-6-LOGOUT: User sdn has exited tty session 2(10.10.10.144)
Feb 10 05:28:24.083: %DMI-5-AUTH_PASSED: Chassis 2 R0/0: dmiauthd: User 'sdn' authenticated successfully from 10.10.10.144:45765 and was authorized
for netconf over ssh. External groups: PRIV15
Feb 10 05:28:34.106: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: sdn] [Source: 10.10.10.144] [localport: 22] at 05:28:34 UTC Wed Feb 10 2021
Feb 10 05:28:34.151: %SYS-6-LOGOUT: User sdn has exited tty session 2(10.10.10.144)
Feb 10 05:28:34.754: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: sdn] [Source: 10.10.10.144] [localport: 22] at 05:28:34 UTC Wed Feb 10 2021
```

Adding a C9800 WLC to DNA Center – Discovery

Inventory Plug and Play

Find Hierarchy

Global

Unassigned Devices (3)

AUS

Branch

DC

gastiez

MH

Global > Unassigned Devices

DEVICES (2)
FOCUS: Inventory

Filter | Add Device | Tag Device | Actions | Take a Tour

Last updated: 4:32 PM | Export | Refresh

	Device Name	IP Address	Device Family	Reachability	Manageability	Compliance	Health Score	Site	MAC Address	
<input type="checkbox"/>	3850-remote	10.10.6.2	Switches and Hubs	Reachable	Managed	Non-Compliant	10	Assign	7c:95:f3:bd:2b:00	
<input type="checkbox"/>	reallylongName2.adamlab.cisco.com	10.10.10.146	Wireless Controller	Reachable	Managed	Compliant	10	Assign	00:0c:29:bc:2f:b1	

Adding a C9800 WLC to DNA Center - Discovery

Cisco DNA Center

Version 2.2.1.0

[Release Notes](#)

[> Packages](#)

C9800-CL
IOS-XE: 17.04.01

```
! If snmp is not configured
snmp-server user adam default v3 auth sha xxxxx
snmp-server group default v3 auth
```

```
! This will be pushed
netconf-yang ssh port 830
netconf-yang
```

```
! Save changes
write memory
```

Adding a C9800 WLC to DNA Center – Assign to Site

Inventory

Plug and Play

Find Hierarchy

Global

Unassigned Devices (2)

AUS

Branch

DC

gastiez

MH

NZ2

OS

SYD

DEVICES (2)

FOCUS: Inventory

Filter

Add Device

Tag Device

Actions

Take a T

Device Name

IP Address

Device

3850-remote 10.10.6.2 Switch

reallylongName2.adamlab.cisco.com 10.10.10.146 Wirele

Choose a site

Find Hierarchy

GUS1

HK1 (1)

23

KOG-1 (1)

F1

PEN-1 (1)

PEN1

WOL-1 (1)

F1

DC (1)

RDC

gastiez

MH (1)

Cancel

Save

Adding a C9800 WLC to DNA Center – Assign to Site – Part 1

C9800-CL
IOS-XE: 17.04.01

! syslog

```
logging host 10.10.10.144 transport udp port 514
logging trap 6
logging source-interface GigabitEthernet2
logging on
```

! snmp (v3 now supported)

```
snmp-server host 10.10.10.144 traps version 3 auth adam udp-
port 162
trapflags ap register
trapflags ap interfaceup
snmp-server enable traps wireless AP wireless_mobility
snmp-server enable traps rf
snmp-server enable traps config
snmp-server source-interface traps GigabitEthernet2
```

! cts

```
cts credentials id 9P015USKRB8 password 9P015USKRB8
```

! Netflow export

```
flow exporter 10.10.10.144
destination 10.10.10.144
transport udp 6007
```

! DNS

```
ip domain name adamlab.cisco.com
ip name-server 10.10.10.151
```

! DNAC PKI

```
no crypto pki trustpoint DNAC-CA
crypto key zeroize rsa DNAC-CA
```

! Correct source interface

```
ip http client source-interface
GigabitEthernet2
ip ssh source-interface GigabitEthernet2
ip ssh version 2
ip domain lookup
```

```
crypto pki trustpoint DNAC-CA
enrollment mode ra
enrollment terminal
usage ssl-client
revocation-check crl none
crypto pki authenticate DNAC-CA
```

Adding a C9800 WLC to DNA Center – Assign to Site – Part 2

! Add Device Certificate

```
crypto pki import sdn-network-infra-iwan pkcs12 http://10.10.10.144/api/v1/trust-point/pkcs12/xx/xx password xxx
```

```
crypto pki trustpoint sdn-network-infra-iwan
auto-enroll 80 regenerate
enrollment url http://10.10.10.144:80/ejbca/publicweb/apply/scep/sdnscep
fqdn reallylongName2.adamlab.cisco.com
revocation-check crl
source interface GigabitEthernet2
rsa-keypair sdn-network-infra-iwan
subject-name CN=C9800-CL-K9_9P015USKRB8_sdn-network-infra-iwan
```

C9800-CL
IOS-XE: 17.04.01

! Example telemetry subscription

```
telemetry ietf subscription 9993
encoding encode-tdl
filter tdl-uri /services;serviceName=ewlc_oper/awips_alarm
receiver-type protocol
source-address 10.10.10.146
stream native
update-policy on-change
receiver name DNAC_ASSURANCE_RECEIVER
```

```
! The telemetry connection to DNAC
telemetry receiver protocol DNAC_ASSURANCE_RECEIVER
host ip-address 10.10.10.144 25103
protocol tls-native profile sdn-network-infra-iwan
```

Adding a C9800 WLC to DNA Center – Assign to Site – Part 3

C9800-CL
IOS-XE: 17.04.01

```
filter tdl-uri /services;serviceName=ewlc/wlan_config
filter tdl-uri /services;serviceName=ewlc/wlanpolicies
filter tdl-uri /services;serviceName=ewlc/wlanpolicies;policy_profile_name=temp_policy_profile/atfpolicymap
filter nested-uri /services;serviceName=ewlc/policylist
filter tdl-uri /services;serviceName=ewlc/site_tag_config
filter tdl-uri /services;serviceName=ewlc/wlan_config
filter tdl-uri /services;serviceName=ewlc/wlanpolicies
filter tdl-uri /services;serviceName=ewlc/wlanpolicies;policy_profile_name=temp_policy_profile/atfpolicymap
filter nested-uri /services;serviceName=ewlc/policylist
filter tdl-uri /services;serviceName=ewlc/site_tag_config
filter tdl-uri /services;serviceName=ewlcevent/wsaapevent
filter tdl-uri /services;serviceName=ewlc_oper/ethernet_mac_wtp_mac_map
filter tdl-uri /services;serviceName=ewlc_oper/oper_data
filter tdl-uri /services;serviceName=ewlc_oper/capwap_data
filter tdl-uri /services;serviceName=ewlc_oper/radio_oper_data
filter tdl-uri /services;serviceName=ewlc_oper/capwap_data
filter tdl-uri /services;serviceName=ewlc_oper/spectrum_aq_table
filter tdl-uri /services;serviceName=ewlc_oper/ethernet_if_stats
filter tdl-uri /services;serviceName=ewlc_oper/rrmAPautoRfdot11Data
filter tdl-uri /services;serviceName=ewlc_oper_emul/emltdApRf
filter tdl-transform dfsRadarCounters
filter tdl-uri /services;serviceName=ewlc_oper/radio_oper_data
filter tdl-uri /services;serviceName=ewlc_oper/common_oper_data
filter tdl-uri /services;serviceName=ewlc_oper/dot11_oper_data
filter tdl-uri /services;serviceName=ewlc_oper/smMainData
filter tdl-uri /services;serviceName=ewlc_oper/lisp_agent_client_data
filter tdl-uri /services;serviceName=ewlc_oper/mobility_oper_data
filter tdl-uri /services;serviceName=ewlc_oper/sisf_db_mac
filter tdl-uri /services;serviceName=ewlc_oper/traffic_stats
filter tdl-uri /services;serviceName=ewlc_oper/client_wsa_info
filter tdl-uri /services;serviceName=ewlc_oper/location_rssi_measurements
```

Adding a C9800 WLC to DNA Center – Assign to Site – Part 4

c9800
IOS-XE: 17.04.01

```
filter tdl-uri /services;serviceName=ewlcevent/wsclientscanreportevent
filter tdl-uri /services;serviceName=ewlcevent/wsclientevent
filter tdl-uri /services;serviceName=ewlc_oper/dc_info
filter tdl-uri /services;serviceName=ewlc_oper/dc_info
filter tdl-uri /services;serviceName=ewlc_oper/policy_data
filter tdl-uri /services;serviceName=ewlc_oper/policy_data
filter tdl-uri /services;serviceName=ewlc_oper/traffic_distribution_airtime_latency
filter tdl-uri /services;serviceName=ios_emul_oper/device_hardware;singleton_id=0?device_system_data
filter tdl-uri /services;serviceName=ios_oper/ha_infra
filter tdl-uri /services;serviceName=ios_emul_oper/device_hardware;singleton_id=0/device_inventory
filter tdl-uri /services;serviceName=ios_emul_oper/smart_license_state;singleton_id=0/smart_license_usage
filter tdl-uri /services;serviceName=ios_oper/ha_infra
filter nested-uri /services;serviceName=sman_oper/control_process;fru=BINOS_FRU_RP;slotnum=0;baynum=0;chassisnum=1?plat_core_stats
filter tdl-uri /services;serviceName=ios_emul_oper/entity_information
filter nested-uri /services;serviceName=ios_oper/platform_component;cname="\Slot\"?platform_properties
filter tdl-uri /services;serviceName=ios_oper/platform_component
filter tdl-uri /services;serviceName=ios_emul_oper/interface
filter tdl-uri /services;serviceName=sman_oper/control_process
filter tdl-uri /services;serviceName=ewlc_oper_emul/ewlcEmLtdClientGlobalStatsData;singleton_id=0
filter tdl-uri /services;serviceName=ewlc_oper_emul/emltd_join_count_stat;singleton_id=0
filter tdl-uri /services;serviceName=ewlc_oper/lisp_agent_ms_msg_stats_data
filter tdl-uri /services;serviceName=ewlc/dot11
filter tdl-uri /services;serviceName=ewlc_oper/radioWsaInfo
filter tdl-uri /services;serviceName=ewlc_oper/radio_reset_stats
filter tdl-uri /services;serviceName=ewlc_oper/traffic_stats
filter tdl-uri /services;serviceName=ewlc_oper/rrmRadSlot
filter tdl-uri /services;serviceName=ewlc_oper/radio_oper_stats
filter tdl-uri /services;serviceName=ewlc_oper/icapApSrcvStats
filter tdl-uri /services;serviceName=rogue_oper/rogue_client_data
filter tdl-uri /services;serviceName=rogue_oper/rogue_data
filter tdl-uri /services;serviceName=ewlc_oper/awips_alarm
```

Adding a C9800 WLC to DNA Center – Telemetry

Inventory Plug and Play

Find Hierarchy

Global > DC > RDC

DEVICES (1)
FOCUS: **Inventory**

Filter | Add Device | Tag Device | Actions ① | Take a Tour | 1 Selected | Last updated: 10:01 AM | Export | Refresh

Device Name	Family	Reachability	Manageability	Compliance	Health Score	Site	MAC Address
reallylongName2.adamlab.cisco.com	s Controller	Reachable	Managed	Compliant	10	.../DC/RDC	00:0c:29:bc:2f:b1

Inventory

Software Image

Provision

Telemetry

Device Replacement

Others

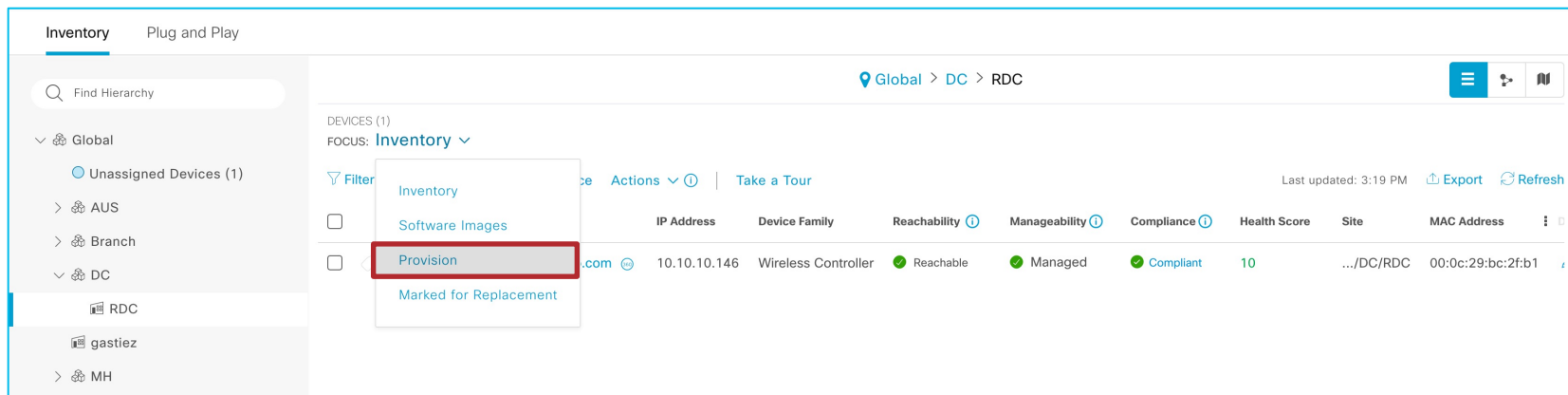
Compliance

Enable Application Telemetry

Disable Application Telemetry

Update Telemetry Settings

Nothing happened? Why did it fail?



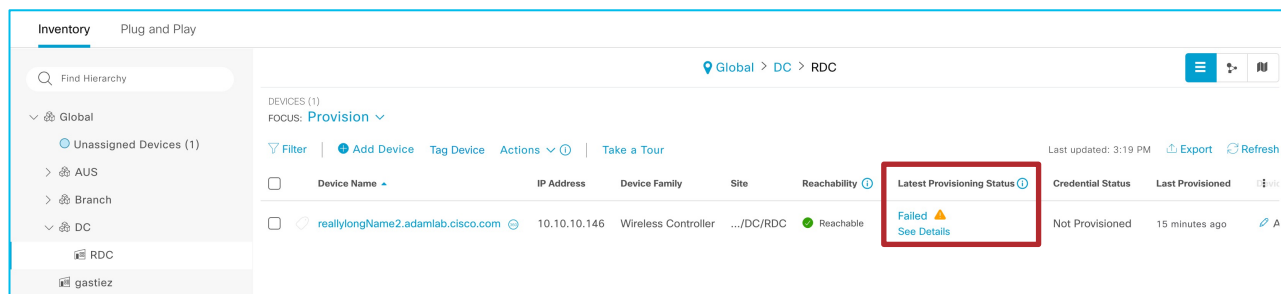
The screenshot shows the Cisco DNA Center 'Inventory' page. The breadcrumb navigation is 'Global > DC > RDC'. The left sidebar shows a hierarchy: Global > Unassigned Devices (1) > AUS > Branch > DC > RDC (selected). The main content area shows a table of devices. A dropdown menu is open over the 'Provision' button for the first device, showing options: 'Inventory', 'Software Images', 'Provision' (highlighted with a red box), and 'Marked for Replacement'.

DEVICES (1)
FOCUS: Inventory

Filter | Add Device | Tag Device | Actions | Take a Tour

Last updated: 3:19 PM | Export | Refresh

	IP Address	Device Family	Reachability	Manageability	Compliance	Health Score	Site	MAC Address
<input type="checkbox"/>	10.10.10.146	Wireless Controller	Reachable	Managed	Compliant	10	.../DC/RDC	00:0c:29:bc:2f:b1



The screenshot shows the same Cisco DNA Center 'Inventory' page, but now the 'Provision' action has been performed. The dropdown menu for the first device is open, showing 'Latest Provisioning Status' (highlighted with a red box) with a status of 'Failed' (indicated by a red triangle icon) and a link to 'See Details'. The table shows the device is 'Not Provisioned' and '15 minutes ago'.

DEVICES (1)
FOCUS: Provision

Filter | Add Device | Tag Device | Actions | Take a Tour

Last updated: 3:19 PM | Export | Refresh

Device Name	IP Address	Device Family	Site	Reachability	Latest Provisioning Status	Credential Status	Last Provisioned
reallylongName2.adamlab.cisco.com	10.10.10.146	Wireless Controller	.../DC/RDC	Reachable	Failed See Details	Not Provisioned	15 minutes ago

Why did it fail?

reallylongName2.adamlab.cisco.com

Management IP 10.10.10.146
Device Type Cisco Catalyst 9800-CL Wireless Controller for Cloud
Device Role ACCESS

App Name Device Controllability and Telemetry
Configured At Feb 11, 2021 3:04 PM

Failed

[See Details](#)

reallylongName2.adamlab.cisco.com

Management IP 10.10.10.146
Device Type Cisco Catalyst 9800-CL Wireless Controller for Cloud
Device Role ACCESS

- Configuration or syslog setting is only applicable upon assign device to site, provision, retry upon failure, or force push, so no operation was performed

Deployment of snmp setting SUCCESS

- Configuration of snmp setting is only applicable upon assign device to site, provision, retry upon failure, or force push, so no operation was performed

Deployment of dns setting SUCCESS

- Configuration of dns setting is only applicable upon assign device to site, provision, retry upon failure, or force push, so no operation was performed

Deployment of netflow setting SUCCESS

- Configuration of netflow setting is only applicable upon assign device to site, provision, retry upon failure, or force push, so no operation was performed

Application telemetry FAILED

- No Telemetry-applicable WLANs found!

[Retry](#)

Solution:
Configure a local mode SSID

Adding a C9800 WLC to DNA Center – Telemetry

C9800-CL
IOS-XE: 17.04.01

```
flow exporter avc_exporter
 destination 10.10.10.144
 source GigabitEthernet2
 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
 default cache entries
 record wireless avc ipv4 assurance
```

```
!
flow monitor avc_ipv4_assurance_rtp
 exporter avc_exporter
 cache timeout active 60
 default cache entries
 record wireless avc ipv4 assurance-rtp

! Apply to SSID (local mode only)
wireless profile policy temp_Global_NF_19d2325f
 shutdown
 ipv4 flow monitor avc_ipv4_assurance input
 ipv4 flow monitor avc_ipv4_assurance output
 ipv4 flow monitor avc_ipv4_assurance_rtp input
 ipv4 flow monitor avc_ipv4_assurance_rtp output
 no shutdown
```

Deleting a C9800 WLC from Inventory – clean up

The screenshot shows the Cisco DNA Center interface. The top navigation bar includes 'Cisco DNA Center', 'Provision', 'Network Devices', and 'Inventory'. A 'Preview Devices 2.0' toggle is visible. The left sidebar shows a hierarchy: 'Global' > 'Unassigned Devices (1)' > 'AUS' > 'Branch' > 'DC' > 'RDC' > 'gastiez' > 'MH' > 'NZ2' > 'OS' > 'SYD'. The main content area shows a list of devices under 'DEVICES (1)' with 'FOCUS: Inventory'. A table lists devices with columns for 'Device Name', 'Compliance', 'Health Score', 'Site', and 'MAC Address'. One device, 'reallylongName2.ad', is selected. A warning dialog is open in the center, asking for confirmation to delete the selected devices. The dialog includes a warning icon, the title 'Warning', and the question 'Are you sure you want to delete the selected devices?'. It explains that ISE entries will not be removed and offers a 'Configuration Clean-Up' option. The dialog has 'Cancel' and 'OK' buttons.

Warning

Are you sure you want to delete the selected devices?

The ISE entry corresponding to the devices will not be removed by Cisco DNA Center. It needs to be removed from ISE console explicitly.

☒ **Configuration Clean-Up**

Selecting cleanup option will attempt to remove the device settings from the device(s). This includes, but is not limited to Network Settings like Netflow destination, AAA settings, Trap settings and the configuration deployed using Cisco DNA Center. Only after a successful cleanup, Cisco DNA Center will proceed with deleting the device(s). On failure to cleanup, the device(s) will not be removed.

Uncheck this option to proceed with device delete without attempting any cleanup.

Deleting a C9800 WLC from Inventory – clean up

```
no radius-server attribute 6 on-for-login-auth
no radius-server attribute 6 support-multiple
no radius-server attribute 8 include-in-access-req no
radius-server attribute 25 access-request include
no radius server dnac-radius 10.10.10.130
no aaa session-id common
no aaa server radius dynamic-author
no aaa group server radius dnac-client-radius-group
no aaa group server radius dnac-network-radius-group
no aaa group server radius dnac-rGrp-branch-ecec6c61
no aaa group server radius dnac-rGrp-temp-0cf30cee
no aaa group server radius dnac-rGrp-temp-eacb6bcb
no aaa authorization exec VTY_author
no aaa authorization exec default
no aaa authorization network default
no aaa authorization network dnac-cts-branch-ecec6c61
no aaa authorization network dnac-cts-list
no aaa authorization network dnac-cts-temp-0cf30cee
no aaa authorization network dnac-cts-temp-eacb6bcb
no aaa authentication dot1x dnac-cts-branch-ecec6c61
no aaa authentication dot1x dnac-cts-temp-0cf30cee
no aaa authentication dot1x dnac-cts-temp-eacb6bcb
no aaa authentication dot1x default
no aaa authentication login default
no aaa authentication login VTY_authen
no aaa authentication login dnac-cts-branch-ecec6c61
no aaa authentication login dnac-cts-list
no aaa authentication login dnac-cts-temp-0cf30cee
no aaa authentication login dnac-cts-temp-eacb6bcb
no aaa accounting identity default
no aaa accounting exec default
no aaa accounting update
```

```
no radius-server deadtime 3
no radius-server dead-criteria time 5 tries 3
no aaa new-model
```

```
! Remove DNAC trustpoint
no crypto pki trustpoint DNAC-CA
crypto key zeroize rsa DNAC-CA
```

```
! Remove DNS
no ip domain name
no ip name-server 10.10.10.151
```

```
! Remove SNMP
no snmp-server host 10.10.10.144 traps adam
no trapflags ap interfaceup
no trapflags ap register
no snmp-server enable traps wireless AP wireless_mobility
no snmp-server enable traps rf
no snmp-server enable traps config
no snmp-server source-interface traps
```

```
no flow exporter 10.10.10.144
```

```
! Remove syslog
no logging host 10.10.10.144 transport udp port 514
no logging trap
no logging source-interface GigabitEthernet2
```

```
! Remove Device Certificate
no crypto pki trustpoint sdn-network-infra-iwan
crypto key zeroize rsa sdn-network-infra-iwan
configure terminal lock
no device classifier
```

Difference between “Managed” vs “Provisioned”

Inventory

Plug and Play

Find Hierarchy

Global

Unassigned Devices (4)

APJC

Canada

Alberta

British Columbia

Ontario

Toronto

BRANCH-AAA

RoLlo-Home

TBRANCH

Floor1

TRN6

vBRANCH-ENFV

DEVICES (10)

FOCUS: Inventory

Filter

Add Device

Tag Device

Actions

Take a Tour

... > Ontario > Toronto > TBRANCH

Last updated: 7:26 PM

Export

Refresh

Device Name	IP Address	Reachability	Manageability	Site	Last Updated	Provision Status
C9K-STACK.cisco.com	10.85.54.54	Reachable	Managed	.../Toronto/TBRANCH	5 minutes ago	Success See Details
TBranch_NonFabric_AP1	10.85.54.26	Unreachable	Managed	.../TBRANCH/Floor1	3 hours ago	Success See Details
TBranch_NonFabric_AP2	10.85.54.27	Unreachable	Managed	.../TBRANCH/Floor1	3 hours ago	Success See Details
TBRANCH-C9200-1.cisco.com	10.85.54.23	Reachable	Managed	.../Toronto/TBRANCH	2 hours ago	Success See Details
TBRANCH-C9200L-2.cisco.com	10.85.54.24	Reachable	Managed	.../Toronto/TBRANCH	3 hours ago	Success See Details Out of Sync
TBRANCH-C9200L-3.cisco.com	10.85.54.25	Reachable	Managed	.../Toronto/TBRANCH	3 hours ago	Success See Details Out of Sync
TBRANCH-C9200L-4.cisco.com	10.85.54.26	Reachable	Managed	.../Toronto/TBRANCH	3 hours ago	Failed

Difference between “Managed” vs “Provisioned”

The screenshot displays the Cisco DNA Center interface, specifically the 'Inventory' section under 'Provision - Network Devices'. The left sidebar shows a hierarchical tree of devices, with 'TBRANCH' selected. The main content area shows details for 'TBRANCH-C9200-1.cisco.com'. The device is a Cisco Catalyst 9200L Switch Stack with Management IP 10.85.54.23 and Role ACCESS. Three configuration entries are listed, each with a 'Success' status and a 'See Details' link. The first two entries are for 'Device Controllability and Telemetry' and the third is for 'Device Provisioning, Template Provisioning'. The first two entries are highlighted with red boxes.

Inventory Plug and Play

Find Hierarchy

- Global
 - Unassigned Devices (4)
- APJC
- Canada
 - Alberta
 - British Columbia
 - Ontario
 - Toronto
 - BRANCH-AAA
 - RoLlo-Home
 - TBRANCH
 - Floor1
 - TRN6
 - vBRANCH-ENFV
 - Quebec
 - Saskatchewan

TBRANCH-C9200-1.cisco.com

Management IP 10.85.54.23
Device Type Cisco Catalyst 9200L Switch Stack
Device Role ACCESS

App Name	Device Controllability and Telemetry	Success ✓
Configured At	Feb 5, 2021 5:43 PM	See Details

App Name	Device Controllability and Telemetry	Success ✓
Configured At	Feb 5, 2021 5:42 PM	See Details

App Name	Device Provisioning, Template Provisioning	Success ✓
Configured At	Feb 5, 2021 5:42 PM	
Description	Provision Device	See Details

Change in Network Settings

```
TBRANCH-C9200-1#show run | i aaa  
no aaa new-model
```

Adding AAA server

Network

Servers: ☒ ISE ☐ AAA

Protocol: ☒ RADIUS ☐ TACACS

Network: 10.85.54.185

DHCP Server: 10.85.48.7

Success: Settings saved successfully!

Find Hierarchy

- Global
 - APJC
- Canada
 - Alberta
 - British Columbia
 - Ontario
 - Toronto
 - BRANCH-AAA

DHCP Server

DHCP: 10.85.48.7

DNS Server

Domain Name: cisco.com

Primary: 64.102.6.247

Secondary: 173.37.137.85

NTP Server

NTP: 10.81.254.131

Additional NTP: 10.81.254.202

```
TBRANCH-C9200-1#show run | i aaa  
no aaa new-model
```

DEVICES (4)

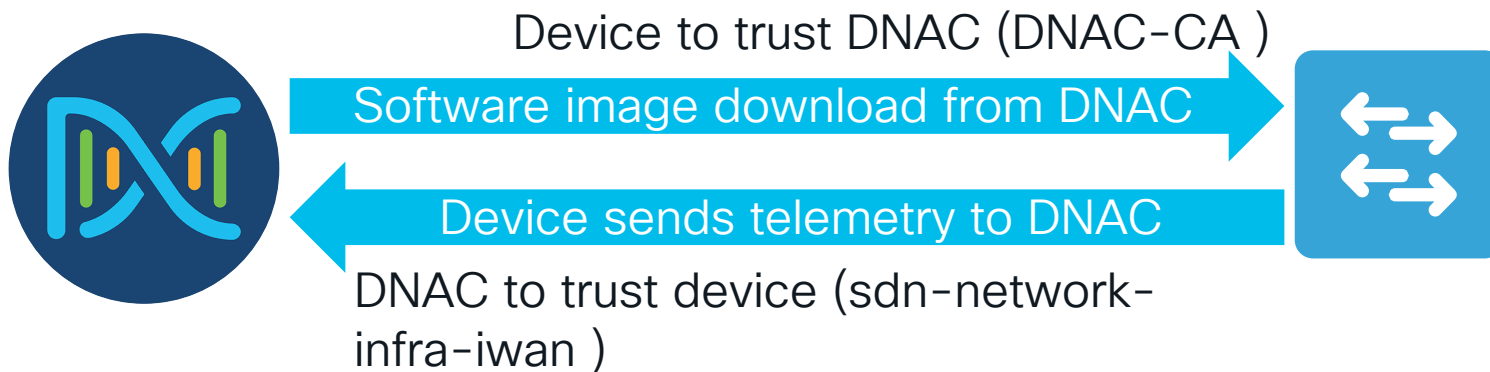
FOCUS: Provision

Device Name	IP Address	Site	Reachability	Provision Status	Credential Status
TBRANCH-C9200-1.cisco.com	10.85.54.23	.../Toronto/BRANCH-AAA	Reachable	Success	Success

Netconf and Certificates



Certificates



2.2.1.0: FQDN only supported – no more SAN IP address

Netconf

Netconf config pushed during discovery. Port 830 is default

Netconf used to configure other settings on 9800 WLC

Netconf used to configure streaming telemetry

Need to be aware of AAA requirements for netconf

```
aaa authorization exec default
```

What happens
when we change
user credentials



Credentials can only be added/changed at global level

Top Screenshot: Global Level

Find Hierarchy

- Global
- APJC
- Canada
 - Alberta
 - British Columbia
- Ontario
 - Toronto

BRANCH-AAA

CLI Credentials

[+ Add](#)

	Name / Description	Username	Password	Enable Password	Actions
<input type="radio"/>	netadmin	netadmin	*****	*****	Edit Delete
<input type="radio"/>	admin	admin	*****	*****	Edit Delete
<input type="radio"/>	Lila	lila	*****	*****	Edit Delete
<input type="radio"/>	NFVIS netadmin	netadmin	*****	*****	Edit Delete

Bottom Screenshot: BRANCH-AAA Level

Find Hierarchy

- Global
- APJC
- Canada
 - Alberta
 - British Columbia
- Ontario
 - Toronto

BRANCH-AAA

CLI Credentials

	Name / Description	Username	Password	Enable Password
<input type="radio"/>	netadmin	netadmin	*****	*****
<input type="radio"/>	admin	admin	*****	*****
<input type="radio"/>	Lila	lila	*****	*****
<input type="radio"/>	NFVIS netadmin	netadmin	*****	*****
<input checked="" type="radio"/>	francis	francis	*****	*****

Changing a local username

Find Hierarchy

Global

APJC

Canada

Alberta

British Columbia

Ontario

Toronto

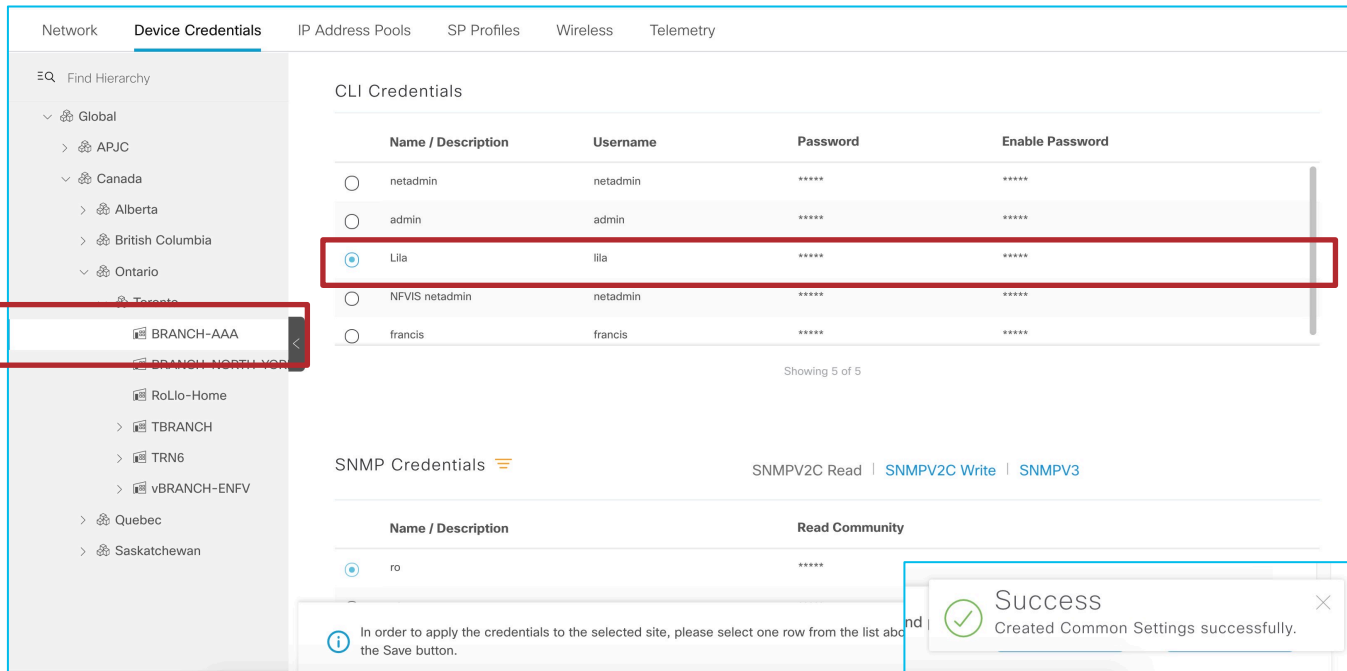
BRANCH-AAA

CLI Credentials

	Name / Description	Username	Password	Enable Password
<input checked="" type="radio"/>	netadmin	netadmin	*****	*****
<input type="radio"/>	admin	admin	*****	*****
<input type="radio"/>	Lila	lila	*****	*****
<input type="radio"/>	NFVIS netadmin	netadmin	*****	*****
<input type="radio"/>	francis	francis	*****	*****

```
TBRANCH-C9200-1#show run | i username
username netadmin privilege 15 password 7 112A4816141D2F22256B
```

Changing a local username



Network **Device Credentials** IP Address Pools SP Profiles Wireless Telemetry

Find Hierarchy

- Global
 - APJC
 - Canada
 - Alberta
 - British Columbia
 - Ontario
 - Toronto
 - BRANCH-AAA**
 - BRANCH-NORTH YORK
 - RoLio-Home
 - TBRANCH
 - TRN6
 - vBRANCH-ENFV
 - Quebec
 - Saskatchewan

CLI Credentials

	Name / Description	Username	Password	Enable Password
<input type="radio"/>	netadmin	netadmin	*****	*****
<input type="radio"/>	admin	admin	*****	*****
<input checked="" type="radio"/>	Lila	lila	*****	*****
<input type="radio"/>	NFVIS netadmin	netadmin	*****	*****
<input type="radio"/>	francis	francis	*****	*****

Showing 5 of 5

SNMP Credentials

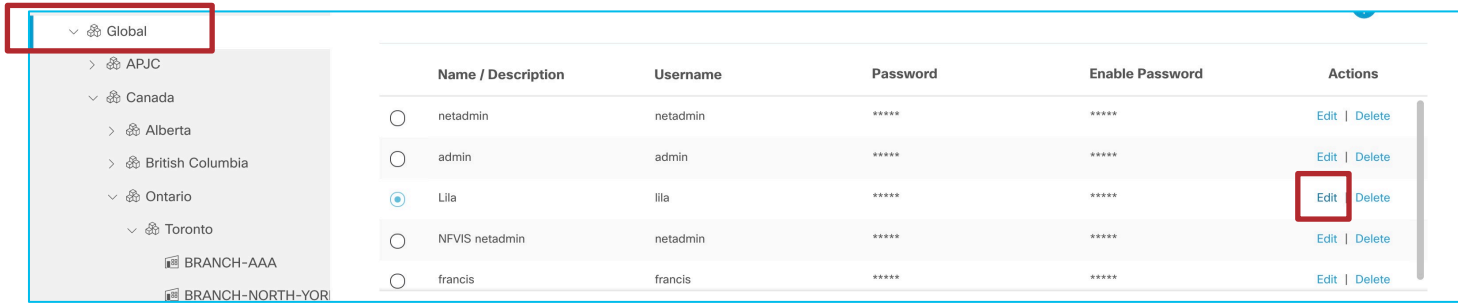
Name / Description	Read Community
<input checked="" type="radio"/> ro	*****

Success
Created Common Settings successfully.

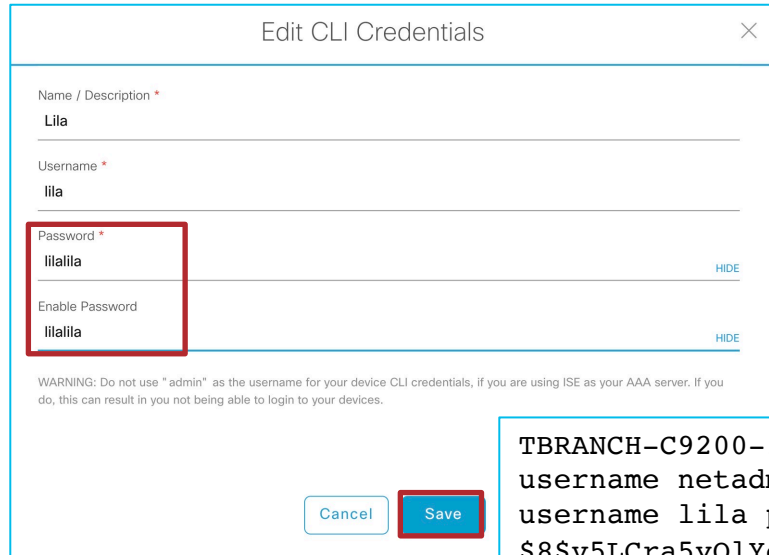
In order to apply the credentials to the selected site, please select one row from the list above and click the Save button.

```
TBRANCH-C9200-1#show run | i username  
username netadmin privilege 15 password 7 112A4816141D2F22256B
```

Changing a local username



	Name / Description	Username	Password	Enable Password	Actions
<input type="radio"/>	netadmin	netadmin	*****	*****	Edit Delete
<input type="radio"/>	admin	admin	*****	*****	Edit Delete
<input checked="" type="radio"/>	Lila	lila	*****	*****	Edit Delete
<input type="radio"/>	NFVIS netadmin	netadmin	*****	*****	Edit Delete
<input type="radio"/>	francis	francis	*****	*****	Edit Delete



Edit CLI Credentials

Name / Description *

Lila

Username *

lila

Password *

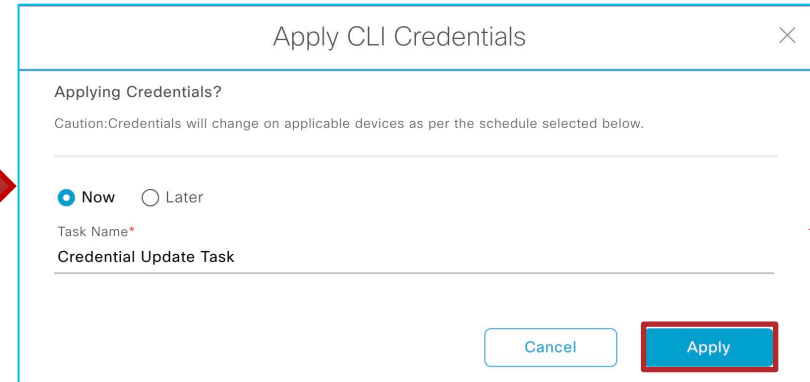
lilalila

Enable Password

lilalila

WARNING: Do not use "admin" as the username for your device CLI credentials, if you are using ISE as your AAA server. If you do, this can result in you not being able to login to your devices.

[Cancel](#) [Save](#)



Apply CLI Credentials

Applying Credentials?

Caution: Credentials will change on applicable devices as per the schedule selected below.

☒ Now ☐ Later

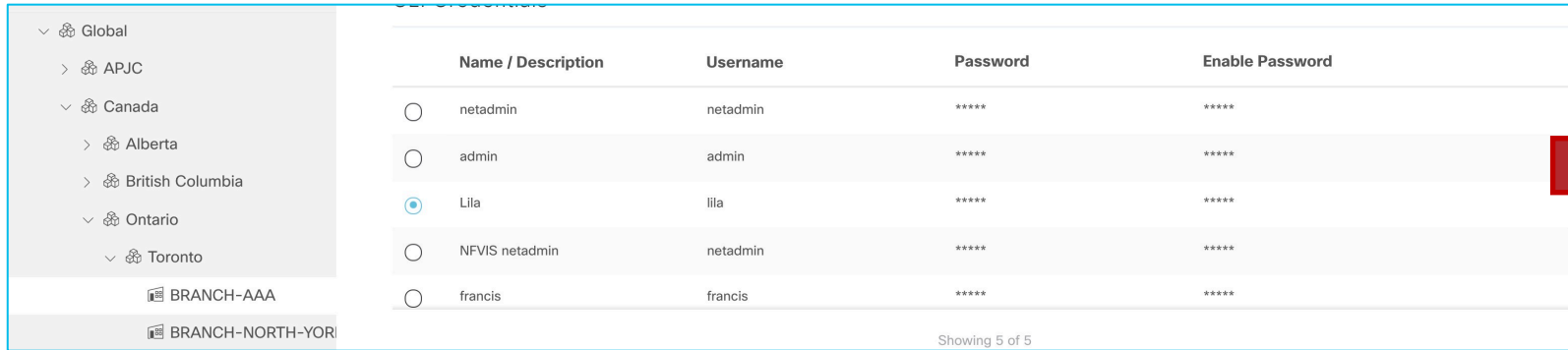
Task Name *

Credential Update Task

[Cancel](#) [Apply](#)

```
TBRANCH-C9200-1#show run | i username
username netadmin privilege 15 password 7 112A4816141D2F22256B
username lila privilege 15 secret 8
$8$v5LCra5y0lYetk$UTrtD9wImIRuTL4cMgCjcJpo4boeJmTfSk1KdczjcSI
```

Changing username credentials

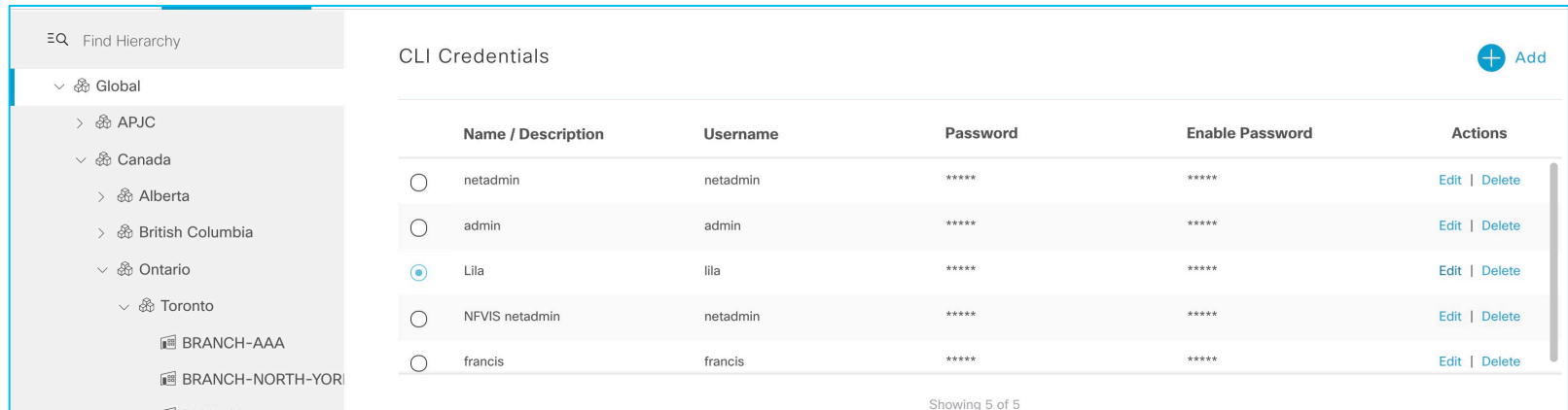


The screenshot shows the Cisco ISE GUI with the following structure:

- Left sidebar: Global, APJC, Canada, Alberta, British Columbia, Ontario, Toronto, BRANCH-AAA, BRANCH-NORTH-YORK.
- Main content area: CLI Credentials table.

	Name / Description	Username	Password	Enable Password
<input type="radio"/>	netadmin	netadmin	*****	*****
<input type="radio"/>	admin	admin	*****	*****
<input checked="" type="radio"/>	Lila	lila	*****	*****
<input type="radio"/>	NFVIS netadmin	netadmin	*****	*****
<input type="radio"/>	francis	francis	*****	*****

Showing 5 of 5



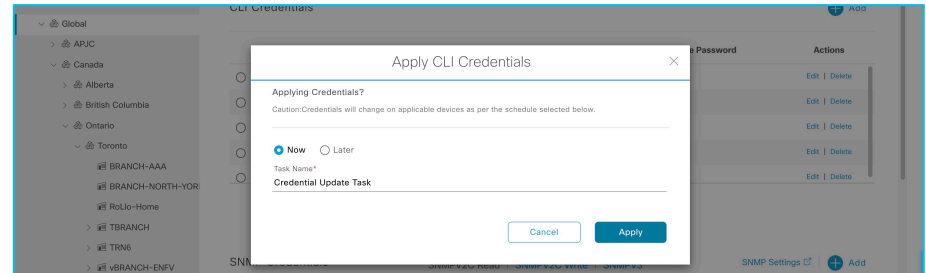
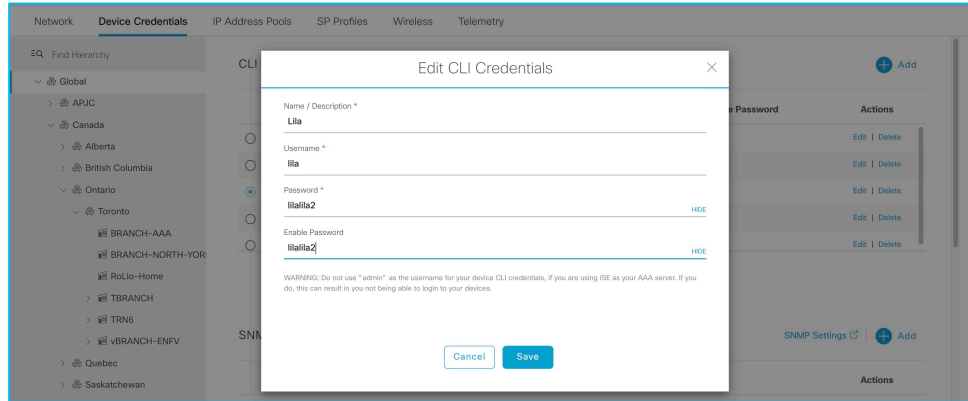
The screenshot shows the Cisco ISE GUI with the following structure:

- Left sidebar: Global, APJC, Canada, Alberta, British Columbia, Ontario, Toronto, BRANCH-AAA, BRANCH-NORTH-YORK.
- Main content area: CLI Credentials table.

	Name / Description	Username	Password	Enable Password	Actions
<input type="radio"/>	netadmin	netadmin	*****	*****	Edit Delete
<input type="radio"/>	admin	admin	*****	*****	Edit Delete
<input checked="" type="radio"/>	Lila	lila	*****	*****	Edit Delete
<input type="radio"/>	NFVIS netadmin	netadmin	*****	*****	Edit Delete
<input type="radio"/>	francis	francis	*****	*****	Edit Delete

Showing 5 of 5

Changing username credentials



Common objections on “Device Controllability”



Objections

- Hard to troubleshoot?
- No support for SNMP v3 for traps?
- IPDT breaks my network?
- Why do I need to add/delete a device to repush telemetry
- How can I undo what DNAC has done?

Simple to troubleshoot

Can now see "Provisioning" status for a device when assigned to site

reallylongName2.adamlab.cisco.com

Management IP 10.10.10.146
Device Type Cisco Catalyst 9800-CL Wireless Controller for Cloud
Device Role ACCESS

Deployment of syslog setting SUCCESS

- Deployment of syslog setting initiated
- COMPLETED: Configuring new Syslog Server Configurations Settings IP: [10.10.10.144] on the device: 10.10.10.146 completed successfully.

Deployment of snmp setting SUCCESS

- Deployment of snmp setting initiated
- COMPLETED: Configuring new SNMP Trap Server Configurations Settings IP: [10.10.10.144] on the device: 10.10.10.146 completed successfully.

Deployment of dns setting SUCCESS

- DNS Configurations pushed successfully
- Process success on all devices.

Deployment of netflow setting SUCCESS

- Deployment of netflow setting initiated
- COMPLETED: Configuring new Netflow Collector Server Configuration Settings IP: [10.10.10.144] and Port: [6007] on the device: 10.10.10.146 completed successfully.

Application telemetry SUCCESS

- Configuration of application telemetry is only applicable upon enable/disable application telemetry action, so no operation was performed

Install of Swim Certificate SUCCESS

- SWIM Certificate was pushed successfully

Deployment of WSA certificate SUCCESS

- ICAP port and Assurance WSA Configuration pushed successfully
- WSA Certificate was pushed successfully

Deployment of Wireless AP Join Certificate SUCCESS

- Certificate already exists on the device.
- Deployment of Wireless AP Join Certificate setting initiated

Deployment of PKCS12 certificate SUCCESS

- Started process: Pkcs12 Internal Certificate Configure
- Reachable DNAC IP:10.10.10.144
- PKI Configurations pushed successfully
- PKCS12 Certificate was pushed successfully

Deployment of IOS WLC NA Certificate configuration SUCCESS

- Setting does not apply to device, so no operation was performed

Deployment of IOS Telemetry Subscriptions configuration SUCCESS

- Configuring Assurance Telemetry Receiver Information
- Configuring Assurance Telemetry Subscriptions
- Configured Telemetry Subscription Receiver on the device with Receiver as 10.10.10.144
- Assurance Telemetry Subscriptions Configuration Success
- App Based Telemetry Subscriptions Configuration Success
- Telemetry Subscriptions was pushed successfully
- App Based Telemetry Subscriptions Configuration Success

Deployment of AP Impersonation configuration SUCCESS

- AP Impersonation pushed successfully
- Deployment of AP Impersonation setting initiated

Deployment of Terminal Width SUCCESS

- Setting does not apply to device, so no operation was performed

Deployment of IPDT SUCCESS

- Cannot push IPDT Configuration on the device with IpAddress: 10.10.10.146 for Product Family: wireless controller (Not Applicable)

SNMPv3 for traps

```
! snmp (v3 now supported)
snmp-server host 10.10.10.144 traps version 3 auth adam udp-port 162
trapflags ap register
trapflags ap interfaceup
snmp-server enable traps wireless AP wireless_mobility
snmp-server enable traps rf
snmp-server enable traps config
snmp-server source-interface traps GigabitEthernet2
```

IPDT is not configurable per site (vs global)

Assign Device to Site ✕

GLOBAL/DC/RDC	reallylongName2 The following settings will be deployed during assignment to site.	
reallylongName2	Syslog Server	Cisco DNA Center
	Netflow Collector	Cisco DNA Center
	IP Device Tracking ^{NEW}	Yes
	IP Device Tracking per site can now be managed from Network Settings.	
	SNMP Trap Receiver	Cisco DNA Center
	DNS Server	(Domain name: adamlab.cisco.com), 10.10.10.151
	Syslog Level	6 - Information Messages
	Cisco TrustSec (CTS) Credentials	Yes
	Controller Certificates	Yes

2.2.1.0 – IPDT can be controlled at site level

Network Device Credentials IP Address Pools SP Profiles Wireless **Telemetry**

Global

AUS

Branch

DC

RDC

gastiez

MH

NZ2

OS

SYD

Configure Syslog, Traps and NetFlow properties for your devices. The system will deploy these settings when devices are assigned to a site or provisioned.

Cisco DNA 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.

Controller as it has a restriction on the number of flow exporters.

☒ Use Cisco DNA Center as NetFlow collector server

INTERFACES FOR APPLICATION TELEMETRY

To enable telemetry on a device, select the device from the Provision table and choose "Actions->Enable Application Telemetry" By default, All access interfaces on a switch OR all LAN-facing interfaces on a router will be provisioned. To override this default behavior, tag specific interfaces to be designated as LAN interface, by putting the keyword "lan" in the interface description. Once specific interfaces are tagged those interfaces will be monitored.

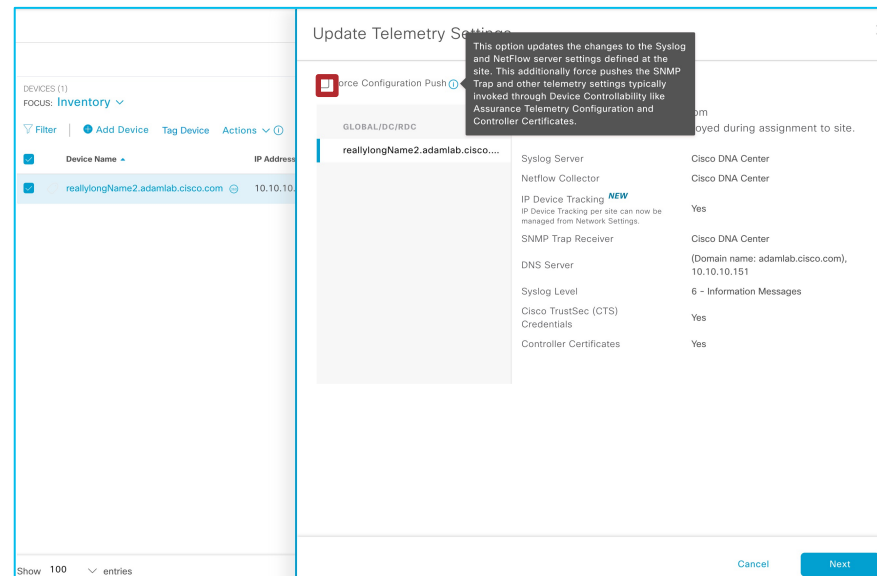
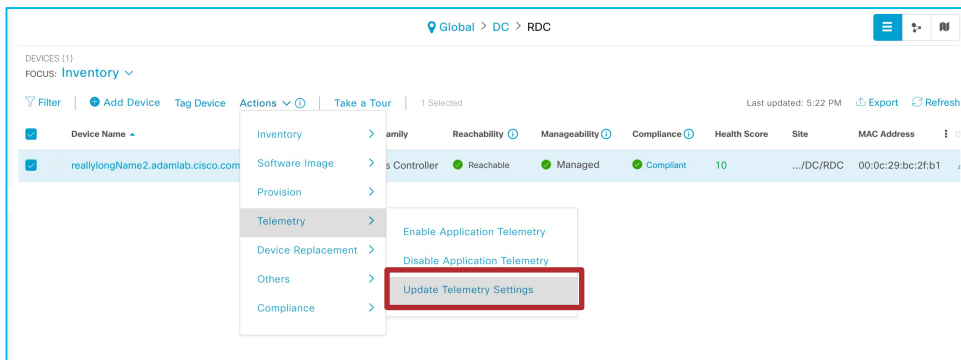
☐ Add an external NetFlow collector server
Only the external server destination will be configured on network devices. Flow records will not be configured.

Wired Client Data Collection

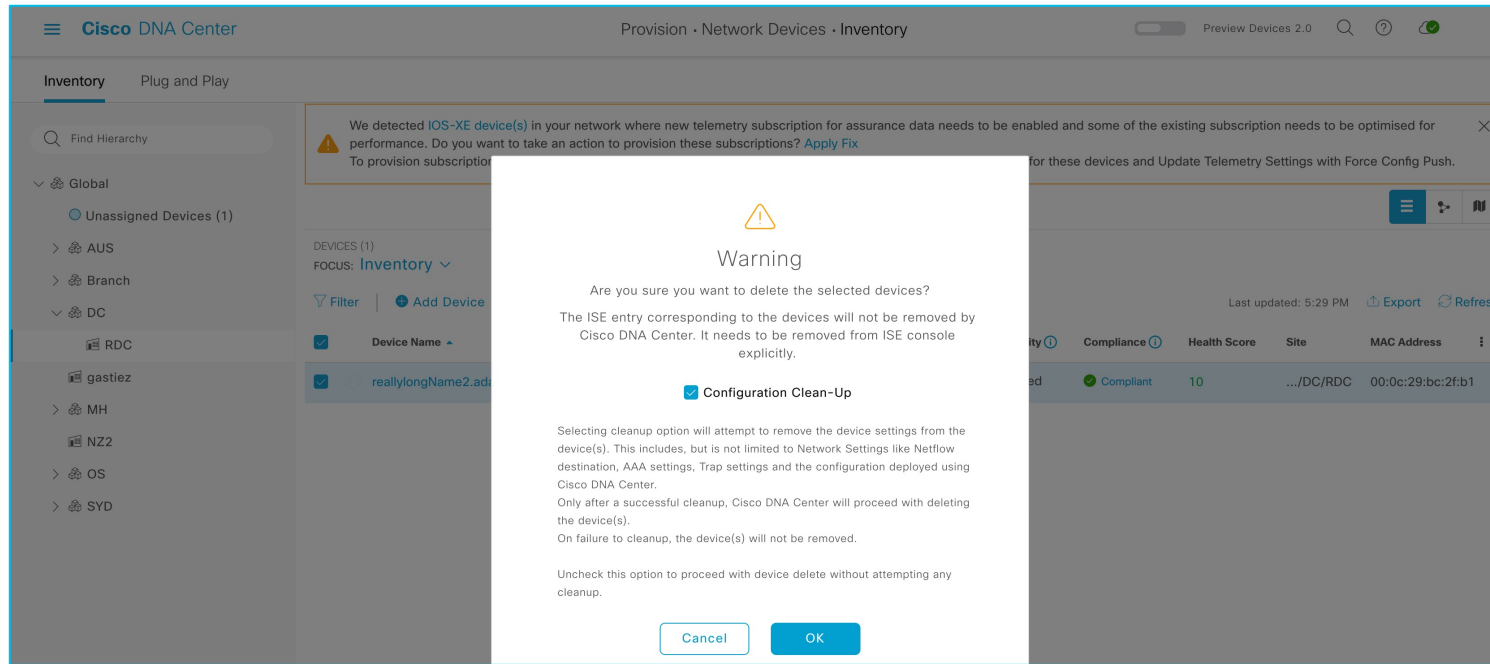
Choose if you want to monitor wired clients on this site. Monitoring wired clients enables IP Device Tracking (IPDT) on access switches.

☒ Monitor wired clients

Easy to update Device Controllability settings



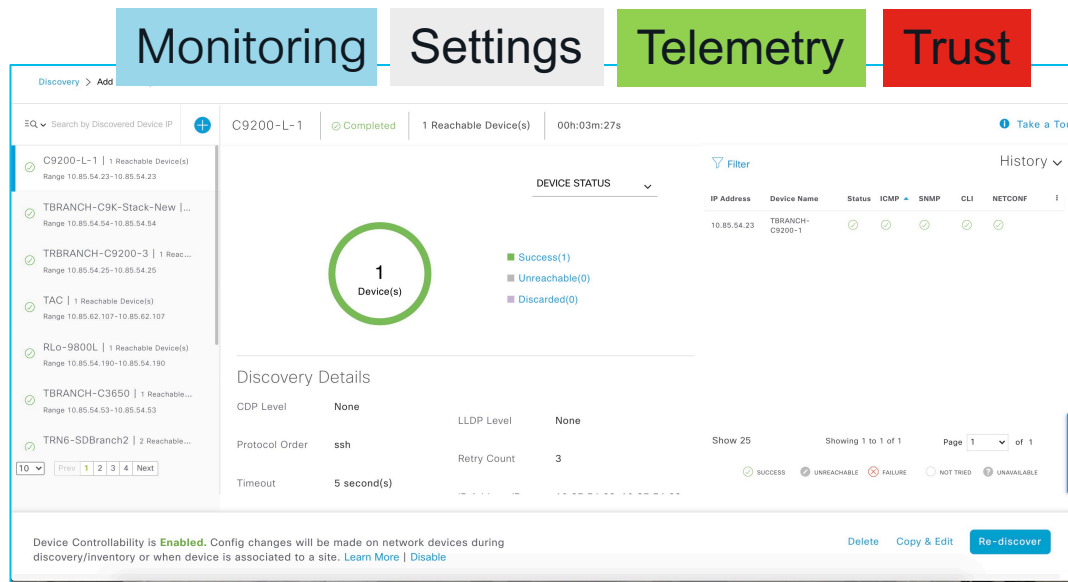
Configuration clean up – remove DNAC pushed config



Conclusion



- Device Controllability allows devices to interact with DNA Center efficiently
- Cisco DNA Center now provides comprehensive visibility into Device Controllability configurations
- Device Controllability is safe and easy to troubleshoot





The bridge to possible

Thank you

CISCO *Live!*

#CiscoLive





TURN IT UP

CISCO *Live!*

#CiscoLive