Software-Defined Access Medium and Large Site Fabric Provisioning

Solution Adoption Prescriptive Reference Deployment Guide

October 2019

First Publish: August 23, 2019
Last Update: October 10, 2019

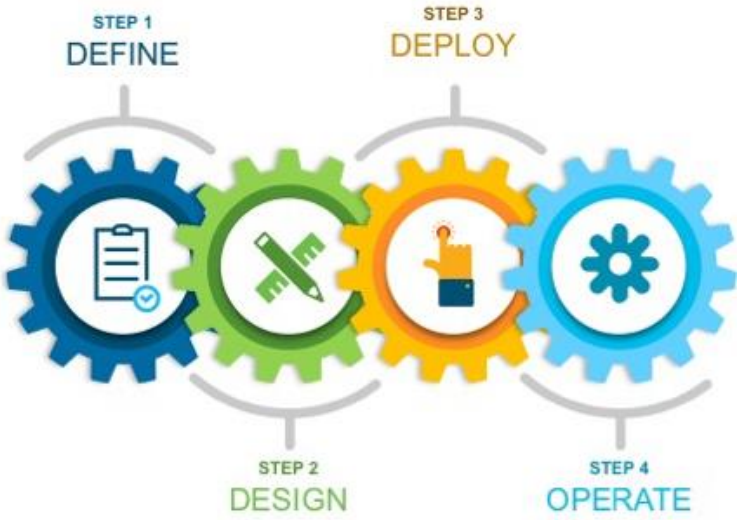
Contents

Hardware and Software Version Summary

Table 1. Hardware and software version summary

Product	Part number	Software version
Cisco DNA Center Appliance	DN2-HW-APL-L (M5-based chassis)	1.2.10.4 (System 1.1.0.754)
Cisco Identity Services Engine	R-ISE-VMM-K9=	2.4 Patch 6
Cisco Wireless LAN Controller	Cisco 8540, 5520, and 3504 Series Wireless Controllers	8.8.111.0 (8.8 MR1)
Cisco IOS XE Software	See Appendix A for complete listing	IOS XE 16.9.3

About this Guide



This guide contains four major sections:

The **DEFINE** section defines Software-Defined Access, its relationship to Cisco DNA Center, and provides information on companion Solution Guides.

The **DESIGN** section shows the deployment topology, described the routing protocols and redistribution modalities, and discussions the drivers behind these modalities.

The **DEPLOY** section showcases the use of the DESIGN and POLICY applications in Cisco DNA Center along with the corresponding Discovery and Inventory Tools. LAN Automation and SWIM are used to onboard devices that will be used as the part of the SD-Access fabric.

The **OPERATE** demonstrates the PROVISION application to deploy a fabric site for both wired and wireless clients. Access to shared services and fusion routers are discussion and manually configured.

Define

This section introduces the Software-Defined Access solution and how its relationship to Cisco DNA Center. It also provides links to additional resources, companion guides, and a link to ensure the current copy is the latest version of this guide.

About SD-Access & Cisco DNA Center

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.

This guide is used to deploy a Cisco Software-Defined Access fabric. The deployment described in this guide is used after deploying the management infrastructure of Cisco DNA Center, Cisco Identity Services Engine (ISE), and Cisco Wireless LAN Controllers (WLC) described in the companion Software-Defined Access & Cisco DNA Center Management Infrastructure Prescriptive Deployment Guide.

Companion Resources

Find the companion Software-Defined Access Solution Design Guide, Software-Defined Access & Cisco DNA Center Management Infrastructure Prescriptive Deployment Guide, Software-Defined Access for Distributed Campus Prescriptive Deployment Guide, related deployment guides, design guides, and white papers, at the following pages:

- https://www.cisco.com/go/designzone
- https://cs.co/en-cvds

If you didn't download this guide from Cisco Community or Design Zone, you can check for the latest version of this guide.

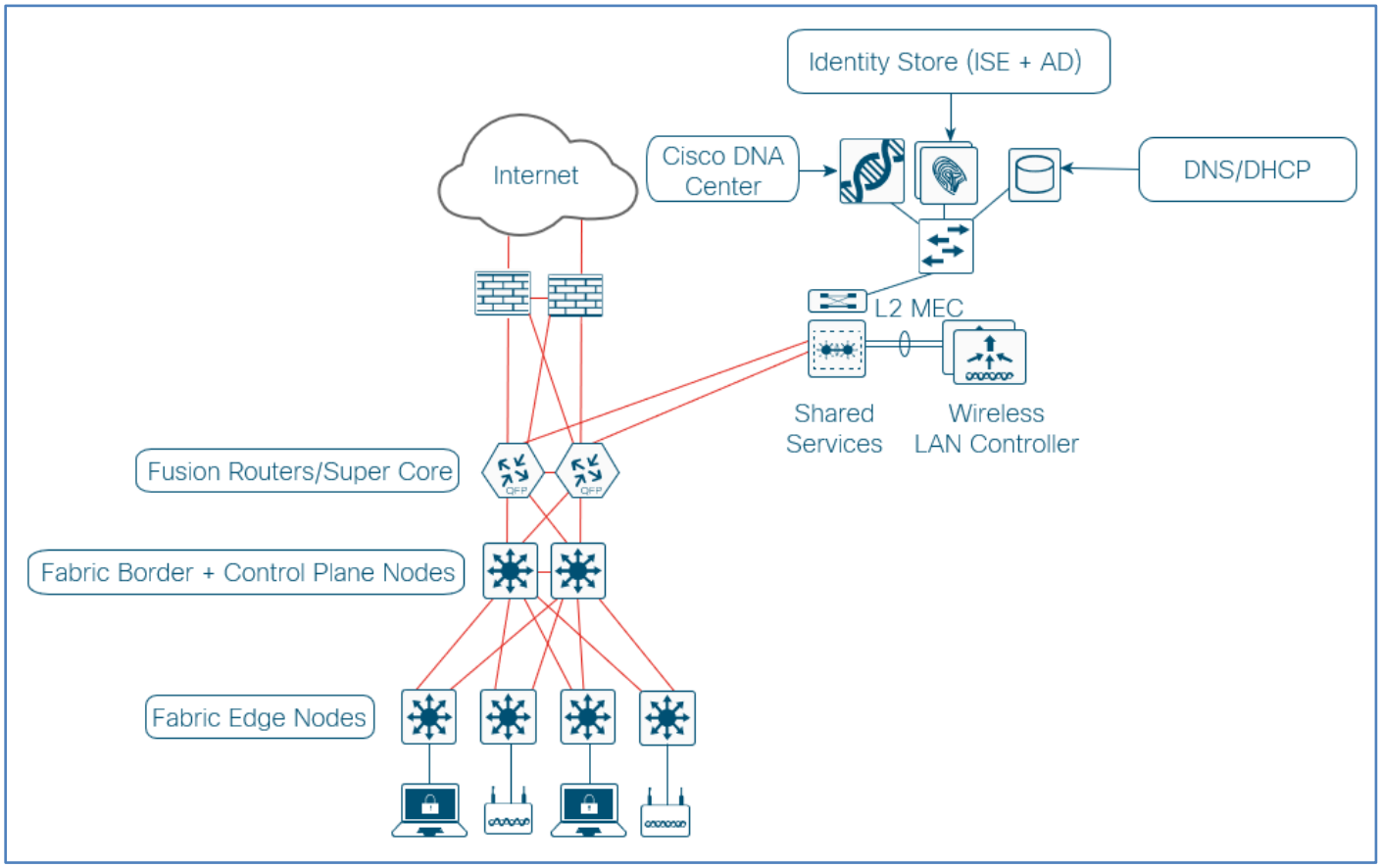
Scale Metrics and Latency Information

For scale metrics and latency information, please see the SD-Access Resources and Latency Design Guidance on Cisco Communities.

Design

This section provides an overview of the topology used throughout this guide as well as the routing modalities used to provide IP reachability.

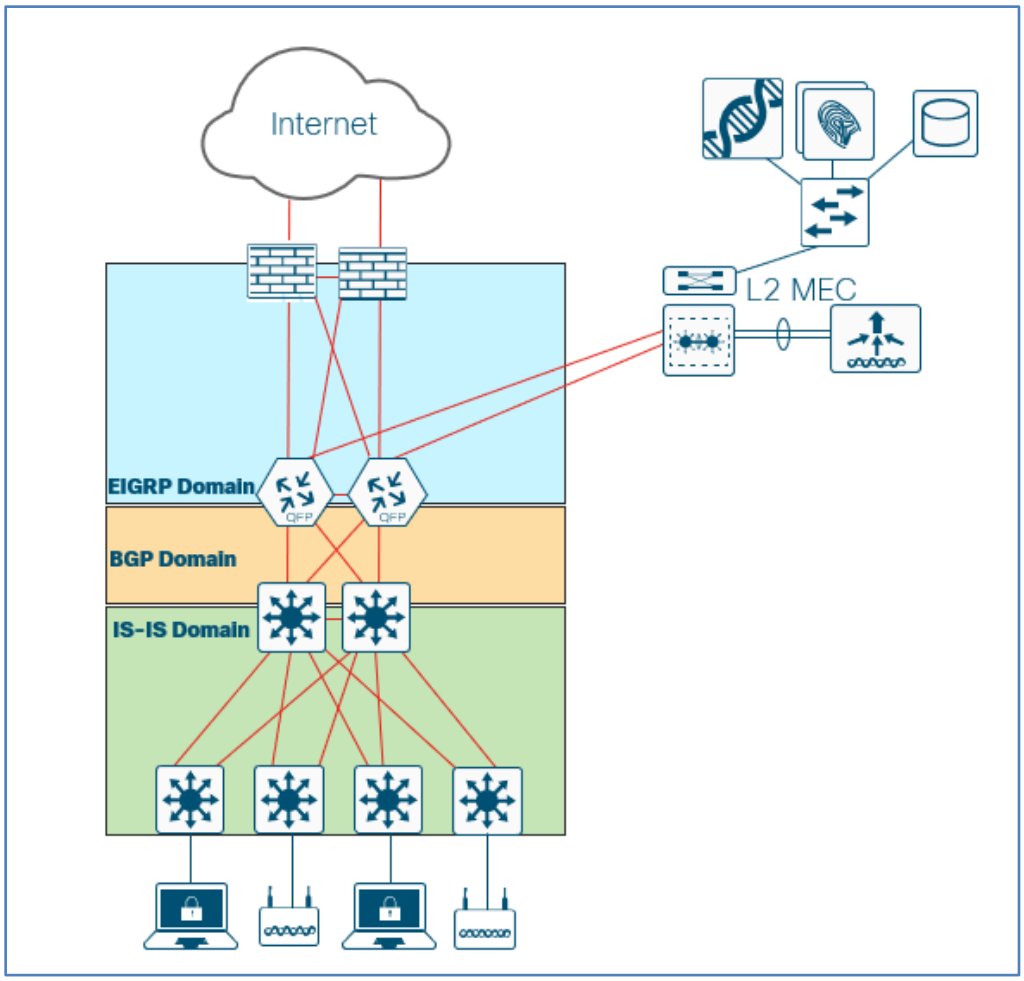
Figure 1. Validation topology



Tech tip
For diagram simplicity and ease of reading, the intermediate nodes (distribution layer) is not show in the topology. For ease of initial understanding, fabric border and control functionally will be collocated on the core switches.

The validation topology represents a medium site as described in the companion Software-Defined Access Solution Design Guide. It shows a single building with multiple wiring closets that is part of a larger multiple-building network that aggregates each building's core switches to a pair of super core routers. The shared services block contains a virtual switching system (VSS) Catalyst 6800 switch providing access to the Wireless LAN Controllers, Cisco DNA Center, the Identity Services Engine, Windows Active Directory, and DHCP/DNS servers.

Figure 2. Routing and Redistribution topology



The existing enterprise network deployment runs the Enhanced Interior Gateway Routing Protocol (EIGRP) as a routing protocol. This provides IP reachability between the super core routers, shared services, and the enterprise edge firewalls.

The building core switches operate as the fabric border and control plane nodes creating the northbound boundary of the fabric site. Taking advantage of the LAN automation capabilities of Cisco DNA Center, the network infrastructure southbound of the core switches run the Intermediate System to Intermediate System (IS-IS) routing protocol.

Between the fabric border and the super core, BGP is used. Routes from the existing enterprise network are mutually redistributed between EIGRP and BGP. A route-map with is used to set an arbitrary tag value to prevent redistribution routing loops between EIRGP and BGP when using multiple redistribution points. Routes from the SD-Access fabric site are mutually redistributed between IS-IS and BGP which in turn are redistributed into EIGRP allowing end-to-end IP reachability.

IP prefixes for shared services must be available to both the fabric underlay and overlay networks while maintaining isolation among overlay networks. To maintain the isolation, VRF-lite extends from the fabric border nodes to a set of fusion routers. The fusion routers implement VRF route leaking using a BGP route target import and export configuration. This is completed in later procedures after the fabric roles are provisioned.

For initial IP reachability between Cisco DNA Center and the fabric site, BGP is manually configured. Once a device is discovered and managed by Cisco DNA Center, it is recommended practice to not manually add configuration, particularly any configuration that might be overridden through the automated configuration placing the device in an unintended state. The exception is the manual IBGP configuration needed between redundant border nodes to help improve convergence times and provide alternative forwarding paths in certain upstream node or interface failure scenarios.

In deployments with multiple points of redistribution between several routing protocols, using BGP for initial IP reachability northbound of the border nodes helps ensure continued connectivity after the fabric overlay is provisioned without the need for additional manual redistribution commands on the border nodes. For additional detail and discussion, please see Appendix C.

Deploy

This section provides an example of using route redistribution to achieve IP reachability between Cisco DNA Center and the devices it will manage. It then demonstrates the workflow to manage devices beginning with the DESIGN and POLICY applications and continuing with device discovery, software image management (SWIM), and LAN Automation.

How to read deployment commands

The guide uses the following conventions for commands that you enter at the command-line interface (CLI).

Commands to enter at a CLI prompt:

```
configure terminal
```

Commands that specify a value for a variable (variable is in bold italics):

```
ntp server 10.4.0.1
```

Commands with variables that you must define (definition is bracketed in bold and italics):

```
router bgp [autonomous-system-number]
```

Commands at a CLI or script prompt (entered commands are in bold):

```
Router# enable
```

Long commands that line wrap on a printed page (underlined text is entered as one command):

```
monitor capture CAPTURE interface
GigabitEthernet1/0/1 both limit pps 10000
```

Process 1: Preparing for Network Management Automation

Get ready to deploy the network designs and policies by creating a functioning network underlay including device management connectivity. As part of the integration of ISE with Cisco DNA Center shown in the companion Software-Defined Access for Distributed Campus Prescriptive Deployment Guide, ISE is configured with TACACS infrastructure device administration support. For TACACS configurations, Cisco DNA Center modifies discovered devices to use authentication and accounting services from ISE and local failover serves by default. ISE must be prepared to support the device administration configurations pushed to the devices during the discovery process.

Procedure 1. Configure underlay network device management using the Cisco IOS Command Line Interface

Use a loopback interface on each device for Cisco DNA Center in-band discovery and management. The following steps configure point-to-point Ethernet connectivity between devices using IS-IS as the routing protocol and SSHv2 for device configuration using the device loopback interfaces. The SNMP configuration is pushed in a later procedure as part of device discovery.

Do not add a configuration to any devices that you intend to discover and configure using LAN Automation as part of a later procedure. Devices with existing configurations cannot be configured using LAN Automation. This example shows a configuration using Cisco IOS XE on a Cisco Catalyst switch.

Step 1. Use the device CLI to configure the hostname to make it easy to identify the device and disable unused services.

```
hostname [hostname]
no service config
```

Step 2. Configure local login and password.

```
username dna privilege 15 algorithm-type scrypt secret [password]
! older software versions may not support scrypt (type 9)
! username dna privilege 15 secret [password]
enable secret [enable password]
service password-encryption
```

Step 3. Configure Secure Shell (SSH) as the method for CLI management access.

```
ip domain-name ciscodna.net
! generate key with choice of modulus with a minimum of 2048 recommended
crypto key generate rsa modulus 2048
ip ssh version 2
line vty 0 15
  login local
  transport input ssh
  transport preferred none
```

Step 4. Configure the switch to support Ethernet jumbo frames. The MTU chosen allows for the extra fabric headers and compatibility with the highest common value across most switches, and the round number should be easy to remember when configuring and troubleshooting.

```
system mtu 9100
```

Tech tip
Underlay connectivity using Cisco IOS XE on routers requires the use of an **mtu** command at the interface configuration level, and Cisco Catalyst and Cisco Nexus® switches not using Cisco IOS XE use a **system jumbo mtu** command at the global configuration level.

Step 5. Configure the switch loopback address and assign SSH management to use it.

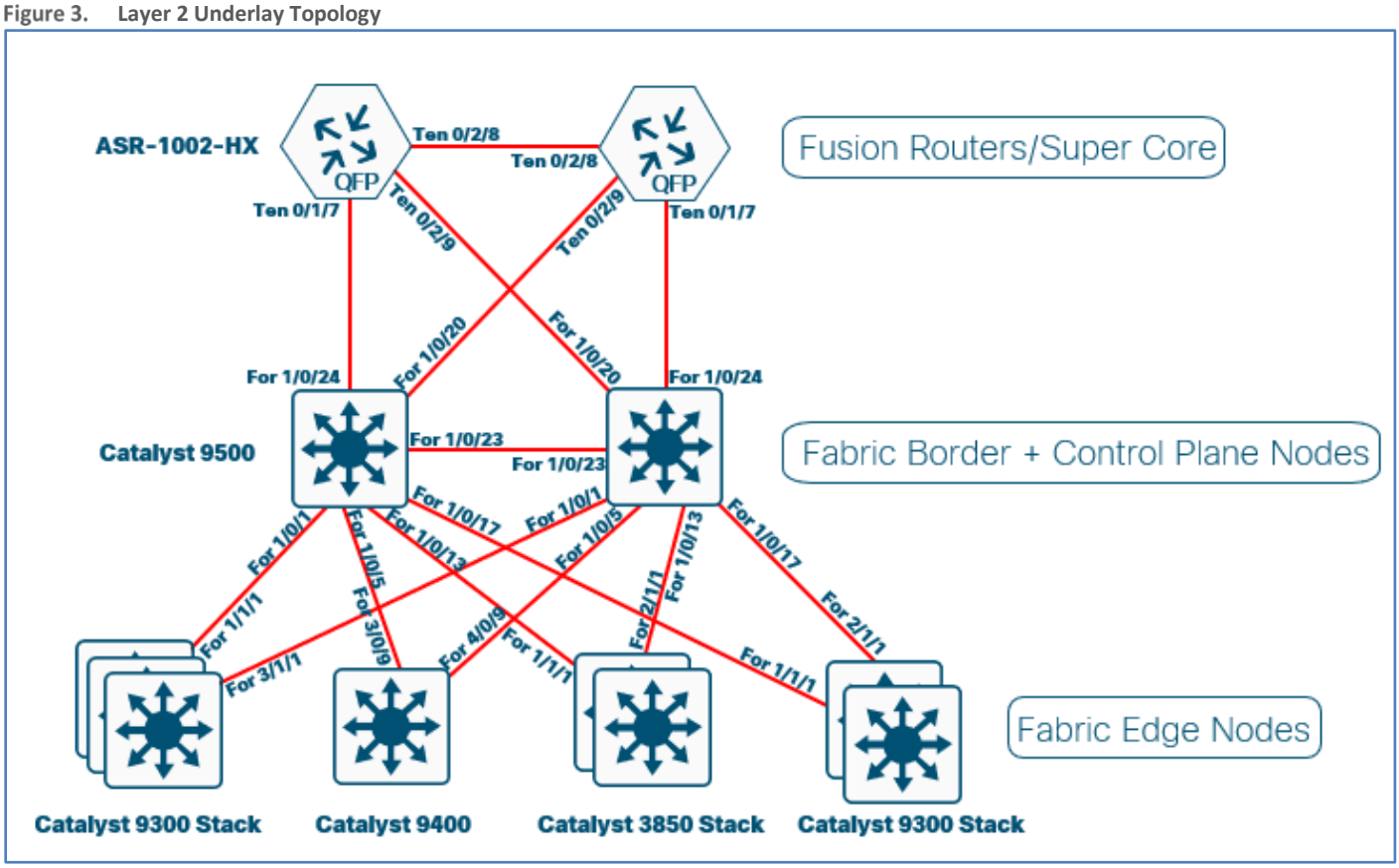
```
interface Loopback0
 ip address [Device loopback IP address] 255.255.255.255
```

Tech tip
Devices operating in a fabric role must have a /32 subnet mask for the IP address of their Loopback 0 interface. This /32 route must be present in the routing table of all fabric devices within the fabric site.

Procedure 2. Configure underlay network links for routed access connectivity

If your underlay network is already configured using a routed access network deployment model, skip this procedure. Typical Layer 2 deployments require this procedure. If LAN Automation will be used to onboard all directly connected switches, you may also skip this procedure.

Figure 3. Layer 2 Underlay Topology



Step 1. Configure the switch connections within the underlay network infrastructure. Repeat this step for every link to a neighbor switch within the fabric underlay. If the underlay device will be provisioned as a fabric border node and the connection is to be used as a handoff from the fabric to the external infrastructure, then use the next procedure instead.

```
interface fortyGigabitEthernet1/0/1
 no switchport
 ip address [Point-to-point IP address] [netmask]
```

Step 2. Enable IP routing and enable the IS-IS routing protocol on the switch.

```
! ip routing is not enabled by default on some switches
ip routing
ip multicast-routing
ip pim register-source Loopback0
ip pim ssm default
router isis
 net 49.0000.0100.0400.0001.00
 domain-password [domain password]
 metric-style wide
 nsf ietf
 log-adjacency-changes
```

```
bfd all-interfaces
```

Tech tip

If multicast communication is required outside of the border nodes towards the fusion routers (the multicast source is outside of the fabric site), the following multicast commands should be enabled on each border node in global configuration mode.

```
ip multicast-routing
ip pim register-source Loopback0
ip pim ssm default
```

And the following commands should be enabled at each interface or subinterface (for each virtual network):

```
ip pim sparse-mode
```

Step 3. Enable IS-IS routing on all configured infrastructure interfaces in the underlay, except for the border handoff interfaces, which are configured in the next procedure. The loopback interface is enabled to share the management IP address and the physical interfaces are enabled to share routing information with the connected infrastructure.

```
interface Loopback0
! ip address assigned in earlier step
 ip router isis
 ip pim sparse-mode
interface range fortyGigabitEthernet1/0/1, fortyGigabitEthernet1/0/5,
fortyGigabitEthernet1/0/13, fortyGigabitEthernet1/0/17
! routed ports with ip addresses assigned via earlier steps
 ip router isis
 isis network point-to-point
 ip pim sparse-mode
 logging event link-status
 load-interval 30
 bfd interval 100 min_rx 100 multiplier 3
 no bfd echo
 dampening
```

Procedure 3. Enable routing connectivity at border toward external router neighbor

If your underlay network is already configured as a routed access network and integrated with the rest of your network using BGP using an 802.1Q handoff as described in the Design section and Appendix C, skip this procedure.

The external device outside of the fabric site handling routing among multiple virtual networks and a global routing instance acts as a fusion router for those non-fabric networks. The separation of connectivity is maintained using VRFs connected by 802.1Q-tagged interfaces between the fusion router and border nodes, also known as VRF-lite. Establishing the underlay connectivity using BGP allows Cisco DNA Center to manage initial discovery and configuration using the link, and then to use the same physical link with additional 802.1Q tags and BGP sessions for overlay VN connectivity.

Configuring BGP to allow Cisco DNA Center IP reachability to the underlay network devices while allowing further provisioning for virtual networks on the interfaces helps minimizes disruption to network connectivity.

Common network services such as DNS, DHCP, WLCs, and Cisco DNA Center are generally deployed outside the fabric site. To connect the SD-Access network to these services, extend your existing enterprise network to the border nodes as shown in later procedures.

Step 1. For each border node, if you are configuring a switch supporting VLAN trunk interfaces such as Cisco Catalyst 9000, 3800, or 6800 Series switches, you must configure a trunk on the connected interface with a dedicated VLAN to establish underlay connectivity for route peering to the fusion router.

```
vlan 100
interface vlan100
 ip address [IP address] [netmask]
 ip pim sparse-mode
 no shutdown
interface FortyGigabitEthernet1/0/24
 switchport
 switchport mode trunk
 switchport trunk allowed vlan add 100
 no shutdown
```

Tech tip
VLAN IDs below 1000 are recommended to avoid overlap with Cisco DNA Center provisioning reserved VLANs.

Tech tip

If your border nodes are ASR or ISR routers, use an alternative subinterface configuration rather than a switch trunk to establish underlay connectivity to the fusion router.
`interface TenGigabitEthernet0/1/0`
`  no shutdown`
`!`
`interface TenGigabitEthernet0/1/0.100`
`  encapsulation dot1Q 100`
`  ip address [IP address] [netmask]`
`  ip pim sparse-mode`
`  no shutdown`

Step 2. Connect the redundant border nodes to each other with at least one routed interface for underlay communication and later IBGP peering. The configuration for integrating into the IS-IS protocol is shown. Repeat this step for each interface connecting redundant border nodes.

```
interface FortyGigabitEthernet1/0/23
 no switchport
 ip address [Point-to-point IP address] [netmask]
 ip router isis
 isis network point-to-point
```

```
 ip pim sparse-mode
 logging event link-status
 load-interval 30
no shutdown
```

Step 3. On each border node, enable BGP routing to the fusion router for connectivity to networks external to the fabric. Repeat this step for each border node.

```
router bgp [underlay AS number]
 bgp router-id [interface]
 bgp log-neighbor-changes
! fusion router is an eBGP neighbor
 neighbor [fusion interface IP address] remote-as [external AS number]
! redundant border is an iBGP neighbor
 neighbor [redundant border Lo0 address] remote-as [underlay AS number]
 neighbor [redundant border Lo0 address] update-source Loopback0
 !
 address-family ipv4
  network [Lo0 IP address] mask 255.255.255.255
 ! advertise underlay IP network summary in global routing table
  aggregate-address [underlay IP network summary] [netmask] summary-only
  redistribute isis level-2
  neighbor [fusion interface IP address] activate
  neighbor [redundant border Lo0 address] activate
 exit-address-family
```

Example Border Node Configuration

```
router bgp 65514
 bgp router-id Loopback0
 bgp log-neighbor-changes
! fusion router is an eBGP neighbor
 neighbor 10.4.2.65 remote-as 65000
! redundant border is an iBGP neighbor
 neighbor 10.4.14.4 remote-as 65514
 neighbor 10.4.14.4 update-source Loopback0
 !
 address-family ipv4
  network 10.4.14.3 mask 255.255.255.255
 ! advertise underlay IP network summary in global routing table
  aggregate-address 10.4.14.0 255.255.255.0 summary-only
  redistribute isis level-2
  neighbor 14.4.2.65 activate
  neighbor 10.4.14.4 activate
 exit-address-family
```

Procedure 4. Redistribute shared services subnets into underlay IGP

A default route in the underlay cannot be used by the APs to reach the WLC. A more specific route (such as a /24 subnet or /32 host route) to the WLC IP address must exist in the global routing table at each node where the APs are physically connected. Permit the more specific routes for the WLC and DHCP shared services needed from BGP (examples: 10.4.174.0/24 and 10.4.48.0/21) into the underlay network through redistributing the shared services route at the border into the underlay IGP routing process using this procedure. Using this process, the prefixes used match prefixes in the BGP routing table.

Step 1. Connect to each border node and add a prefix-list and route-map for subnets used for the shared services.

```
ip prefix-list SHARED-SERVICES-NETS seq 5 permit 10.4.48.0/21
ip prefix-list SHARED-SERVICES-NETS seq 10 permit 10.4.174.0/24
route-map GLOBAL-SHARED-SERVICES-NETS permit 10
 match ip address prefix-list SHARED-SERVICES-NETS
```

Step 2. At each border node, redistribute the prefixes into your underlay routing protocol. This example assumes ISIS.

```
router isis
 redistribute bgp [underlay AS number] route-map GLOBAL-SHARED-SERVICES-NETS metric-type external
```

Procedure 5. Enable connectivity at external fusion router towards border neighbor

The fusion routers connected to your fabric border routers require CLI configuration for underlay connectivity consistent with the previous procedures. Follow this procedure at each external fusion router device that is connected to a border node.

The example fusion router is configured with a VRF (VRF-GLOBAL-ROUTES) containing the enterprise-wide global routes. The fusion router uses this VRF to peer with the global routing table on the fabric border for the underlay reachability.

An alternative approach is to place the enterprise-wide routes in the global routing table on the fusion router and peer with the fabric border without using a VRF.

Step 1. On each external fusion router, create the VRF, route distinguisher, and route targets for the initial management connectivity to the border.

```
vrf definition VRF-GLOBAL-ROUTES
 rd 100:100
 address-family ipv4
  route-target export 100:100
  route-target import 100:100
exit-address-family
```

Step 2. For each interface on the fusion router connected to a fabric border, enable the interface, VLAN-tagged subinterface, and IP addressing. This example uses 802.1Q VLAN tagging on a router with subinterfaces. For switches, which require trunk port configurations, match the corresponding configuring completed in previous procedures.

```
interface TenGigabitEthernet0/1/7
 description Connected to D2-9500-1.ciscodna.net Border
 mtu 9100
 no ip address
 no shutdown
interface TenGigabitEthernet0/1/7.100
 encapsulation dot1Q 100
 vrf forwarding VRF-GLOBAL-ROUTES
```

```
ip address [IP network] [netmask]
```

IP connectivity is now enabled for the VLAN (example: 100) on the 802.1Q tagged connection between the fusion router and the border node.

Step 3. Create route maps to tag routes and avoid routing loops when redistributing between the IGP used within the rest of the network and BGP when connecting using multiple links. IGPs can vary—the example shown is for EIGRP, completing the routing connectivity from IS-IS to BGP to EIGRP.

```
route-map RM-BGP-TO-EIGRP permit 10
 set tag 100
!
route-map RM-EIGRP-TO-BGP deny 10
 match tag 100
route-map RM-EIGRP-TO-BGP permit 20
```

Step 4. Enable BGP peering from redundant fusion routers to the border nodes and redistribute the IGP that is used to reach the networks beyond the fusion routers.

```
router bgp [AS number]
 bgp router-id [loopback IP address]
 bgp log-neighbor-changes

address-family ipv4 vrf VRF-GLOBAL-ROUTES
  redistribute eigrp 100 route-map RM-EIGRP-TO-BGP
  neighbor [redundant fusion IP] remote-as [external AS number]
  neighbor [redundant fusion IP] activate
  neighbor [border IP address] remote-as [underlay AS number]
  neighbor [border IP address] activate
    default-information originate
 exit-address-family
```

Example BGP Configuration on Fusion Router

```
router bgp 65500
 bgp router-id 10.4.0.1
 bgp log-neighbor-changes
 !
address-family ipv4 vrf VRF-GLOBAL-ROUTES
  redistribute eigrp 100 route-map RM-EIGRP-TO-BGP
  neighbor 10.4.0.2 remote-as 65500
  neighbor 10.4.0.2 activate
  neighbor 172.16.172.29 remote-as 65514
  neighbor 172.16.172.29 activate
  default-information originate
 exit-address-family
```

Step 5. Redistribute BGP into the IGP to enable reachability. IGPs can vary—the example shown is for EIGRP Named Mode.

```
router eigrp [name]
  address-family ipv4 unicast vrf [VRF] autonomous-system [AS number]
  topology base
   redistribute bgp [AS number] metric 1000000 1 255 1 9100 route-map [route-map]
  exit-af-topology
  network [external IP network address] [netmask]
  eigrp router-id [loopback IP address]
 exit-address-family
```

Example Redistribution Configuration on Fusion Router

```
router eigrp LAN
 address-family ipv4 unicast vrf VRF-GLOBAL-ROUTES autonomous-system 100
  topology base
   redistribute bgp 65000 metric 1000000 1 255 1 9100 route-map
    RM-BGP-TO-EIGRP
  exit-af-topology
  network 10.4.0.0.0.255.255
  eigrp router-id 10.4.0.1
 exit-address-family
```

Procedure 6. Configure MTU and routing on intermediate devices

Optional

It is an advantage to have Cisco DNA Center manage all devices in a fabric domain. Cisco DNA Center already manages fabric edge nodes and border nodes; however, if you have intermediate devices within the fabric site that will not be operating in a fabric role, then the devices must still meet the requirements for transporting SD-Access traffic. The primary requirements are that they:

- Must be Layer 3 devices that are actively participating in the routing topology within the other fabric underlay devices.
- Must be able to transport the jumbo frames that are offered by the fabric encapsulation techniques.

For fabric intermediate node devices, you must set an appropriate MTU (example: 9100) and manually configure routing with the other devices in the underlay. Configuration guidance for this situation is device-specific and not discussed further in this guide.

Do not add a configuration to any devices that you intend to discover and configure using LAN Automation as part of a later procedure. Devices with existing configurations cannot be configured using LAN Automation.

Process 2: Using Cisco DNA Center for Initial Network Design and Discovery

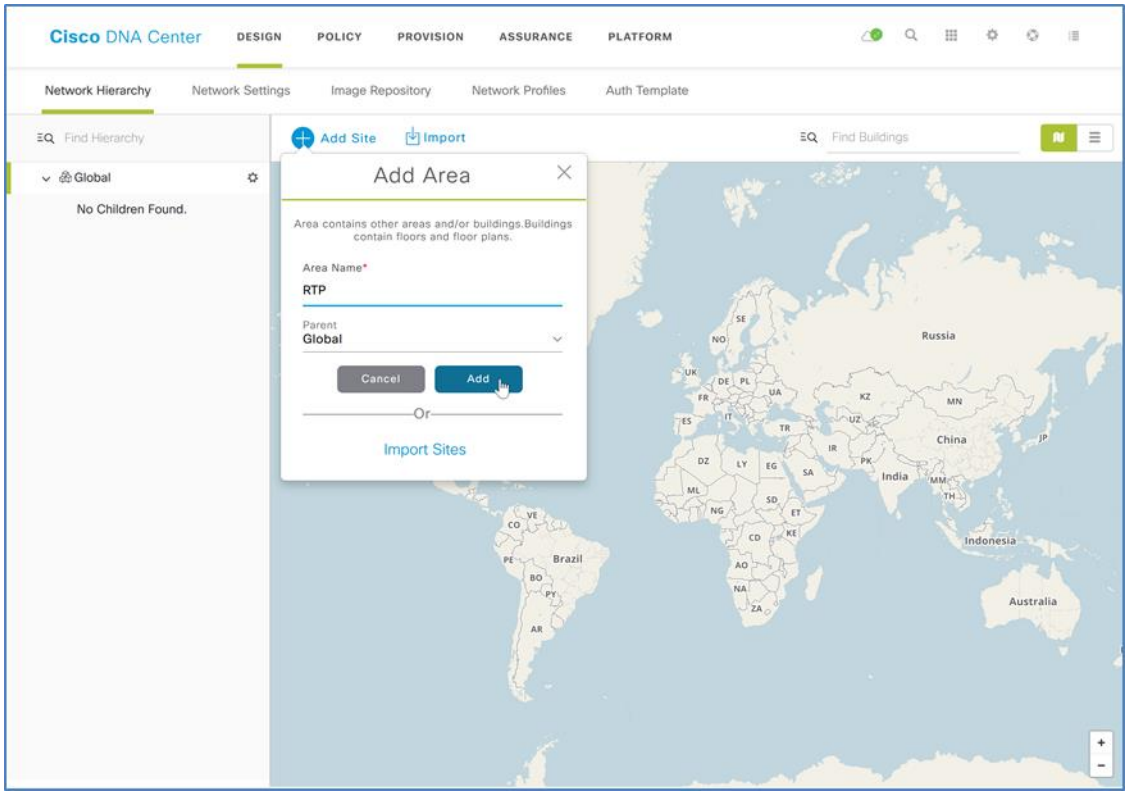
Cisco DNA Center provides a robust Design Application to allow customers of varying sizes and scales to easily define their physical sites and common resources. Using a hierarchical format that is intuitive to use, the Design Application removes the need to redefine the same resources, such as DHCP, DNS, and AAA servers, in multiple places when provisioning devices. The network hierarchy created in the Design Application should mimic the actual, physical network hierarchy of your deployment.

Using Cisco DNA Center, you create a network hierarchy of areas that can contain additional sub-areas, buildings, and floors within areas. In later steps, devices are assigned into the buildings and floors and then provisioned with the network services described in the next procedure.

Procedure 1. Create network sites

Step 1. Log in to Cisco DNA Center. From the main Cisco DNA Center dashboard, navigate to **DESIGN** > **Network Hierarchy**.

Step 2. Click **Add Site**, in the drop-down menu select **Add Area**, supply an appropriate **Area Name**, and then click **Add**.



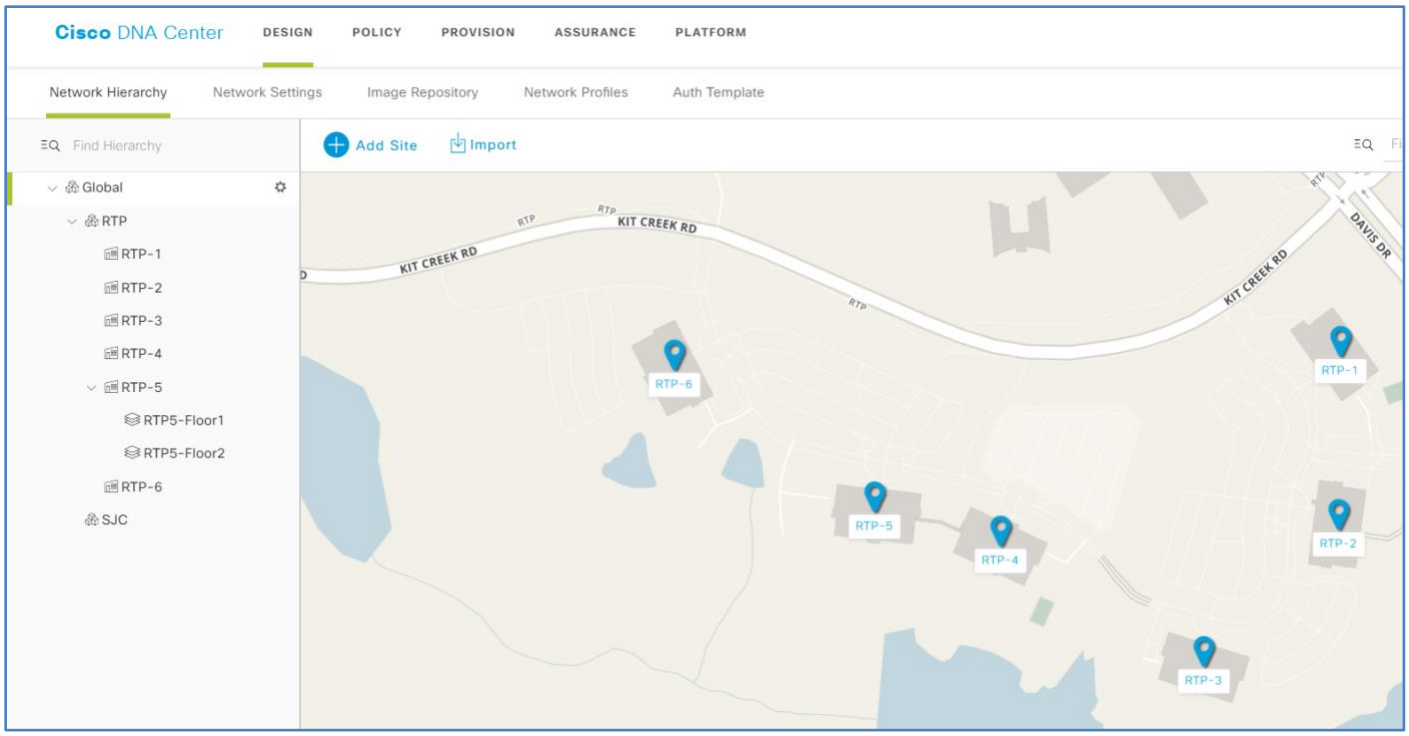
Step 3. Click **Add Site**, in the drop-down menu select the **Add Building** button, supply an appropriate **Building Name**, select the site created in the previous step as the **Parent**, complete the wizard to assign a location, and then click **Add**.

To add a building, you can use an approximate street address near the building within the wizard and, if desired, refine the building position on the map by clicking the target location.

Step 4. Repeat the previous step as required to add sites and buildings, creating a hierarchy that represents the actual, physical network hierarchy of the deployment.

Step 5. If you are integrating wireless to a building or require more granularity for network choices within a building, select the building on the map (or select the gear icon next to a building in the hierarchy), choose **Add Floor**, and complete the wizard with the details.

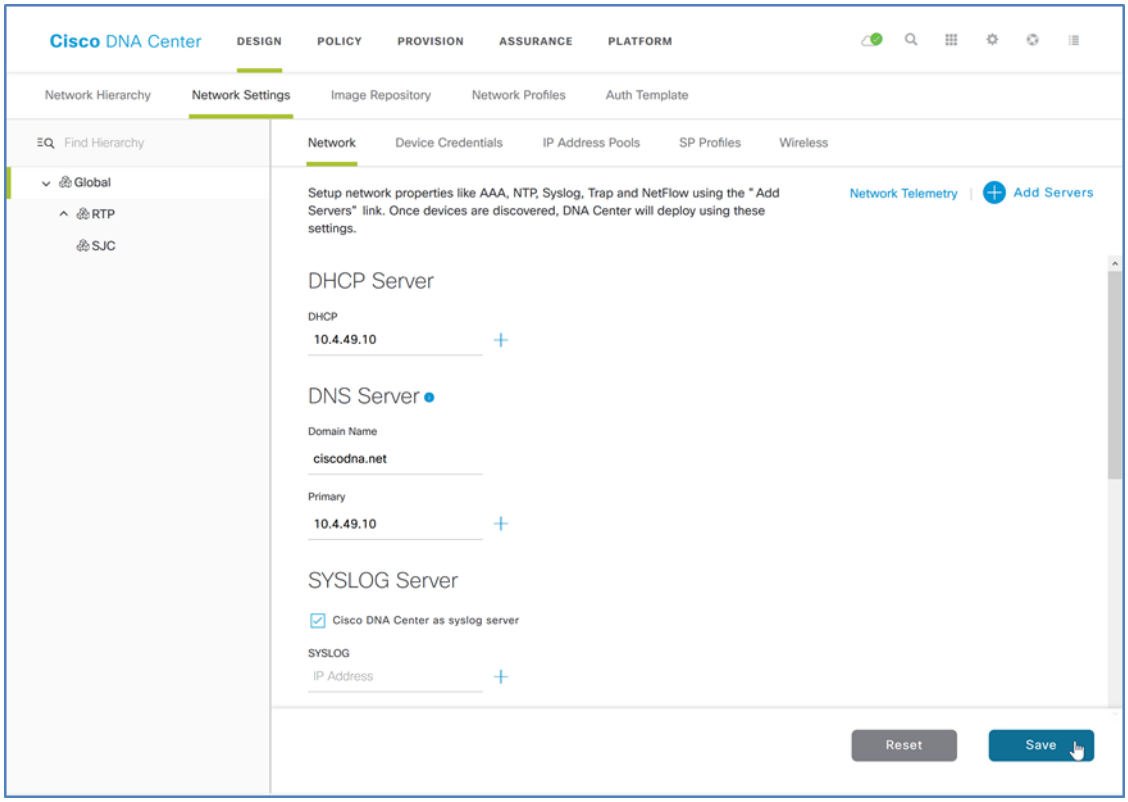
Floors are referenced during the wireless provisioning, as Access Points must be assigned to building floors in the hierarchy. If you have floor map diagrams in DXF, DWG, JPG, GIF, or PNG formats, add them to any defined floors as a useful component for wireless deployments.



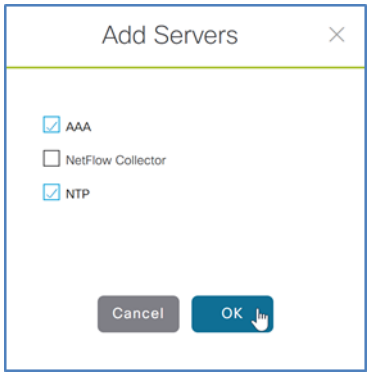
Procedure 2. Configure network services for sites

Configure AAA, DHCP, and DNS services that align to the hierarchy in Cisco DNA Center. If the services use the same servers across the complete hierarchy, then you can configure them globally, and the inheritance properties of the hierarchy makes the global settings available to all sites. Differences for individual sites can then be applied on a site-by-site basis. This procedure shows the configuration globally.

Step 1. Within Cisco DNA Center, navigate to **DESIGN > Network Settings > Network**. Within the left pane in the site hierarchy, select the appropriate level (example: Global), fill in the **DHCP Server** IP address (example: 10.4.49.10), under DNS Server fill in the Domain Name (example: ciscodna.net) and server **Primary** IP Address (example: 10.4.49.10), add any redundant or additional servers (you can leave the default selections to use Cisco DNA Center for the SYSLOG and SNMP server), and then click **Save**.



Step 2. Near the top, next to **Network Telemetry**, click the **+ Add Servers** button, select the **AAA** and **NTP** check boxes, and then click **OK**.



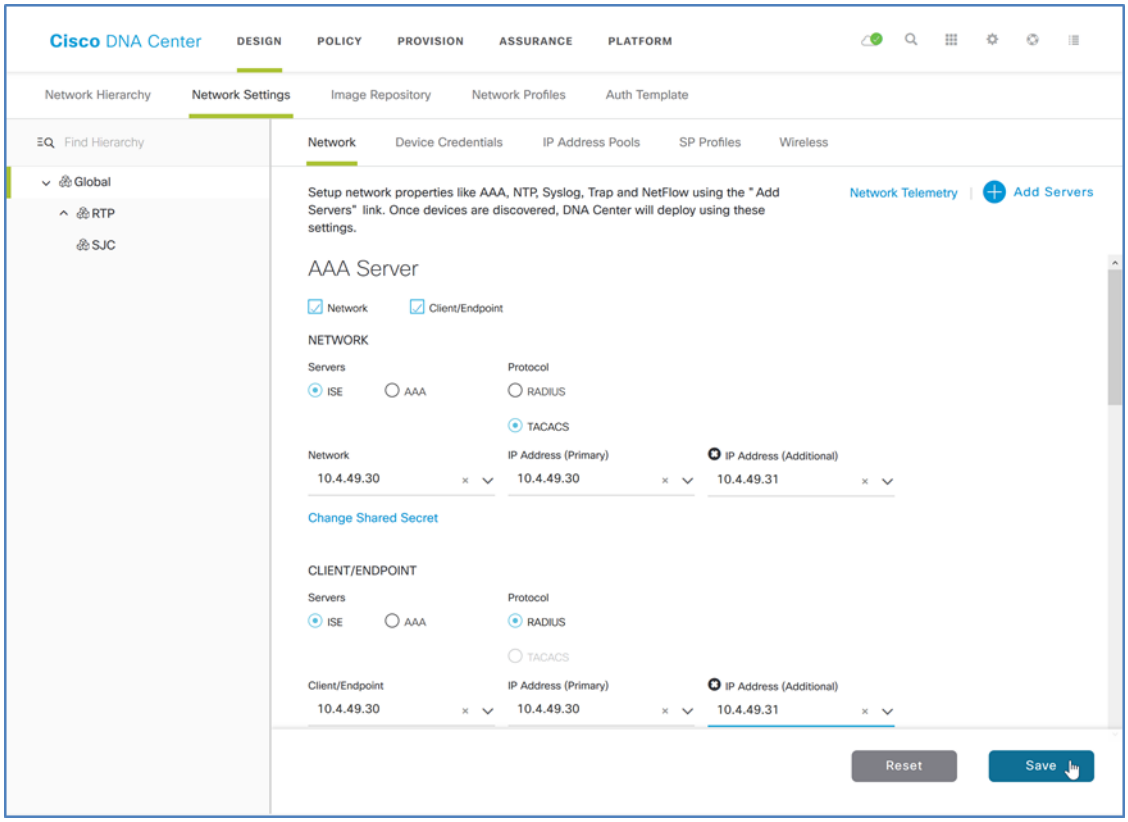
The configuration pane is updated with **AAA Server** and **NTP Server** as available configuration sections. You configure AAA services for both the network infrastructure device administration and the client endpoints connecting to the infrastructure. For this example, the high-availability standalone ISE nodes are used.

Tech tip
Many organizations use TACACS+ for infrastructure device administration support. If you intend to enable TACACS+ on the same ISE server being used for RADIUS client authentication, then you integrate it with Cisco DNA Center during this step also by using the **View Advanced Settings** drop down menu. You can find ISE configuration information for enabling TACACS+ integration by navigating within ISE to **Work Centers > Device Administration > Overview**. For additional information, please see Appendix B.

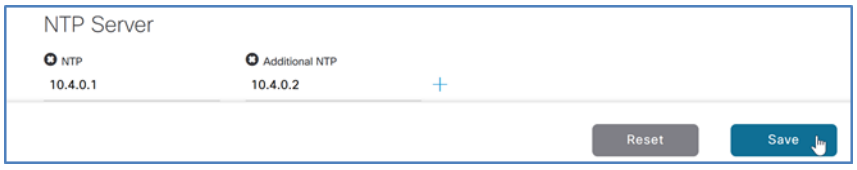
Step 3. Under **AAA Server** select the **Network** and **Client/Endpoint** check boxes, under **NETWORK**, select the **ISE** radio button, under **Network** use the pull-down to select the prepopulated ISE server (example:10.4.49.30), under **Protocol**, select the **TACACS** radio button, under **IP Address (Primary)** use the second pull-down to select the primary ISE server (example: 10.4.49.30), click the plus sign (**+**) button, and then under the **IP Address (Additional)** pull-down select the redundant ISE server node (example: 10.4.49.31).

To ensure ISE server redundancy is properly enabled, verify that the primary and additional IP addresses are displayed along with the selected network address before continuing.

Step 4. Under **CLIENT/ENDPOINT** and **Servers**, select the **ISE** radio button, under **Client/Endpoint**, use the pull-down to select the prepopulated ISE server. Under **Protocol**, select the **RADIUS** radio button, under **IP Address (Primary)** use the pull-down to select the primary ISE server, click the plus sign (**+**) button, and then under **IP Address (Additional)** use the pull-down to select the redundant ISE server node, and then click **Save**.



Step 5. On the same screen, scroll down to **NTP Server**, add the **IP Address** of the NTP server (example: 10.4.0.1), if you have one or more additional NTP servers, select the plus sign (**+**) button, and then in the **Additional NTP** add the IP address of the redundant NTP servers (example:10.4.0.2), and then click **Save**.



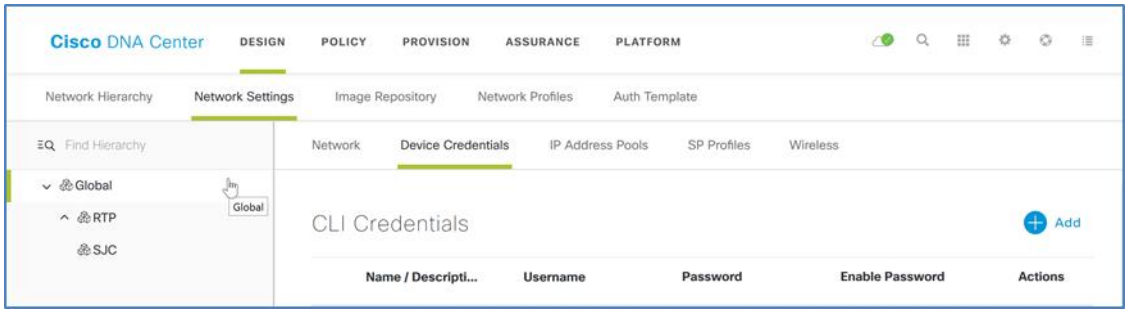
The ISE servers for AAA, and the servers for DHCP, DNS, and NTP for the selected level in the site hierarchy, are all saved to be used during fabric provisioning.

Procedure 3. Add device credentials for discovery and management

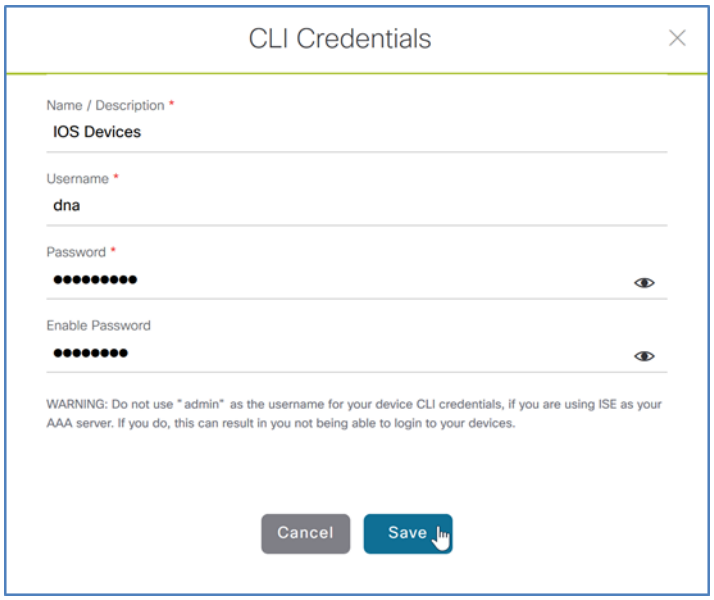
When you deploy the SD-Access underlay using devices that are already configured and which are network reachable by Cisco DNA Center, you discover and manage the devices by supplying the CLI and Simple Network Management Protocol (SNMP) credentials.

As an option, you can deploy LAN switches without existing configurations into the underlay by using the Cisco DNA Center LAN Automation capabilities. Cisco Network Plug and Play (PnP) is the mechanism enabling connectivity and initial configuration for supported switches. For LAN Automation deployments, you also supply CLI and SNMP credentials to access and prepare one or more supported PnP seed devices, such as Cisco Catalyst 9500 Series Switches in a distribution or core. LAN Automation discovers switches directly connected to chosen seed device interfaces and their immediate neighbor switches using Cisco Discovery Protocol, all of which must be running the PnP agent and have no previous configuration. The credentials supplied allow Cisco DNA Center and seed devices to work together to configure the discovered devices and add them into managed inventory. These credentials are used for discovery and, later, for management of the network.

Step 1. Within Cisco DNA Center, navigate to **Design > Network Settings > Device Credentials** and select an appropriate level of the site hierarchy in the left pane (example: Global, for common credentials across the hierarchy).



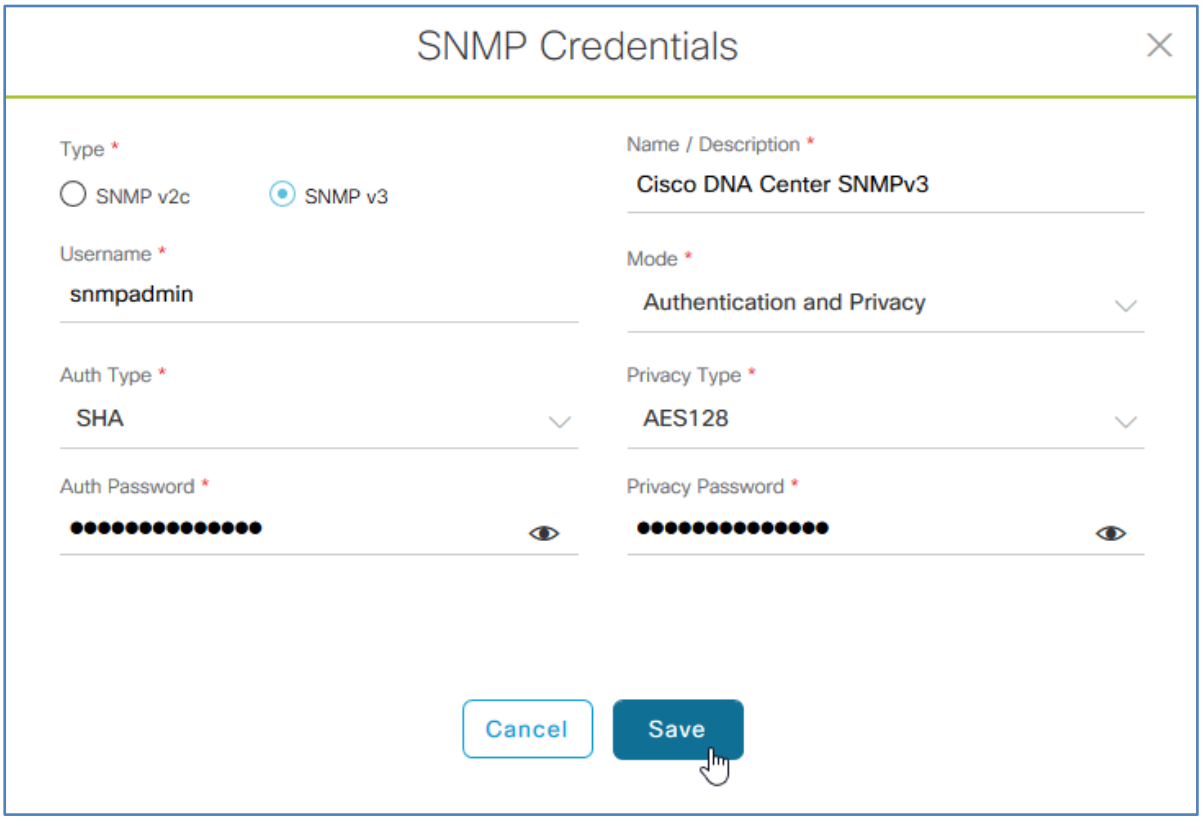
Step 2. At the top of the **CLI Credentials** section, click **Add**, complete the **Name / Description** (example: IOS Devices), **Username**, **Password**, and **Enable Password** fields, and click **Save**.



Caution

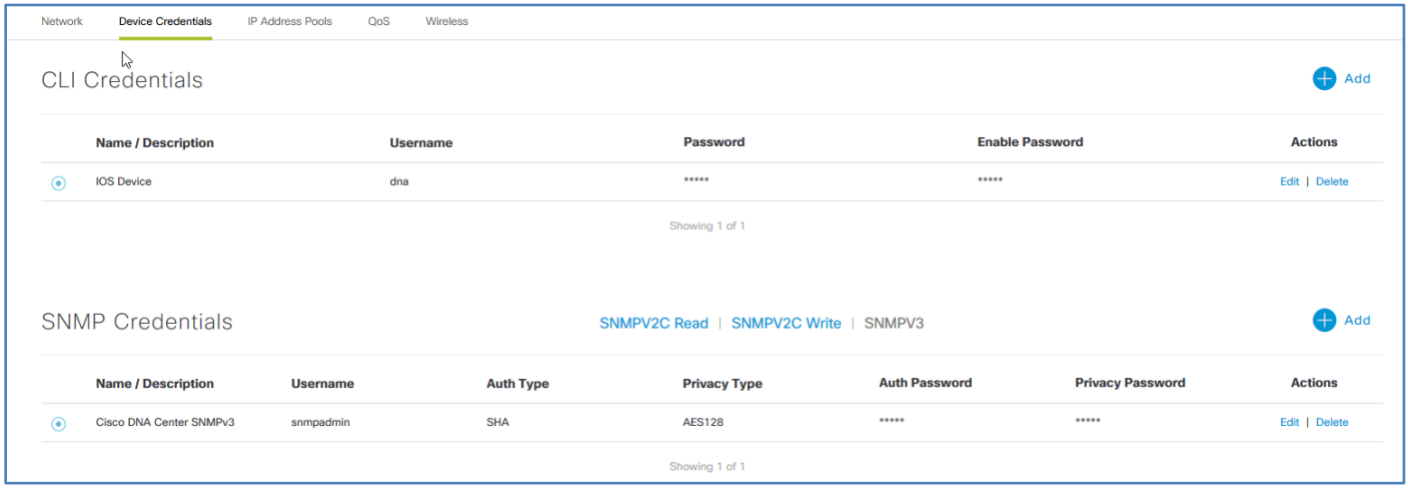
If you are using ISE as your AAA server, avoid using **admin** as the username for device CLI credentials, which can lead to username conflicts with the ISE administrator login, resulting in the inability to log in to devices.

Step 3. At the top of the **SNMP Credentials** section, select an SNMP credential type to update (example: SNMPV3). Click **Add**, select the radio button in the row next to the credential to update (a single credential per row at a time), fill out the credential details (minimum twelve character passwords are recommended to be compatible with Cisco WLCs), and then click **Save**.



Step 4. Repeat steps 2 and 3 for any additional credentials required in the hierarchy. **CLI Credentials** and either **SNMPV3** or both **SNMPV2C Read** and **SNMPV2C Write** are required.

Step 5. For each of the CLI and SNMP credentials assigned, click all radio buttons next to each assignment created. After each selection, at the bottom of the Device Credentials screen, click **Save**. If you have used more than one SNMP credential type, repeat this step by toggling to each of the SNMP credential options, click the radio button next to the option, and then click **Save**.



A Created Common Settings Successfully acknowledgment is displayed. The device credentials to be used for network discovery and management are now available in Cisco DNA Center.

Procedure 4. Define global IP address pools

Define IP addresses for your networks by manually assigning them in Cisco DNA Center. Optionally, push the IP address assignments to an IP address manager (IPAM) (examples: Infoblox, Bluecat) by integrating the IPAM through APIs. You integrate with an IPAM by navigating to the **System Settings > Settings > IP Address Manager** and filling out the form with the specifics of your IPAM provider. IPAM integration is not used in this example. You manually configure IP addressing and DHCP scopes on your DHCP servers to correspond to assignments in Cisco DNA Center.

DHCP scopes configured on the DHCP server should support the address allocations and any additional DHCP options required to make a device work. For example, some IP telephony vendors require specific DHCP options to enable their devices to function correctly (example: DHCP Option 43 for Access Points to associate with their corresponding WLC).

This procedure shows how to manually define the IP address pools that are used during the pool reservation process. These pools are assigned to the sites in your network, and the assignment steps are required for both manual and integrated IPAM deployments. You have the flexibility to create a larger global pool and then reserve a subset of a pool at lower levels in the hierarchy. IP address pools are created only at the global level, and you reserve addresses at lower levels in the hierarchy.

The deployment described in this guide uses the global address pools listed in the Table 1. Larger global address pools support many smaller address space reservations throughout the site hierarchy, as shown with the Table 2.

Table 2. Example global address pools

Pool name	Network/mask	IP gateway	DHCP server	DNS server
TEN_SLASH_EIGHT	10.0.0.0/8	10.0.0.1	10.4.49.10	10.4.49.10
ONE_SEVEN_TWO_SLASH_TWELVE	172.16.0.0/12	172.16.0.1	10.4.49.10	10.4.49.10

Table 3. Example address pool reservations from global pool

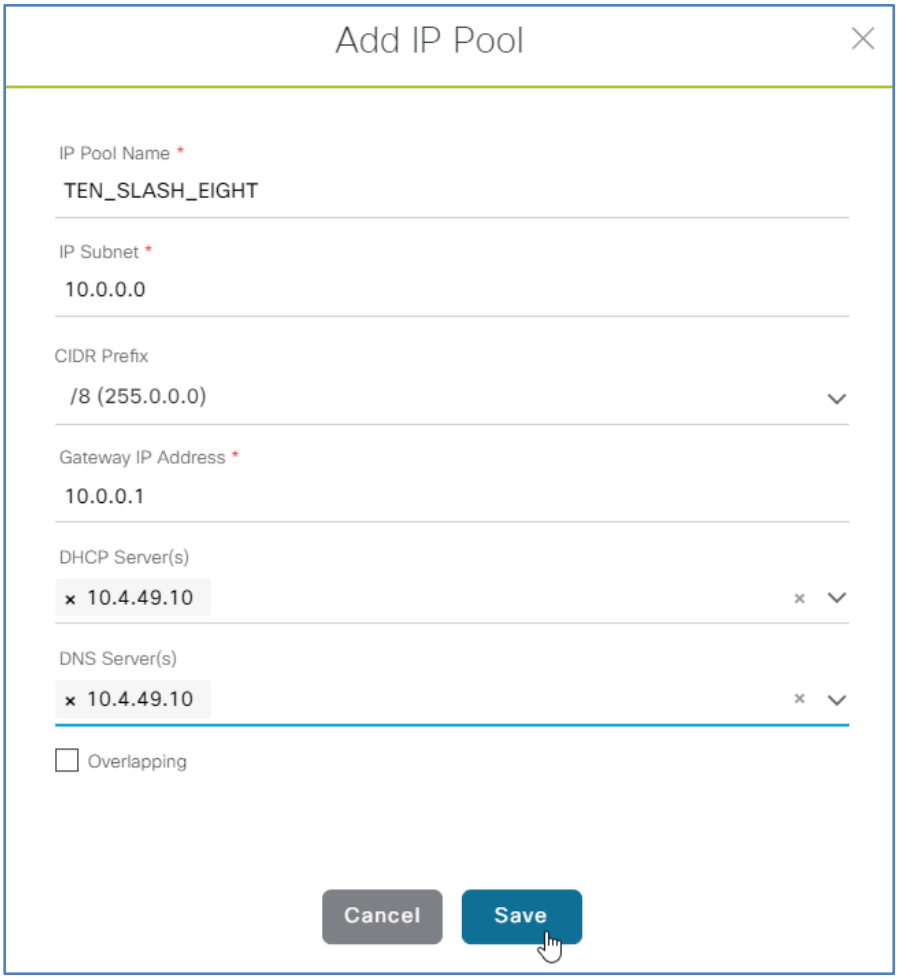
Pool name	Network/mask	IP gateway	DHCP server	DNS server
EMPLOYEE_DATA_RTP-5	10.101.114.0/24	10.101.114.1	10.4.49.10	10.4.49.10
EMPLOYEE_PHONE_RTP-5	10.101.214.0/24	10.101.214.1	10.4.49.10	10.4.49.10
BUILDING_CONTROL_RTP-5	10.102.114.0/24	10.102.114.1	10.4.49.10	10.4.49.10
GUEST_RTP-5	10.103.114.0/24	10.103.114.1	10.4.49.10	10.4.49.10
LAN_AUTOMATION_RTP-5	10.5.100.0/24	10.5.100.1	10.4.49.10	10.4.49.10
BORDER_HANDOFF_RTP-5	172.16.172.0/24	—	—	—
MULTICAST_PEER_RTP-5	172.16.173.0/24	—	—	—
ACCESS_POINT_RTP-5	172.16.174.0/24	172.16.174.1	10.4.49.10	10.4.49.10

Tech tip

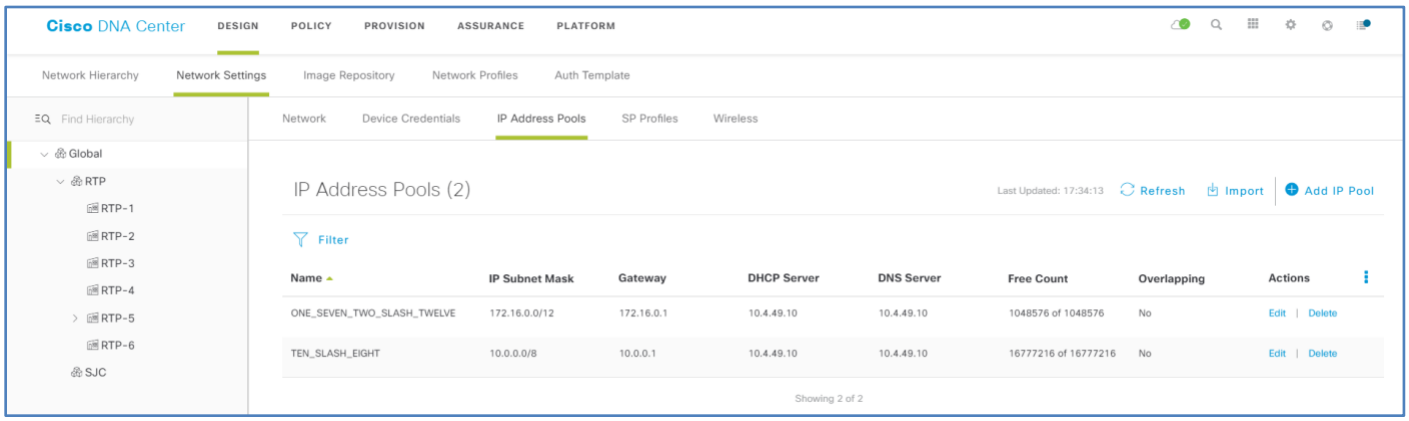
IP Pool names support letters, numbers, hyphens, underscores, periods, and forward slashes only. Other characters and spaces are not supported.

IP gateways, DHCP, and DNS servers should be defined for all IP pools that will be used for endpoints and clients in the network.

Step 1. Add a global pool in Cisco DNA Center by navigating to **DESIGN > Network Settings > IP Address Pools**. In the site hierarchy on the left, select **Global**, and click **+ Add IP Pool**. Fill in the **IP Pool Name**, **IP Subnet**, **CIDR Prefix**, and **Gateway IP Address**. Use the drop-down menus to assign the **DHCP Server(s)** and **DNS Server(s)**. Do not select **Overlapping**. When you are done, click **Save**.



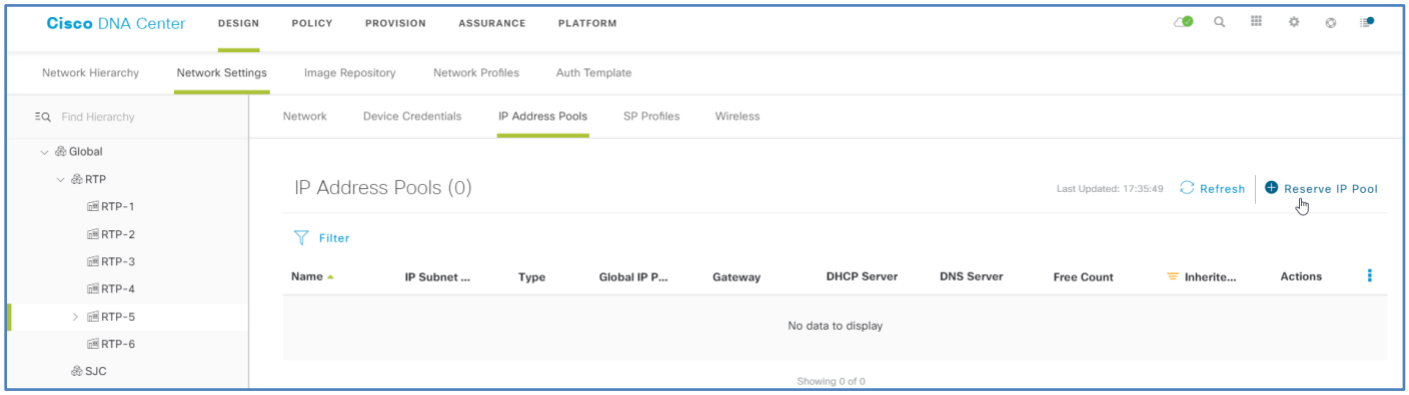
Step 2. Repeat the previous step for any additional global IP pools that include subnets at the site and building levels. The pools are added to the list of global pools.



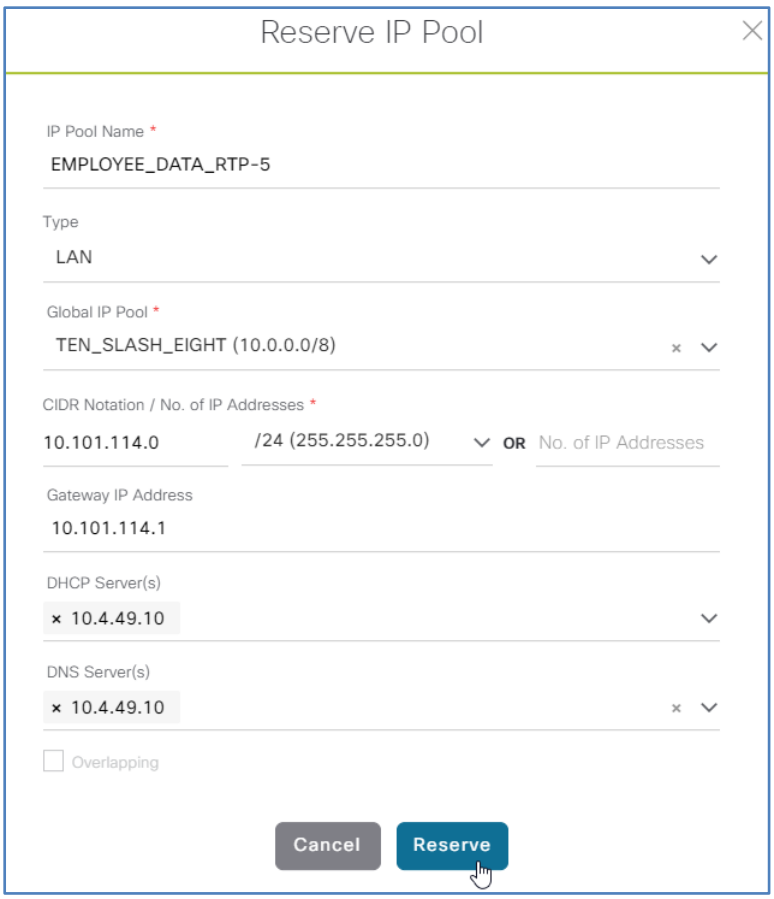
Procedure 5. Reserve IP address pools

Use the defined global IP address pools to reserve IP addresses for sites in your design using the network hierarchy. When you reserve addresses from the defined global IP address pools, the DNS and DHCP servers are available to use in those reservations, or they can be overwritten.

Step 1. Within Cisco DNA Center, navigate to **DESIGN > Network Settings > IP Address Pools**, on the left within the site hierarchy select a site or lower level for an IP address pool reservation (example: RTP-5), and then in the top right click **Reserve IP Pool**.

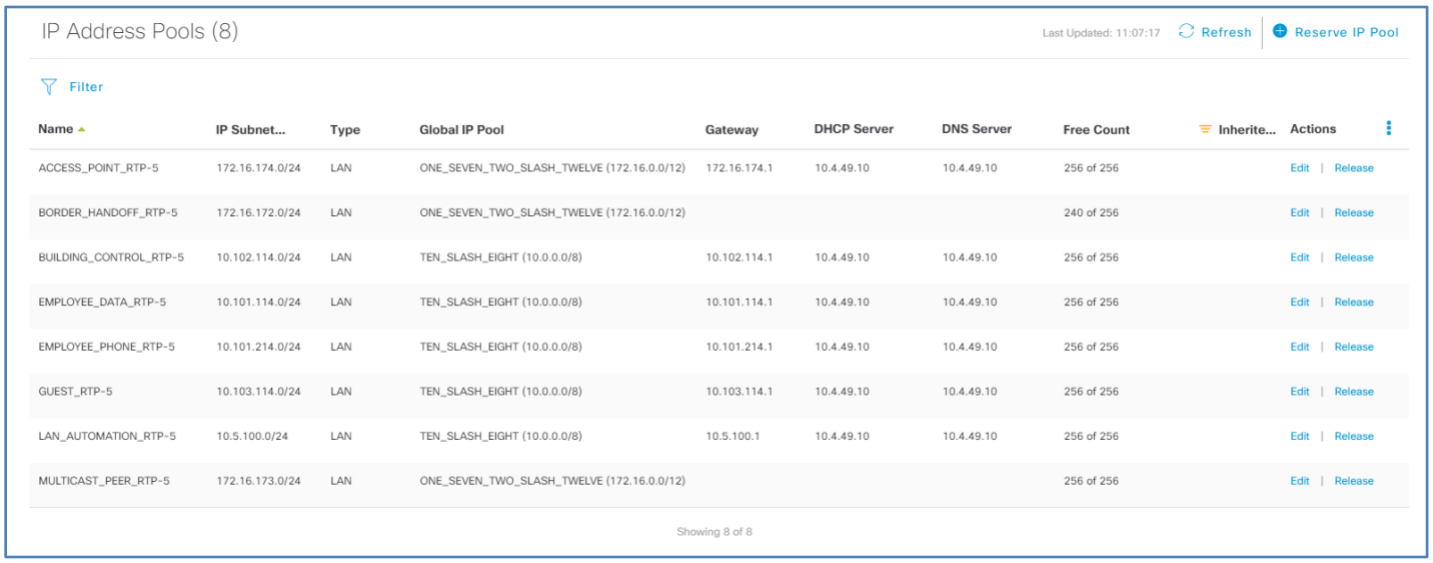


Step 2. Fill in the **IP Pool Name** (example: EMPLOYEE_DATA_RTP-5), under **Type** select **LAN**, select the **Global IP Pool** source for the reservation (example: EMPLOYEE), under **CIDR Notation / No. of IP Addresses** select the portion of the address space to use (example: 10.101.114.0/24), assign a **Gateway IP Address** (example: 10.101.114.1), use the drop-down menu to assign the **DHCP Server(s)** and **DNS Servers(s)**, and then click **Reserve**.



Step 3. Repeat the previous step for all global pool address blocks required to be reserved in the hierarchy for each site.

The hierarchy shows the assigned address pools. This example shows pool reservations within the RTP area, at the RTP-5 building level.

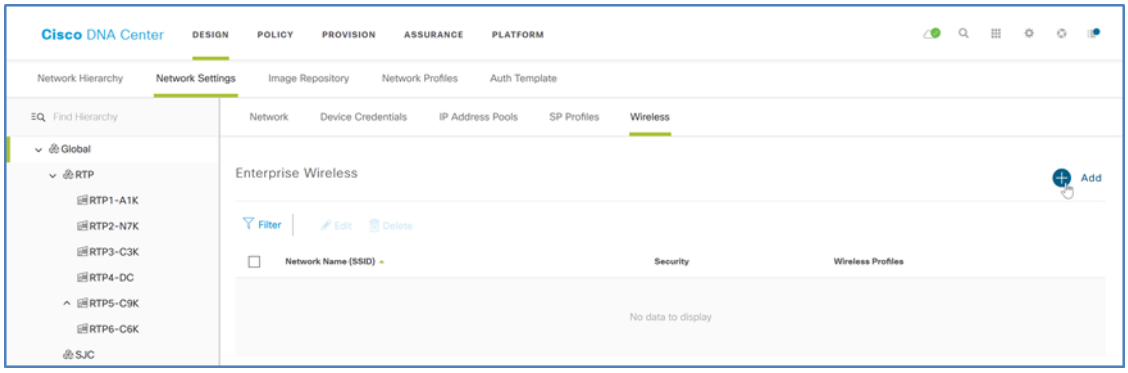


Name	IP Subnet...	Type	Global IP Pool	Gateway	DHCP Server	DNS Server	Free Count	Inherite...	Actions
ACCESS_POINT_RTP-5	172.16.174.0/24	LAN	ONE_SEVEN_TWO_SLASH_TWELVE (172.16.0.0/12)	172.16.174.1	10.4.49.10	10.4.49.10	256 of 256		Edit | Release
BORDER_HANDOFF_RTP-5	172.16.172.0/24	LAN	ONE_SEVEN_TWO_SLASH_TWELVE (172.16.0.0/12)				240 of 256		Edit | Release
BUILDING_CONTROL_RTP-5	10.102.114.0/24	LAN	TEN_SLASH_EIGHT (10.0.0.0/8)	10.102.114.1	10.4.49.10	10.4.49.10	256 of 256		Edit | Release
EMPLOYEE_DATA_RTP-5	10.101.114.0/24	LAN	TEN_SLASH_EIGHT (10.0.0.0/8)	10.101.114.1	10.4.49.10	10.4.49.10	256 of 256		Edit | Release
EMPLOYEE_PHONE_RTP-5	10.101.214.0/24	LAN	TEN_SLASH_EIGHT (10.0.0.0/8)	10.101.214.1	10.4.49.10	10.4.49.10	256 of 256		Edit | Release
GUEST_RTP-5	10.103.114.0/24	LAN	TEN_SLASH_EIGHT (10.0.0.0/8)	10.103.114.1	10.4.49.10	10.4.49.10	256 of 256		Edit | Release
LAN_AUTOMATION_RTP-5	10.5.100.0/24	LAN	TEN_SLASH_EIGHT (10.0.0.0/8)	10.5.100.1	10.4.49.10	10.4.49.10	256 of 256		Edit | Release
MULTICAST_PEER_RTP-5	172.16.173.0/24	LAN	ONE_SEVEN_TWO_SLASH_TWELVE (172.16.0.0/12)				256 of 256		Edit | Release

Showing 8 of 8

Procedure 6. Configure fabric enterprise wireless SSIDs

Step 1. From the main Cisco DNA Center dashboard, navigate to **DESIGN > Network Settings> Wireless**, in the left hierarchy pane, select the **Global** level, in the **Enterprise Wireless** section click **+ Add**.



The **Create an Enterprise Wireless Network** wizard appears.

Step 2. Use the **Create an Enterprise Wireless Network** wizard to supply the following information:

- Enter the **Wireless Network Name(SSID)** (example: Employee).
- Under **TYPE OF ENTERPRISE NETWORK**, select Voice and Data and Fast Lane.
- Select or confirm the **WIRELESS OPTION.**
- For **LEVEL OF SECURITY** select an option (example: WPA2 Enterprise).
- Under **ADVANCED SECURITY OPTIONS** select Adaptive.

Step 3. Click **Next** to continue in the wizard, and supply the following information:

- Enter a **Wireless Profile Name** (example: RTP5-Wireless).
- Under **Fabric**, select **Yes.**
- Under **Choose a site**, select the location where the SSID broadcasts (example: Global/RTP/RTP5-C9K), and include floors to include in SSID coverage (example: Global/RTP/RTP5-C9K/Floor 1).

Tech tip
The purpose of a wireless profile is to define the SSID as Fabric or non-Fabric and to define the sites where this SSID will be broadcast. New profiles can be created as part of the SSID workflow. Additional profiles can be created outside of the SSID workflow by navigating to **DESIGN** > **Network Profiles**.

Step 4. Click **Finish** to continue. The **DESIGN > Network Settings> Wireless** screen is displayed.

Step 5. Repeat this procedure for additional SSIDs using the same network profile and any new location profiles to be associated with an SSID.

Procedure 7. Configure a fabric guest wireless SSID

Step 6. Navigate to **DESIGN > Network Settings> Wireless**, in the **Guest Wireless** section click **+ Add**, in the **Create a Guest Wireless Network** wizard, and supply the following information:

- Enter the **Wireless Network Name(SSID)** (example: Guest).
- Under **LEVEL OF SECURITY** select **Web Auth.**
- Under **AUTHENTICATION SERVER** select **ISE Authentication.**

Leave the other default selections and click **Next** to continue in the wizard.

Tech tip
Selection ISE Authentication as the Authentication Server will cause the workflow to create a Guest Portal in ISE. This Guest Portal can then be customized as part of the workflow.

Step 7. In the **Wireless Profiles** step, select the **Profile Name** corresponding to the deployment location (example: RTP5-Wireless), in the slide-out panel keep the default **Fabric** selection of **Yes**, keep the other default information, at the bottom of the panel click **Save**, and then click **Next**.

Step 8. In the **Portal Customization** step, click **+ Add**. The **Portal Builder** screen appears.

Step 9. Supply a **Guest Portal** name (example:Guest-RTP5), make any desired customizations, and then at the bottom of the screen click **Save**. A guest web authentication portal is generated for the site, and you return to the previous screen.

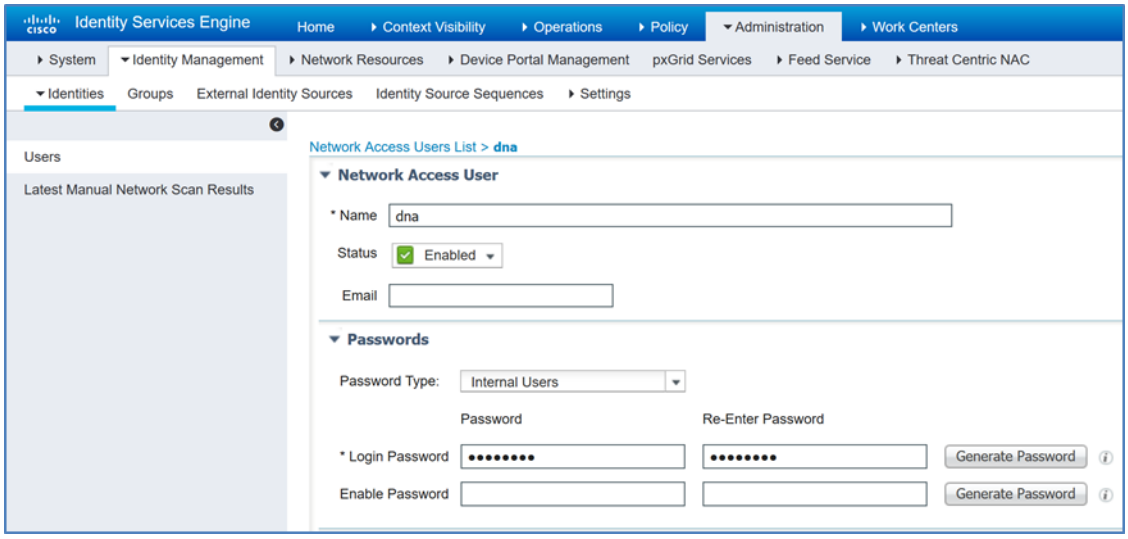
Step 10. Click **Finish**.

The wireless LAN design is created and is ready to deploy.

Procedure 8. Create a Cisco DNA Center administrative login in ISE

When devices are provisioned, they receive configurations appropriate for the assigned site, including the centralized AAA configuration using ISE. This configuration authenticates the console and VTY lines against the AAA servers. To maintain the ability to manage the devices after provisioning, the credentials defined in a Discovery job must be available from the ISE server. These can either be locally defined in ISE (Internal User) or available through an external identity source such as Active Directory integrated with ISE.

Step 1. Log in to ISE, navigate to **Administration > Identity Management > Identities**, click +**Add**, enter the **Name** (matching what was used for Cisco DNA Center discovery, and different from the ISE administrator), enter the associated **Login Password** and **Re-Enter Password**, and then, at the bottom of the screen, click **Submit**.



The network administrative user login is now available from ISE, and the same user ID is created on each device each discovered device if using LAN Automation as described in later procedures.

Process 3: Creating Segmentation and Policy for the SD-Access Network

As part of the design decisions in preparation for your SD-Access network deployment, you decide network segmentation strategies for the organization. Macro segmentation uses additional overlay networks (VNs) in the fabric, and micro segmentation uses scalable group tags (SGTs) to apply policy to groups of users or device profiles.

In some cases, disparate device isolation is required. In a retail store example, the point-of-sale machines should never communicate with the video surveillance network infrastructure, which in turn should never communicate with the building HVAC system. In cases where the isolation need extends from the edge of the network all the way to the core of the network to access centralized services, macro segmentation using VNs is the best choice. Governmental and industrial compliance requirements – such as PCI DSS – and an organization's risk policies often drive the choice to use macro segmentation.

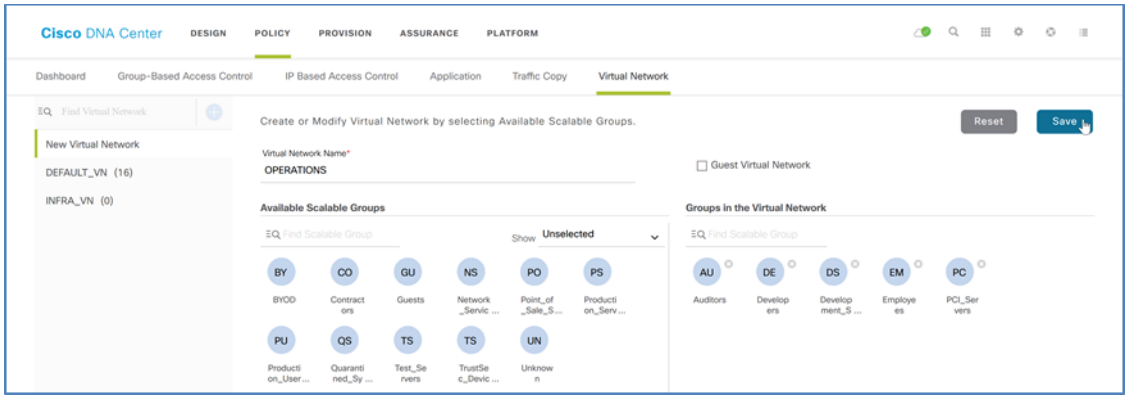
Group policies are used to easily accommodate the desired outcomes of policy application using micro segmentation. In a university example, students and faculty machines both may be permitted to access printing resources, but student machines should not communicate directly with faculty machines, and printing devices should not communicate with other printing devices.

For a deeper exploration of designing segmentation for SD-Access, with use cases, see the Software-Defined Access Segmentation Design Guide on Cisco.com.

Use these procedures as examples for deploying your macro and micro segmentation policies.

Procedure 1. Add an overlay VN to the SD-Access network

Step 1. From the main Cisco DNA Center dashboard, navigate to **POLICY > Virtual Network**, click the **+** (plus sign) to create a new virtual network, enter a **Virtual Network Name** (example: OPERATIONS), drag scalable groups from the **Available Scalable Groups** pool into the **Groups in the Virtual Network** pool (example: Auditors, Developers, Development_Servers, Employees, and PCI_Servers), and then click **Save**.



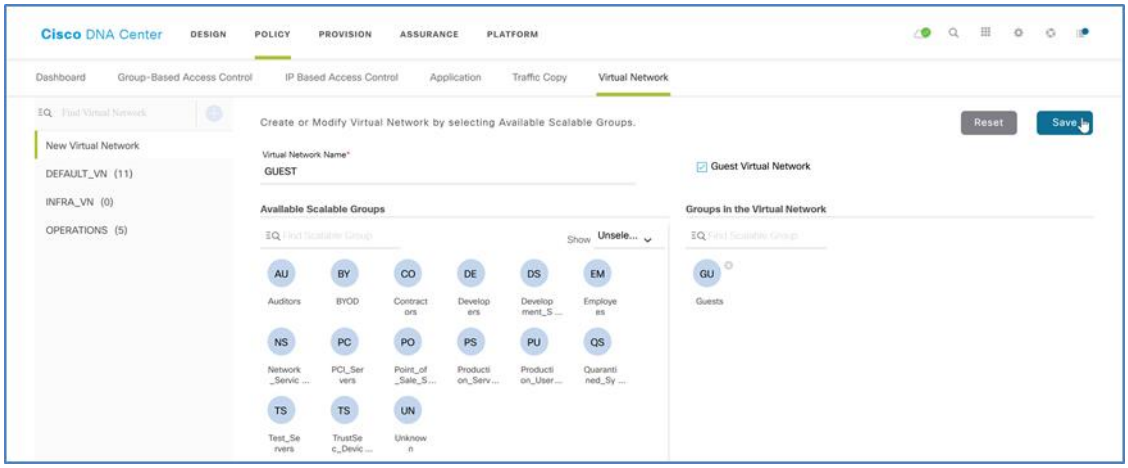
The VN with associated groups is defined and appears in the list of defined virtual networks. These virtual network definitions are available for provisioning fabrics.

Tech tip
If you don't see any groups, then likely the pxGrid connectivity between Cisco DNA Center and ISE is not fully operational. In this case, review the integration procedures for ISE with Cisco DNA Center and be sure to approve the pxGrid connection request in ISE from Cisco DNA Center.

Step 2. If your organization requires groups different than the default groups, create custom groups by navigating to **POLICY > Group-Based Access Control > Scalable Groups**, and then click the **Add Groups** to create a new group (SGT). This provides a cross launch into ISE for SGT creation.

Step 3. Repeat the first two steps for each overlay network. You can also return to these steps after the fabric is provisioned to create more overlay networks.

Step 4. Many networks require a guest service for wireless users — create a guest VN to support this feature. From the main Cisco DNA Center dashboard, navigate to **POLICY > Virtual Network**, click the **+** (plus sign) to create a new virtual network, enter a **Virtual Network Name** (example: GUEST), select the check box next to **Guest Virtual Network**, drag the **Guests** scalable groups from the **Available Scalable Groups** pool into the **Groups in the Virtual Network** pool, and then click **Save**.

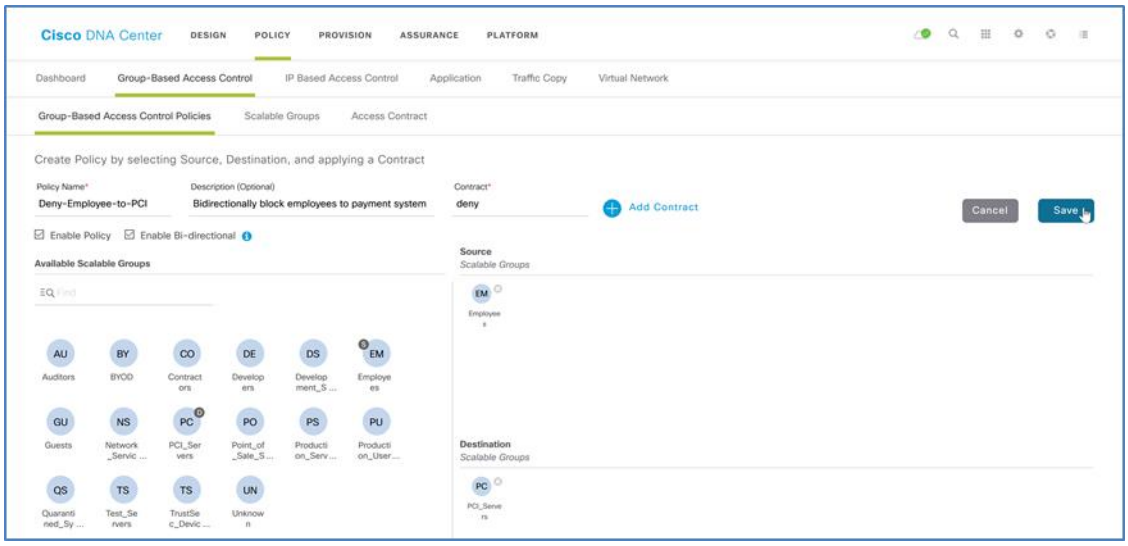


Tech tip
The Guest Virtual Network check box allows the defined VN to be used in other guest-related workflows in later procedures such as guest SSID and signifies that clients access this VN will use the Guest Portal created in earlier procedures.

Procedure 2. Create a micro-segmentation policy using SGTs

Micro-segmentation policies are customized for an organization's deployment. This simple example shows a basic policy that can be used to deny users from the Employee group from communicating with the PCI_Servers group. When authentication profiles appropriately assign an SGT to an endpoint or user, ISE captures the intent of this policy and renders it into the network.

Step 1. From the main Cisco DNA Center dashboard, navigate to **POLICY > Group-Based Access Control > Group-Based Access Control Policies**, click **+ Add Policy**, from the **Available Scalable Groups** pane drag the **Employees** group and drop it into the **Source** pane, drag the **PCI_Servers** group into the **Destination** pane, input a **Policy Name** (example: Deny-Employee-to-PCI), enter a **Description**, select **Enable Policy**, select **Enable Bi-directional**, click **+ Add Contract**, select **deny**, click **OK**, and then click **Save**.



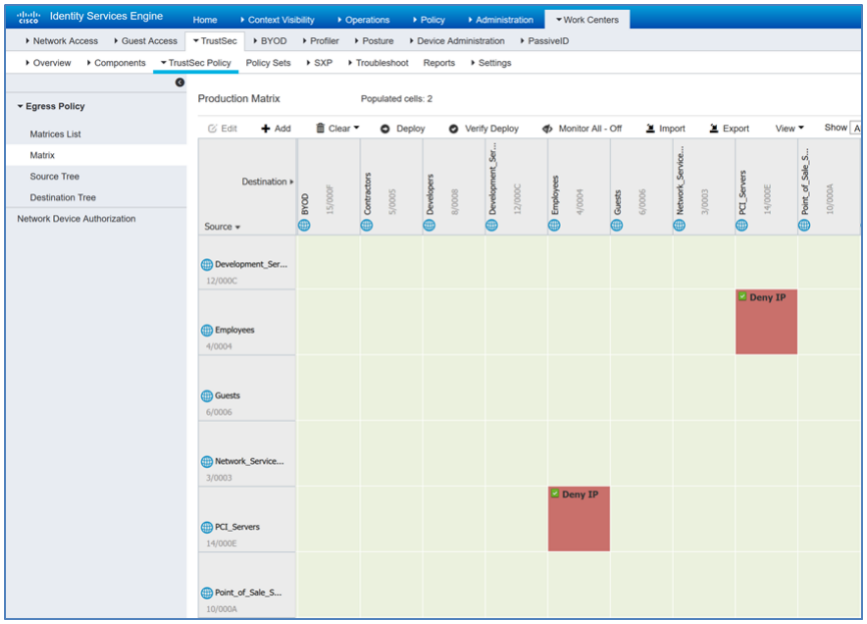
The policy is created and listed with a status of **CREATED**. Because of the bidirectional option selection, the reverse policy is also created.

Step 2. Select the policies created, and then click **Deploy**.

The status changes to **DEPLOYED** and the policies are available to be applied to SD-Access fabrics Cisco DNA Center creates and are also available in ISE, viewable using the Cisco TrustSec policy matrix.

Step 3. At the top right, click **Advanced Options**. The link is a shortcut to logging in to ISE, navigating to **Work Centers > TrustSec > TrustSec Policy**, and then on the left side selecting **Matrix**. You are redirected to log in to ISE, which redirects the browser and displays the TrustSec policy matrix.

Verify that the policy has been created in the ISE TrustSec policy matrix.



Process 4: Using Cisco DNA Center for Device Discovery

Procedure 1. Discover and manage network devices

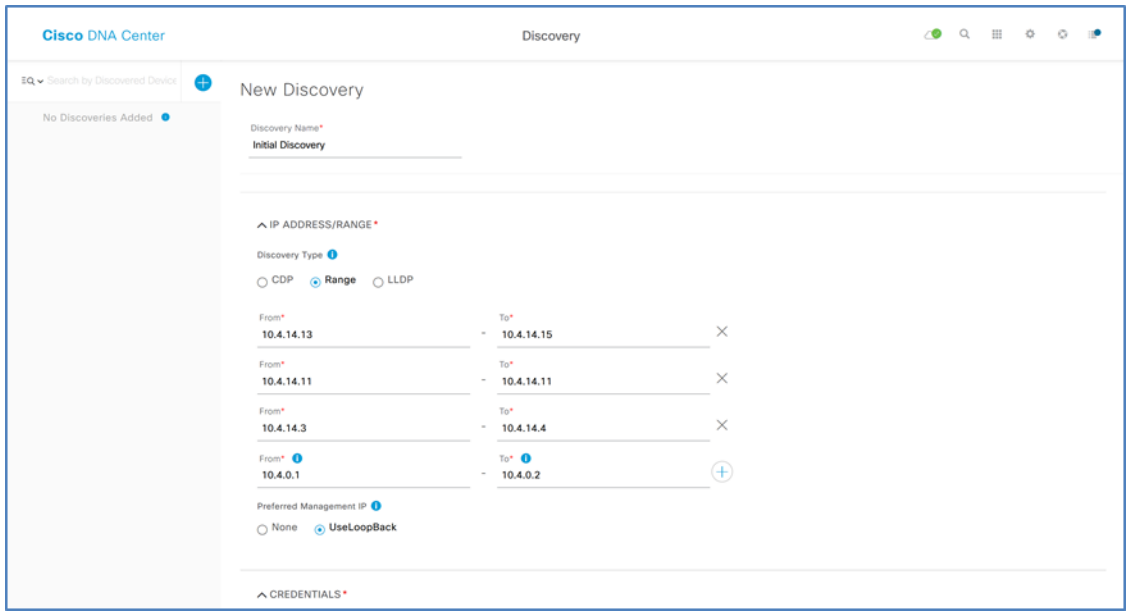
You use Cisco DNA Center to discover and manage the underlay network devices for SD-Access by enabling IP connectivity to the devices and supplying Cisco DNA Center with management credentials. Use this procedure for any LAN Automation seed devices and all other devices that you do not plan to discover and manage using LAN Automation in the next procedure.

These steps show how to initiate discovery by supplying an IP address range or multiple ranges for scanning network devices, which constrains the discovery and potentially saves time. Alternatively, for the devices not using LAN Automation onboarding, you can supply an initial device for discovery and direct Cisco DNA Center to use Cisco Discovery Protocol to find connected neighbors. When using Cisco Discovery Protocol, reduce the default number of hops down to a reasonable number to speed the discovery.

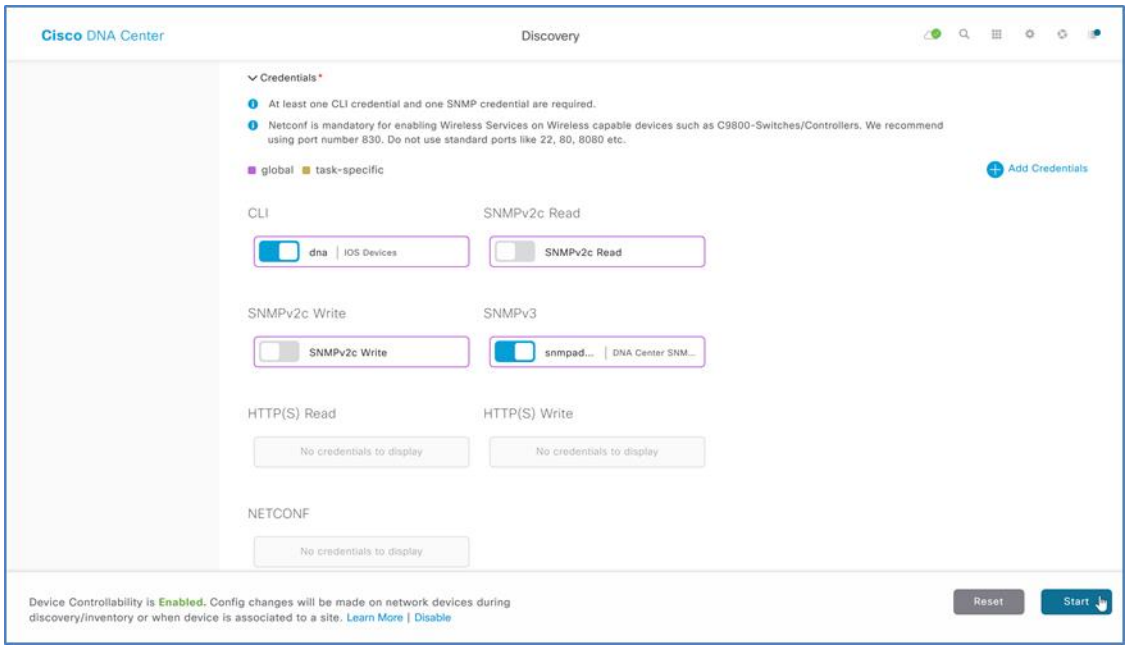
Step 1. Navigate to the main Cisco DNA Center dashboard, scroll to the **Tools** section, click **Discovery** and supply a **Discovery Name**. Select **Range** and enter a start and end IP loopback address for **IP Ranges** (to cover a single address, enter that address for both the start and end of the range). For **Preferred Management IP**, if a device has a loopback interface used for management then select **UseLoopBack**.

Tech tip
If you are using a Cisco Catalyst 6800 Series switch with a very large configuration, you can avoid discovery timeouts by adding the following command to that switch in configuration mode: `snmp mib flash cache`

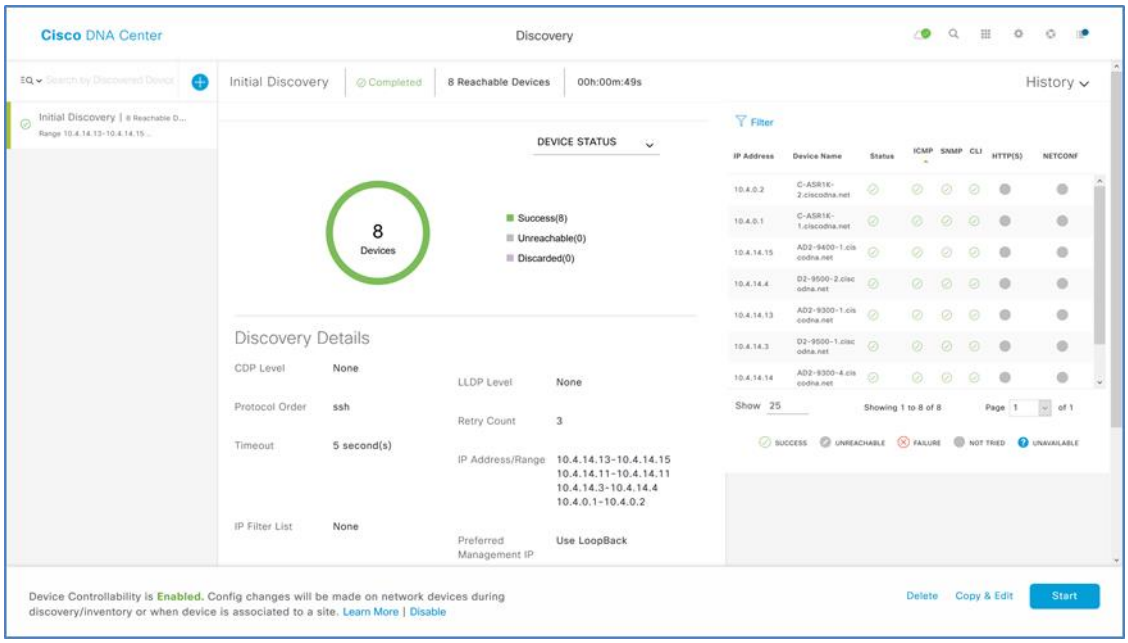
Step 2. If you have any additional ranges, next to the first range click **+** (plus sign), enter the additional range, and repeat for any remaining ranges.



Step 3. Scroll down to verify the CLI credentials used for the discovery and the SNMP credential configurations pushed to the device by the Cisco DNA Center Device Controllability feature, and then at the bottom click **Start**.

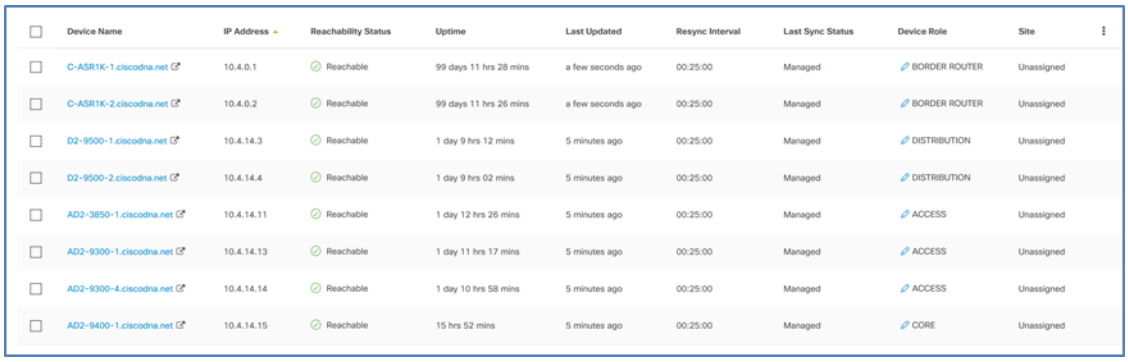


The discovery details are displayed while the discovery runs.



Step 4. If there are any discovery failures, inspect the devices list, resolve the problem, and restart the discovery for those devices along with any additional devices to add to the inventory.

Step 5. After successfully completing all discovery tasks, navigate to the main Cisco DNA Center dashboard, and then, under the **Tools** section, click **Inventory**. The discovered devices are displayed. After inventory collection completes, each device shows a **Managed** sync status, signifying that Cisco DNA Center maintains an internal model mirroring the device physical deployment.



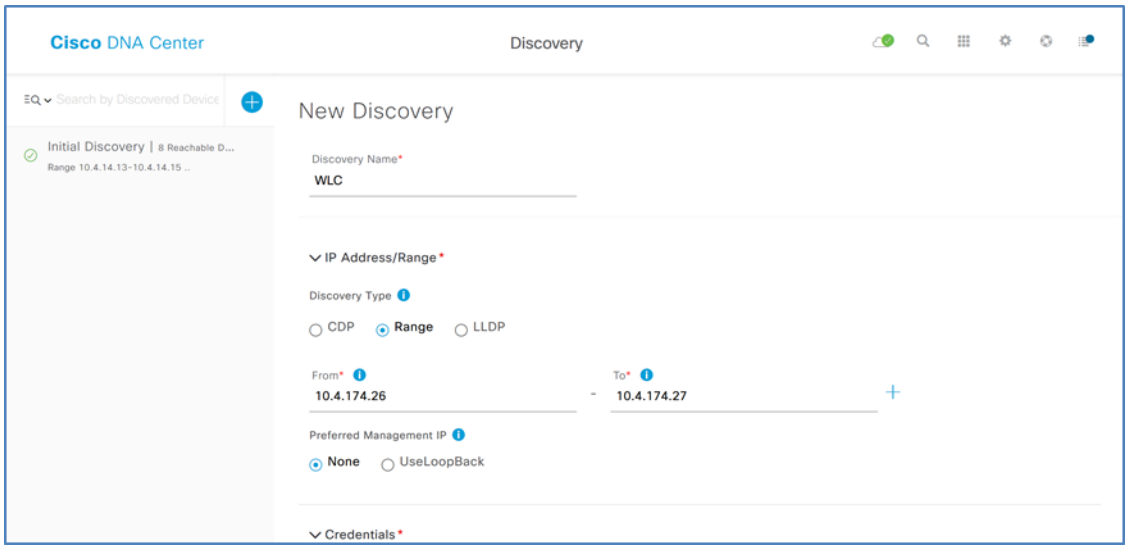
Cisco DNA Center can now access the devices, synchronize the configuration inventory, and make configuration changes on the devices.

Tech tip
At the right side of the title row for the Inventory table, you can adjust which columns are displayed. Use the **Device Role** column to see the device role assigned by discovery based on device type and to adjust the role to best reflect the actual deployment of a device, such as access, distribution, core, or border router. Adjusting the role now can improve the appearance of the initial topology maps, versus adjusting the roles in later procedures.

Procedure 2. Add the wireless controllers into inventory

If the wireless LAN controllers are not in the Cisco DNA Center inventory, you must add them before the wireless integration. For resiliency, you should also use two WLCs of the same type to create an HA SSO pair which can be automated as shown in later procedures.

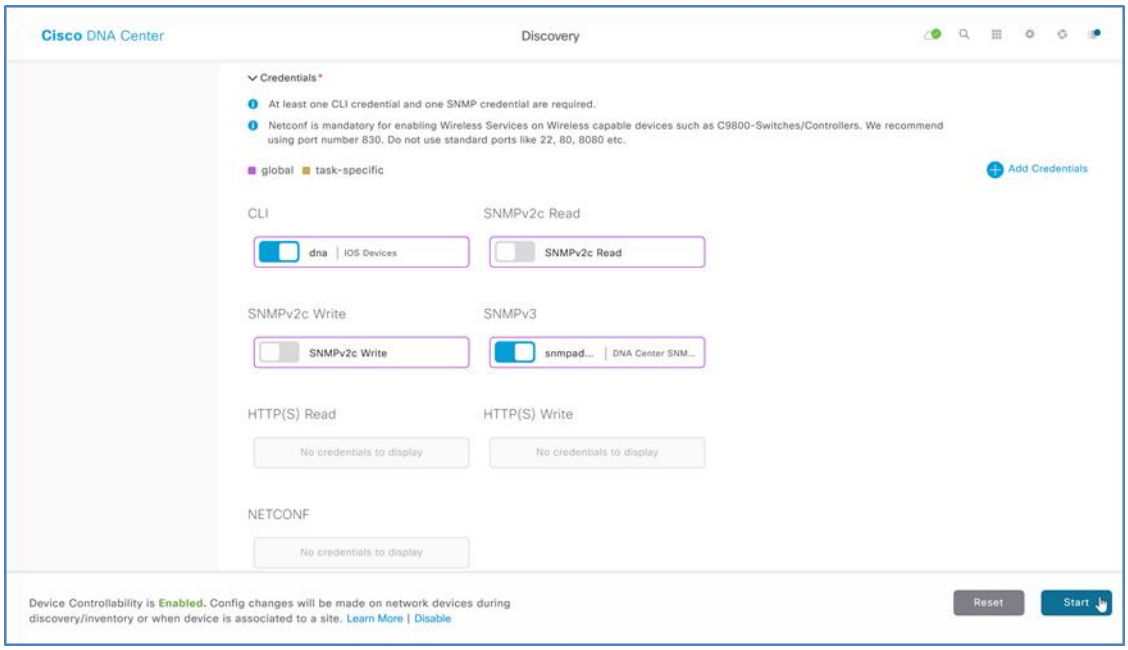
Step 1. Navigate to the main Cisco DNA Center dashboard, scroll to the **Tools** section, click **Discovery** and supply a **Discovery Name**. Select **Range** and enter a start and end IP loopback address for **IP Ranges** (to cover a single address, enter that address for both the start and end of the range). For **Preferred Management IP**, use **None**.



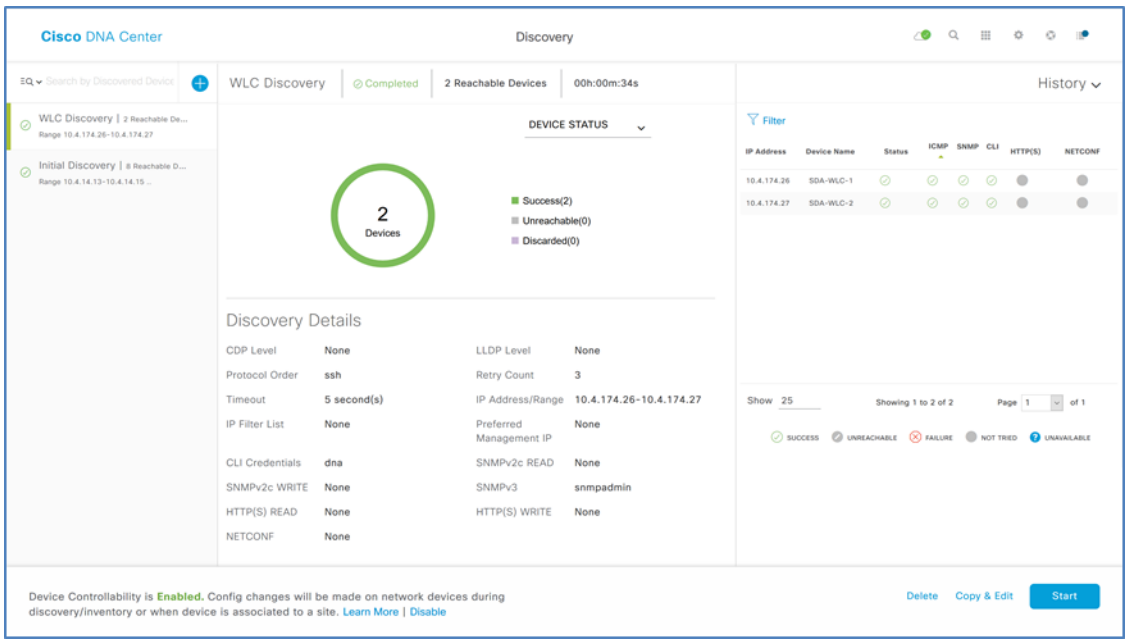
Step 2. If you have any additional ranges, next to the first range click **+** (plus sign), enter the additional range, and repeat for any remaining ranges.

Step 3. Scroll down to verify the CLI credentials used for the discovery. If you have discovery-specific unique credentials for the device click **+ Add Credentials** add each new credential, save them, and then at the bottom click **Start**.

Tech tip
If Device Controllability is enabled, as it is by default, SNMP and NETCONF credentials are configured on the device during the Discovery process if they are not currently present.



The discovery details are displayed while the discovery runs.



Step 4. If there are any discovery failures, inspect the devices list, resolve the problem, and restart the discovery for those devices along with any additional devices to add to the inventory.

Step 5. After successfully completing all discovery tasks, navigate to the main Cisco DNA Center dashboard, and then, under the **Tools** section, click **Inventory**. The discovered devices are displayed. After inventory collection completes, each device shows a **Managed** sync status, signifying that Cisco DNA Center maintains an internal model mirroring the device physical deployment.

Cisco DNA Center can now access the devices, synchronize the configuration inventory, and make configuration changes on the devices.

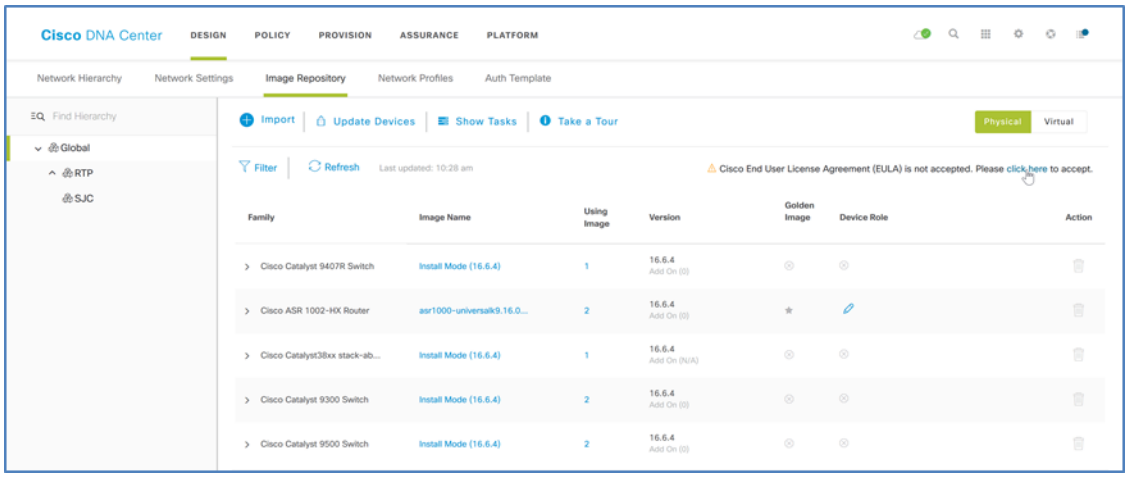
Process 4: Managing Device Software Images

To achieve the full capabilities of SD-Access, the SD-Access package in Cisco DNA Center has minimum software version requirements for the devices that it provisions. The software image management capability built into Cisco DNA Center is used to upgrade any devices that are not running a recommended image version. You can find supported images for SD-Access using the SD-Access Hardware and Software Compatibility Matrix on Cisco.com. The images used for validation are listed in Appendix A: Product List.

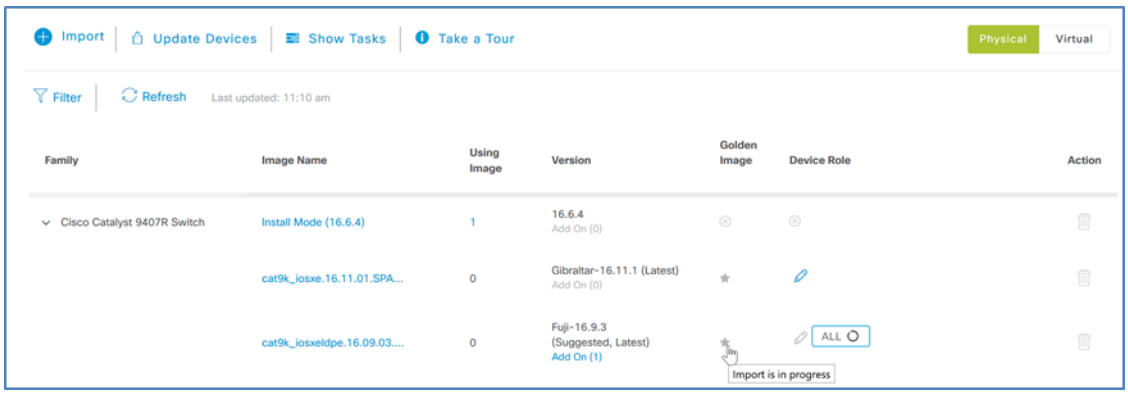
Procedure 1. Manage software images for devices in inventory

Use the following steps to apply software updates of images and software maintenance updates (SMUs) to the devices, by importing the required images, marking images as golden, and applying images to devices.

Step 1. Navigate to the main Cisco DNA Center dashboard, click **Design**, and then click **Image Repository**. If this is the first time using the software, then at the top right **Cisco End User License Agreement** notification, select **click here**, and then click **Accept License Agreement**.



Step 2. Under the **Image Name** column click the down arrow next to the image listed for a device family, and then click the **Golden Image** star to mark the appropriate image as the preferred one for the platform.

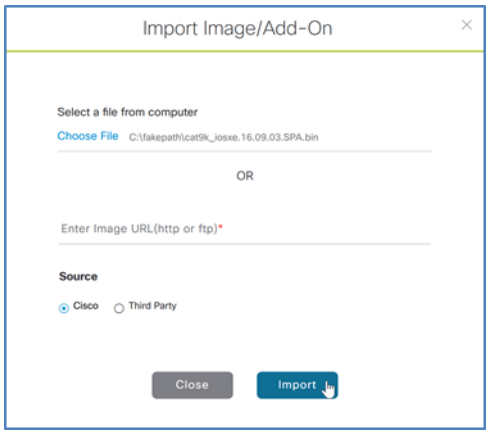


Images that are not yet imported are automatically imported, using Cisco.com credentials. You can update Cisco.com credentials using **Settings** (gear) **> System Settings > Settings > Cisco Credentials**.

Tech tip
Only Latest and Suggested images are available to be downloaded from Cisco.com. If the image is available on managed device in flash, Cisco DNA Center will import the image from the device.

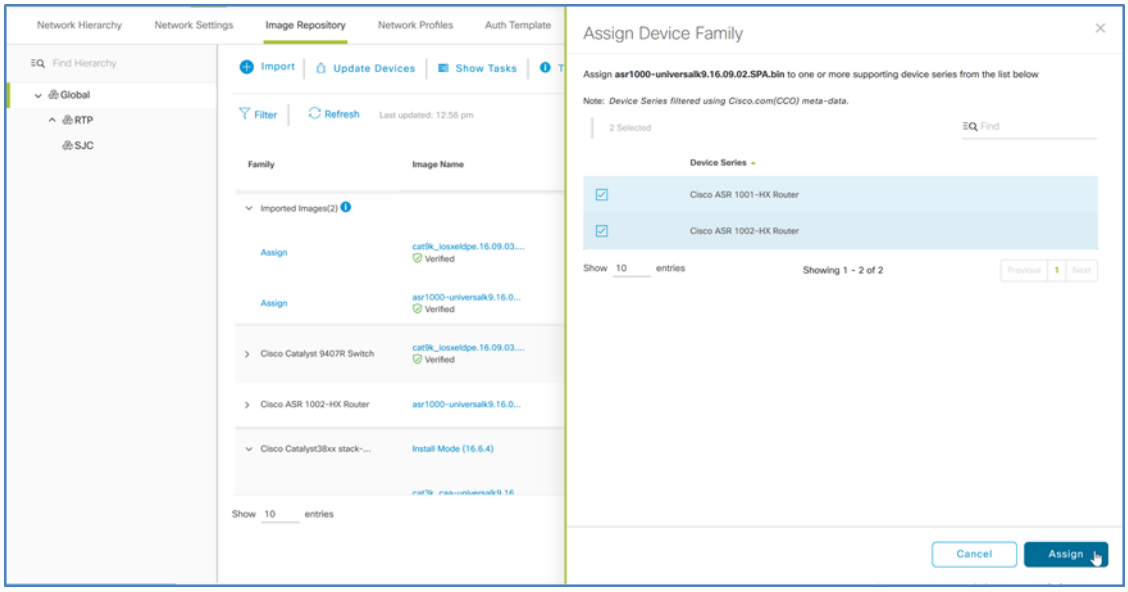
Step 3. Repeat the importing and tagging images as golden until all devices are marked with an appropriate image.

Step 4. To import an image from your local machine, then click **+ Import**, in the Import Image/Add-On dialog, choose a file location, and then click **Import**.



The image import into Cisco DNA Center starts.

Step 5. After the import is complete, assign the imported image to devices. Next to the imported image, click **Assign**, select the devices to use the image, and then in the pop out click **Assign**.



The image is in the repository and available to tag as golden for those devices.

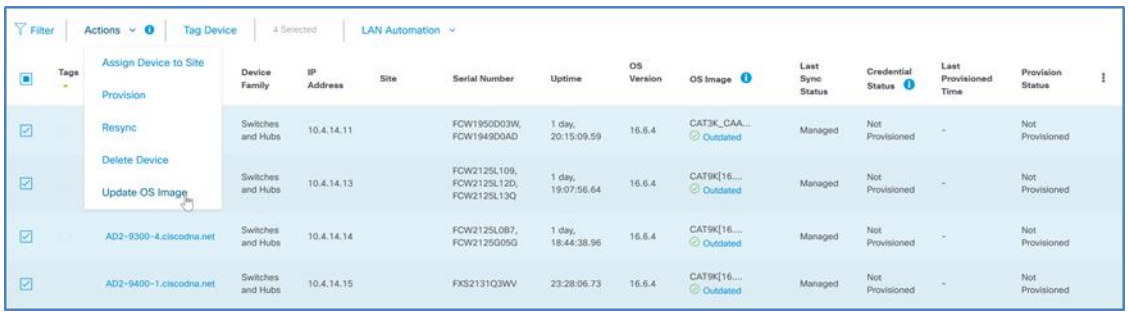
Step 6. For each device with a newly assigned image, click the **Golden Image** star to mark the appropriate image as the preferred one for the platform.

Step 7. Repeat these steps for all images that you wish to deploy using Cisco DNA Center. All device types with an assigned golden image are ready for the distribution of the software image.

Procedure 2. Use software image management to update device software

Cisco DNA Center runs a compliance check of devices in inventory compared to images tagged as golden. Devices out of compliance with the golden image are marked as **Outdated** in inventory. Update the images to the version marked golden. Inventory collection must have completed successfully, and the devices must be in the **Managed** state before continuing. You distribute the software images first and schedule or manually activate the devices with the distributed images.

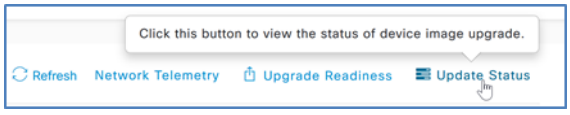
Step 1. Navigate to **PROVISION > Devices > Inventory**, select all devices marked **Outdated**, and then in the **Actions** menu, click **Update OS Image**. For more control of the updates, start OS updates on devices that can reboot without affecting connectivity to other devices that you are updating.



Step 2. In the slide out that appears, under **Distribute > When** select **Now**, click **Next**, under **Activate** select **Schedule Activation after Distribution is completed**, click **Next**, and then under **Confirm** click the **Confirm** button.

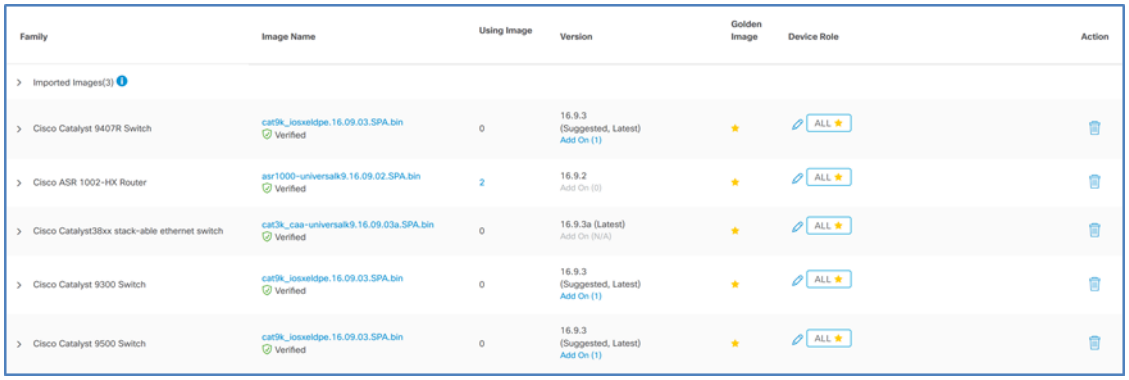
Images are distributed to the selected devices.

Step 3. At the top right, click **Update Status**.



The status screen gives more details than the main screen, including explanation of any failures. Use the **Refresh** button to observe when the **In Progress** status is changed to **Successful**.

Step 4. Repeat this procedure as needed to update the device software to the required versions for the network deployment. At completion, all devices for the deployment are associated with a golden image and have the image installed.



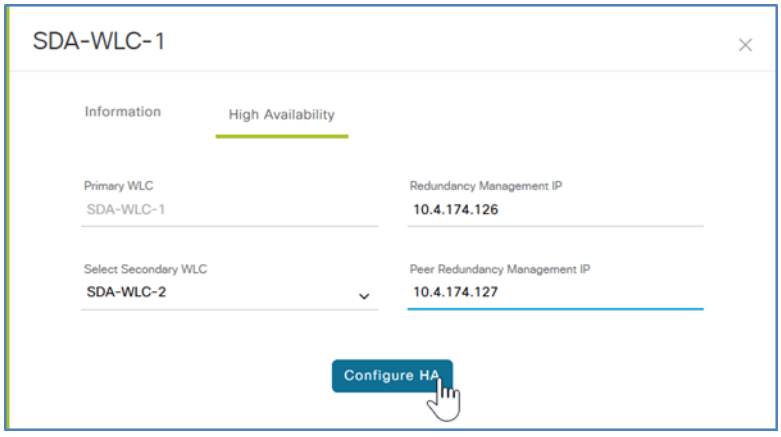
Process 5: Creating a WLC HA SSO Pair

Cisco DNA Center can be used to automate the configuration necessary to create an HA SSO pair between two WLCs which have been discovered and added to inventory.

Procedure 1. Create an HA SSO Pair

Optional

Step 1. If you are creating an HA SSO pair with a set of controllers that are currently unpaired, go to the main Cisco DNA Center dashboard, navigate to **PROVISION > Devices > Inventory**, click the text of the **Device Name** of the primary WLC (example: SDA-WLC1), on the right side in the pop-out at the top select **High Availability**, under **Select Secondary WLC** select the second WLC in the HA SSO pair (example: SDA-WLC-2), supply **Redundancy Management IP** and **Peer Redundancy Management IP** (examples: 10.4.174.126, 10.4.174.127), click **Configure HA**, and then at the reboot warning pop up, click **OK**.



On the browser, warning messages display.

```
Configuring HA for Primary. Please do not Refresh the page..
Configuring HA for Secondary...
```

The reconfiguration and reboot can take many minutes.

Step 2. Use the refresh button at the top of the display to refresh the display until the WLCs in HA mode display as one device. Check the HA status by clicking the text of the **Device Name** of the primary WLC (example: SDA-WLC1), on the right side in the pop-out at the top select **High Availability**, and check that **Redundancy State** is **SSO**, and **Sync Status** is **Complete**.

Proceed to the next step after the HA configuration is complete.

Step 3. Go to the main Cisco DNA Center dashboard, navigate to **DESIGN > Image Repository**. Find the device family and check the software version. If the WLC image is the correct version, then continue. If the image needs to be updated, and the image is listed, then click the star next to the image to mark the image as golden and update the software. If you need an image not listed, then at the top, click Import Image/SMU, follow the instructions to import, refresh the screen, use the drop-down for the device to mark the image golden.

Step 4. If you are upgrading the device, navigate to **PROVISION > Devices > Inventory**, select the WLC marked **Outdated**, and then in the **Actions** menu, select **Update OS Image**. Confirm the selection of device to update, use the default **When** selection of **Now**, click **Apply**, and then at the popup warning about devices being rebooted click **OK**.

Images are distributed to the selected device, and then the device reboots to activate the new image immediately after the image distribution is complete. Use the **Refresh** button to see when the **In Progress** status is removed.

Process 6: Provisioning the Underlay Network for SD-Access

After Cisco DNA Center discovers and has management control of devices that are running the appropriate software versions for SD-Access, use Cisco DNA Center to provision the devices in the underlay network.

Procedure 1. Provision underlay switches using the LAN Automation feature

Optional

Use this procedure if you are deploying new, unconfigured LAN switches into the underlay by using Cisco DNA Center's LAN Automation capabilities. Use the previous procedures to configure one or more seed devices (the managed devices where the new, unmanaged network connects), the device CLI and SNMP credentials to be pushed by PnP, and the network-reachable IP address pool used for connectivity. Although it's not a strict requirement, each seed device is typically a switch assigned in later procedures as a border, and must have an appropriate VTP mode and MTU configuration (examples: *vtp mode transparent, system mtu 9100*). Ports on the seed device connected to devices to be discovered must be in Layer 2 mode (access port versus routed port), and the seed device ports cannot be dedicated out-of-band (OOB) management ports.

Tech tip

LAN Automation enables discovery of supported switches from supported seed devices (switches used in this validation are listed in the appendix). Discovered switches are directly connected to chosen seed device interfaces (OOB management ports cannot be connected during LAN Automation device onboarding, because it will block LAN Automation on the non-OOB ports) and up to one additional hop of connected switches, for a total of two hops away from the seed device. The credentials supplied allow Cisco DNA Center and seed devices to work together to configure the discovered devices and add them into managed inventory. Because the discovered devices must be running the PnP agent with no previous configuration, any previously configured switch to be used must be restored to a state where the PnP agent is running, accomplished by using the following configuration mode and exec mode commands:

```
(config)#config-register 0x2102
(config)#crypto key zeroize
(config)#no crypto pki certificate pool
delete /force vlan.dat
delete /force nvram:*.cer
delete /force nvram:pnp*
delete /force flash:pnp*
delete /force stby-nvram:*.cer
delete /force stby-nvram:*.pnp*
! previous two lines only for HA systems
write erase
reload
```

Do not save the configurations for the reload process. To prepare switch stacks for LAN Automation, use the same restoration commands for each switch in the stack.

Switch stacking requirements do not change for LAN Automation—all switches in a stack must be running the same software license and version supporting IP routing features. If you desire the most control over port numbering and stack behavior, then in advance of starting the LAN Automation process, you can adjust the switch stack numbering and also influence a switch to become the ACTIVE role within a stack through an increased priority by using the following commands in exec mode:

```
switch [switch stack number] renumber [new stack number]
switch [switch stack number] priority 15
```

If a golden image has been tagged as described in the previous procedure, image upgrade will occur during LAN Automation if the discovered device is running in INSTALL mode. If the golden image has been tagged and the discovered device is running in BUNDLE mode, LAN Automation will fail for the device.

Identify one or two devices that are in the inventory and managed by Cisco DNA Center to assign to the seed device role at a site. The same seeds can be used for multiple runs of the LAN Automation feature, allowing the discovered devices to be assigned to different buildings or floors for each run.

Step 1. From the main Cisco DNA Center dashboard, navigate to **PROVISION > Devices > Inventory**. Select up to two seed devices, in the **Actions** drop-down, click **Assign Device to Site**, in the **Assign Device to Site** screen, select the devices site assignments, and then click **Apply**.

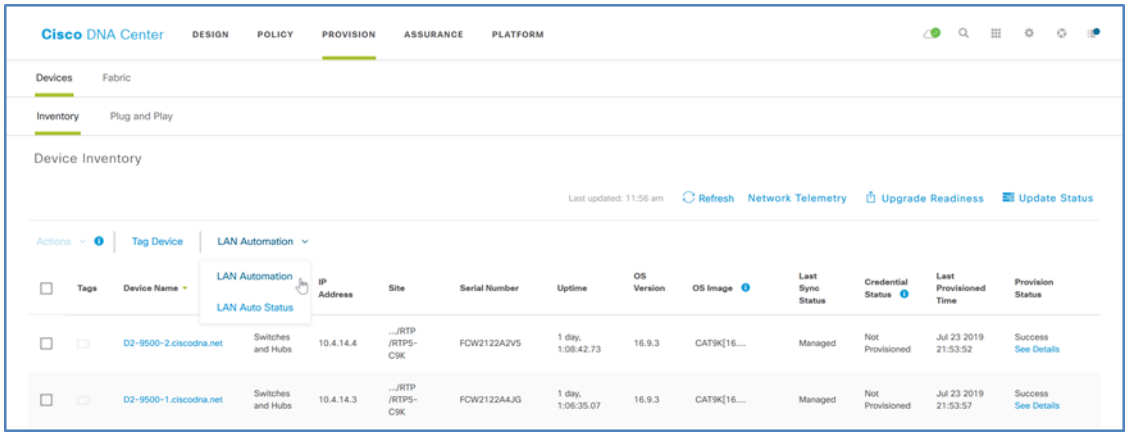
Step 2. If you are using a Catalyst 6800 Series seed device, use the interface configuration mode command to change the ports towards discovered devices to be Layer 2 ports.

```
switchport
```

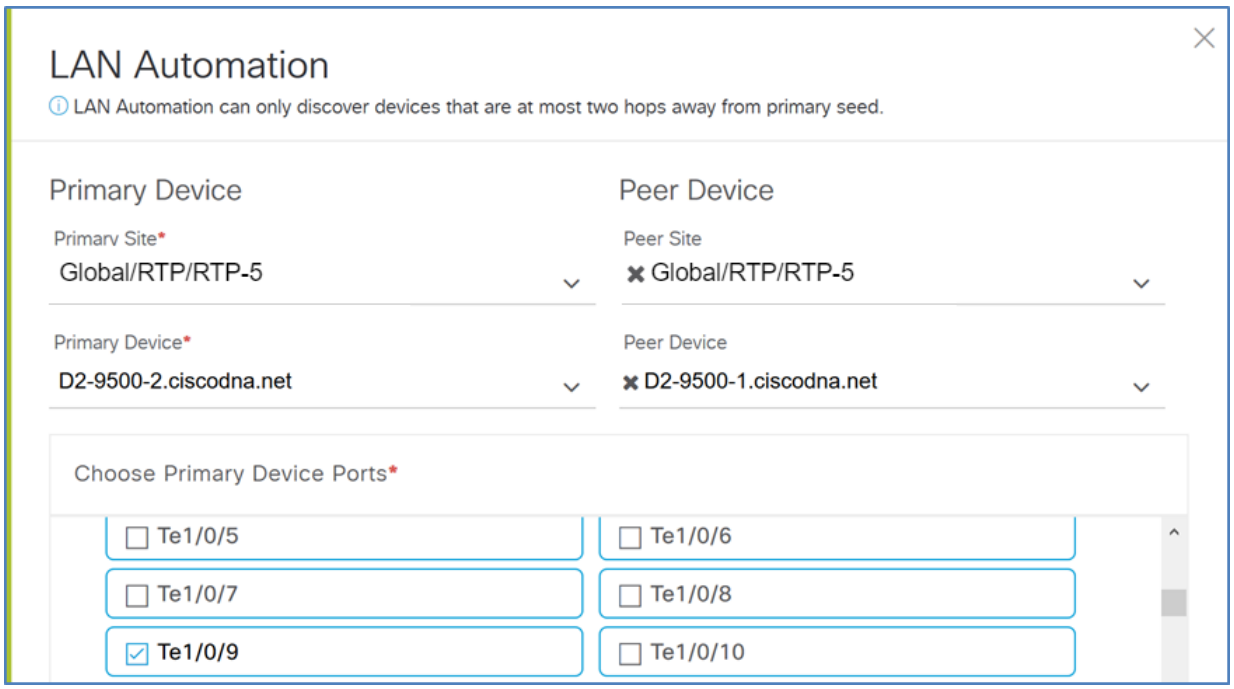
After you have saved the configuration change, resync the device by navigating to the main Cisco DNA Center dashboard, under **Tools** select **Inventory**, select the modified Catalyst 6800 switch, and then at the top, in the **Actions** pull-down, select **Resync**.

Tech tip
The IP pool used for LAN Automation should be sized significantly larger than the number of devices to be discovered. A minimum pool size of at least /25 is required. Addresses in the LAN Automation pool need to be reachable by Cisco DNA Center to successfully complete provisioning and must not be used anywhere else in the network. You must ensure that the route to the LAN Automation IP pool is available via the enterprise network infrastructure port. If the IP pool is not included in the configured routes on Cisco DNA Center, connect to Cisco DNA Center using SSH port 2222, and then login as maglev and execute the command: `sudo maglev-config update` Use the configuration wizard to configure the static routes to include the IP pool on the appropriate network adapter before starting LAN Automation.

Step 3. Navigate to **PROVISION > Devices > Inventory**. At the top, click the **LAN Automation** drop-down, and then click **LAN Automation**.

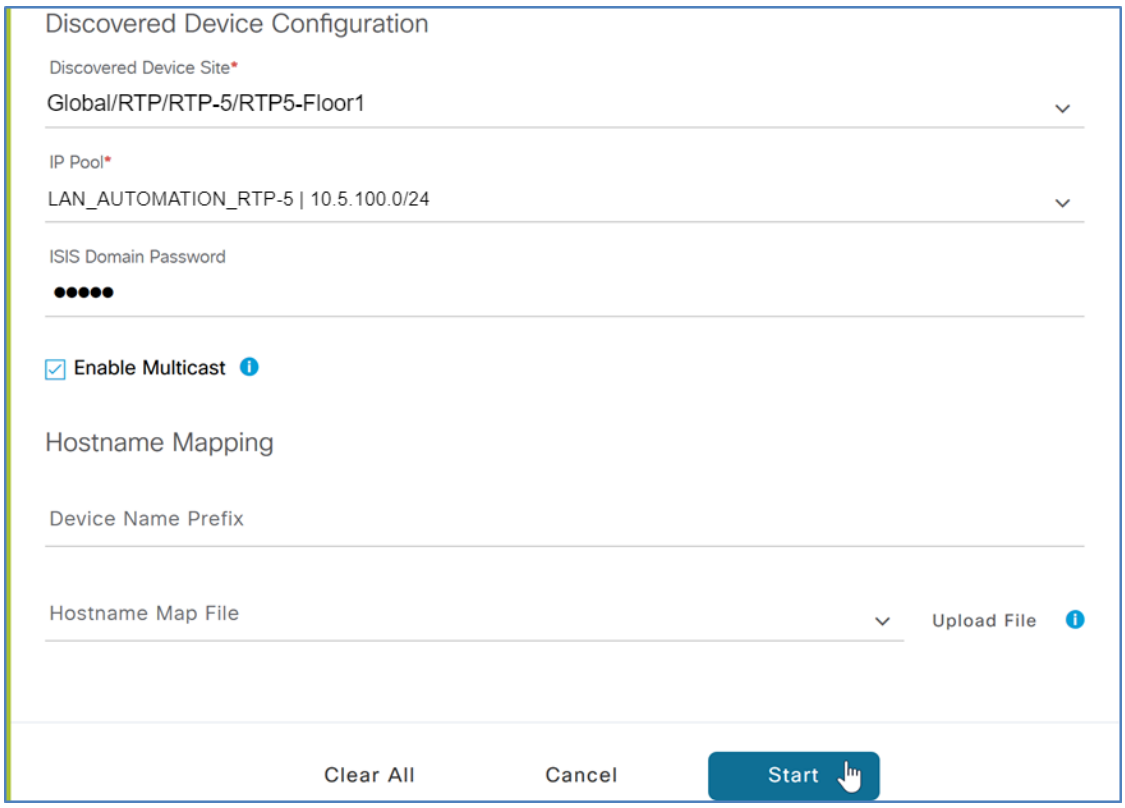


Step 4. On the right in the LAN Automation slide-out, fill in the parameters for the discovery. Under **Primary Device**, supply **Primary Site***, **Primary Device***, **Choose Primary Device Ports***, Under **Peer Device**, supply **Peer Site**, and **Peer Device**.

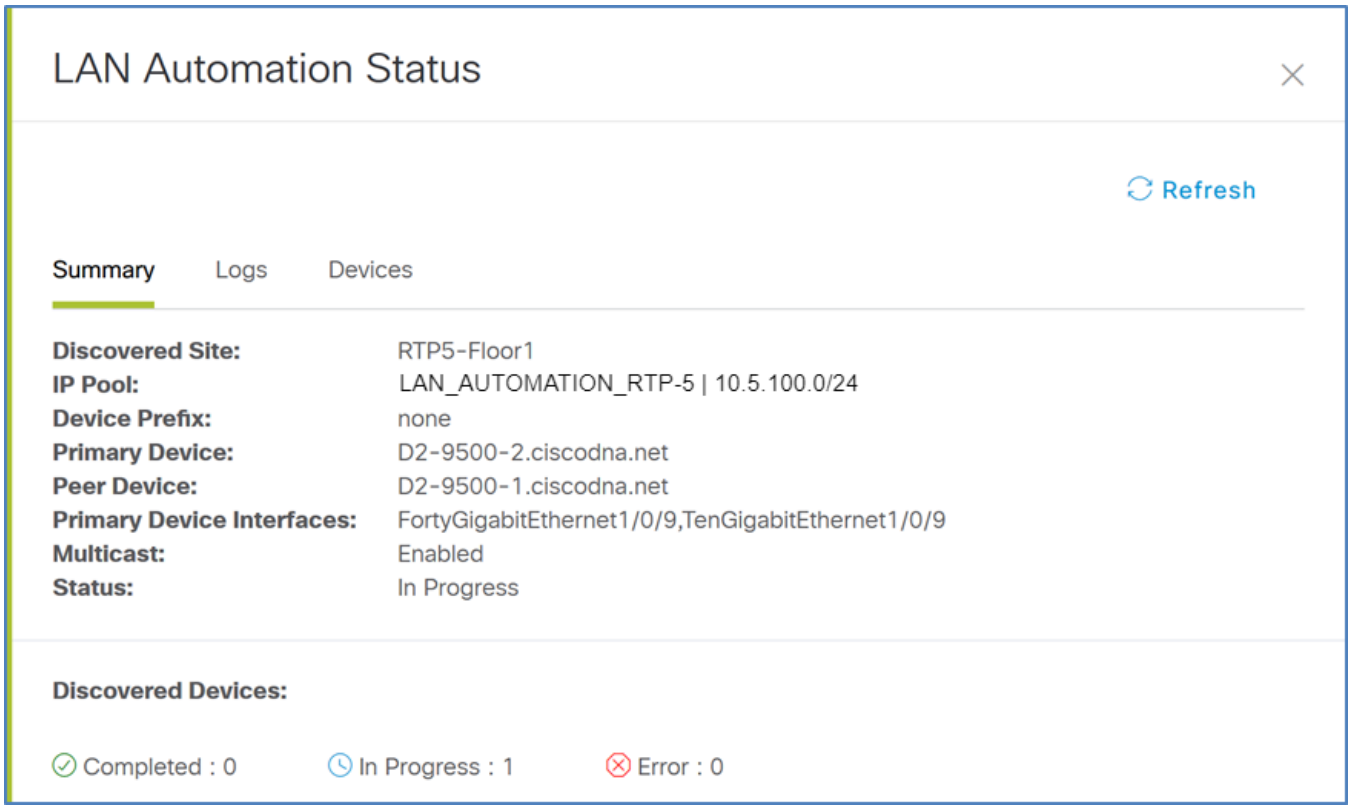


Tech tip
Select ports on the Primary Device where discovered devices are connected to or connected through. Example: If devices are connected to Te1/0/9 and Te1/0/10 in the example above, only the devices directly connected to or through Te1/0/9 will be discovered.

Step 5. On the right in the LAN Automation slide-out, continue filling in the parameters for the discovery. Under **Discovered Device Configuration**, supply **Discovered Device Site***, **IP Pool***, if used, supply the **ISIS Domain Password**, select **Enable Multicast**, then click **Start**.

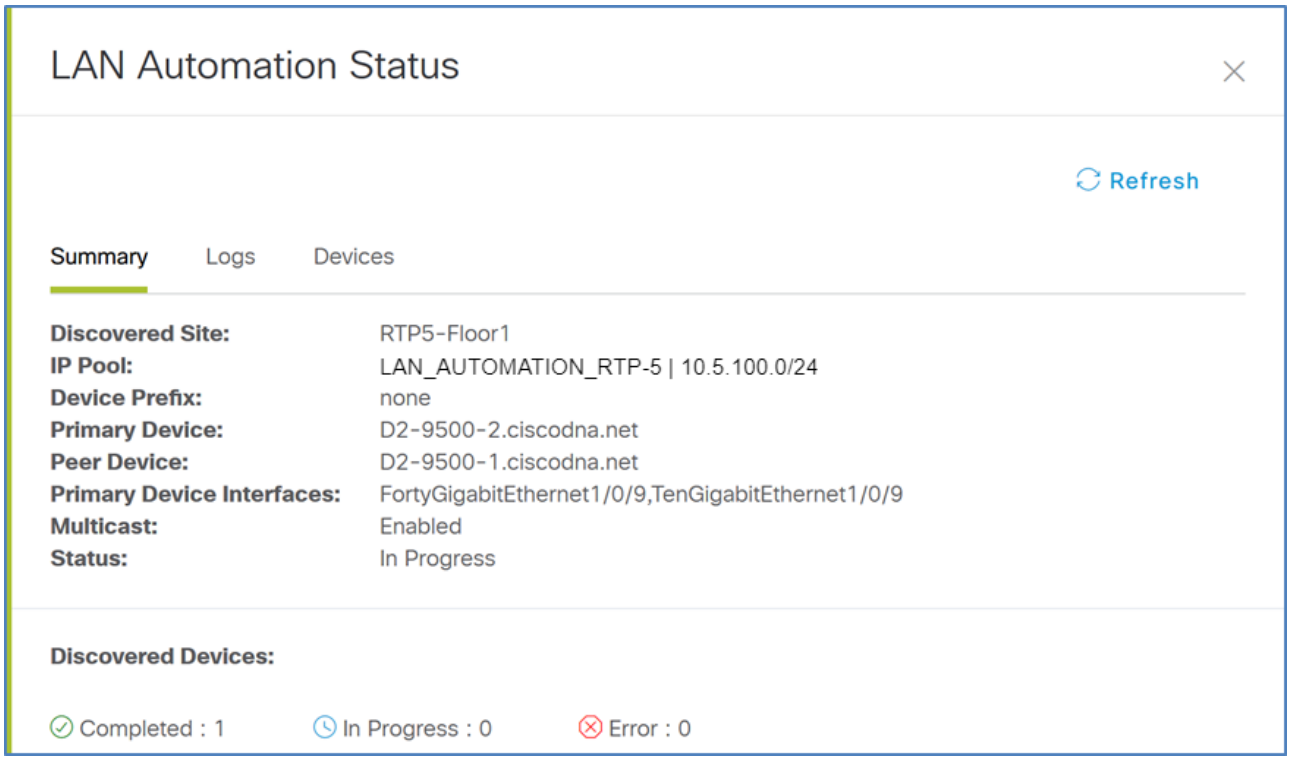


Step 6. At the top, click the **LAN Automation** drop-down, and then click **LAN Auto Status** to view progress.

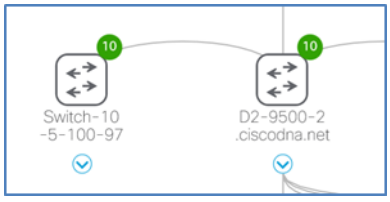


Do not click **Stop** in this step. Wait until all devices show a state of **Completed**, and then proceed to the next verification step. Prematurely stopping the LAN Automation process leaves the device in a state needing manual intervention for recovery as

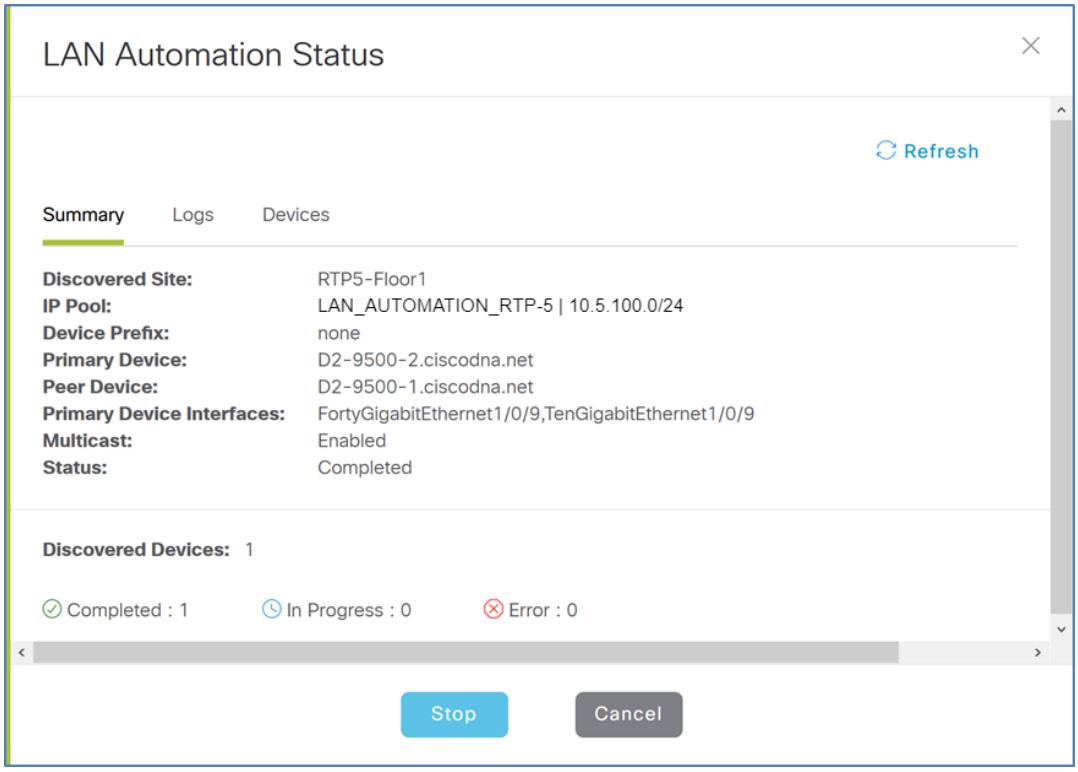
described in the Tech tip at the beginning of this procedure. Discovering devices an additional hop away from the seed can take significantly more time to reach completion.



Step 7. Navigate to the main Cisco DNA Center dashboard, under **Tools** select **Topology**. All links should be discovered. If any links are missing from the topology, verify the physical connectivity.



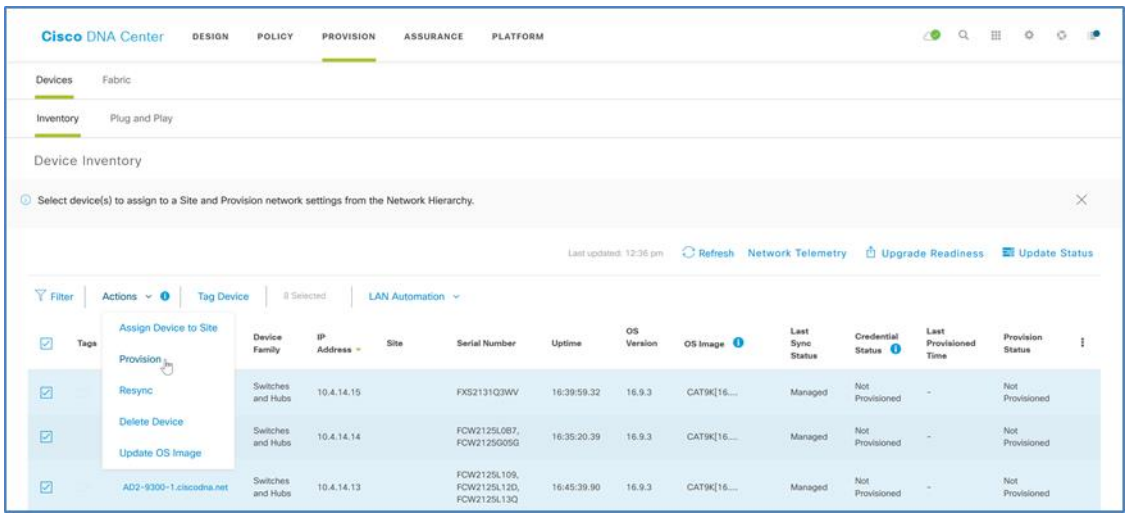
Step 8. Navigate to **PROVISION > Devices > Inventory**. At the top, click the **LAN Automation** drop-down, click **LAN Auto Status**. After the devices discovered all reach **Completed** state, click **Stop**. LAN Automation tears down all Layer 2 connectivity on VLAN 1 and the underlay IS-IS routing process is used for reachability to the discovered devices, and these devices are added and managed in Inventory.



Procedure 2. Provision devices and assign to sites to prepare for SD-Access

Provision the network devices, and then assign the devices to a site for integration into an SD-Access network.

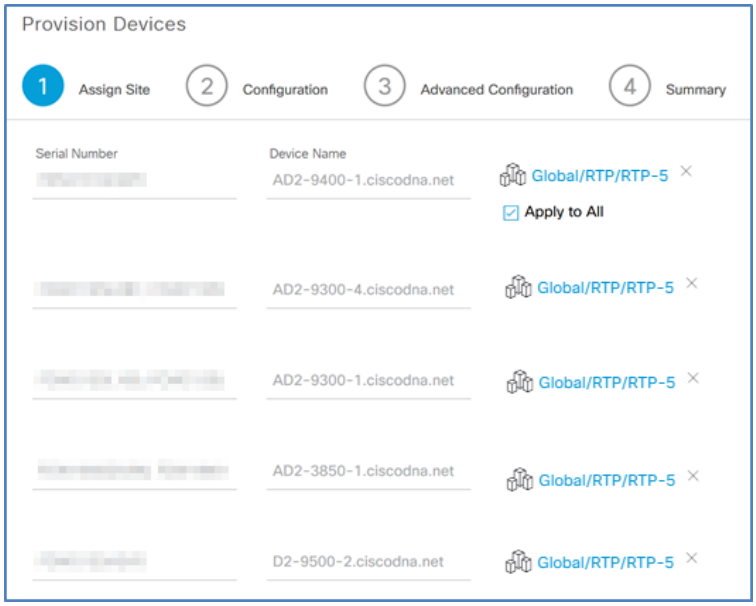
Step 1. In Cisco DNA Center, navigate to **PROVISION > Devices > Inventory**, select the devices of the same type (example: all switches) to provision into the network, click **Actions**, and then click **Provision**.



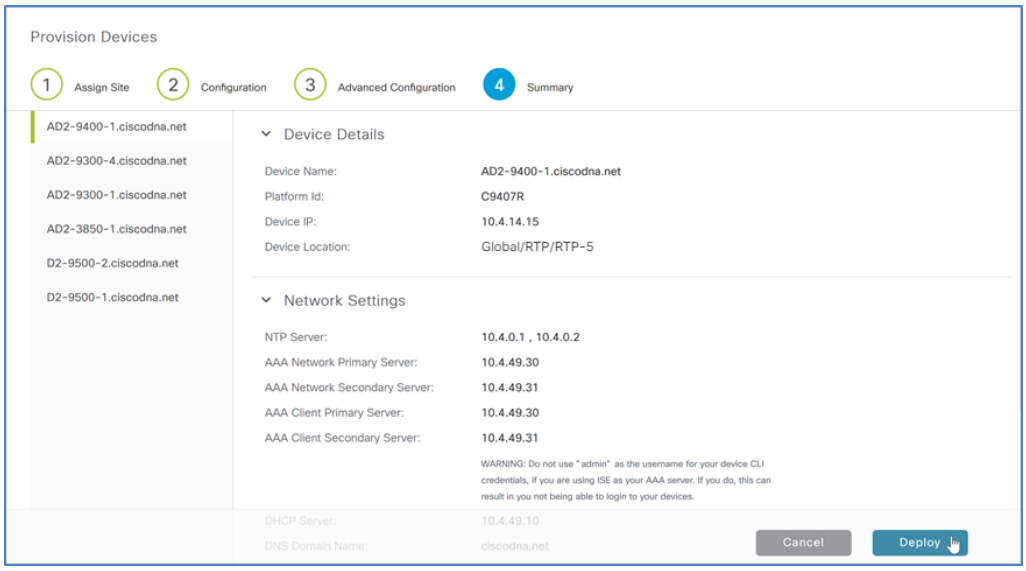
A **Provision Devices** wizard screen appears.

Tech tip
Devices must be of the same type (example: all routers) to provision them at the same time. You can group provisioning operations in multiple small batches for common site assignments as needed.

Step 2. Within the first wizard screen, select the site assignments for the devices, and then at the bottom of the screen click **Next**.



Step 3. Click **Next** twice to skip the **Configuration** and **Advanced Configuration** screens, in the **Summary** screen review the details for each device, and then click **Deploy**.

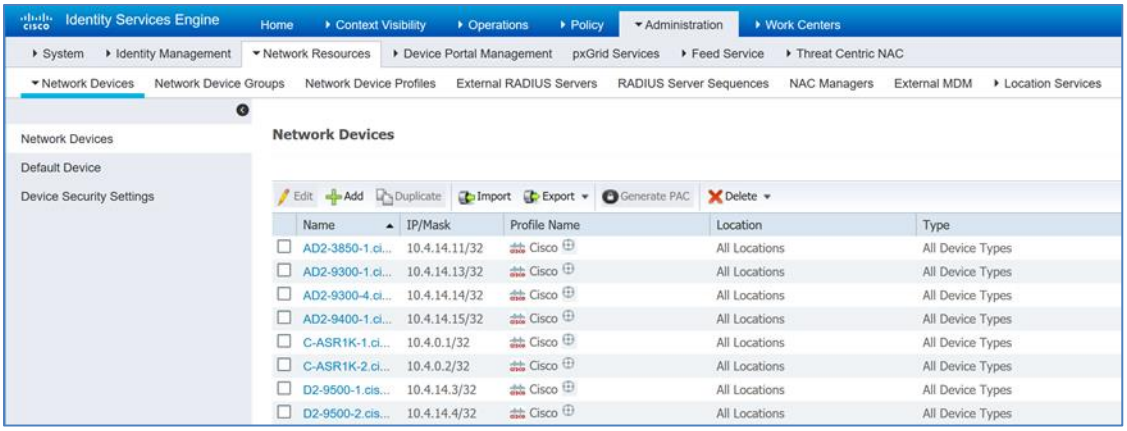


Step 4. At the popup screen, leave the default selection of **Now**, and click **Apply**.

Configuration of each device begins, and status messages appear as each device is provisioned successfully. The Device Inventory screen updates with **Provision Status** and **Sync Status**. Use the **Refresh** button to update the see the final provisioning status.

Step 5. Repeat the Cisco DNA Center provisioning steps for each batch of devices being added. The Cisco DNA Center pxGrid integration updates the devices in ISE.

Step 6. Verify the devices have been added to ISE as Network Devices by logging in to ISE and navigating to **Administration > Network Resources > Network Devices**. The provisioned devices appear.

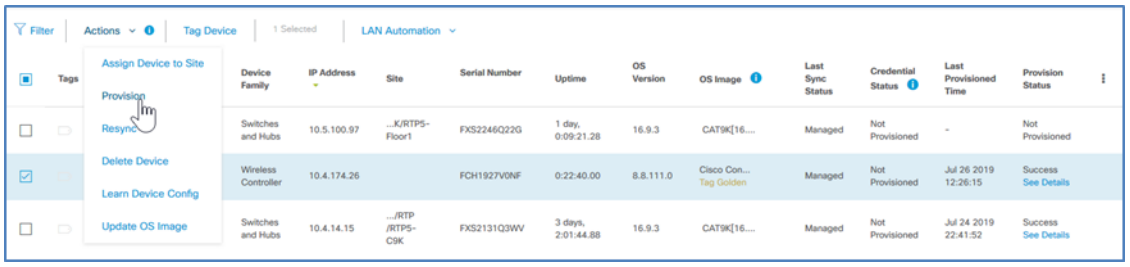


Procedure 3. Provision the WLC for SD-Access Wireless fabric integration

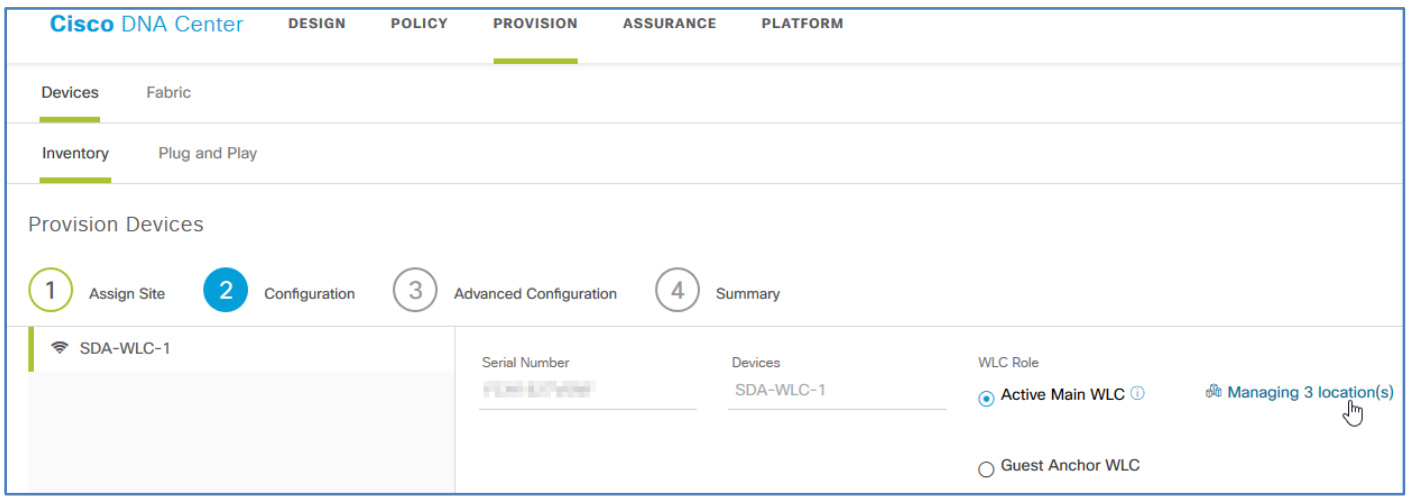
With the SD-Access Wireless design completed in previous steps, the configuration from the Design Application can be provisioned to the WLC.

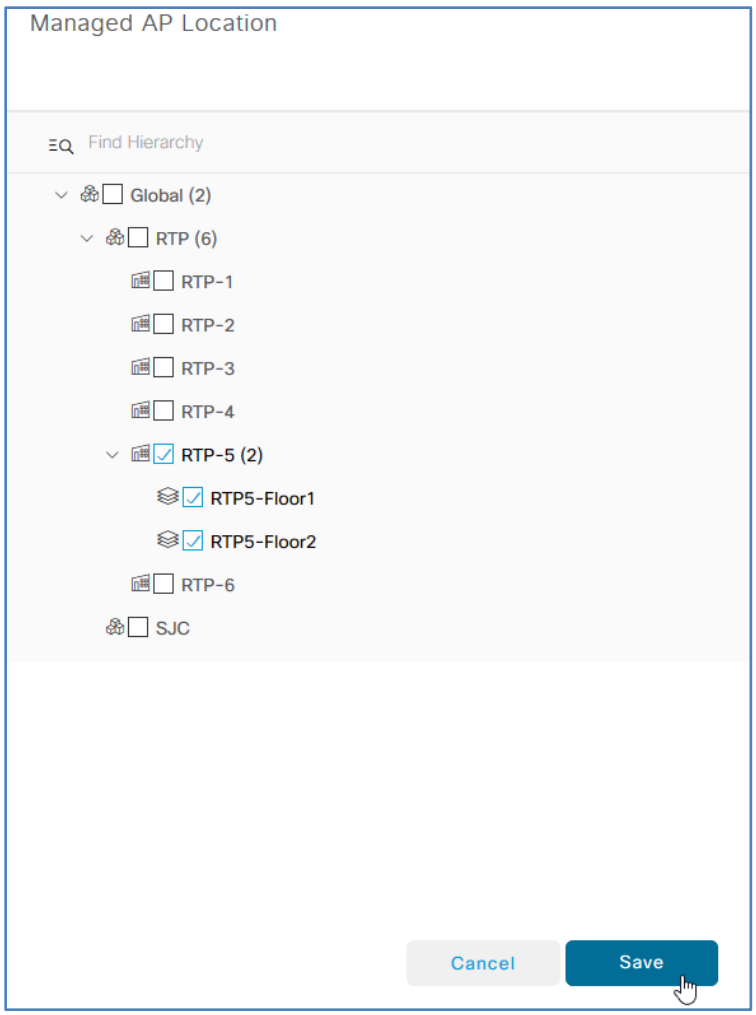
Step 1. Navigate to **PROVISION** > **Devices** > **Inventory**, select the checkbox next to the WLC, and then at the top of the screen under the **Actions** pull-down, select **Provision**. The Provision Devices wizard opens.

Tech tip
When a pair of WLCs is has been provisioned in HA SSO mode, a single WLC appears in the Cisco DNA Center inventory. You can verify that an HA SSO pair is configured by clicking the device name and then clicking the **High Availability** tab.



Step 2. Assign the site (example: Global/RTP/RTP-5), click **Next**, at the **Configuration** step under **Managed AP Location** select the additional floor assignments for APs managed by the WLC (example: Global/RTP/RTP5-C9K/Floor 1), click **Next**, and then at the **Advanced Configuration** step click **Next**.





Step 3. At the **Summary** step review the configurations, click **Deploy**, at the slide-out panel keep the default selection **Now**, and then click **Apply**.

The WLC is assigned to the site and the provisioning starts. Use the **Refresh** button until **Provision Status** shows **Success** before proceeding.

Operate

With IP reachability achieved, Cisco DNA Center is able to discover devices and add them to inventory. Using the DESIGN and POLICY applications, the desired intent for the network has been programmatically created. With LAN automation and SWIM, additional network devices have been onboarded into Cisco DNA Center, and their device code has been upgraded. With these steps complete, intent becomes reality as the previous processes, procedures, and steps culminate into the provisioning devices to create the SD-Access fabric.

Process 1: Provisioning the SD-Access Overlay Network

A fabric overlay network is created in Cisco DNA Center using the discovered devices added to inventory and provisioned to a site. Cisco DNA Center automates the additional device configuration supporting the SD-Access overlay networks.

The SD-Access solution supports provisioning of the following fabric constructs:

- Fabric site: An independent fabric, including control plane node and edge node functions, using a fabric border node to egress the fabric site and usually including an ISE PSN and fabric-mode WLC
- Transit site: Also known as a transit network, connects a fabric site to an external network (IP-based transit) or to one or more fabric sites while natively preserving segmentation (SD-Access transit)
- Fabric domain: Encompasses one or more fabric sites and any corresponding transit sites

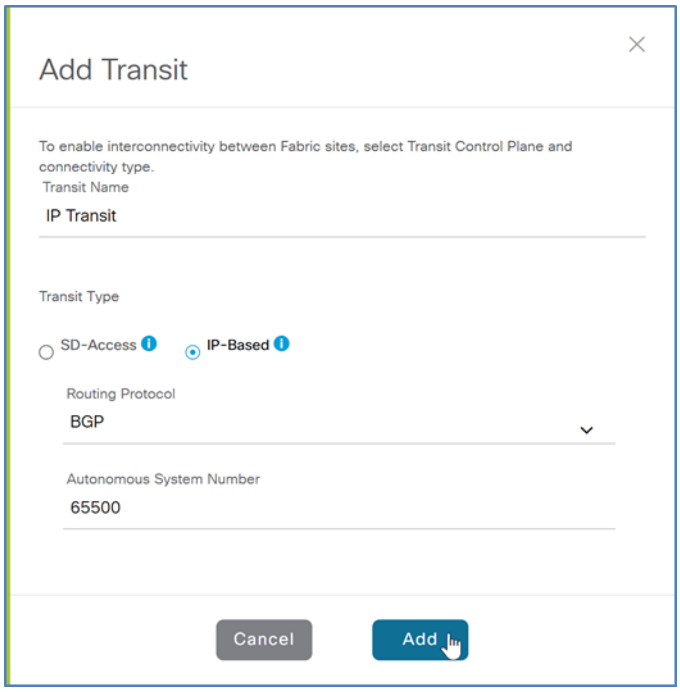
IP-based transit networks connect the fabric to external networks, typically using VRF-lite for IP connectivity. SD-Access transits carry SGT and VN information, inherently carrying policy and segmentation between fabric sites, creating a distributed campus.

Tech tip
Cisco DNA Center software and Cisco IOS software listed in the appendix does not include validation of the SD-Access transit, covered in the Software-Defined Access for Distributed Campus Prescriptive Deployment Guide. You can find alternative software versions that may support additional options by searching Cisco.com for SD-Access Hardware and Software Compatibility Matrix.

Procedure 1. Create an IP-based transit site, fabric domain, and fabric sites

The IP-based transit site represents the BGP remote autonomous system (AS). The local BGP AS is configured as part of the fabric border provisioning in a subsequent procedure.

Step 1. Using Cisco DNA Center, navigate to **PROVISION > Fabric**, at the top right click **+ Add Fabric or Transit**, click **Add Transit**, in the slide-out supply a **Transit Name** (example: IP Transit), select **IP-Based**, for **Routing Protocol** select **BGP**, enter an **Autonomous System Number** for the remote BGP AS (example: 65500), and then click **Add**.



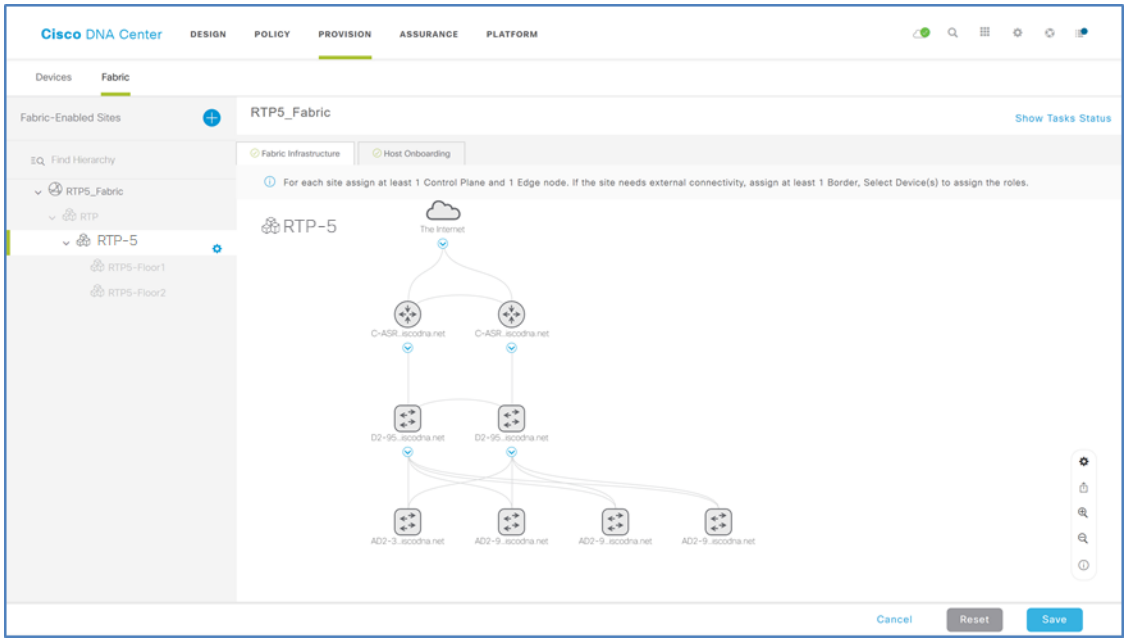
A status message appears, and the transit is created.

Step 2. Create a fabric domain by navigating to **PROVISION > Fabric**, at the top right click **+ Add Fabric or Transit**, click **Add Fabric**, in the slide-out supply a **Fabric Name** (example: RTP5_Fabric), use the site hierarchy to select a location including the sites for enabling the fabric (example: RTP5-C9K), and then click **Add**.

Tech tip
The Fabric Name (Fabric Domain name) cannot be the same as any other area, site, building, or floor defined in the hierarchy.

The new fabric domain is created.

Step 3. Click the fabric domain name just created (example: RTP5_Fabric), in the **Fabric-Enabled Sites** hierarchy on the left, choose the site added in the previous step (example: RTP5-C9K). A view of the fabric and related sites is displayed.



If the fabric topology diagram shown does not mimic the two-tier (distribution/access) or three-tier (core/distribution/access) topology that is deployed, correct the topology by navigating to **Tools > Inventory**, on the right side of the title row for the inventory table adjust which columns are displayed to include **Device Role**, and then adjust the role to best reflect the actual deployment of a device. Return to the fabric domain topology view after modifying device roles for an updated view.

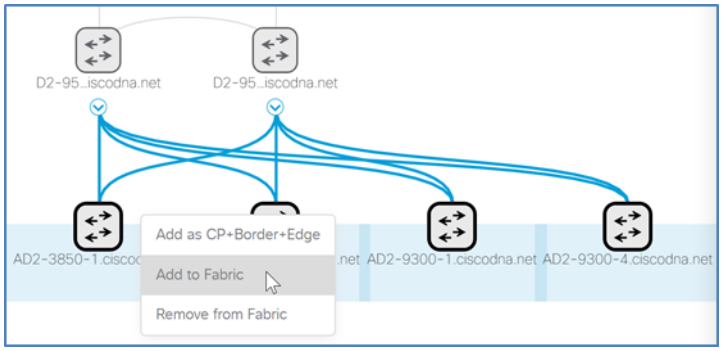
Tech tip

The device role is used to position devices in the Cisco DNA Center topology maps under the ***Fabric*** tab in the Provision application and in the Topology tool. The device positions in these applications and tools are shown using the classic three-tiered Core, Distribution, and Access layout.

Device Role	Topology Position
Internet (Not Selectable)	Top Row
Border Router	Below Internet (displayed with lines connected to the Internet Cloud)
Core	Third Row
Distribution	Fourth Row
Access	Bottom Row
Unknown	To the side of the Bottom Row

Procedure 2. Create a fabric overlay

Step 1. In the fabric domain topology view, hold the shift key, click all nodes that are fabric edge nodes, and then in the popup box, click **Add to Fabric**.



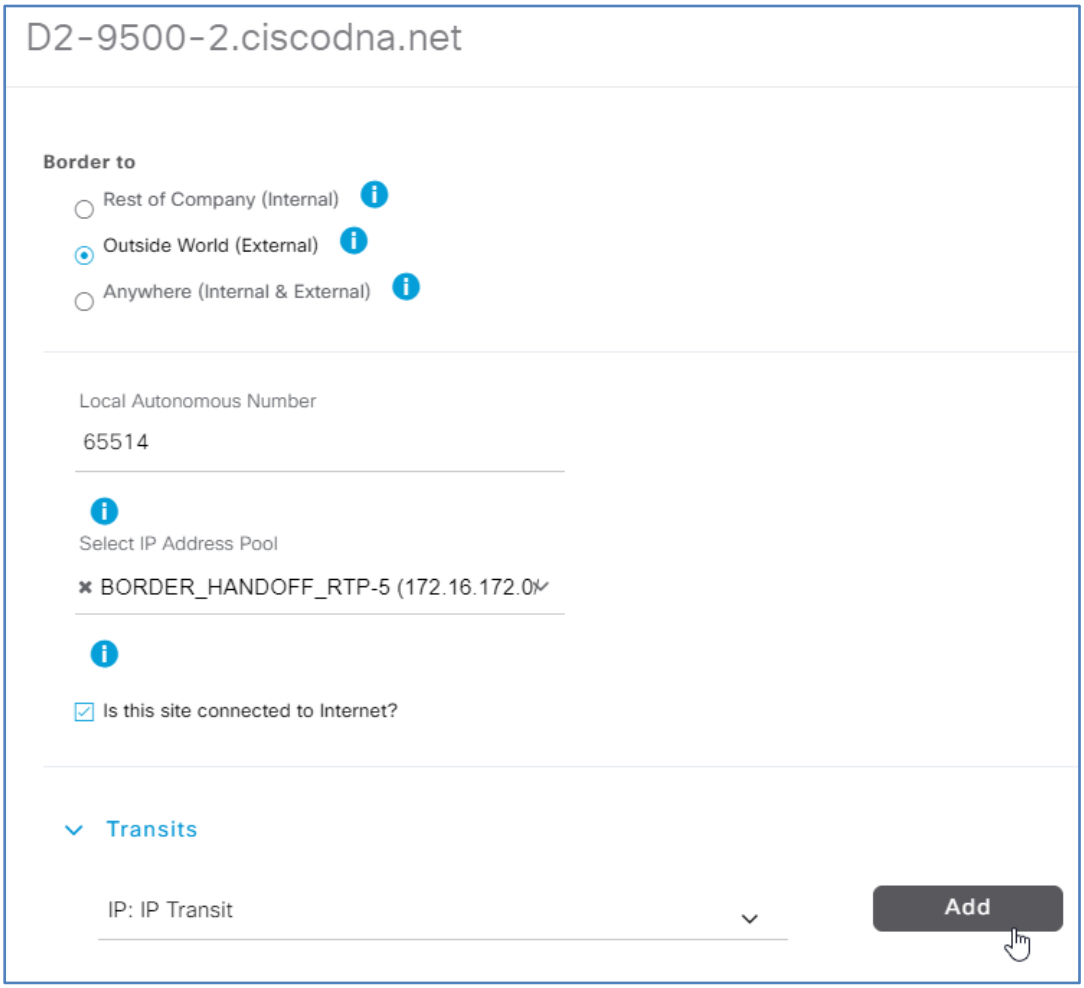
Blue icon borders and fabric role symbols appear, signifying the intended target behavior for the devices.

Step 2. If you have a node for the fabric dedicated to the role of being a control plane node without border functionality, click it, and then in the popup box, click **Add as CP** (control plane).

Repeat this step for a redundant dedicated control plane node without border functionality.

Tech tip
If the border nodes are Cisco Nexus 7700 Series Switches using the software listed in Appendix A: Product List, you use dedicated control plane nodes and connect them directly to the 7700 Series, configured as external border nodes. If your version of NX-OS requires it, enable the MPLS license. Configure MPLS LDP on the physical links to the control plane nodes to support the control plane connectivity.

Step 3. Click a device to perform the fabric border role, in the popup box click either **Add as Border** or **Add as CP+Border** (if skipping the previous step) and fill in the additional slide-out dialog. Under **Layer 3 Handoff**, select **Border** to (example: Outside World (External)), supply the **BGP Local Autonomous Number** (example: 65514), under **Select IP Address Pool** choose the global pool configured previously for border connectivity functionality (example: BORDER_HANDOFF-RTP5), for external borders select **Is this site connected to the Internet?**, in the **Transit** menu select the transit (example: IP: IP Transit), and then next to the transit click the gray **Add** button.



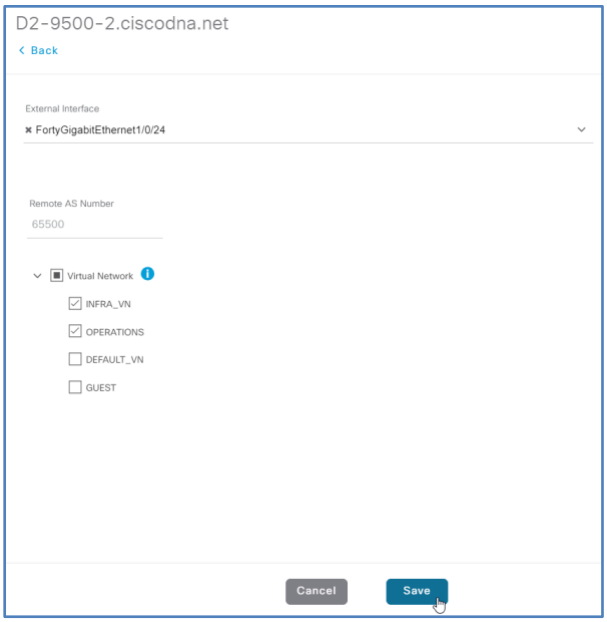
An additional **IP Transit** section appears.

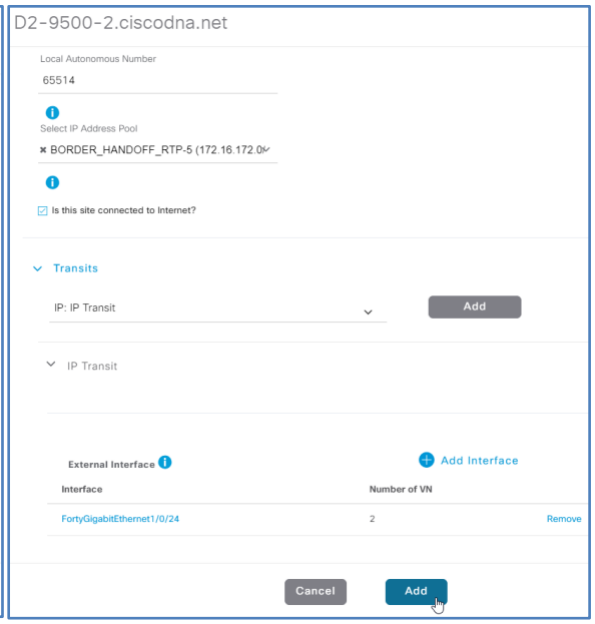
Tech tip

If the border is the only path to exit the fabric to the rest of the network, you should choose an external border. In cases where you have a combined control plane and border node functionality and the node uses internal border functionality, additional control plane filtering may be necessary when using the validated releases shown in Appendix A: Product List.

Step 4. Click the **IP Transit** text, click the **+ Add Interface** that appears, in the slide-out box select the interface for the connection to the fusion router outside of the fabric, below the BGP **Remote AS Number** for the device outside of the fabric that is displayed, expand the **Virtual Network** selection panel, select each VN used in the fabric to include in the Layer 3 handoff outside the fabric (examples: INFRA_VN, OPERATIONS), click **Save**, and then click **Add**.

Tech tip
INFRA_VN is special, predefined VN for infrastructure devices such as APs and Extended Nodes. It is not provisioned as a VRF definition on the devices. It is part of the overlay network, although is associated with the Global Routing Table.

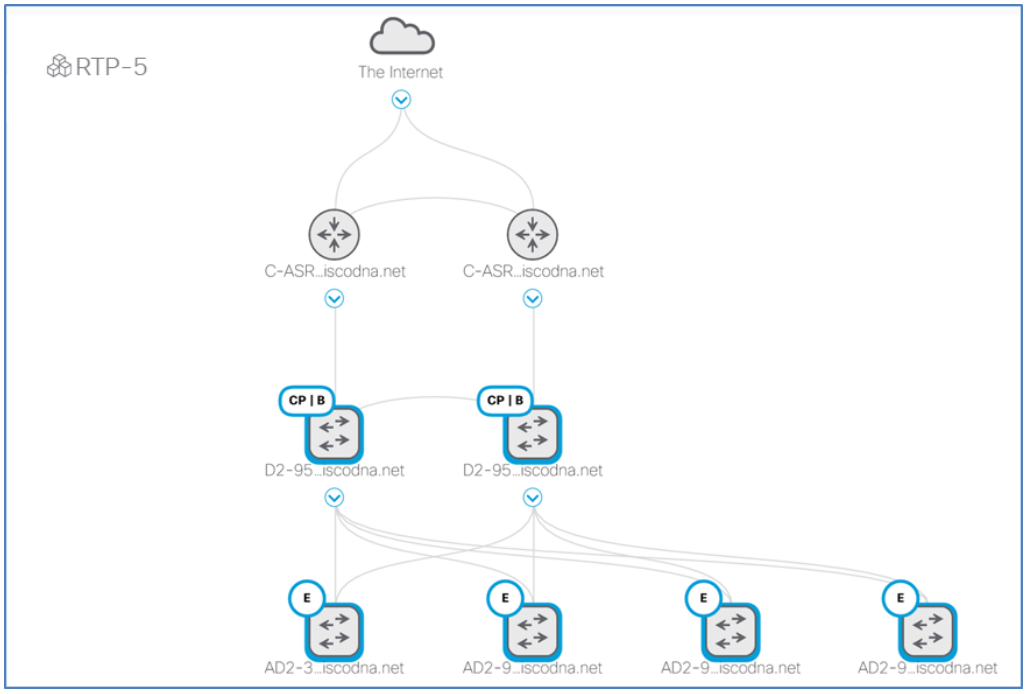




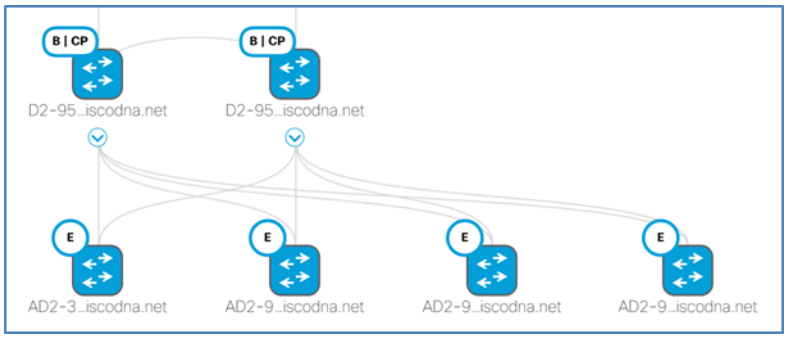
Acknowledge any additional informational pop-ups.

Step 5. If you have an additional fabric border node, repeat the previous two steps for it.

Step 6. After all required roles are assigned to the nodes in the fabric, at the bottom click **Save**, use the default choice **Now**, and then click **Apply**. Your campus fabric domain is created.



The fabric icons turn blue, signaling your intent to create the fabric. Actual provisioning of the devices can take longer to complete.



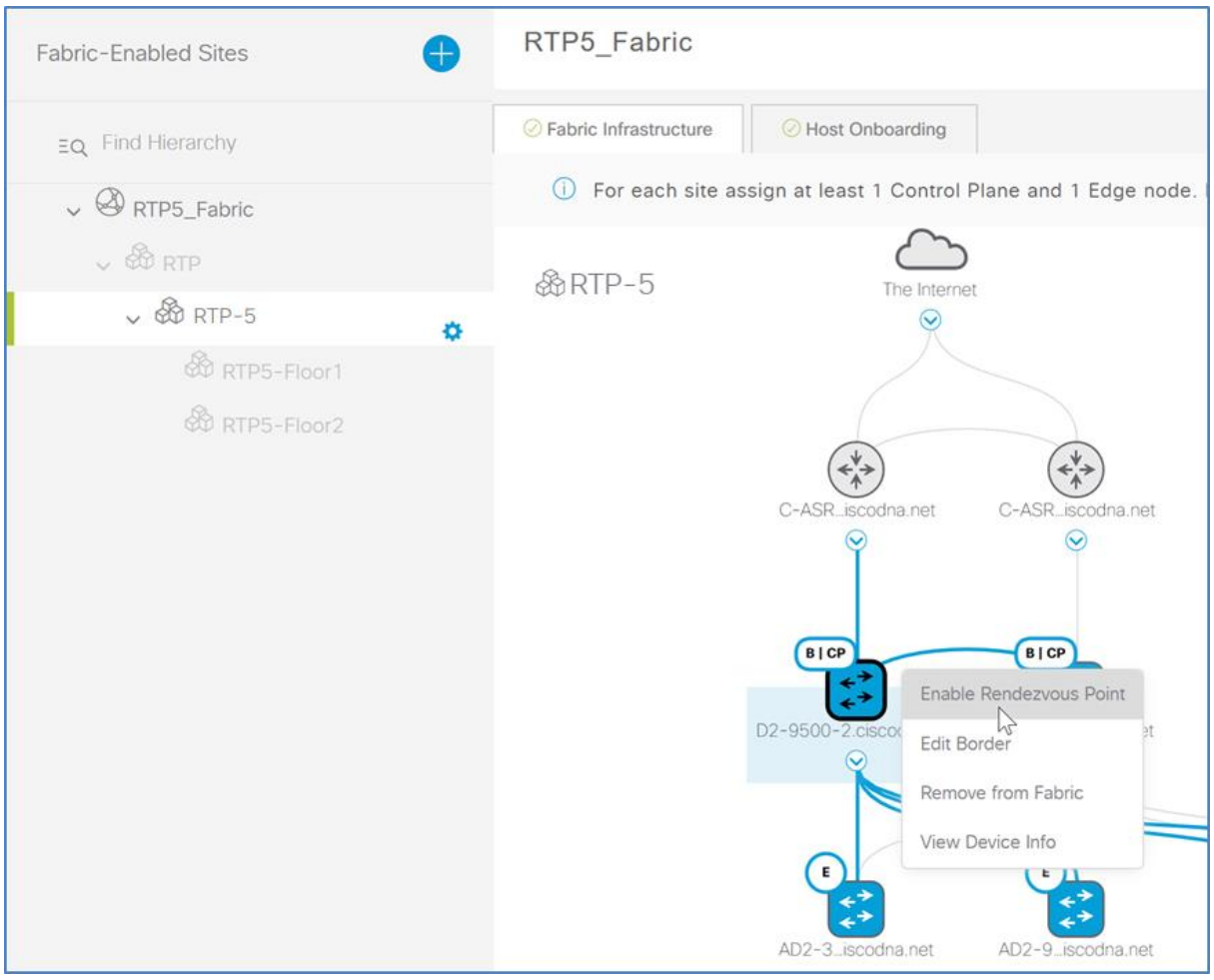
Procedure 3. Enable multicast for fabric

Use this procedure to configure native multicast support in the fabric overlay.

SD-Access fabrics can support Any Source Multicast (ASM) and Source Specific Multicast (SSM). Sources can be within the VN or outside of the fabric, and Rendezvous Point should be configured at fabric border nodes. PIM messages are unicast between the border nodes and the fabric edges, and multicast packets are replicated at the head end fabric border devices toward the fabric edge nodes.

Step 1. A global pool in Cisco DNA Center that is dedicated for unicast IP interfaces is used to configure multicast for each VN where multicast is enabled. If one does not exist, revisit the “Define Global IP Address Pools” procedure to create one.

Step 2. From the Cisco DNA Center dashboard, navigate to **PROVISION > Fabric**, under **Fabrics** click the created fabric site (example: RTP5_Fabric), in the left navigation pane, click the fabric site (example: RTP-5), at the top click the **Fabric Infrastructure** tab, click on a fabric border node, and then select **Enable Rendezvous Point**.



Step 3. Within the **Associate Multicast Pools to VNs** popup window at the right, under Associate Virtual Networks, choose the VN (example: OPERATIONS), under **Select IP Pools**, choose the pool created for multicast (example: MULTICAST_PEER_RTP-5), click **Next**, select a VN (example: OPERATIONS), and then click **Enable**.

Step 4. Repeat the previous step for any additional fabric border nodes. At the bottom of the screen, click **Save**, and then click **Apply**.

Cisco DNA Center provisions the multicast configurations to the fabric nodes and creates the loopbacks and Multicast Source Discovery Protocol (MSDP) peering for the rendezvous point (RP) state communication between the border nodes.

Step 5. If multicast communication is required outside of the border toward the fusion router, enable the following commands on each border node.

Global:

```
ip multicast-routing
ip pim rp address [RP Address]
ip pim register-source Loopback0
ip pim ssm default
```

Interface or subinterface (for each virtual network):

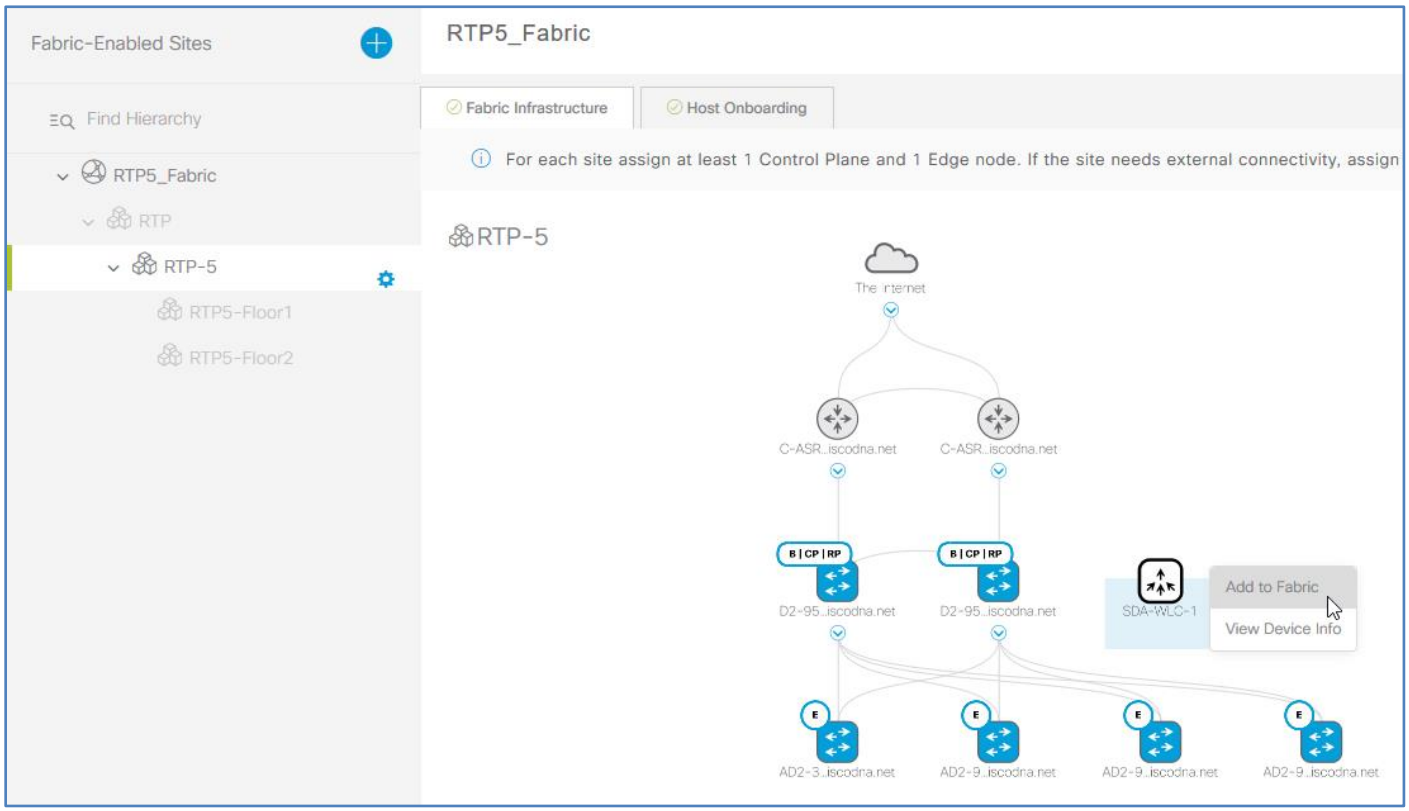
```
ip pim sparse-mode
```

Step 6. In the left navigation panel at the site configured with the fabric, next to the site name click the gear icon, click **Enable Native Multicast for IPv4**, at the bottom click **Save**, at the slide out window, leave the default selection of **Now**, and then click **Apply**.

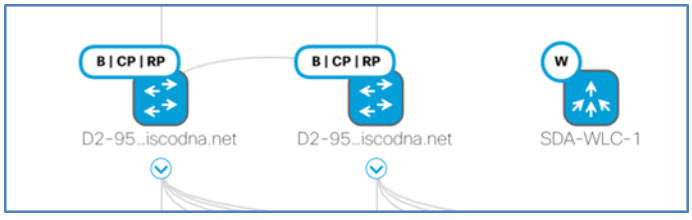
Tech tip
Multicast in the fabric overlay uses head end replication. The closest fabric node to the multicast source will replicate (create a unicast stream) for each receiver fabric node using the overlay. When Native Multicast is enabled, a designated PIM-SSM group in the underlay is used for replication resulting in more efficient use of the infrastructure.

Procedure 4. Provision SD-Access Wireless into the fabric

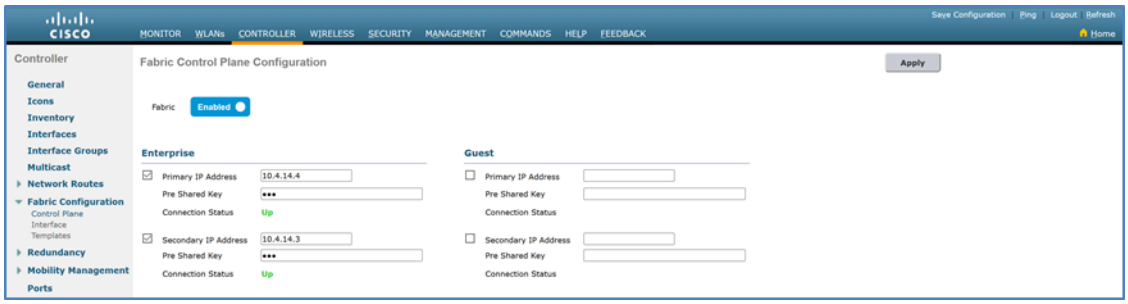
Step 1. From the Cisco DNA Center dashboard, navigate to **PROVISION > Fabric**, under **Fabric** click the created fabric site (example: RTP5_Fabric), on the left in the **Fabric-Enabled Sites** navigation click the associated site (example: Global/RTP/RTP-5), click the WLC, and then in the popup box click **Add to Fabric**.



Step 2. At the bottom of the screen click **Save**, in the slide-out menu keep the default selection **Now**, and then click **Apply**. The WLC configurations are created to establish a secure connection to the fabric control plane nodes.



You can verify that WLC controller pair is integrated into the fabric from the WLC management console by navigating to **CONTROLLER > Fabric Configuration > Control Plane**, which shows the fabric integration is enabled with the connection status up.



Procedure 5. Enable eBGP connectivity for VN at neighbor (fusion) to border router

The SD-Access application in Cisco DNA Center configures the fabric border node BGP handoff to external networks. In the SD-Access version described, you manually configure the external network peers of the border devices with the compatible VRF-Lite and BGP peering information.

Tech tip
The VRF name, route distinguisher, and route target you configure on the fusion router should match the configuration on the border node.

Step 1. Use the CLI to login to the border devices to observe the automated configurations for IP connectivity outside of the border created by the Cisco DNA Center SD-Access application. Some of the following commands may be helpful.

```
show running-config brief
show running-config | section vrf definition
show running-config | section interface Vlan
show running-config | section router bgp
```

Tech tip
You protect against connectivity failures between border nodes and fusion routers by deploying a resilient pair of border nodes with a direct connection between them. To enable automatic traffic redirection, create an iBGP neighbor relationship between the border nodes for every configured VN. Support the multiple logical connections using 802.1Q tagging using trunk port configurations on switches and subinterfaces on routers.

Step 2. Log in to each fusion device external to the fabric that is connected to the border, using the border configuration as a guide, and configure the same VRF configuration. VRFs separate communication between groups of interfaces and virtual network contexts within the fabric.

```
vrf definition [VRF name]
 rd [Route Distinguisher]
 address-family ipv4
  route-target export [Route Target]
  route-target import [Route Target]
 exit-address-family
```

As an example, if the following configuration is provisioned on the border:

```
vrf definition OPERATIONS
 rd 1:4099
 !
```

```
 address-family ipv4
  route-target export 1:4099
  route-target import 1:4099
 exit-address-family
```

Configure the same VRFs and route-targets on the fusion router.

Repeat this step for each virtual network context (including the GUEST VRF, if you have configured one), consistent with the border node configuration.

Step 3. Configure each interface to the neighbor. Some devices support VLAN subinterface configuration directly on trunks, and other devices require VLAN interfaces to be created and associated with a trunk. Repeat the neighbor interface configuration for each neighbor on each peer to the border.

```
interface [Peer physical interface]
 switchport mode trunk
interface [VLAN interface]
 vrf forwarding [VN/VRF name]
 ip address [Peer point-to-point IP address]
```

As an example, if the following configuration is provisioned on the border:

```
vlan 3003
vlan 3004
interface FortyGigabitEthernet1/0/24
 switchport mode trunk
interface Vlan3003
 description vrf interface to External router
 vrf forwarding OPERATIONS
 ip address 172.16.172.9 255.255.255.252
interface Vlan3004
 description vrf interface to External router
 ip address 172.16.172.13 255.255.255.252
```

Configure compatible connectivity and addressing for the fusion router. A VLAN interface without an associated VRF forwarding statement is used for the INFRA_VN communication to the global route table.

```
interface TenGigabitEthernet0/1/7.3003
 description vrf interface to External router
 encapsulation dot1q 3003
 vrf forwarding OPERATIONS
 ip address 172.16.172.10 255.255.255.252
interface TenGigabitEthernet0/1/7.3004
 description vrf interface to External router
 encapsulation dot1q 3004
 description vrf interface to External router
 ip address 172.16.172.14 255.255.255.252
```

Step 4. Configure BGP IPv4 unicast routing towards the border to support connectivity for each VRF associated with each VN in the fabric.

```
router bgp [Local BGP AS]
 bgp router-id interface Loopback0
 bgp log-neighbor-changes
 neighbor [Border VLAN IP Address] remote-as [Fabric BGP AS]
 neighbor [Border VLAN IP Address] update-source [VLAN interface]
 ! repeat for any additional neighbors
address-family ipv4
  network [Loopback IP Address] mask 255.255.255.255
  neighbor [Border VLAN IP Address] activate
! repeat for any additional neighbors
  maximum-paths 2
 exit-address-family
 address-family ipv4 vrf [VN/VRF name]
  neighbor [Border VLAN IP Address] remote-as [Fabric BGP AS]
  neighbor [Border VLAN IP Address] update-source [VLAN interface]
  neighbor [Border VLAN IP Address] activate
! repeat for any additional neighbors
 exit-address-family
```

As an example, if the following configuration is provisioned on the border:

```
router bgp 65514
 bgp router-id interface Loopback0
 neighbor 172.16.172.14 remote-as 65500
 neighbor 172.16.172.14 update-source Vlan3004
 !
 address-family ipv4
  network 172.16.173.1 mask 255.255.255.255
  aggregate-address 172.16.173.0 255.255.255.0 summary-only
  neighbor 172.16.172.14 activate
exit-address-family
 !
 address-family ipv4 vrf OPERATIONS
  neighbor 172.16.172.10 remote-as 65500
  neighbor 172.16.172.10 update-source Vlan3003
  neighbor 172.16.172.10 activate
exit-address-family
```

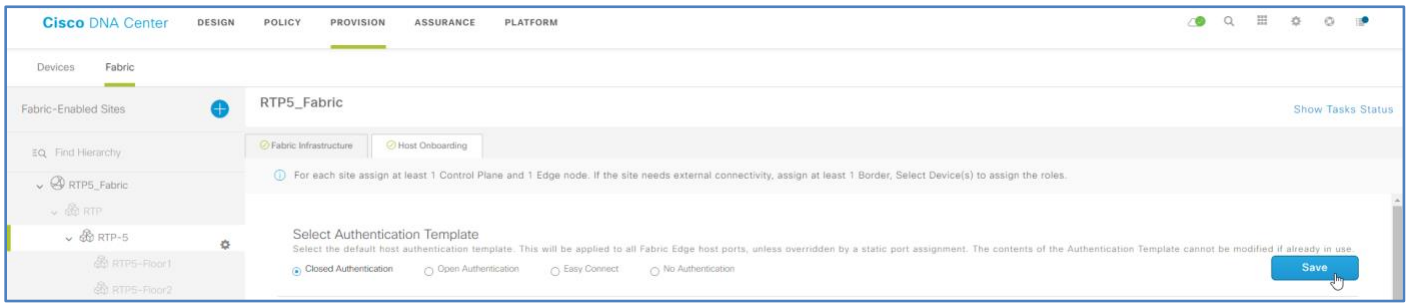
Configure the following on the fusion router:

```
router bgp 65500
 bgp router-id interface Loopback0
 bgp log-neighbor-changes
```

```
 neighbor 172.16.172.13 remote-as 65514
 neighbor 172.16.172.13 update-source TenGigabitEthernet0/1/7.3004
 !
 address-family ipv4
  neighbor 172.16.172.13 activate
 exit-address-family
 !
 address-family ipv4 vrf OPERATIONS
  neighbor 172.16.172.9 remote-as 65500
  neighbor 172.16.172.9 update-source TenGigabitEthernet0/1/7.3003
  neighbor 172.16.172.9 activate
exit-address-family
```

Procedure 6. Assign wired clients to VN and enable connectivity

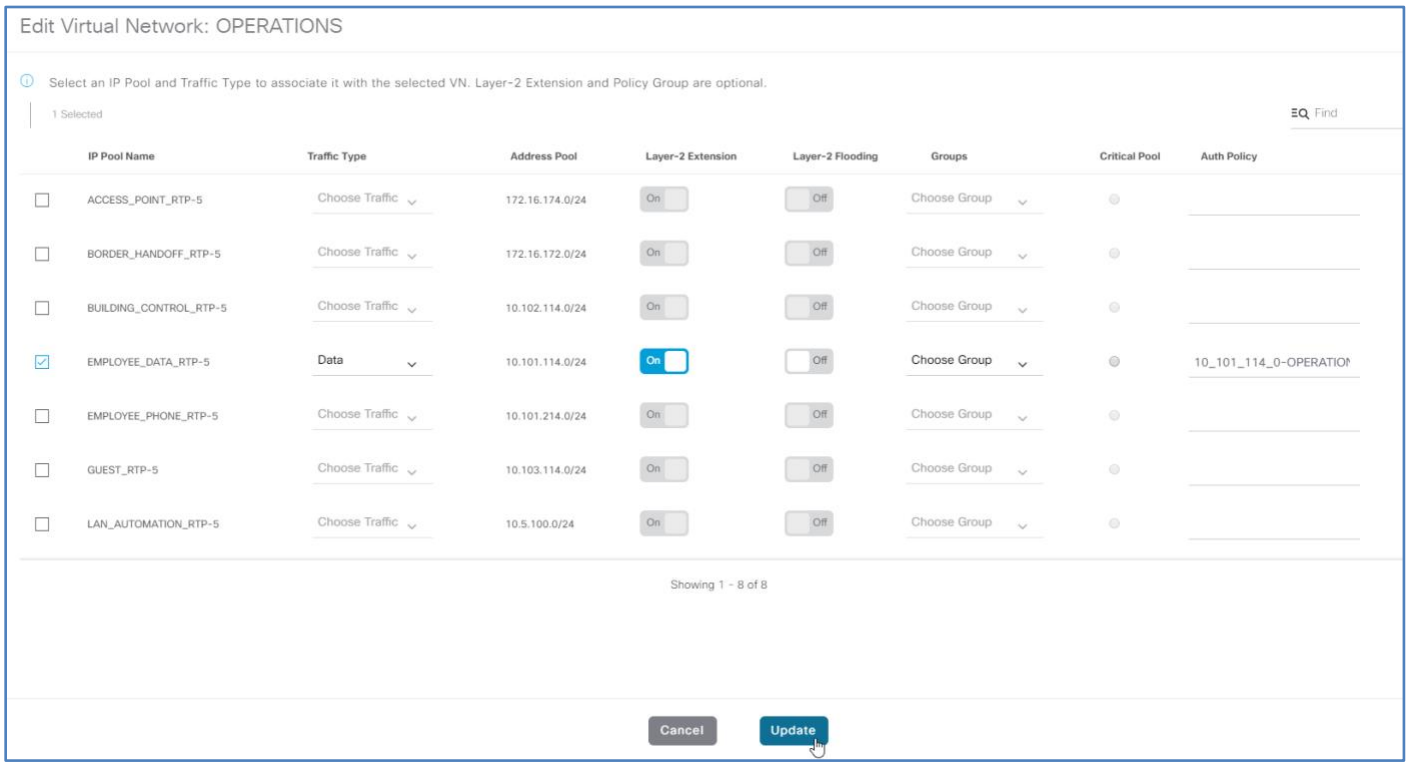
Step 1. From the Cisco DNA Center dashboard, navigate to **PROVISION > Fabric**, under **Fabrics** click the created fabric site (example: RTP5_Fabric), in the left navigation pane, click the fabric site (example: RTP5-C9K), at the top click the **Host Onboarding** tab, under **Select Authentication template** select **Closed Authentication**, at the top of the section click **Save**, and then click **Apply**.



Closed authentication is set as the default for host ports, requiring 802.1x authentication for an endpoint to connect to the fabric; this setting can be overridden by port for other purposes, such as for AP ports.

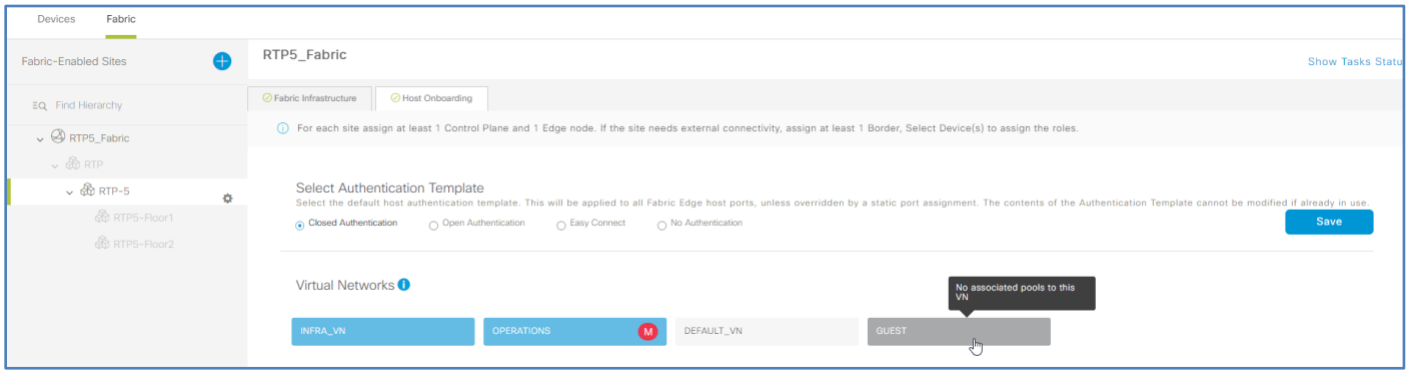
Tech tip
An authentication template must be selected before moving onto the next step. These templates are predefined in Cisco DNA Center and are pushed down to all devices that are operating as edge nodes within a site.

Step 2. Under **Virtual Networks**, select a VN to be used for wired clients (example: OPERATIONS), in the **Edit Virtual Network: *OPERATIONS*** slide-out pane, select the names of **IP Pools** to add to the VN (example: EMPLOYEE_DATA_RTP-5), select a **Traffic Type** of **Data**, verify that **Layer 2 Extension** is **On**, optionally change the **Auth Policy**, click **Update**, and then click **Apply**.

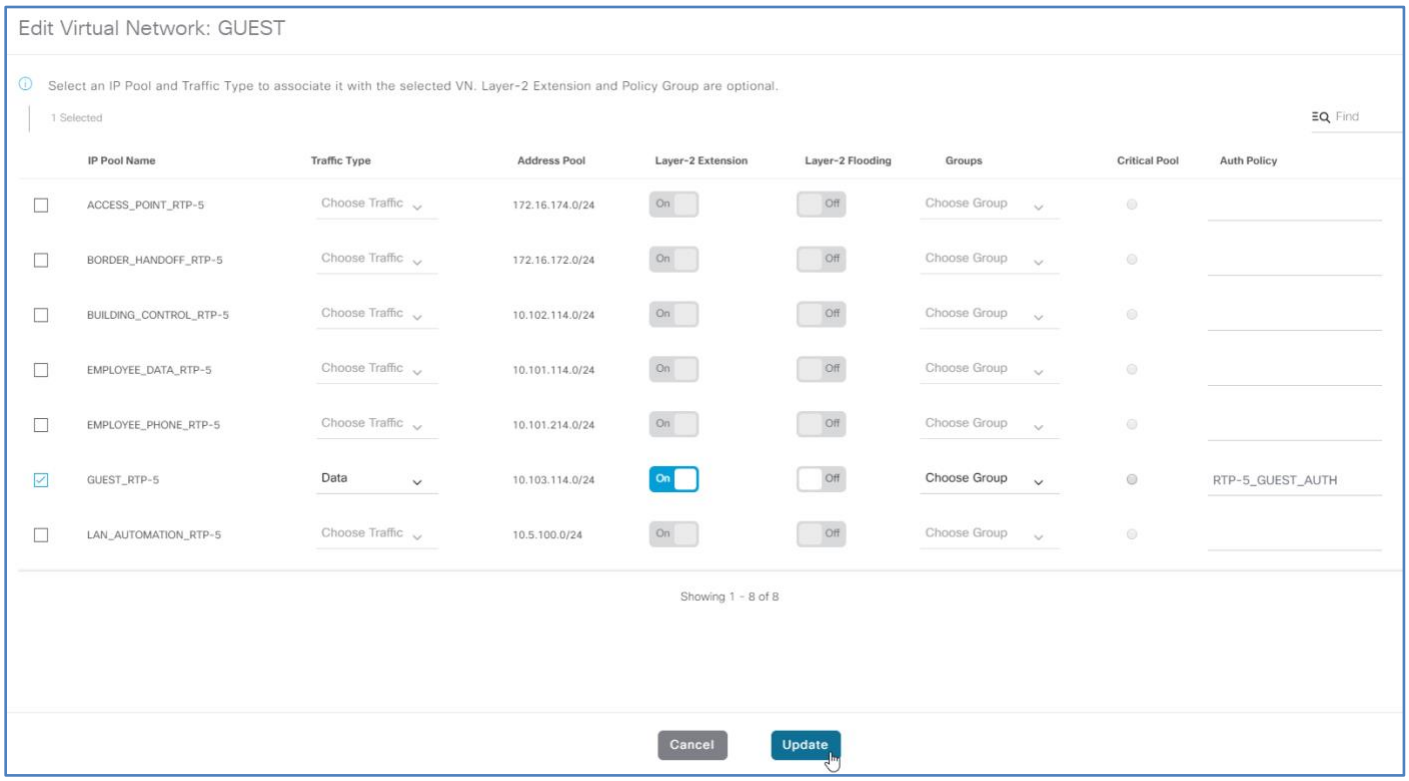


A status message displays, and then the **Host Onboarding** screen displays.

Step 3. If you have created a guest virtual network, associate an IP pool for guest services. Under **Virtual Networks**, select a VN to be used for guest wireless clients (example: GUEST).



Step 4. In the **Edit Virtual Network: *GUEST*** slide-out pane, select the names of **IP Pools** to add to the VN (example: GUEST_RTP-5), select a **Traffic Type** of **Data**, verify that **Layer 2 Extension** is **On**, optionally change the **Auth Policy** (example: RTP-5_GUEST_AUTH), click **Update**, and then click **Apply**.



A status message displays, and then the **Host Onboarding** screen displays.

Tech tip
Beginning with Cisco DNA Center 1.2.5, the VLAN name, which also corresponds to the **Auth Policy** name, for a given IP subnet is pushed to the Authorization Profile page in ISE. This can be found by navigation to **ISE** > **Policy** > **Policy Elements** > **Results** > **Authorization** > **Authorization Profiles**. You can use the VLAN name that is generated by default in Cisco DNA Center or modify the VLAN name as needed to help ease Authorization Policy creation workflows in ISE.

Procedure 7. Enable fabric edge ports for client onboarding

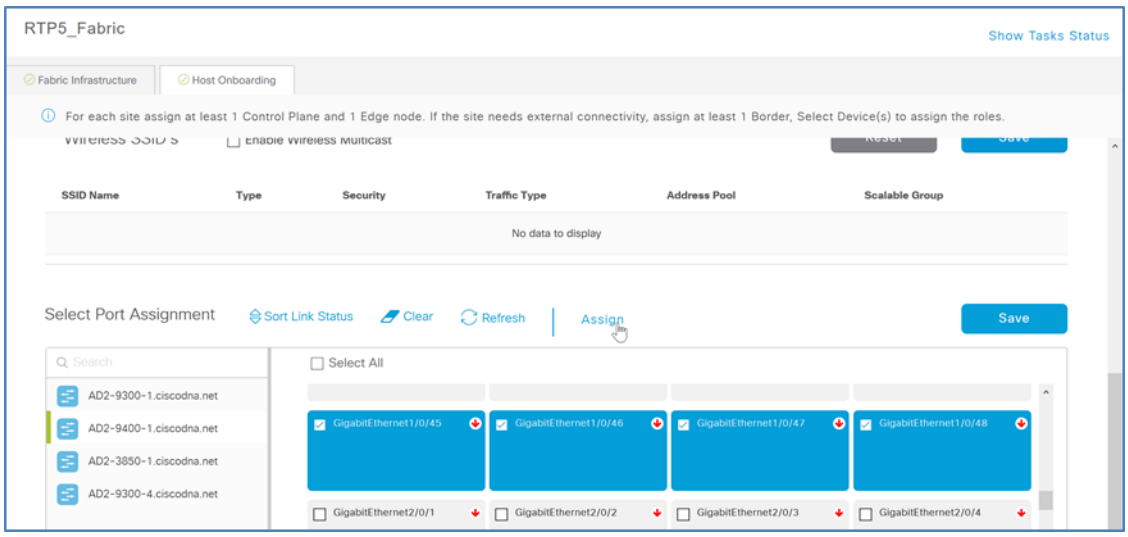
Optional

Overwrite the default authentication template (closed authentication) assigned in the previous procedure, when you have devices connected that do not support 802.1x, or when using other authentication methods, such as MAB authentication for IOT devices, or when manually assigning an address pool to a port.

Repeat this procedure for each fabric edge switch with clients connecting to fabric edge ports requiring an overwriting of the default authentication template.

Step 1. Navigate to **PROVISION > Fabric**, under **Fabrics** click the created fabric site (example: RTP5_Fabric), in the left navigation pane, click the fabric site (example: RTP5-C9K), at the top click the **Host Onboarding** tab, and under the **Select Port Assignment** section, in the left column, select a switch.

Step 2. Within the list of switch ports, select a set of wired fabric edge ports to participate in a fabric VN, and then click **Assign**.



Step 3. In the slide-out, select the appropriate **Connected Device Type** (example: User Devices (ip-phone,computer,laptop)), select the **Address Pool** (example: 10_101_114_0(EMPLOYEE-DATA-RTP5)), select the **Group** (example: Employees), select a **Voice Pool** if it is required, select an **Auth Template** (example: No Authentication), and then click **Update**.

Tech tip
The group assignment is used to statically assign a group if the fabric edge port does not receive its assignment dynamically from ISE.

Step 4. To the right of the **Select Port Assignment** section, select **Save**, leave the default selection of **Now**, and then click **Apply**.

Step 5. Repeat the previous steps for each additional switch being added.

Devices can now connect at the fabric edge ports using the wired network overlay and authentication method created.

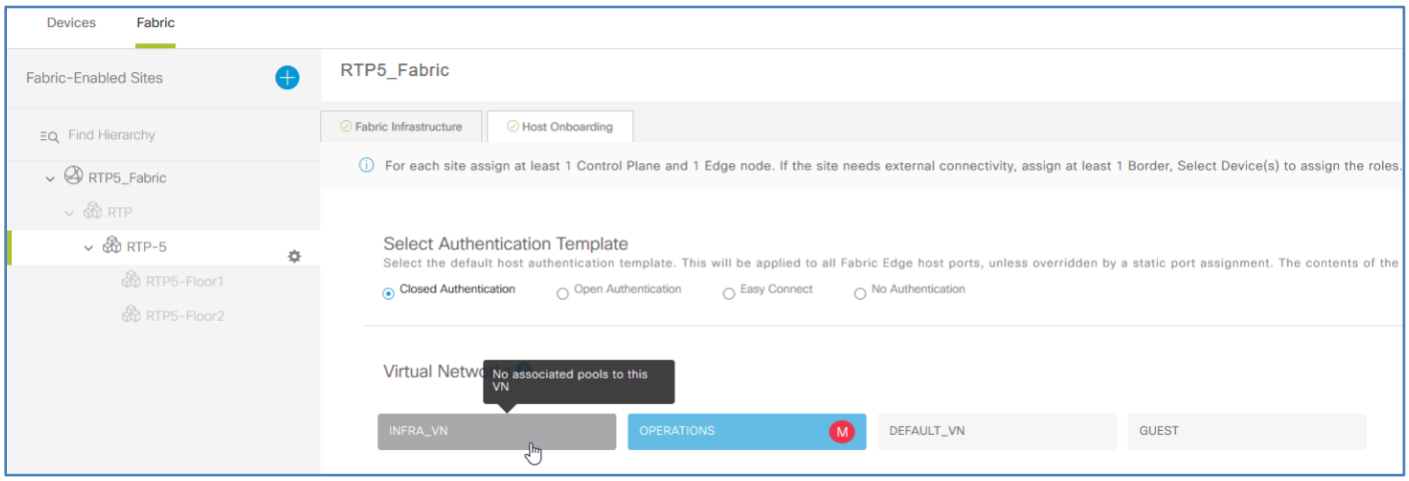
Procedure 8. Enable onboarding of access points into the wireless fabric

The APs are infrastructure devices that join the fabric and are assigned into a pre-defined VN named INFRA_VN. This special VN for infrastructure devices such as APs, enables management communication between the APs at the fabric edge nodes using the fabric control plane and the WLC sitting outside of the fabric as a part of global routing connectivity.

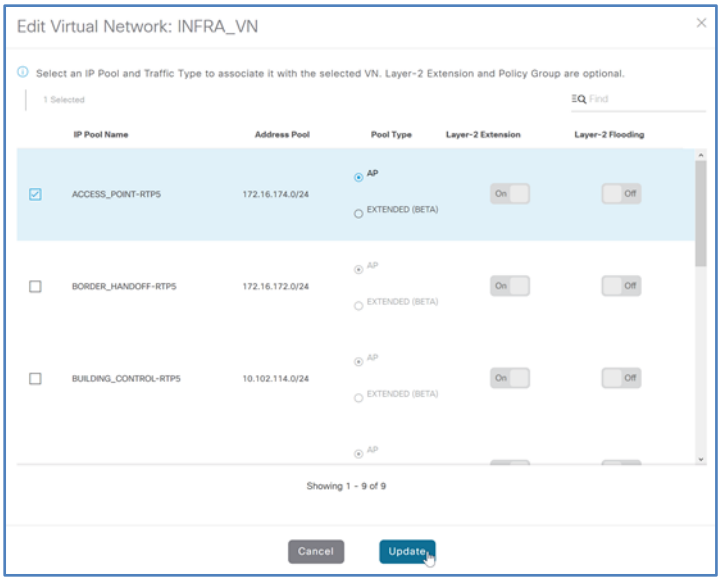
Step 1. Connect APs to be used for the fabric directly to an edge node within the fabric.

Step 2. From the Cisco DNA Center dashboard, navigate to **PROVISION > Fabric**, under **Fabric Domains** click the created fabric site (example: RTP5_Fabric), on the left in the **Fabric-Enabled Sites** navigation click the associated site (example: Global/RTP/RTP5-C9K), and then click **Host Onboarding**.

Step 3. Under **Virtual Networks**, select **INFRA_VN**.

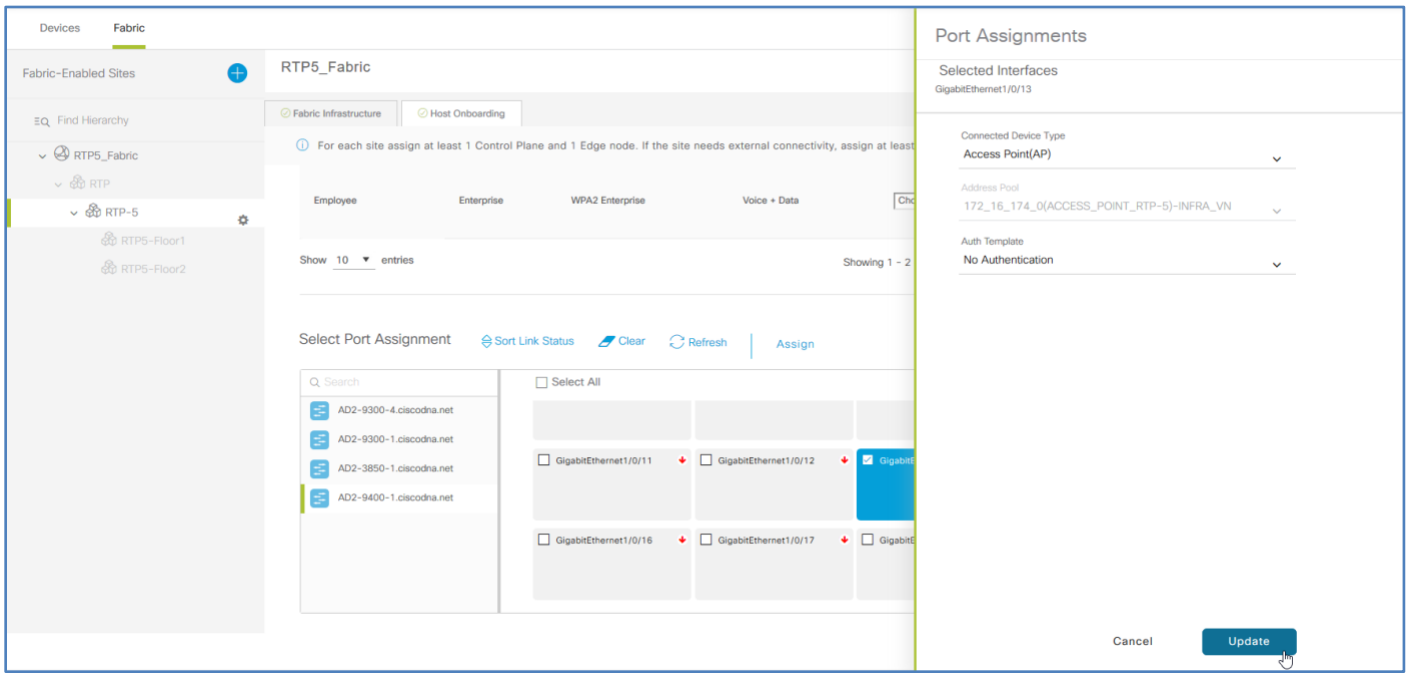


Step 4. Select the check box next to the IP Pool Name for the APs (example: ACCESS_POINT-RTP5), under **Pool Type** select **AP**, and then click **Update**.



Step 5. In the Modify Virtual Network slide-out panel, keep the default selection **Now**, and then click **Apply**.

Step 6. Under **Select Port Assignment**, select a switch, select any ports on the switch to be used for APs, select **Assign**, in the **Port Assignments** slide-out, under **Connected Device Type** select **Access Point (AP)**, leave the default **Address Pool** selection, under **Auth Template** select **No Authentication**, and then click **Update**.



Tech tip
Cisco DNA Center enables automatic onboarding of APs by provisioning a CDP macro at the fabric edge switches when the site Authentication template to is set to **No Authentication**. This CDP macro assigns the port to the correct VLAN associated with the IP Pool. Alternatively, if another Authentication is used, you use the switch port assignments in Cisco DNA Center to assign a port to the IP address pool for the APs.

Step 7. Repeat the previous step for any additional switches that have ports used for APs.

Step 8. After all ports supporting APs have been selected, at the top of the **Select Port Assignment** section, click **Save**, keep the default selection of **Now**, and then click **Apply**.

After the update is complete, the edge node switch ports connected to the APs are enabled with a device tracking configuration recognizing APs and permitting the APs to get network connectivity.

Tech tip
A default route in the underlay cannot be used by the APs to reach the WLC. A more specific route (such as a /24 subnet or /32 host route) to the WLC IP addresses must exist in the global routing table at each node where the APs connect to establish connectivity.

Step 9. Navigate to the main Cisco DNA Center dashboard, under **PROVISION > Devices > Inventory**, and then at the top, in the **Actions** pull-down menu, select **Resync**. The APs associated with the WLC are added to the inventory without waiting for an inventory refresh.

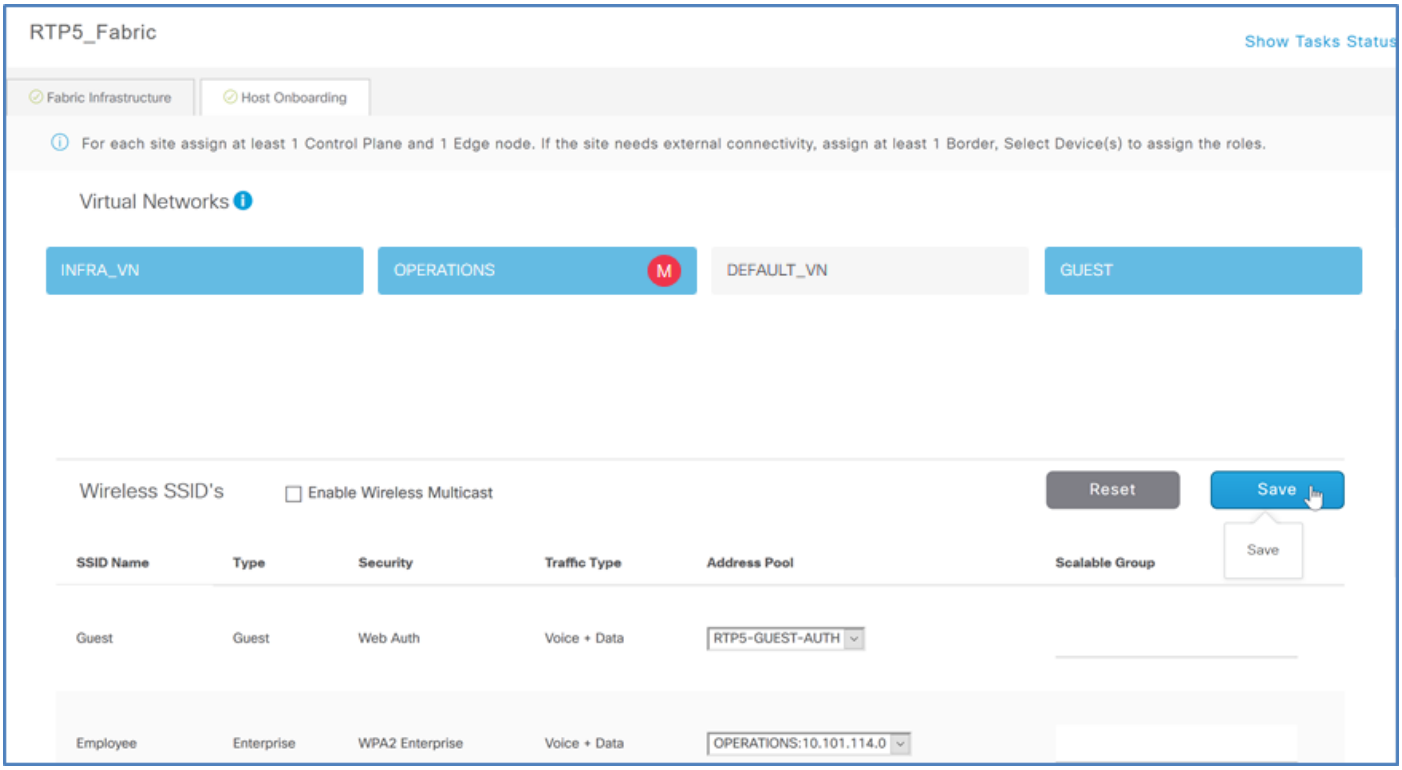
Step 10. Navigate to the main Cisco DNA Center dashboard, under **PROVISION > Devices > Inventory** select the APs being added, and at the top, in the **Actions** pull-down menu, select **Provision**.

Step 11. On the **Provision Devices** screen, assign the APs to a floor (example: Global/RTP/RTP5-C9K/ Floor 1), click **Next**, for **RF Profile**, if you have not created your own, select **TYPICAL**, click **Next**, at the **Summary** page click **Deploy**, and in the slide-out panel, leave the default selection of **Now**, and then click **Apply**. Acknowledge any warnings about reboots.

Procedure 9. Assign wireless clients to VN and enable connectivity

Step 1. From the Cisco DNA Center dashboard, navigate to **PROVISION > Fabric**, under **Fabric Domains** click the created fabric site (example: RTP5_Fabric), on the left in the **Fabric-Enabled Sites** navigation click the associated site (example: Global/RTP/RTP5-C9K), and then click the **Host Onboarding** tab.

Step 2. Under the **Wireless SSID's** section, for each **SSID Name** select an associated **Address Pool**, select any associated **Scalable Group**, click **Save**, keep the default selection of **Now**, and then click **Apply**.



Devices can now connect via the wireless networks.

Appendix A: Product List

The following products and software versions were included as part of validation in this deployment guide, and this validated set is not inclusive of all possibilities. Additional hardware options are listed in the associated Software-Defined Access Solution Design Guide, the SD-Access Product Compatibility Matrix, and the Cisco DNA Center data sheets may have guidance beyond what was tested as part of this guide. Updated Cisco DNA Center package files are regularly released and available within the packages and updates listings.

Table 4. Cisco DNA Center

Product	Part number	Software version
Cisco DNA Center Appliance	DN2-HW-APL-L (M5-based chassis)	1.2.10.4 (System 1.1.0.754)

Table 5. Cisco DNA Center packages

All packages running on the Cisco DNA Center during validation are listed—not all packages are included as part of the testing for SD-Access validation.

Package	Version
Application Policy	2.1.28.170011
Assurance - Base	1.2.11.304
Assurance – Sensor	1. 2.10.254
Automation – Base	2.1.28.600244.9
Automation – Intelligent Capture	2.1.28.60244
Automation – Sensor	2.1.28.60244
Cisco DNA Center UI	1.2.11.19
Command Runner	2.1. 28.60244
Device Onboarding	2.1.18.60024
DNAC Platform	1.0.8.8
Image Management	2.1.28.60244
NCP – Base	2.1.28.60244
NCP – Services	2.1.28.60244.9
Network Controller Platform	2.1.28.60244.9
Network Data Platform – Base Analytics	1.1.11.8
Network Data Platform – Core	1.1.11.77
Network Data Platform – Manager	1.1.11.8

Package	Version
Path Trace	2.1.28.60244
SD-Access	2.1.28.60244.9

Table 6. Identity Management

Functional area	Product	Software version
Cisco ISE Server	Cisco Identity Services Engine	2.4 Patch 6

Table 7. SD-Access fabric border and control plane

Functional area	Product	Software version
Border and control plane	Cisco Catalyst 9500 Series Switches	16.9.3
Border and control plane	Cisco Catalyst 9400 Series Switches	16.9.3
Border and control plane – small site	Cisco Catalyst 3850 XS switches (10-Gbps fiber)	16.9.3
Border and control plane	Cisco 4000 Series Integrated Services Routers	16.9.2
Border and control plane – large scale	Cisco ASR 1000-X and 1000-HX Series Aggregation Services Routers	16.9.2
Border	Cisco Catalyst 6807 7-slot chassis with Supervisor Engine 6T or Supervisor Engine 2T and 6800 32-port 10 GE with dual integrated DFC4	15.5(1)SY2
Border	Cisco Catalyst 6880-X and 6840-X switches	15.5(1)SY2
External Border	Cisco Nexus 7700 switches 2-slot chassis with Supervisor 2 Enhanced module and Cisco Nexus 7700 M3-Series 48-port 1/10 Gigabit Ethernet module	8.3(2)
Control plane	Cisco Cloud Services Router 1000V Series	16.9.2

Table 8. SD-Access fabric edge

Functional area	Product	Software Version
Fabric edge	Cisco Catalyst 9300 Series – stackable	16.9.3
Fabric edge	Cisco Catalyst 9400 Series with Supervisor Engine-1 – modular chassis	16.9.3

Functional area	Product	Software Version
Fabric edge	Cisco Catalyst 3850 Series – stackable	16.9.3
Fabric edge	Cisco Catalyst 3650 Series – standalone with optional stacking	16.9.3
Fabric edge	Cisco Catalyst 4500E Series with Supervisor 8-E – modular chassis	3.10.2E

Table 9. SD-Access Wireless

Functional area	Product	Software Version
Wireless LAN controller	Cisco 8540, 5520, and 3504 Series Wireless Controllers	8.8.111.0 (8.8 MR1)
Fabric mode access points	Cisco Aironet® 1800, 2800, and 3800 Series (Wave 2)	8.8.111.0 (8.8 MR1)

Table 10. LAN Automation switches tested for this guide (not inclusive of all possibilities)

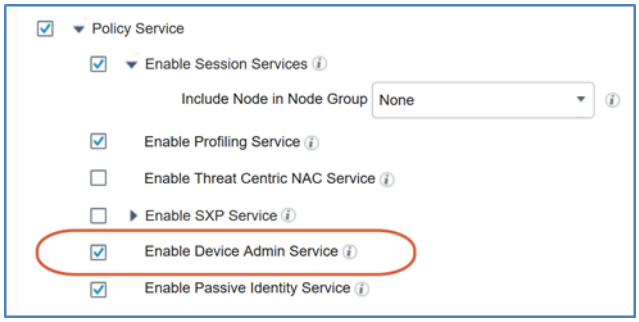
Functional area	Product
Cisco Catalyst 9500 Series (standard performance versions)	Seed device
Cisco Catalyst 3850 XS switches (10 Gbps fiber)	Seed device
Cisco Catalyst 9300 Series – stackable	Seed device Discovered device
Cisco Catalyst 9400 Series with Supervisor Engine-1 – modular chassis	Seed device Discovered device (10Gbps interface)
Cisco Catalyst 3850 Series – stackable	Discovered device
Cisco Catalyst 3650 Series – standalone with optional stacking	Discovered device
Cisco Catalyst 4500E Series with Supervisor 8-E – modular chassis	Discovered device

Appendix B: Configuring TACACS

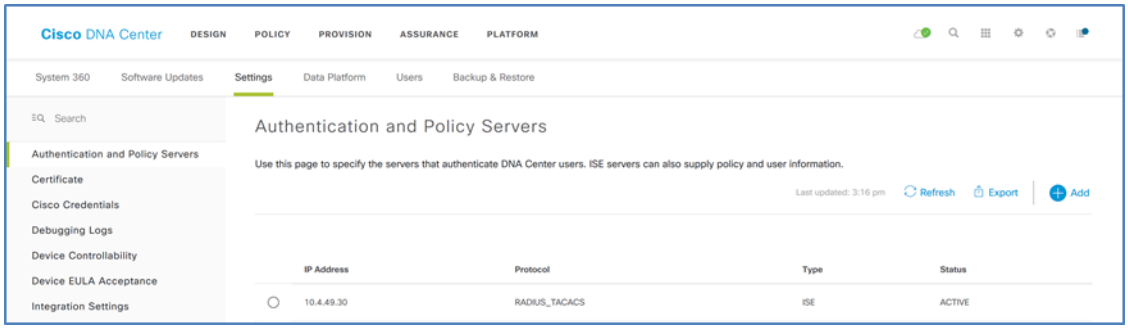
For TACACS configurations, Cisco DNA Center modifies discovered devices to use authentication and accounting services from ISE and local failover serves by default. ISE must be prepared to support the device administration configurations pushed to the devices during the discovery process.

Procedure 1. Verify ISE and Cisco DNA Center TACACS configuration

Step 1. Using ISE, navigate to **Administration > System > Deployment**. Under **Policy Service**, verify that **Device Admin Service** is selected.



Step 2. Log in to the Cisco DNA Center web interface. At the top-right corner, click the **Settings** (gear) icon. At the top, click **System Settings**. On the right, click **Authentication and Policy Servers**, and verify that ISE is active and supporting the TACACS protocol in addition to RADIUS.

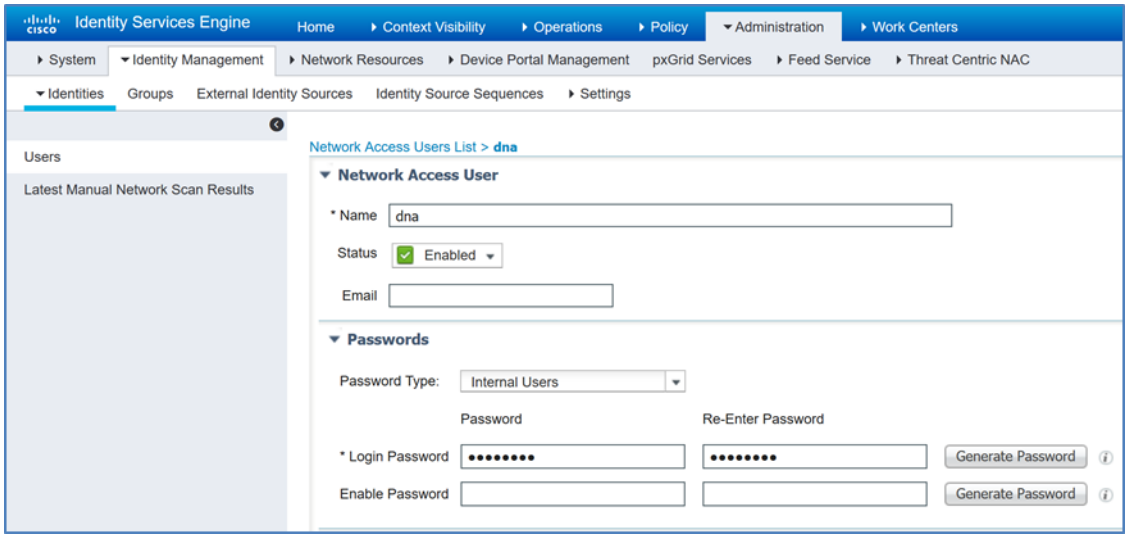


Procedure 2. Create a Cisco DNA Center administrative login in ISE

Update the ISE configuration with credentials supporting centralized authentication.

Tech tip
When devices are provisioned, they receive configurations appropriate for the assigned site, including the centralized AAA configuration using ISE. This configuration authenticates the console and VTY lines against the AAA servers. To maintain the ability to manage the devices after provisioning, the credentials defined in a Discovery job must be available from the ISE server. These can either be locally defined in ISE (Internal User) or available through an external identity source such as Active Directory integrated with ISE.

Step 3. Log in to ISE, navigate to **Administration > Identity Management > Identities**, click +**Add**, enter the **Name** (matching what was used for Cisco DNA Center discovery, and different from the ISE administrator), enter the associated **Login Password** and **Re-Enter Password**, and then, at the bottom of the screen, click **Submit**.

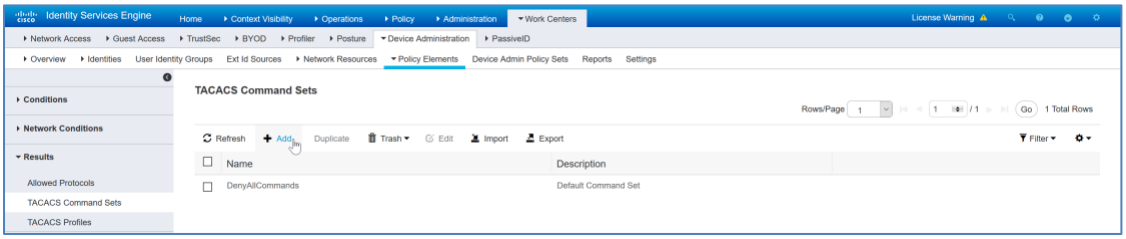


The network administrative user login is now available from ISE.

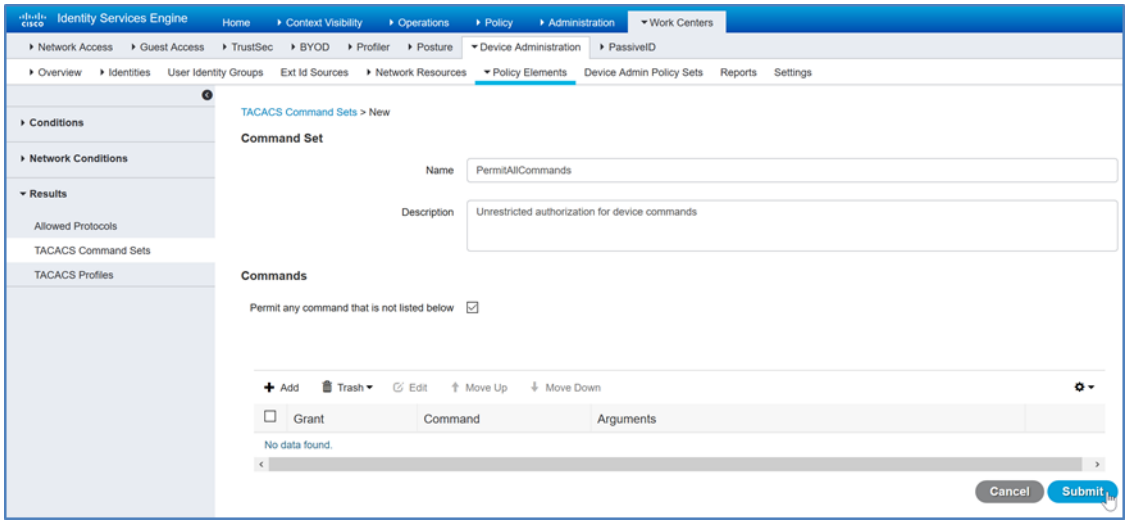
Procedure 3. Use ISE to configure TACACS command sets

Centralized authentication includes authorization capabilities, which can be used to limit the commands to a device that are permitted. The default ISE authorization policy denies all commands. The following example creates a command set that does not restrict the commands available to the authenticated user which may not be desired for many deployments. For additional details on Device Administration, Commands Sets, and TACACS, please see Deploying Cisco ISE for Device Administration Prescriptive Deployment Guide.

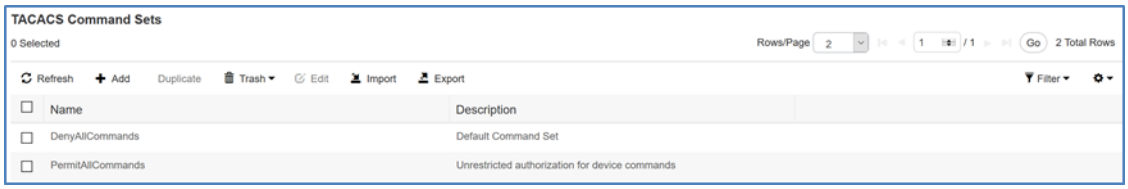
Step 4. Log in to ISE, navigate to **Work Centers > Device Administration > Policy Elements**. On the left side, navigate to **Results > TACACS Command Sets**, and then click **Add**.



Step 5. In the form under **Command Set**, supply a **Name** (example: PermitAllCommands) and a **Description**. Under **Commands**, select **Permit any command that is not listed below**, and then click **Submit**.



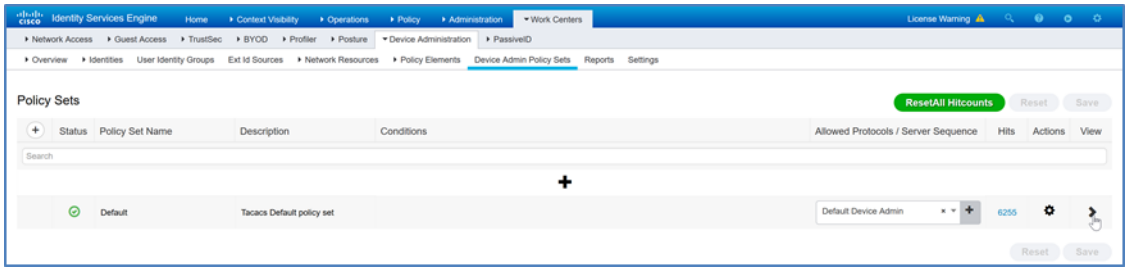
The new command set is saved and added to the list of available command sets.



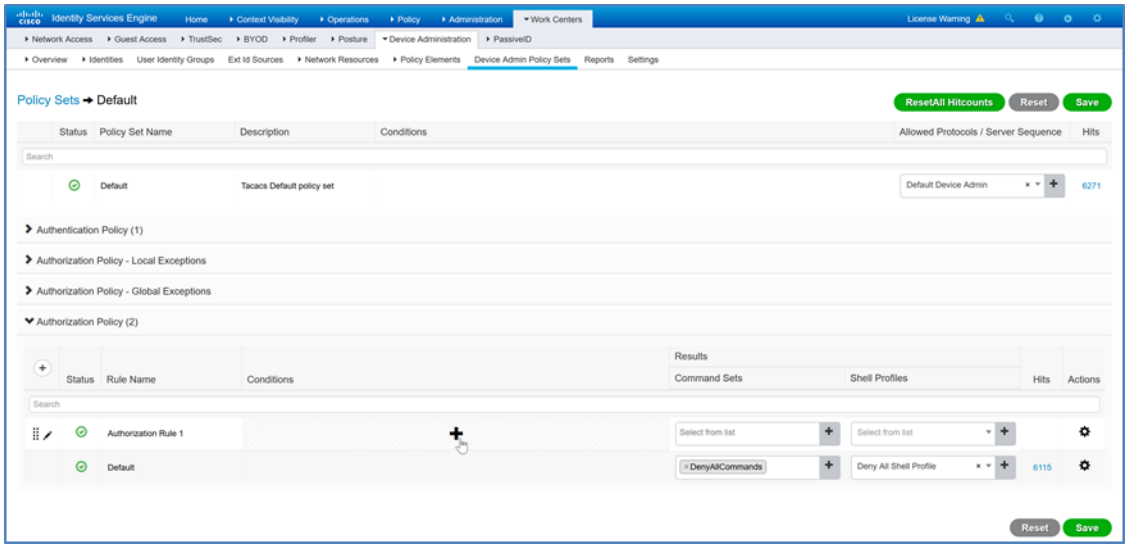
Procedure 4. Use ISE to configure TACACS device authorization

The new command set is applied to the authorization policy rules to change the default deny-all authorization behavior.

Step 6. Navigate to **Work Centers > Device Administration > Device Admin Policy Sets**, and then, to the right of the **Default** policy set, click **>** to expand the policy set.

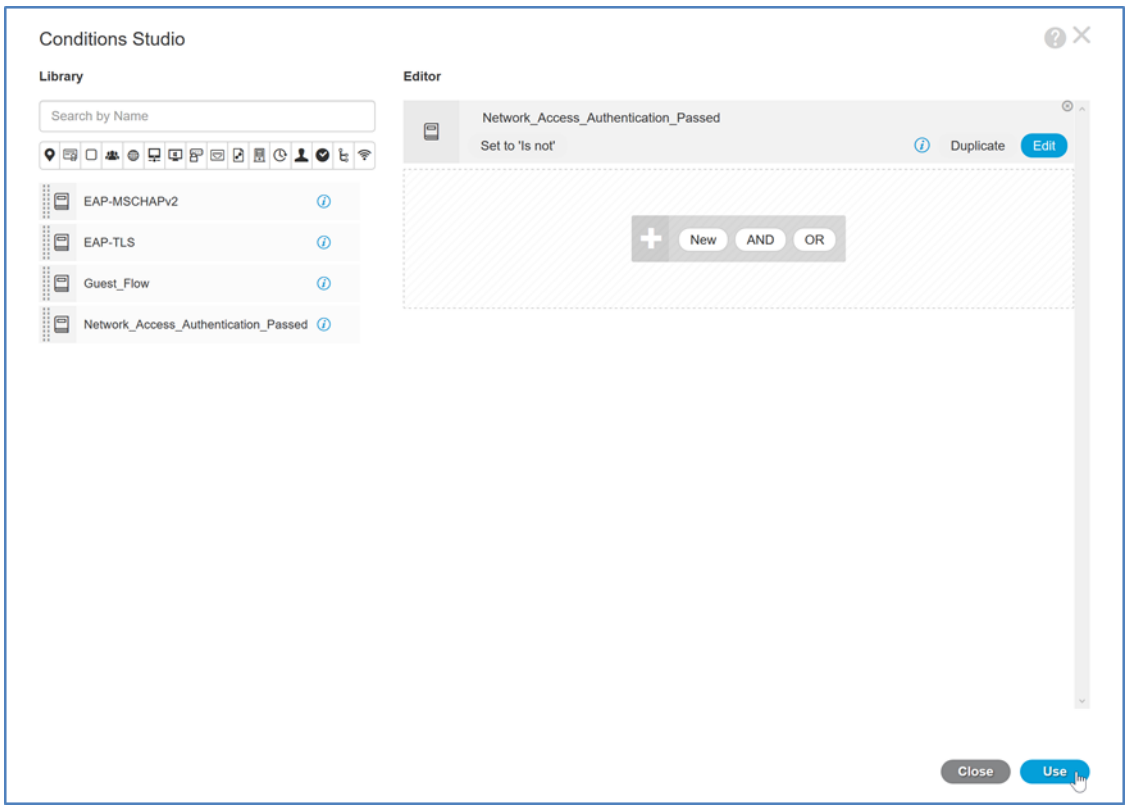


Step 7. To the left of **Authorization Policy**, click **>** to expand the policy. Above the rule named **Default**, click **+** (plus) to insert **Authorization Rule 1**, and then, under conditions, click **+** (plus) to add a condition.

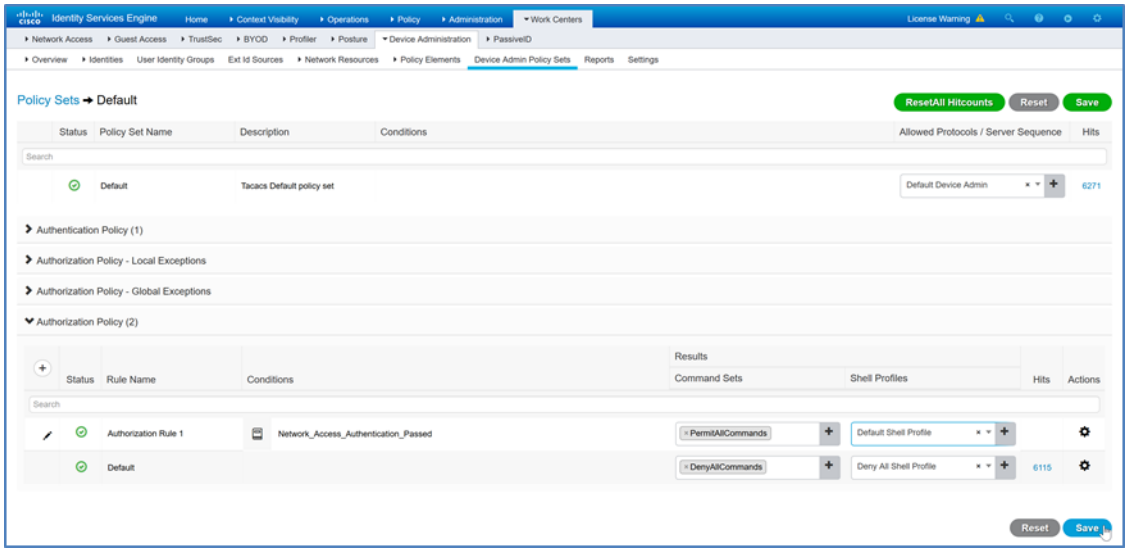


The **Conditions Studio** wizard appears.

Step 8. From the **Library** on the left, drag **Network_Access_Authentication_Passed** to the **Editor** window, and then, at the bottom, click **Use**.



Step 9. Under **Results, Command Sets**, select **PermitAllCommands**. Under **Results**, **Shell Profiles**, select **Default Shell Profile**, and then click **Save**.



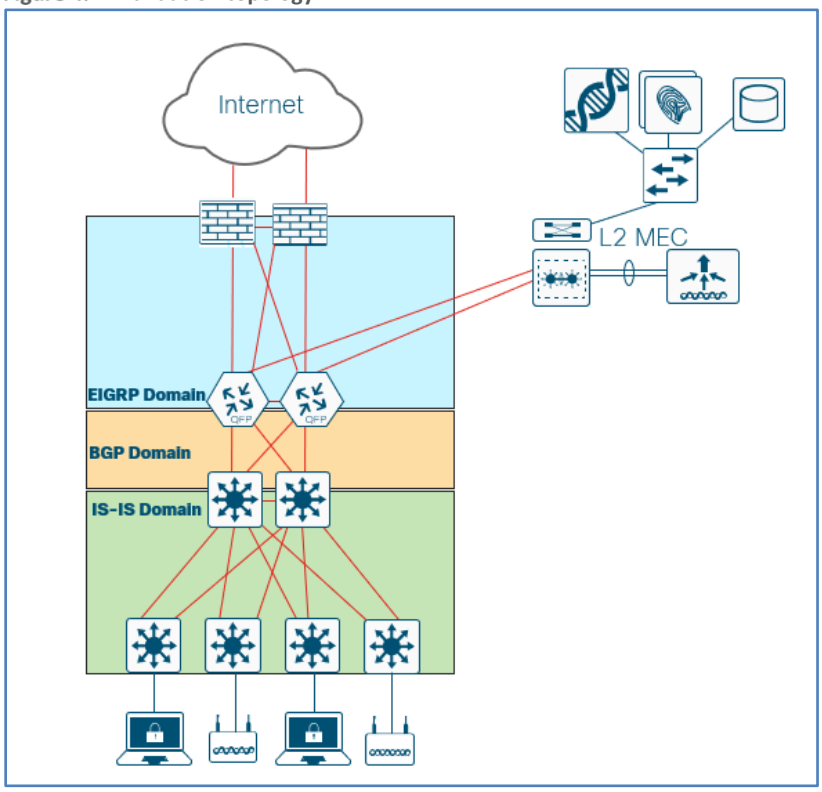
The default authorization policy set is saved, allowing the authenticated Cisco DNA Center login to have command authorization to update the network devices.

Appendix C: Initial IP Reachability and Route Redistribution

The requirement to have IP reachability between Cisco DNA Center and its managed devices and to provide a more specific route (the default route cannot be used) to the Wireless LAN controller in the underlay can be achieved in multiple ways.

In the deployment topology used in this guide, the existing network northbound of the border node (outside of the fabric site) uses EIGRP as the routing protocol. To take advantage of LAN automation, the IS-IS routing protocol is used southbound of the border node towards the edge nodes.

Figure 4. Validation topology

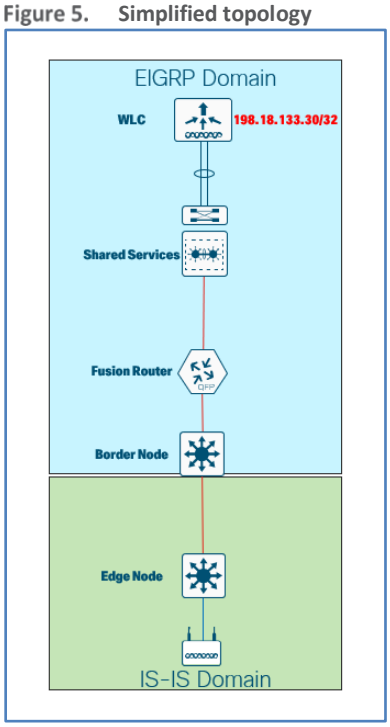


In deployments with multiple points of redistribution between several routing protocols, using BGP for initial IP reachability northbound of the border nodes helps ensure continued connectivity after the fabric overlay is provisioned without the need for additional manual redistribution commands on the border nodes. Once a device is discovered and managed by Cisco DNA Center, it is recommended practice to not manually add configuration, particularly any configuration that might be overridden through the automated configuration placing the device in an unintended state.

To understand why manual BGP is preferred for initial IP reachability requires understanding the result of provisioning a Layer 3 handoff (VRF-lite) on the border node as it relates to the global routing table from the perspective of the edge node. This Appendix describes this provisioning and results.

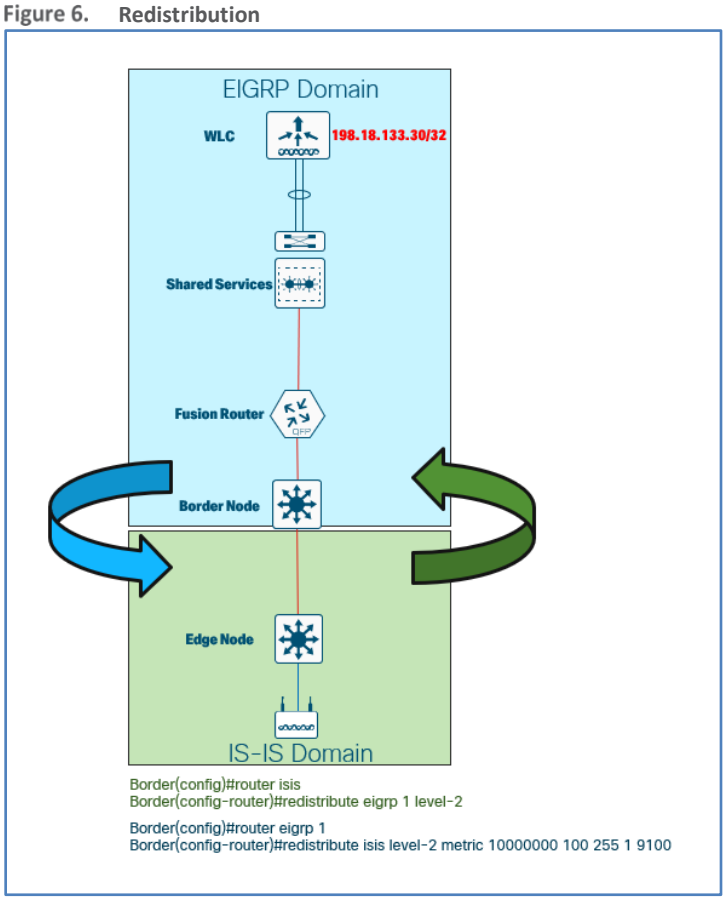
Consider the following simplified topology.

Figure 5. Simplified topology



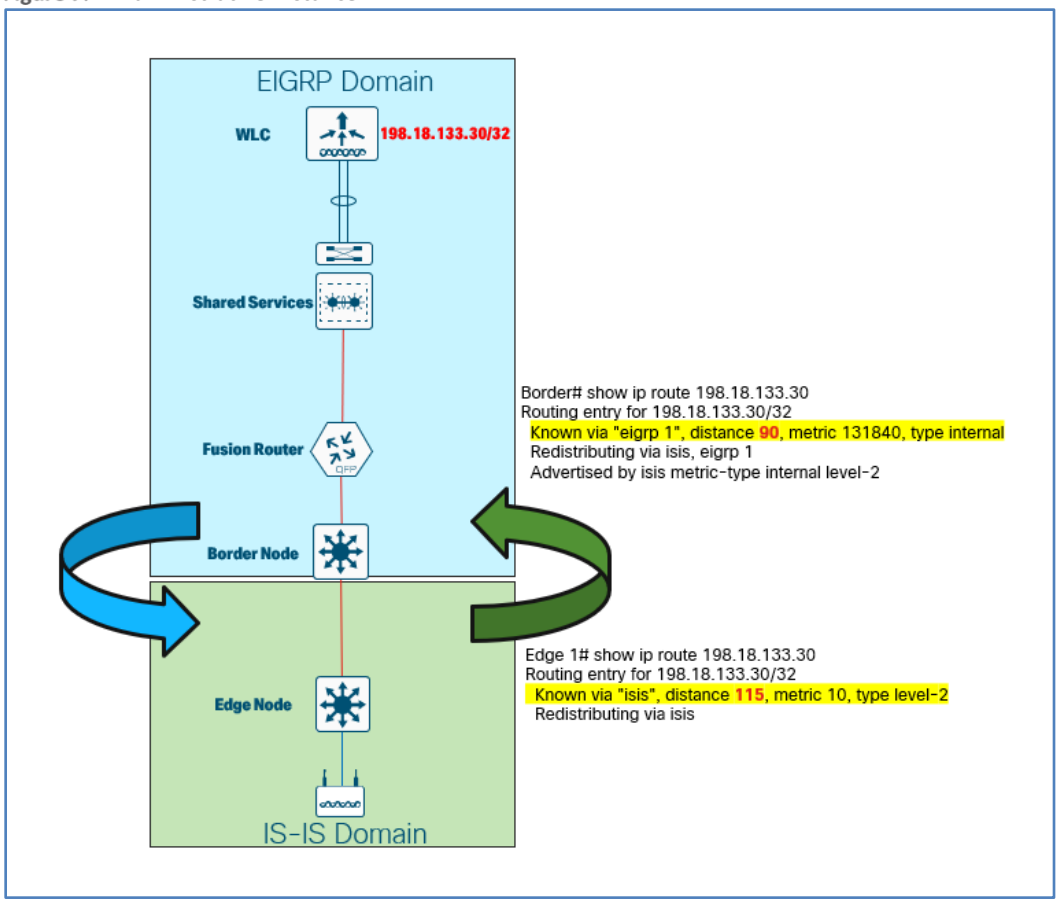
To provide IP reachability to the WLC, who's route is known via EIGRP, the border node must mutually redistribute EIGRP and IS-IS. For simplicity, a single redistribution point (one border) is shown.

Figure 6. Redistribution



From the perspective of the border node, the WLC is reachable via EIGRP with an administrative distance of 90. From the perspective of the edge node, the WLC route is redistributed into IS-IS which as a default administrative distance of 115.

Figure 7. Administrative Distance

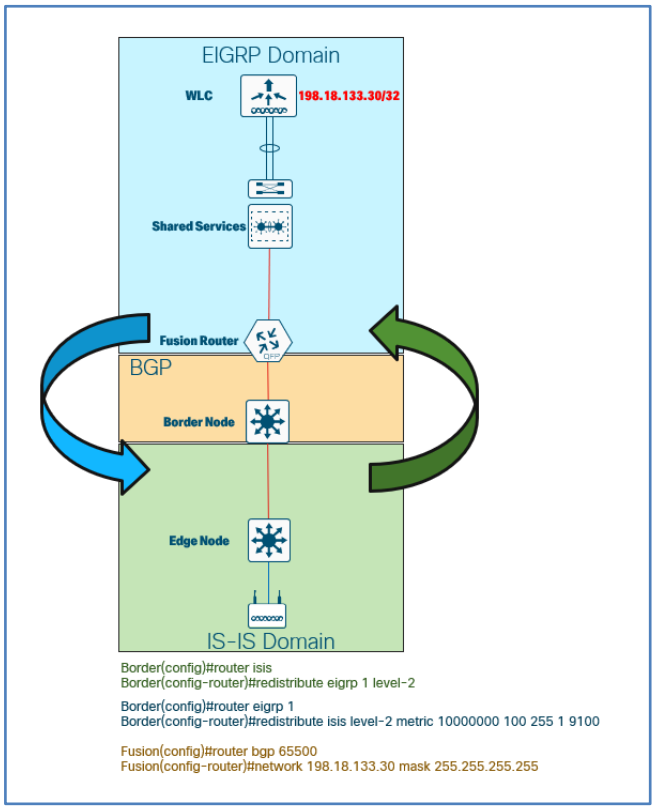


When using the Layer 3 handoff border automation, the VNs associated with the fabric are extended outside of the network to provide reachability to shared services. This includes INFRA_VN which is a special VN for infrastructure devices such as APs and Extended Nodes. While it is part of the overlay network, it is associated with the Global Routing Table. Extending INFRA_VN with the BGP and VRF-lite Layer 3 handoff automation ensures that the access points are able to reach the wireless LAN controller.

Figure 8. INFRA_VN Handoff

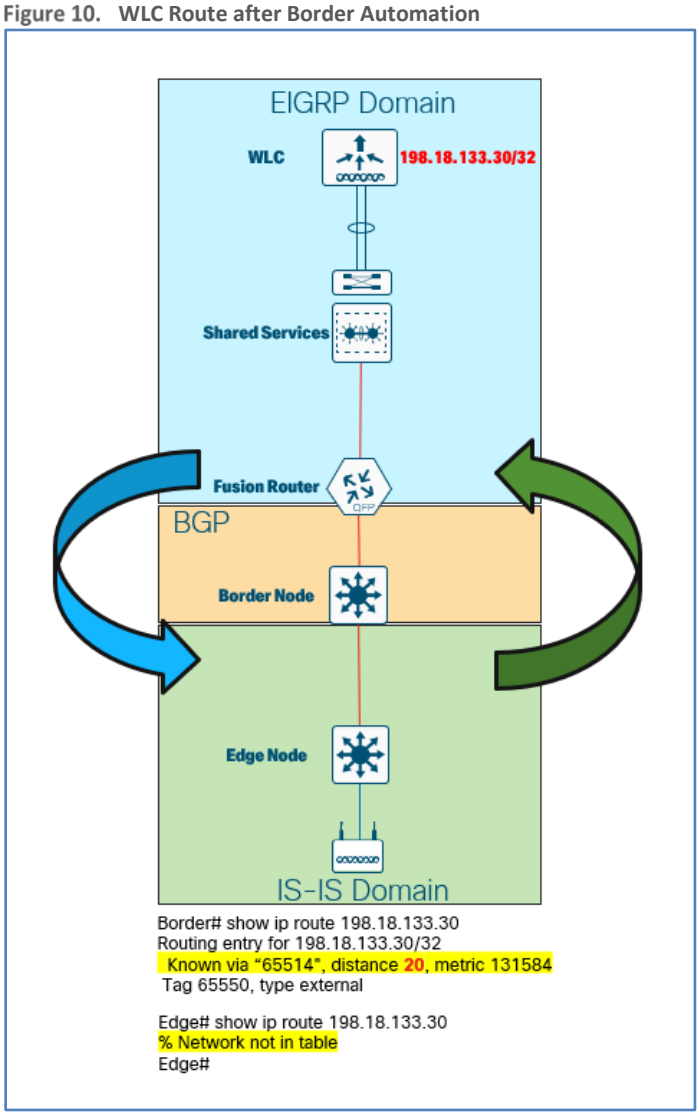
Once the VRF-lite automation is complete, you configure the fusion router with a corresponding configuration as shown with the **Remote IP** in screen shot above. The WLC subnet must be advertised into BGP on the fusion routers, as this is the routing protocol automated between the border nodes and the fusion routers.

Figure 9. INFRA_VN Handoff



The result is that the WLC's subnet is known through both BGP and through EIGRP. BGP has an administrative distance of twenty (20) which will result in its route in routing table instead of the route from EIGRP.

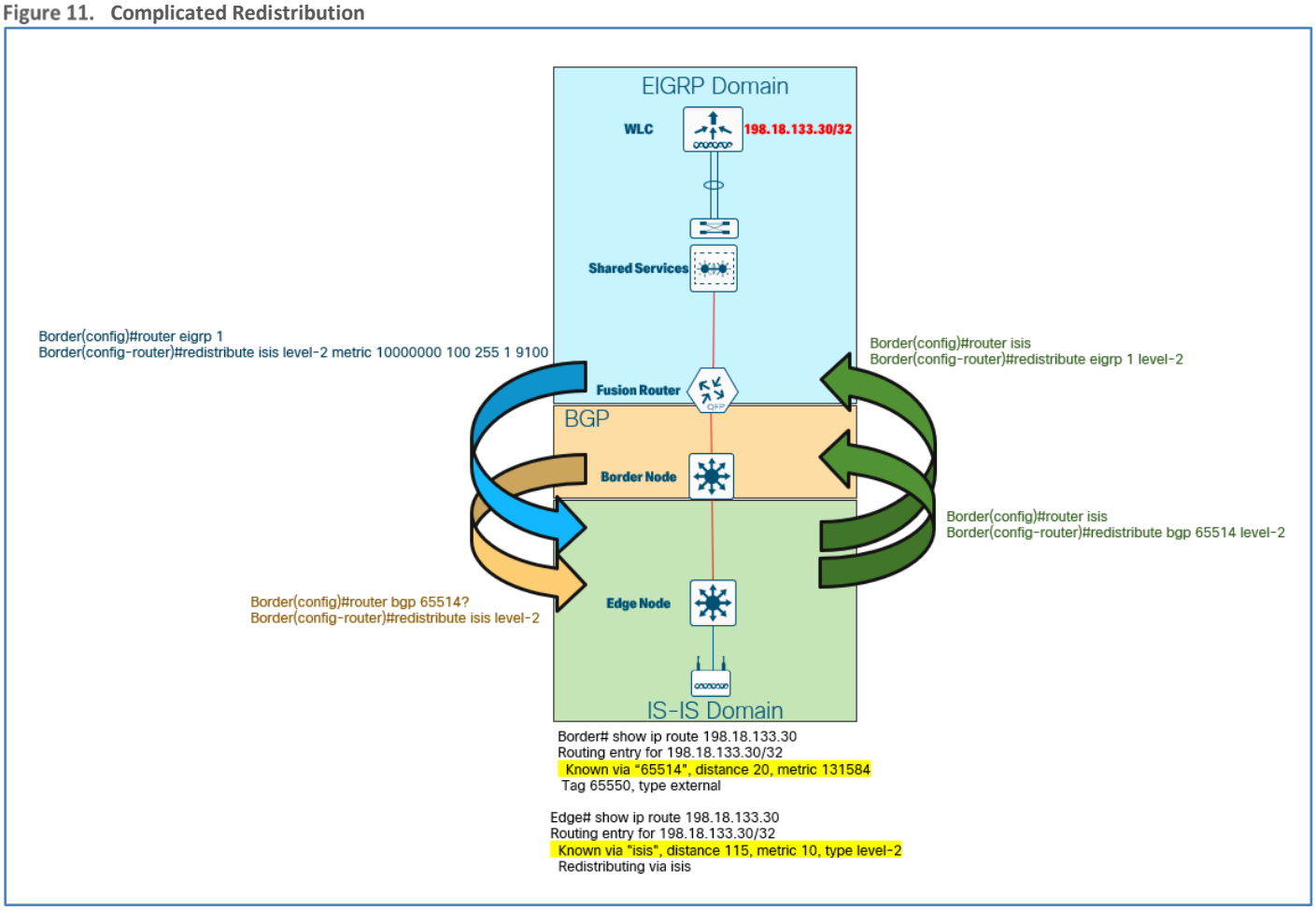
Figure 10. WLC Route after Border Automation



From the perspective of the edge node, the WLC route is no long reachable, as EIGRP and IS-IS were mutually redistributed.

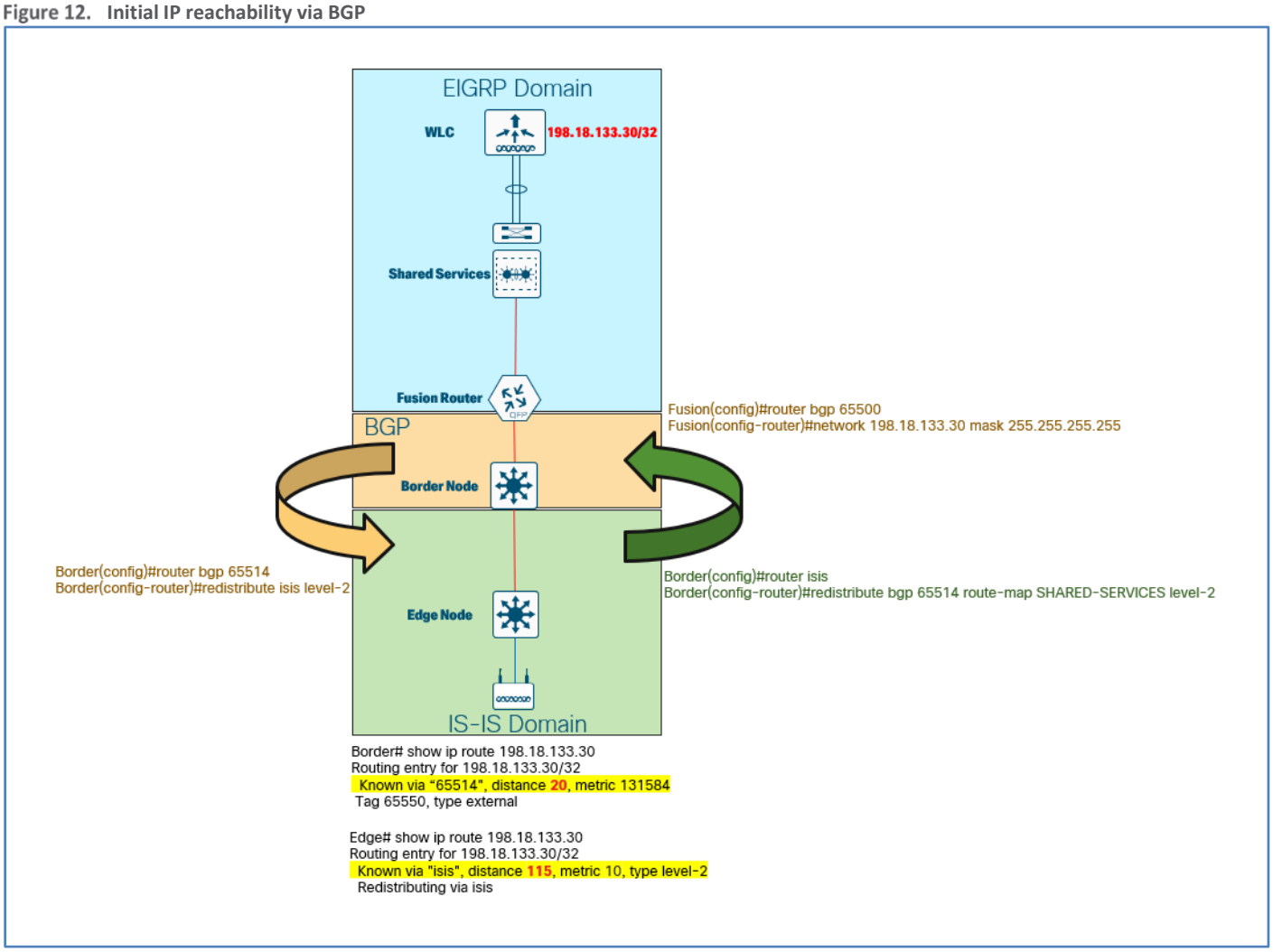
A method to address this would be to redistribute BGP into IS-IS and IS-IS back into BGP on the border node. Not only does this create multiple, mutual redistribution points, it also requires direct and manual interaction on a device management by Cisco DNA Center.

Figure 11. Complicated Redistribution



In contrast, if initial IP reachability is created through BGP, this scenario is not encountered.

Figure 12. Initial IP reachability via BGP



Feedback

For comments and suggestions about this guide and related guides, join the discussion on Cisco Community.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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