# Validated Profile: Cisco Large Enterprise and Government Vertical

Revised: December 20, 2023

# Solution Overview

Cisco Software-Defined Access (SD-Access) is the evolution from traditional campus LAN designs to networks that directly implement the intent of an organization. SD-Access is enabled with an application package that runs as part of the Cisco DNA Center software for designing, provisioning, applying policy, and facilitating the creation of an intelligent campus wired and wireless network with assurance.

Fabric technology, an integral part of SD-Access, enables wired and wireless campus networks with programmable overlays and easy-to-deploy network virtualization, permitting a physical network to host one or more logical networks to meet the design intent.

The enterprise market segment can be divided into different verticals: government, financial, health, and retail. This document covers the government vertical.

An enterprise/government environment typically contains a large number of devices and endpoints in the main fabric site. The solution focuses on validating all the fabric automation use cases and assurance at scale. The key components are:

- End-to-end solution deployment with the maximum fabric scale.
- Multiple Cisco DNA Center instances with a common Cisco ISE cluster.

  A large government deployment requires more than one Cisco DNA Center instance. The Multi-Cisco DNA Center feature provides the functionality for multiple Cisco DNA Centers to integrate with the same Cisco ISE cluster. All the virtual networks, security groups, access contracts, and security policies are created and shared among Cisco DNA Centers. The operations are performed through the primary node (Author node) and pushed to Cisco ISE and other Cisco DNA Center.
- Migration to IPv6.

  Devices increasingly run on IPv6, while network infrastructures are likely to continue on IPv4. Cisco DNA Center provides a seamless workflow for IPv6 migration.
- Wireless migration (from deploying the wireless OTT to the migration of fabric wireless).

  Some enterprise deployments choose to migrate to an SD-Access network in phases. The wired network is migrated first; the traditional wireless network is carried on top of the fabric wired network. This type of network is known as wireless over the top of fabric, or *wireless OTT*. The next phase migrates and enables the fabric wireless network.
- Cisco DNA Assurance.

  Assurance provides visibility to the actual experiences of users and applications across the end-to-end network.

# Hardware and Software Specifications

The solution is validated with the hardware and software listed in the following table.

***Table 1: Hardware and Software Profile Summary***

| Role | Hardware Platform | Software Release | Software Release |
|---|---|---|---|
| Cisco DNA Center Controller | DN2-HW-APL-XL | 2.3.3.7 | 2.3.5.5 |
| Identity Management, RADIUS Server | ISE-VM-K9 | 3.0 Patch 6, 3.1 Patch 3 | 3.0 Patch 6, 3.1 Patch 3 |

| Role | Hardware Platform | Software Release | Software Release |
|---|---|---|---|
| Cisco SD-Access Fabric Border | C9500-24Y4C | 17.6.6a/17.9.4a | 17.6.6a/17.9.4a |
| Cisco SD-Access Fabric Edge | C9500-40X, C9404R, C9300 | 17.6.6a/17.9.4a | 17.6.6a/17.9.4a |
| Cisco SD-Access Transit Node | C9500-24Y4C | 17.6.6a/17.9.4a | 17.6.6a/17.9.4a |
| Cisco Wireless Controller | C9800-80-K9<br>AIR-CT-8540 | 17.6.6a/17.9.4a<br>8.10.183.0 | 17.6.6a/17.9.4a<br>8.10.185.0 |
| Cisco Access Point | C9115AX, C9120AX, C9130AX<br>AIR-AP-3800, AIR-AP-4800 | 17.6.6a/17.9.4a<br>8.10.183.0 | 17.6.6a/17.9.4a<br>8.10.185.0 |

# Solution Use Case Scenarios

The validated solution supports the following Automation and Assurance use cases.

## Automation

- Deploy the large government fabric site
  - Fabric device onboarding with LAN automation
  - Virtual network and IP segment addition
  - IP and TCP transit
  - Multicast enablement
- Multi-Cisco DNA Center integration with the same Cisco ISE cluster
  - Virtual network, security group tags, access contracts, and secure policy creation
  - Role change (promotion of author node) among Cisco DNA Centers
  - Policy enforcement and Change of Authorization (COA)
- Wireless OTT deployment and migration to the fabric wireless
- Migration from an IPv4-only network to a dual-stack network
- Wired and wireless fabric device image upgrade validation
  - Site-level device image upgrade, including wired and wireless devices
- Cisco DNA Center three-node cluster upgrade validation
  - Cisco DNA Center upgrade from 2.3.3.7 to 2.3.5.5
- Network and service failover/redundancy validation
  - Cisco DNA Center high availability

  - ISE PAN, PSN, and pxGrid service failover
  - ISE unreachable with critical VLAN
  - Border SVL and access switch stack failover
- Fabric device RMA workflow and AP refresh workflow
  - Fabric device and faulty AP RMA
  - Entire AP replacement from Wav2 AP to 11ax AP
- Fabric scale and performance

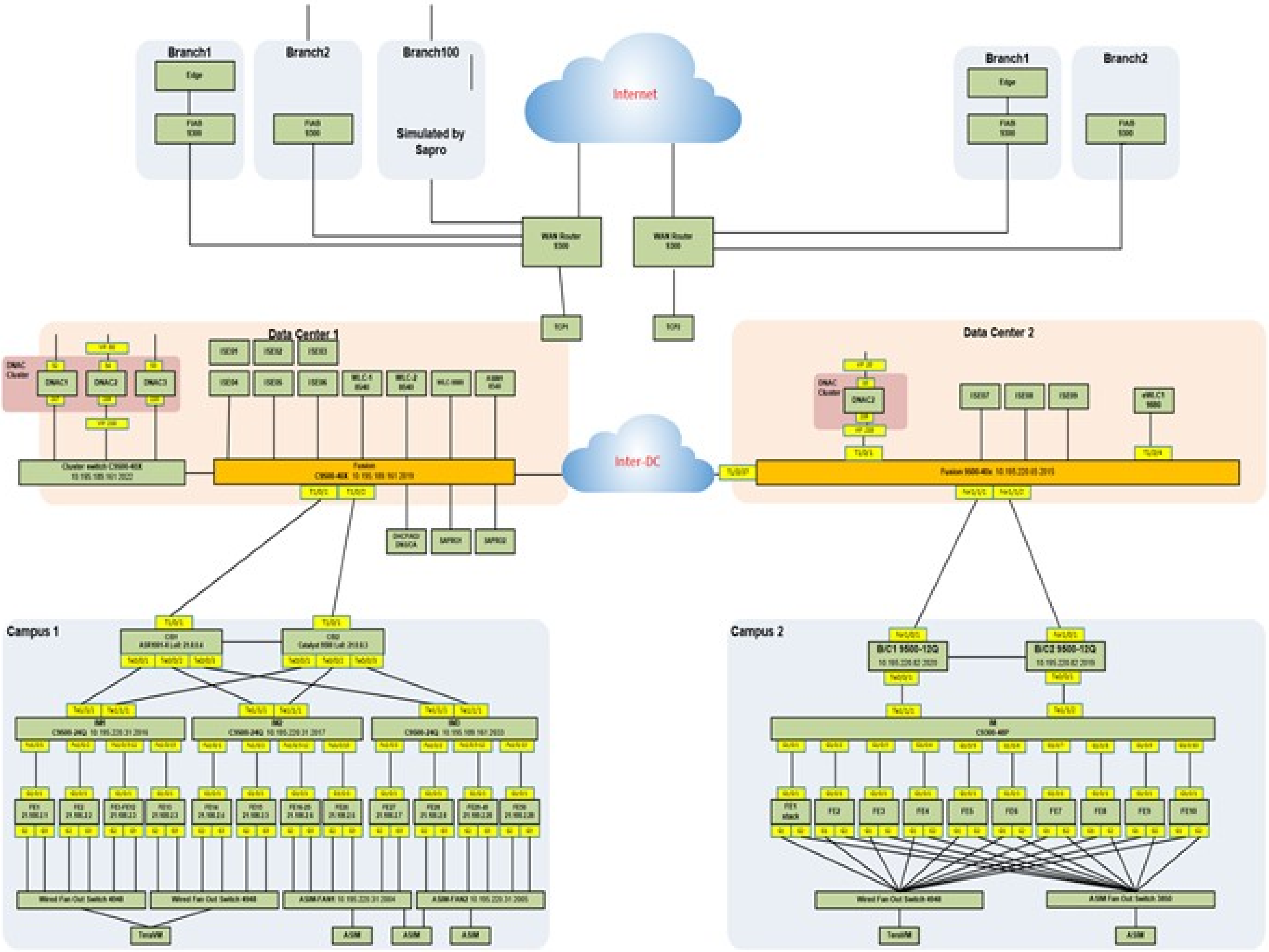
## Assurance

- Dual-stack fabric client onboarding
  - Wired and wireless dual-stack client onboarding
  - Client dashboard shows the list of onboarded client devices with their correct health scores and all other expected information
- Network device onboarding
  - Network dashboard shows the list of onboarded network devices with their correct health scores and all other expected information
- Assurance issue reporting
  - Link down issue generation for network devices
  - AP down issue generation
  - Stack member down
- Client health drill down
  - Assurance charts in the Client Health page
  - Assurance charts in the Client 360 page
- Network health drill down
  - Assurance charts in the Network Health page
  - Assurance charts in the Device 360 page
- Fabric Assurance
  - Fabric health score and Assurance charts in the Fabric Health page
- Assurance with scale
  - Assurance charts with 300,000 concurrent endpoints and 750,000 transient endpoints
- Longevity/soak test

# Solution Environment

## Topology

The topology illustrates the solution environment for large enterprise and government deployments.



- Controller integration:
  - Data Center 1: One three-node, 112-core Cisco DNA Center cluster, two ISE PAN/MNTs, and three PSN nodes.
  - Data Center 2: One single-node, 112-core Cisco DNA Center with three ISE PSN nodes.
- The shared service contains DNS, DHCP, AD, NTP, HTTP, TFTP, and backup servers. WLCs also reside in the shared service.
- Two large fabric campus sites:
  - Campus 1: Dual-fabric borders/CP, 1000 fabric edges, 1000 IP segments.

- Campus 2: Border with SVL, 1000 fabric edges, 600 IP segments.

- Branches: FIAB in branch with communication to the campus via transit CP nodes (one for each campus).
- Both campuses contain numerous simulated fabric nodes, APs, and simulated wired/wireless endpoints.

## Scale

Solution test verified the scale numbers listed in the following table. For the hardware capacity, see the Cisco DNA Center Data Sheet.

***Table 2: Solution Scale Profile***

| Category | Value | Notes |
|---|---|---|
| Cisco DNA Center clusters | 4 | One three-node and one single-node, 112-core appliance |
| Cisco ISE clusters | 8 | Two x PAN/MNT, six PSNs (including two pxGrid) |
| Devices in inventory | 10,000 | Routers, switches, and wireless controllers |
| Devices per fabric | 1000 | Two border/control plane + 50 switches + 950 simulated switches |
| Static host ports | 480,000 | 480,000 physical interfaces |
| Site elements in the network hierarchy | 10,000 | Sites, buildings, and floors |
| VNs in the fabric | 256 | — |
| IP pools in a fabric site | 1000 | 1000 IP segments |
| Wireless controllers in a fabric site | 2 | C9800-80<br>AIR-CT-8540 |
| SSIDs | 6 | — |
| APs in inventory | 25,000 | — |
| APs in a fabric site | 6000 | — |
| Endpoints | 300,000 | 200,000 wired<br>100,000 wireless |
| Cisco DNA Center instances in a multi-Cisco DNA Center environment | 2 | — |
| SGTs | 4000 | — |
| ACA policies | 25,000 | — |

*Table 3: Solution Scale Performance Data (based on Solution Scale Profile)*

| Operation | Performance Measurement |
|---|---|
| Add an IP segment | 30 minutes |
| Delete an IP segment | 30 minutes |
| Add a fabric edge node | 27 minutes |
| Remove a fabric edge node | 15 minutes |
| Add an external border/control plane | 40 minutes |
| Remove an external border/control plane | 39 minutes |
| Enable multicast in VN | 2 hours, 54 minutes |
| Disable multicast in VN | 2 hours, 58 minutes |
| Enable IPv6 in one IPv4 segment | 35 minutes |
| Provision 100 APs | 4 minutes |
| Distribute image to 50 switches via SWIM | 14 minutes |
| Activate image on 50 switches via SWIM | 28 minutes |
| Change the multi-Cisco DNA Center role (includes synchronization time) | 33 minutes (4000 SGTs) |
| Back up Cisco DNA Center | Fusion data: 22 minutes (46 GB) |

# Best Practices and Recommendations

This section describes the technical notes useful for deploying the solution.

## Wireless OTT Migration

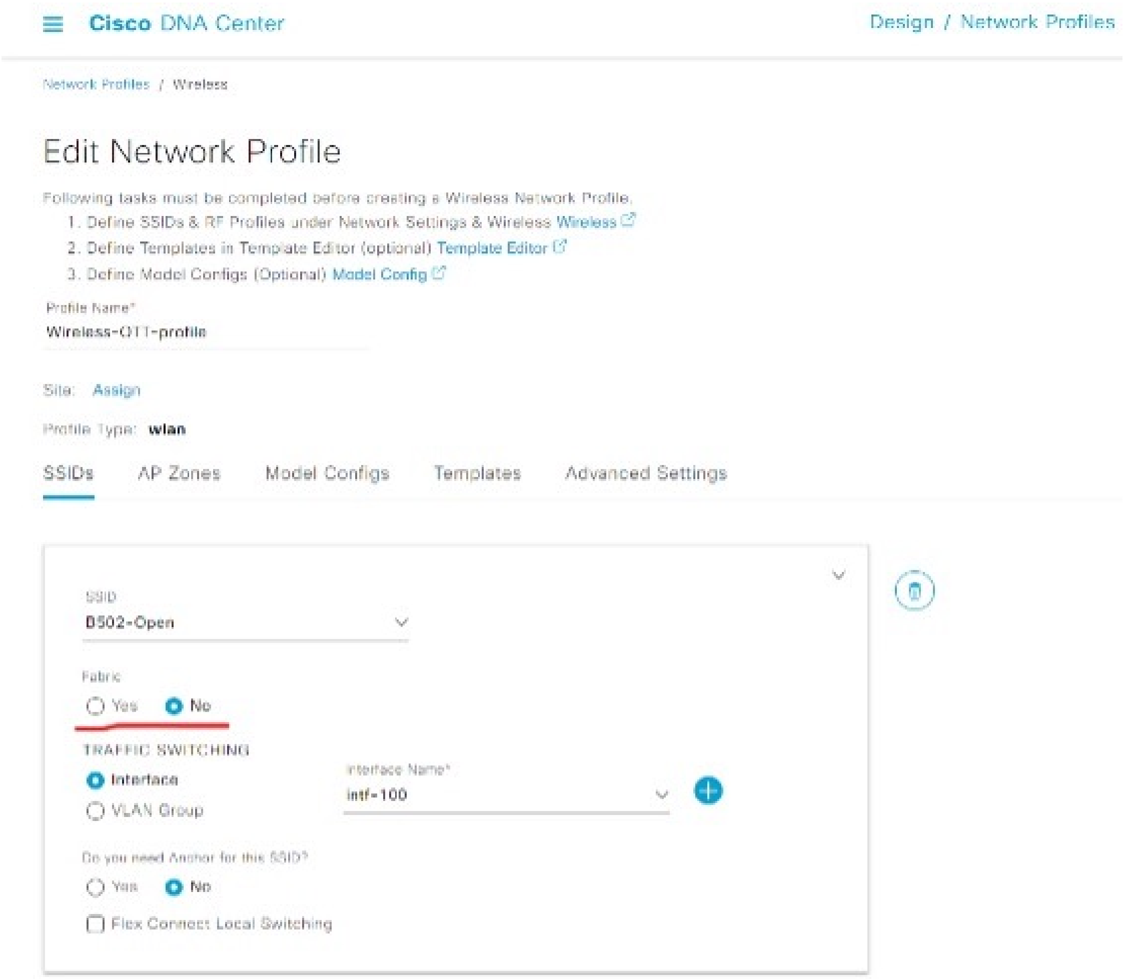
Wireless OTT is the traditional wireless carried on top of the SD-Access fabric. This mode is important as a migration step for customers who decide to implement SD-Access first on the wired network and then plan the wireless integration. When migrating an OTT deployment to an SD-Access wireless network, the following steps are recommended to retain the same SSID names for the wireless network.

### Procedure

**Step 1** On the Fabric page, add the wireless controller to the fabric site.

**Step 2** To retain the same SSIDs in the fabric network as the OTT, create a new network profile and add the same SSIDs to the profile with fabric enabled.

The original network profile for the OTT network:



Edit Network Profile

Following tasks must be completed before creating a Wireless Network Profile.

1. Define SSIDs & RF Profiles under Network Settings & Wireless Wireless
2. Define Templates in Template Editor (optional) Template Editor
3. Define Model Configs (Optional) Model Config

Profile Name*
Wireless-OTT-profile

Site: Assign

Profile Type: wlan

SSID
B502-Open

Fabric
○ Yes ● No

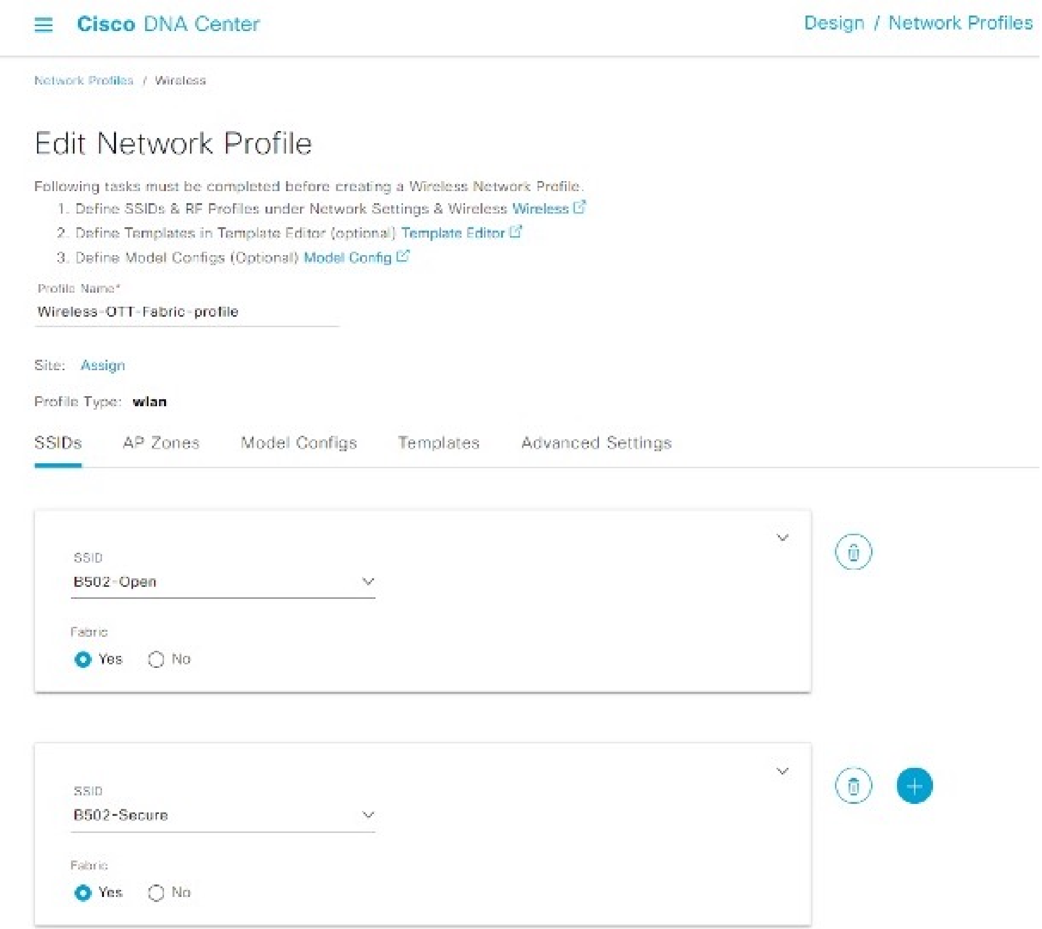
TRAFFIC SWITCHING
● Interface
○ VLAN Group

Interface Name*
intf-100

Do you need Anchor for this SSID?
○ Yes ● No

□ Flex Connect Local Switching

The new network profile for the fabric wireless (with the same SSID and fabric enabled):



Edit Network Profile

Following tasks must be completed before creating a Wireless Network Profile.

1. Define SSIDs & RF Profiles under Network Settings & Wireless Wireless
2. Define Templates in Template Editor (optional) Template Editor
3. Define Model Configs (Optional) Model Config

Profile Name*: Wireless-OTT-Fabric-profile

Site: Assign

Profile Type: wlan

SSID: B502-Open

Fabric: ● Yes ○ No

SSID: B502-Secure

Fabric: ● Yes ○ No

**Step 3** Assign the floors to the new network profile.

**Step 4** Reprovision the wireless controller with the new network profile. This removes the old nonfabric SSIDs and generates new fabric SSIDs.

**Step 5** On the **Host Onboarding** > **Wireless SSID** page, assign wireless pools to the SSIDs in the fabric. This enables the fabric SSIDs in the wireless controller.

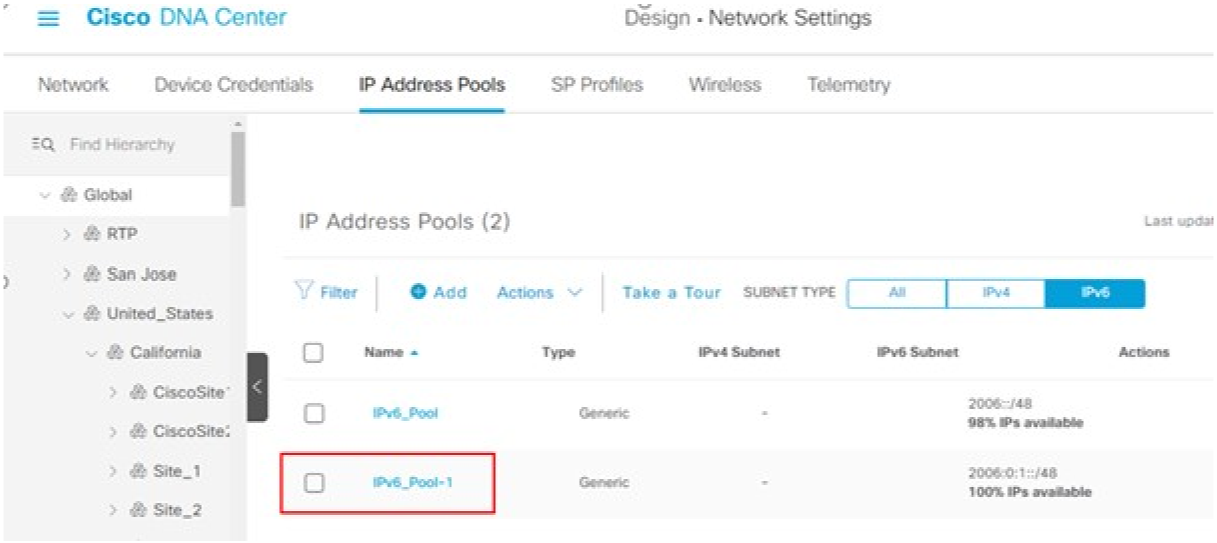
**Step 6** Reprovision the APs in the assigned floors. APs reboot and start to broadcast the fabric SSIDs. Access tunnels are created for each fabric AP in the fabric edge nodes.

## IPv6 Migration (Dual-Stack Enablement)

Many deployments have IPv4-only segments. When migrating to a dual-stack environment that supports IPv6, the following steps are recommended.

### Procedure

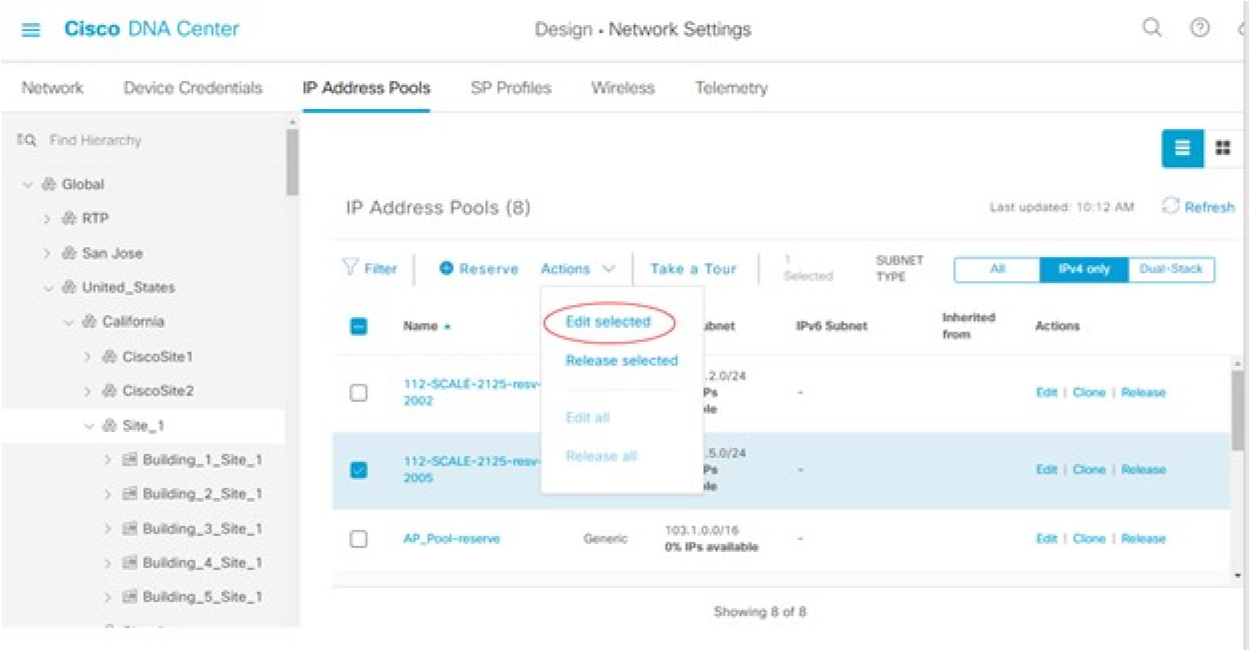
**Step 1** Create an IPv6 global pool.



IP Address Pools (2)

| Name | Type | IPv4 Subnet | IPv6 Subnet | Actions |
|---|---|---|---|---|
| IPv6_Pool | Generic | - | 2006::/48<br>98% IPs available | |
| IPv6_Pool-1 | Generic | - | 2006:0:1::/48<br>100% IPs available | |

**Step 2** Select the IPv4 pool and add it to the IPv6 pool.

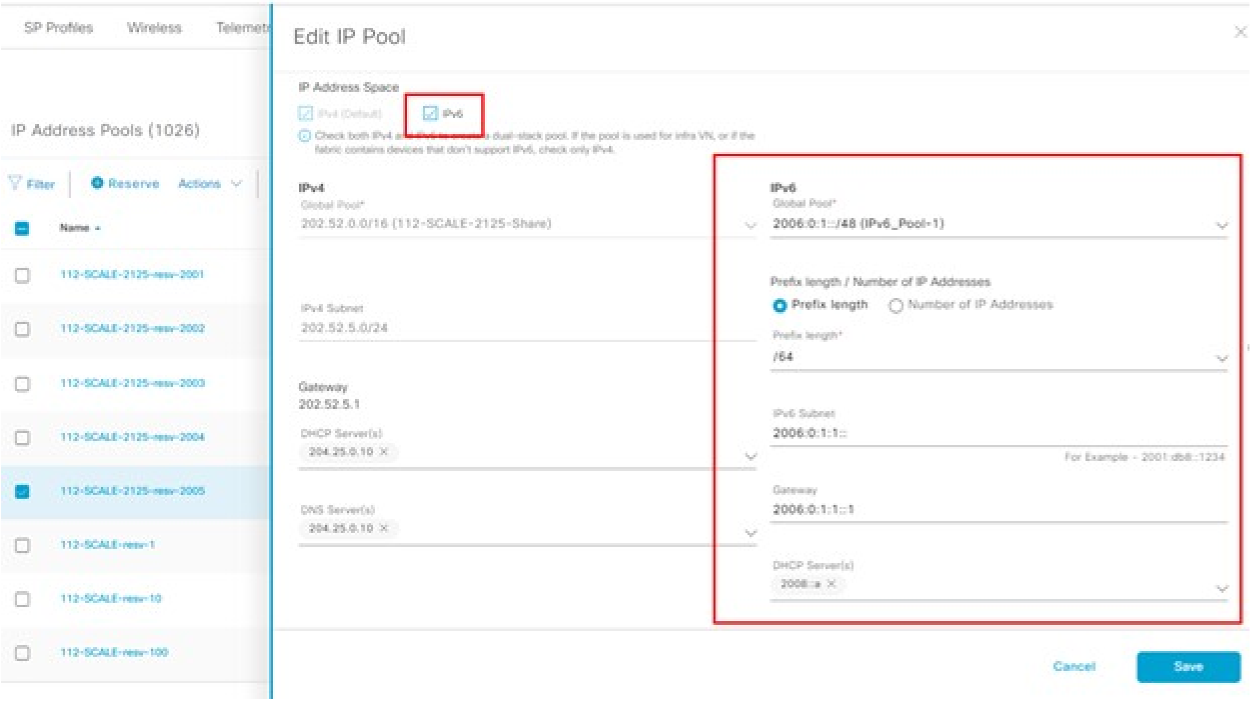


IP Address Pools (8)

Last updated: 10:12 AM

| Name | | bnet | IPv6 Subnet | Inherited from | Actions |
|---|---|---|---|---|---|
| ☐ 112-SCALE-2125-resv-2002 | | .2.0/24<br>Ps<br>le | - | | Edit \| Clone \| Release |
| ☑ 112-SCALE-2125-resv-2005 | | .5.0/24<br>Ps<br>le | - | | Edit \| Clone \| Release |
| ☐ AP_Pool-reserve | Generic | 103.1.0.0/16<br>0% IPs available | - | | Edit \| Clone \| Release |

Showing 8 of 8



SP Profiles | Wireless | Telemetry

IP Address Pools (1026)

Filter | Reserve | Actions

| | Name |
|---|---|
| ☐ | 112-SCALE-2125-resv-2001 |
| ☐ | 112-SCALE-2125-resv-2002 |
| ☐ | 112-SCALE-2125-resv-2003 |
| ☐ | 112-SCALE-2125-resv-2004 |
| ☑ | 112-SCALE-2125-resv-2005 |
| ☐ | 112-SCALE-resv-1 |
| ☐ | 112-SCALE-resv-10 |
| ☐ | 112-SCALE-resv-100 |

Edit IP Pool

IP Address Space

☑ IPv4 (Default) ☑ IPv6

Check both IPv4 and IPv6 to create a dual-stack pool. If the pool is used for infra VN, or if the fabric contains devices that don't support IPv6, check only IPv4.

IPv4

Global Pool*: 202.52.0.0/16 (112-SCALE-2125-Share)

IPv4 Subnet: 202.52.5.0/24

Gateway: 202.52.5.1

DHCP Server(s): 204.25.0.10

DNS Server(s): 204.25.0.10

IPv6

Global Pool*: 2006:0:1::/48 (IPv6_Pool-1)

Prefix length / Number of IP Addresses: ● Prefix length ○ Number of IP Addresses

Prefix length*: /64

IPv6 Subnet: 2006:0:1:1::

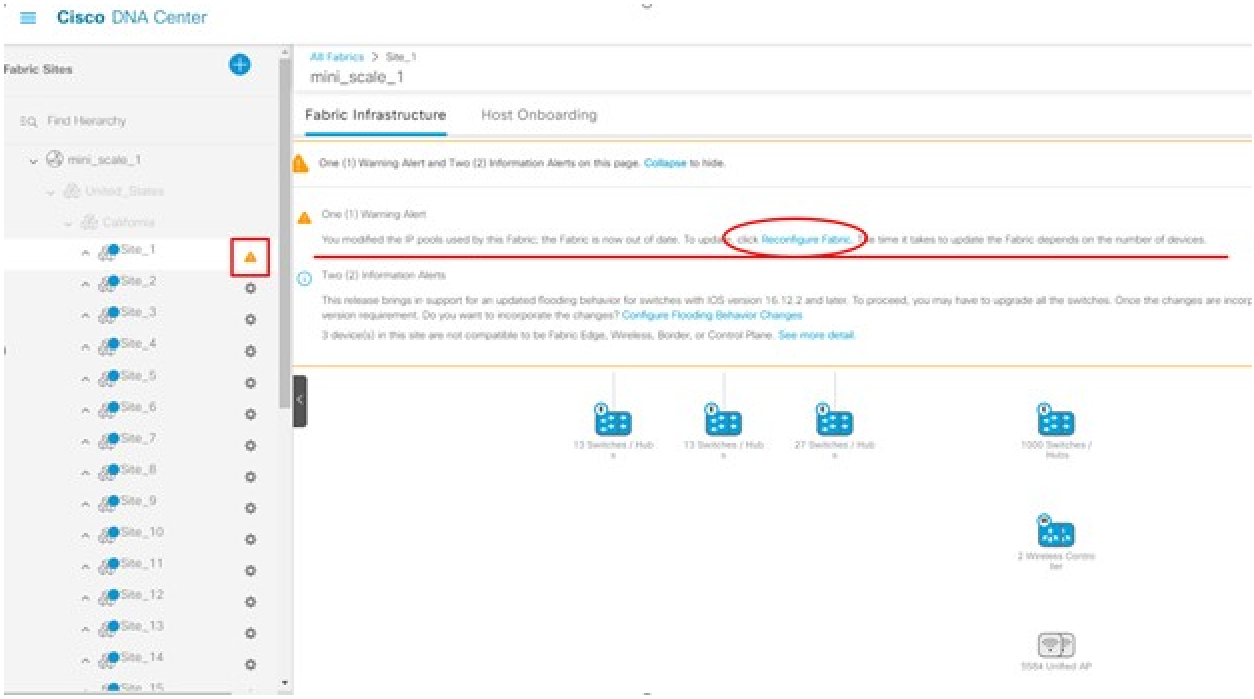
For Example - 2001:db8::1234

Gateway: 2006:0:1:1::1

DHCP Server(s): 2006::a

Cancel | Save

**Step 3** After the pool information is saved, Cisco DNA Center adds an alert on the Fabric page and prompts you to reconfigure the fabric.



Cisco DNA Center

Fabric Sites

Find Hierarchy

mini_scale_1 > United_States > California > Site_1, Site_2, Site_3, Site_4, Site_5, Site_6, Site_7, Site_8, Site_9, Site_10, Site_11, Site_12, Site_13, Site_14, Site_15

All Fabrics > Site_1

mini_scale_1

Fabric Infrastructure | Host Onboarding

One (1) Warning Alert and Two (2) Information Alerts on this page. Collapse to hide.

One (1) Warning Alert

You modified the IP pools used by this Fabric; the Fabric is now out of date. To update, click Reconfigure Fabric. The time it takes to update the Fabric depends on the number of devices.

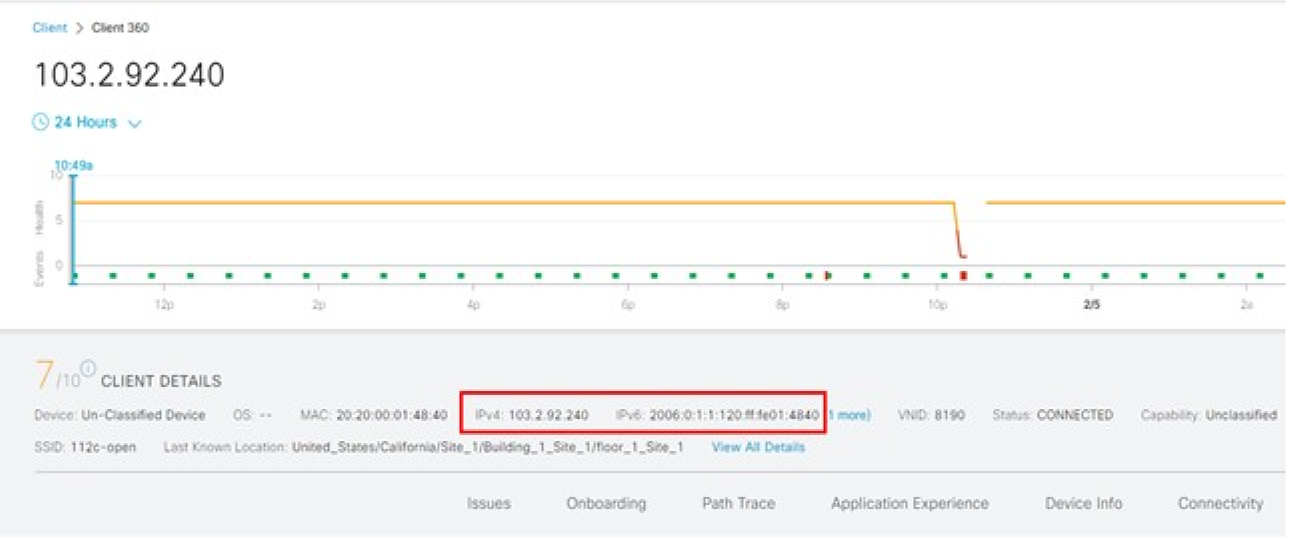
Two (2) Information Alerts

This release brings in support for an updated flooding behavior for switches with IOS version 16.12.2 and later. To proceed, you may have to upgrade all the switches. Once the changes are incorp version requirement. Do you want to incorporate the changes? Configure Flooding Behavior Changes

3 device(s) in this site are not compatible to be Fabric Edge, Wireless, Border, or Control Plane. See more detail.

**Step 4** After the provisioning is complete, onboard the hosts and endpoints. The onboarding hosts get both IPv4 and IPv6 addresses.

**Step 5** On the Assurance page, view the dual addresses.



103.2.92.240

7/10 CLIENT DETAILS

Device: Un-Classified Device OS: -- MAC: 20:20:00:01:48:40 IPv4: 103.2.92.240 IPv6: 2006:0:1:1:120:ff:fe01:4840 (1 more) VNID: 8190 Status: CONNECTED Capability: Unclassified

SSID: 112c-open Last Known Location: United_States/California/Site_1/Building_1_Site_1/floor_1_Site_1 View All Details

## Multi-Cisco DNA Center Deployment

Cisco DNA Center systems cannot scale to more than 25,000 to 100,000 endpoints (25,000 for 44-core appliances, 40,000 for 56-core appliances, and 100,000 for 112-core appliances). The Cisco Identity Service Engine can scale to 2,000,000 endpoints. Before release 1.3.3.x, only one Cisco DNA Center system could integrate with one Cisco ISE system. Now, large Cisco ISE deployments can benefit by integrating multiple Cisco DNA Center clusters with a single Cisco ISE. This feature for the Access Control App in Cisco DNA Center allows you to integrate up to four Cisco DNA Center clusters with a single Cisco ISE system.

Note the following for a multi-Cisco DNA Center deployment:

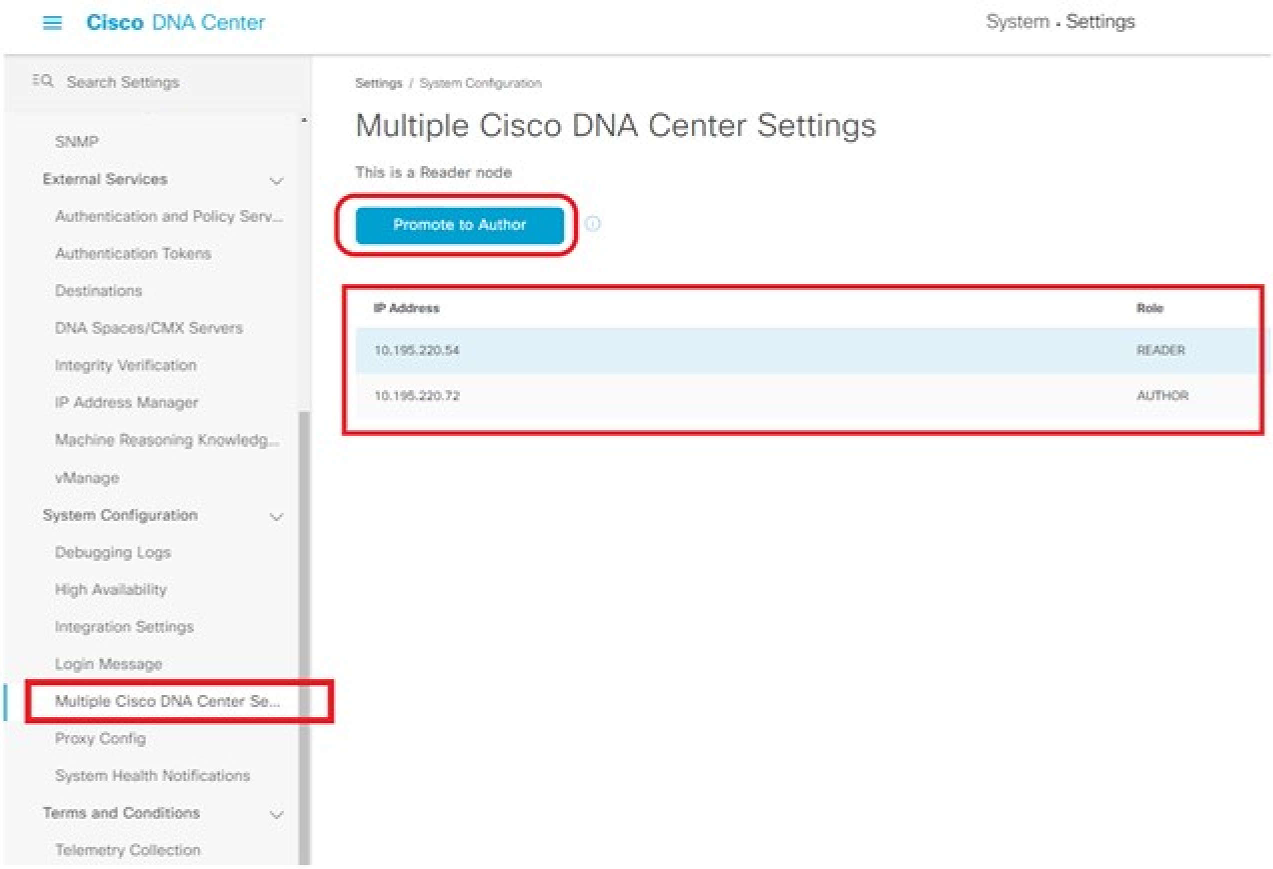
1. The multiple Cisco DNA Center cluster functionality isn’t currently available in Cisco DNA Center for General Availability. A Limited Availability package (called “Multi-DNAC”) is available only to eligible customers. If you’re eligible, you can download and install the package to provide the functionality.

2. In a multi-Cisco DNA Center deployment, all the Cisco DNA Center clusters must be the same release to integrate with the same Cisco ISE cluster. Cross-release of Cisco DNA Center is not supported in a multi-Cisco DNA Center deployment.

3. The dependency package for the Multi-DNAC package is the Access Control Application package. You must install the ACA package before installing the Multi-DNAC package.

4. In a deployment with one Cisco ISE system and multiple Cisco DNA Center clusters, only the Author node can manage SDA policy objects. The first Cisco DNA Center cluster that you integrate with Cisco ISE assumes the Author node role. The Author node is the single point of administration for virtual networks, scalable groups, access contracts, policies, and scalable group–virtual network associations. The Reader node has a read-only view of virtual networks, scalable groups, and the virtual network associations between scalable groups. The Reader node cannot display access contracts or policies. The Reader node has a link to cross-launch to the Author node.

5. When integration with the Cisco ISE system is complete, you can confirm the role status as an Author/Reader node on the **System Settings** > **Settings** > **Multiple Cisco DNA Center Settings** page.



Multiple Cisco DNA Center Settings

This is a Reader node

| IP Address | Role |
|---|---|
| 10.195.220.54 | READER |
| 10.195.220.72 | AUTHOR |

6. The Reader node can be promoted to the Author node to replace the current Author node. After the promotion, the new Author node must perform a resync of the Cisco ISE database for the policy data. If the cluster has a large number of SGTs, the resync time increases. After the resync is complete, the new Author node can be used to manage all the access control policies for the entire deployment.

## Assurance

### Procedure 1: Assurance Summary from Cisco DNA Center Home page

The Assurance Summary dashboard from the Cisco DNA Center home page displays the overall health status of the network. From this dashboard, drill down to the Assurance Overall page or the Assurance Issues page.

### Procedure 2: Assurance Overall page

From the top-left corner, click the menu icon and choose **Assurance** > **Health** to view aggregate health information for network devices and clients. The default view shows data for the last 7 days; you can adjust the display to the last 3 hours or 24 hours.

### Procedure 3: Network Health page

From the top-left corner, click the menu icon and choose **Assurance** > **Health**. Click the **Network** tab to open the Network Health page.

The Network Health page has sections for Network Device Reachability, Top N APs by High Interference, Total APs Up/Down, Top N APs by Client Count, PoE Operational State Distribution, PoE Powered Device Distribution, and PoE Insights.

### Procedure 4: Client Health page

From the top-left corner, click the menu icon and choose **Assurance** > **Health**. Click the **Client** tab to open the Client Health page.

The Client Health page has sections for Wireless Clients and Wired Clients.

The Network Health page has panels for Client Onboarding Times, Connectivity RSSI, Connectivity SNR, Client Roaming Times, Client Count per SSID, and Connectivity Physical Link.

### Procedure 5: Device 360 page

From the top-left corner, click the menu icon and choose **Provision** > **Inventory**. Click a device and then click **View 360**.

### Procedure 6: Client 360 page

From the top-left corner, click the menu icon and choose **Assurance** > **Health**. Click the **Client** tab to open the Client Health page.

The Client 360 page displays a 360° view of the client device.

### Procedure 7: Fabric Assurance

Analytics provided for the fabric overlay include the following:

- Fabric reachability: Connectivity checks between all fabric nodes.
- Fabric device: Fabric nodes mapping entries, protocols, and performance.
- Fabric clients: Client onboarding and shared services (DHCP, DNS, AAA, RADIUS).

All fabric overlay charts are available in the Device 360 and Client 360 pages.

### Troubleshooting Assurance

- If multiple Assurance dashboards show no data, use the **magctl appstack status** command to check that all Assurance services are running. Use the Flink tool to check that all Assurance pipelines are running.
- If the Network Health page intermittently shows no data, check the Network-health processor or Graph-Writer LAG in Grafana.
- If wired clients don’t show the correct details, check for any Wired Pipeline LAG in Grafana.

## Cisco DNA Center Air Gap Upgrade

Some government agencies have strict security requirements that restrict the deployment of management solutions in a cloud environment. Cisco DNA Center supports offline software updates, allowing Cisco DNA Center appliances deployed in secure, air-gapped networks to be updated to the latest Cisco DNA Center software and application versions, without having to access the Cisco Connected DNA Cloud. To upgrade your Cisco DNA Center appliance in an air-gapped environment, see the "2.3.2.x, 2.3.3.x, or 2.3.4.x to 2.3.5.x" chapter in the *Cisco DNA Center Air Gap Deployment Guide*.

**Americas Headquarters**
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

**Asia Pacific Headquarters**
CiscoSystems(USA)Pte.Ltd.
Singapore

**Europe Headquarters**
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.