CISCO VALIDATED DESIGN

Software-Defined Access Deployment Guide

October 2018
Solution 1.2

Table of Contents

Software-Defined Access introduction

Cisco® Software-Defined Access (SD-Access) is the evolution from traditional campus LAN designs to networks that directly implement the intent of an organization. SD-Access is enabled with an application package that runs as part of the Cisco DNA Center™ software for designing, provisioning, applying policy, and facilitating the creation of an intelligent campus wired and wireless network with assurance. ***Fabric*** technology, an integral part of SD-Access, enables wired and wireless campus networks with programmable overlays and easy-to-deploy network virtualization, permitting a physical network to host one or more logical networks to meet the design intent. In addition to network virtualization, fabric technology in the campus network enhances control of network communications, providing software-defined segmentation and policy enforcement based on user identity and group membership. Software-defined segmentation is seamlessly integrated using Cisco TrustSec® technology, providing micro-segmentation through the use of scalable groups within a virtual network. Using Cisco DNA Center to automate the creation of virtual networks reduces operational expenses by simplifying deployment, reduces risk through integrated security, and improves network performance through assurance and analytics capabilities.

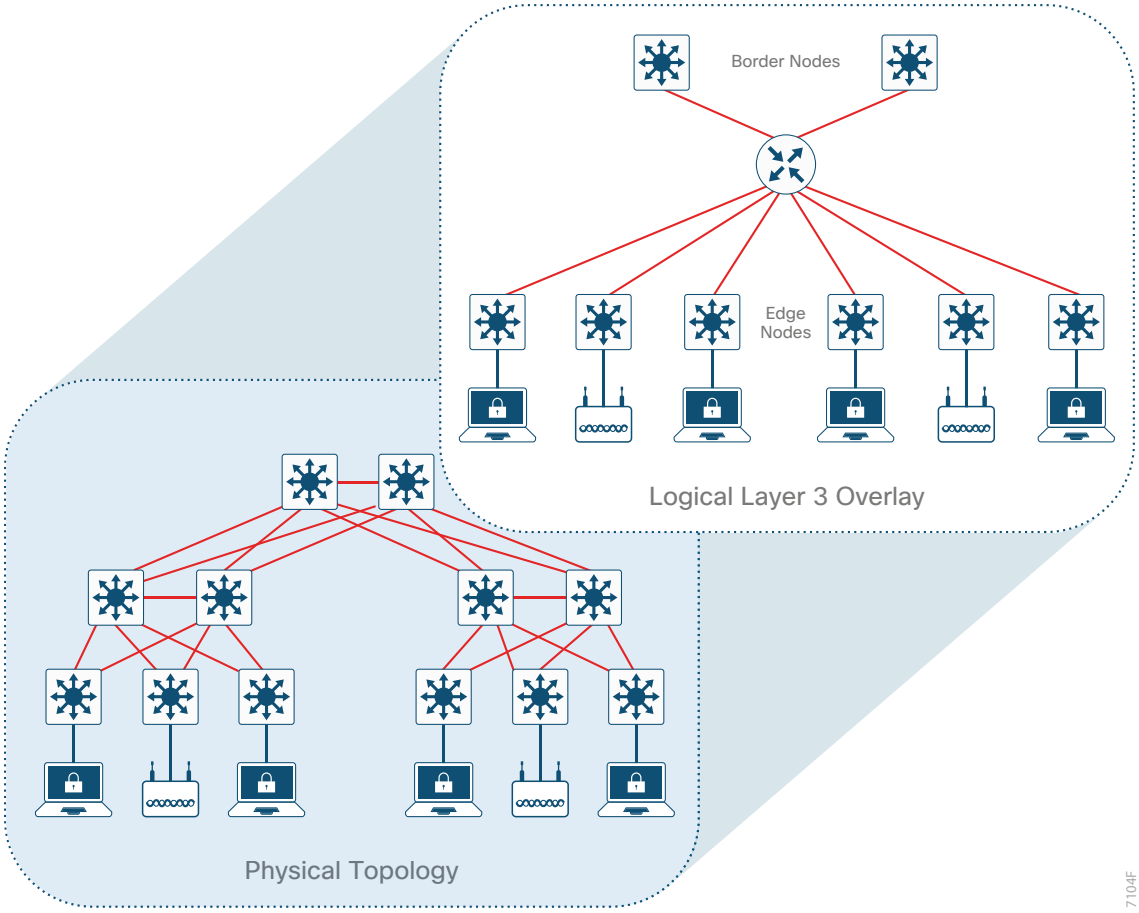
This deployment guide describes how to use Cisco DNA Center to implement an SD-Access network connected to an existing enterprise network. The virtual networks that SD-Access builds (overlay networks) run on a physical network (underlay network), creating alternative topologies for connecting devices in the campus LAN. Similarly, overlay networks are commonly used to provide Layer 2 and Layer 3 logical networks with virtual machine mobility in data center fabrics (examples: Cisco ACI™, VXLAN/EVPN, and Cisco FabricPath). Overlay networks are also used in wide-area networks to provide secure tunneling from remote sites (examples: MPLS, DMVPN, and GRE). This guide helps you understand important elements of automating SD-Access configurations and the integration of SD-Access into existing networks.

As described in the Software-Defined Access Design Guide, the underlay network is defined by the physical switches and routers that are used to deploy the SD-Access network. All network elements of the underlay must establish IP connectivity via the use of a routing protocol. Instead of using arbitrary network topologies and protocols, the underlay implementation for SD-Access uses a well-designed Layer 3 foundation inclusive of the campus edge switches (also known as a ***routed access*** design), helping ensure the performance, scalability, and high availability of the network. In SD-Access, the underlay switches support the end-user physical connectivity. However, end-user subnets are not part of the underlay network—end-user subnets are part of a programmable Layer 2 or Layer 3 overlay network.

When creating one or more overlay networks, the overlays run across the supporting physical infrastructure of the underlay network. The data plane traffic and control plane signaling is contained within each virtualized network, maintaining isolation among the networks in addition to independence from the underlay network. The SD-Access fabric implements virtualization by encapsulating user traffic in overlay networks, using IP packets that are sourced and terminated at the boundaries of the fabric. The fabric boundaries include borders for ingress and egress to a fabric, fabric edge switches for wired clients, and fabric APs for wireless clients.

Because IP-based connectivity within each Layer 3 overlay is an abstraction from the physical connectivity, multiple IP networks can be a part of each virtual network. You preserve IP address space traffic separation beyond the fabric border using typical virtualization techniques—including adding devices to remediate addressing conflicts (typically using network address translation) and enabling communication with permitted common external IP services such as DNS and the Internet.

Figure 1. Layer 3 overlay—connectivity logically routed



In addition to network virtualization, SD-Access integrates Cisco TrustSec technology to enable software-defined segmentation and policy enforcement based on user identity and group membership. In this deployment, Cisco DNA Center manages the definition of security policies to be rendered into the network infrastructure by Cisco Identity Services Engine (ISE). Scalable group tags (SGTs) are integrated into the headers used for fabric encapsulation. For group policies that extend outside of the SD-Access fabric, you configure the propagation of the SGT information from the fabric border node to the network external to the fabric by either transporting the tags to Cisco TrustSec aware devices using SGT Exchange Protocol (SXP) or by directly mapping SGTs into the Cisco Meta Data field in a packet using inline tagging capabilities implemented for connections to the border node.

Implementation overview

Although there are certainly a wide variety of alternative deployment options to the topologies, routing protocols, and designs shown in this implementation, organizations are encouraged to start their implementations with the configurations presented and then customize the configurations to fit their needs.

The deployment of the underlay network supporting SD-Access uses a Layer 3 routed access topology. The example deployment uses the Intermediate System to Intermediate System (IS-IS) routing protocol, bidirectional forwarding detection (BFD) for fast failure detection, and equal-cost multipath (ECMP) routing using redundant interconnections for fast network convergence. Layer 2 access designs and Layer 2 EtherChannel must not be used in the underlay implementation for the SD-Access solution.

The overlay networks connect with the rest of the enterprise network at the fabric border nodes, and the deployment example uses switches in the core tier of a campus three-tier (core, distribution, access) network for that border role. Each overlay network appears as a virtual routing and forwarding (VRF) instance at the border for connectivity to external networks. You preserve the overlay separation when extending the networks outside of the fabric by using VRF-lite, maintaining the network separation within devices connected to the fabric and also on the links between VRF-enabled devices.

Typically, you maintain the separation of overlay networks using VRF-lite when connecting the fabric to external networks, while still allowing connectivity from some or all overlay networks to services that are available throughout the enterprise network. These shared services, such as the Internet, domain name services, or data center applications, often reside within the global routing table or are assigned to a dedicated VRF. The connectivity from the fabric border to the external networks is often accomplished using a handoff to a ***fusion router***—a device specifically configured for the role of governing the access between the VRFs and the shared services.

When you consider integrating the campus fabric into an existing enterprise network, the integration choice is driven by the currently deployed enterprise network design:

- **Nonvirtualized enterprise network**: If the existing enterprise network is not yet virtualized, the recommended, validated interconnection between the fabric border and the existing nonvirtualized network uses an intermediate fusion router to enable route exchange between the fabric and external domains and access to the shared services. Deploy dual fusion routers for increased availability and use Border Gateway Protocol (BGP) for exchanging routes among border nodes and fusion routers, which inherently accommodates loop avoidance.
- **Virtualized enterprise network**: If the existing enterprise network is already virtualized (for example, using Layer 3 VPN), use VRF-lite to extend the VRFs at the campus fabric border nodes into the existing virtualized infrastructure, and continue using the techniques available in the existing virtualized network for enabling required access to shared services.

In the deployment described, the campus core layer hosts the fabric border functionality. An alternative border for smaller networks uses a collapsed core/distribution with stackable switches. Using the core tier as the border allows an overlay network to span across any portion of, or all of, the three-tier campus domain, with the core being a logical choice as the common exit point for network traffic. The location where traffic exits the fabric as the default path to all other networks is an ***external border***. An ***internal border*** used to access a well-defined set of networks, such as a data center, and an ***anywhere border*** (serving both internal and external border roles), are not included as part of the described deployment.

If there is a requirement to have another location in the fabric as an alternative exit point for a specific set of non-default traffic (perhaps a WAN location, for example), additional border devices are used to support the requirement. The scope of border deployment guidance in this version of the deployment guide is for the more common external border configurations.

Design considerations

When deploying SD-Access, there are a number of significant deployment decisions to consider prior to starting, as described in the Software-Defined Access Design Guide. These considerations include:

- Are you ready to deploy a Layer 3 (routed) access layer? This deployment assumes a Layer 3 access layer deployment model for the network. Although any topology and routing protocol could be used in the underlay, the implementation of a well-designed Layer 3 foundation all the way to the campus edge is required to ensure support for performance, scalability, and high availability of the network. The Cisco DNA Center LAN Automation feature is an alternative to manual underlay deployments for new networks, and uses an IS-IS routed access design. Though there are many alternative routing protocols, the IS-IS selection offers operational advantages such as neighbor establishment without IP protocol dependencies, peering capability using loopback addresses, and agnostic treatment of IPv4, IPv6, and non-IP traffic.

- Subnet planning is an integral consideration if you are planning a migration from a Layer 2 access layer to a routed access layer.
- SD-Access introduces flexibility to the traditional routed access layer. Client subnets in the overlay are associated to the closest physical Layer 3 gateway, allowing subnets to stretch through the SD-Access fabric. Policies for the overlay allow client subnets to be configured to support a specific function, such as connectivity for computers, unified communications, wireless BYOD, or wireless guest networks.
- Do you plan to deploy the underlay manually, as an extension to the routing protocol already used throughout an organization, or do you intend to use an interior gateway protocol (IGP) that may be unique to the fabric underlay? This deployment shows IS-IS as the underlay IGP selection, which is aligned to the LAN automation available for new network deployments.
- Are there requirements to deploy multiple Layer 3 overlay networks (such as for multitenant use cases described in the introduction), or does a single Layer 3 overlay with multiple subnets across the fabric meet the requirements? The deployment accommodates both by supporting one or multiple VRFs, including handoff outside the fabric domain. Multiple overlays require additional planning for the integration of shared services. Plan for and document all overlay subnets and VRFs so that you are prepared to integrate them into your Dynamic Host Configuration Protocol (DHCP) services.
- Have you identified the appropriate locations for the edge, border, and control plane roles in your network? Do you have the proper platforms in place to support those fabric roles? Full discussion of these platforms and roles is covered in the associated Software-Defined Access Design Guide. It is important to understand that, unlike in a pilot deployment, a production deployment will present operational challenges if you deploy the border role in one location and later decide to relocate the border role to another location, so careful consideration of the future scope of the fabric boundaries is important. In the validated deployment described, the most common scenarios with supported platforms are shown, and Appendix A: Product list lists the equipment specifically validated for roles in this deployment.

Additional information

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

You can find the Software-Defined Access Design Guide, User-to-Data Center Access Control Using TrustSec Deployment Guide, and related design guides, deployment guides, and white papers in the Design Zone at the following page:

https://www.cisco.com/go/designzone

Deployment details

How to Read Commands

This 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:

```
ntp server 10.10.48.17
```

Commands with variables that you must define:

```
class-map [highest class name]
```

Commands at a CLI or script prompt:

```
Router# enable
```

Long commands that line wrap are underlined. Enter them as one command:

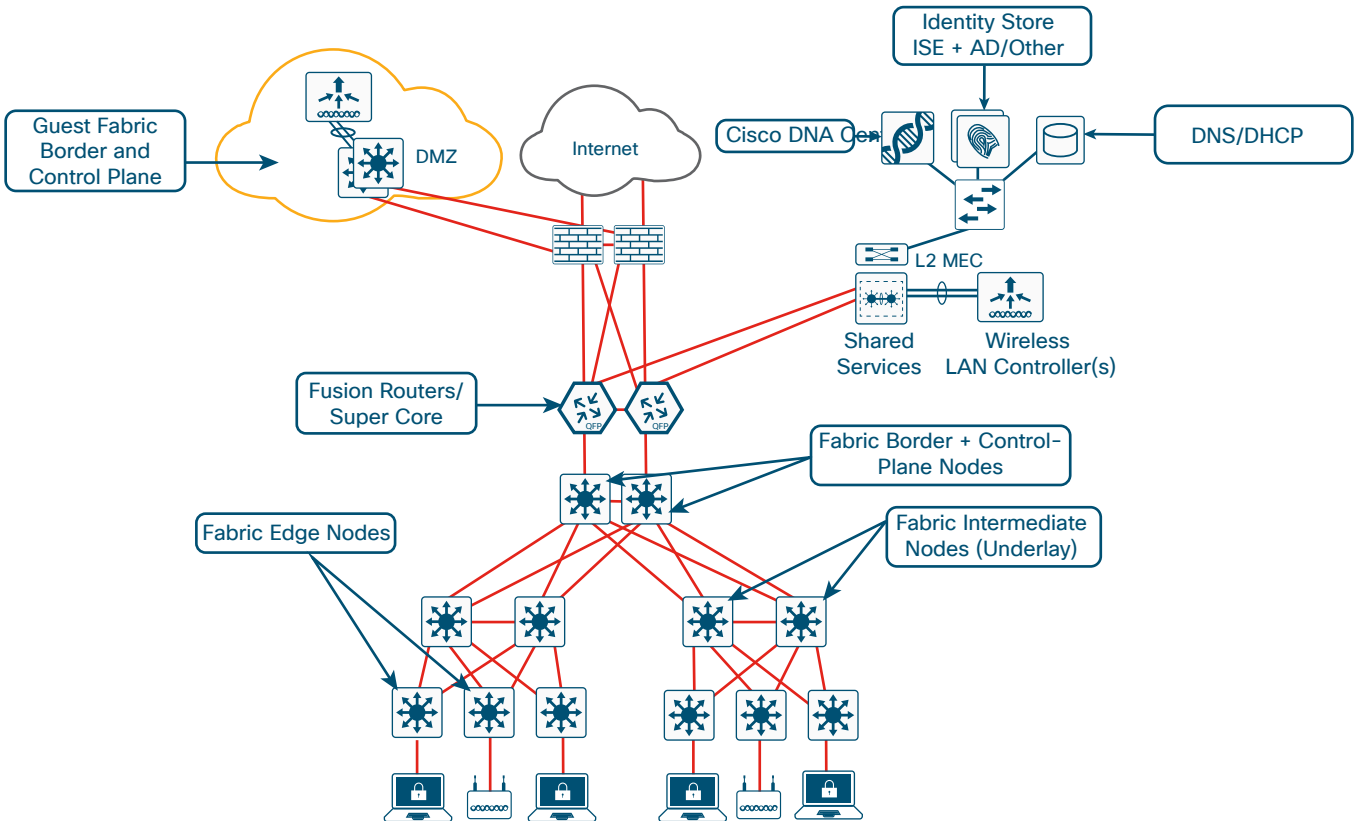
```
police rate 10000 pps burst 10000
packets conform-action
```

Noteworthy parts of system output (or of device configuration files) are highlighted:

```
interface Vlan64
  ip address 10.5.204.5 255.255.255.0
```

The enterprise network integrated with the described campus fabric deployment is nonvirtualized and runs Enhanced Interior Gateway Routing Protocol (EIGRP) as a routing protocol. IP prefixes from the campus, including 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 and perform mutual redistribution with EIGRP in the enterprise network and with BGP to the campus fabric. A route-map configuration for dynamic tagging and filtering of redistributed routes provides a simple and dynamic way to prevent routing loops while accommodating multiple redistribution points in the high-availability design.

Figure 2. Validation topology



Installing SD-Access network management

The Cisco SD-Access solution described uses a single Cisco DNA Center hardware appliance, prepared for future inclusion as part of a three-node cluster. For this solution, the Cisco DNA Center software integrates with two ISE nodes configured for redundancy and dedicated to the SD-Access deployment, as detailed in the installation. To support SD-Access Wireless, the solution includes two wireless LAN controllers (WLCs) for controller redundancy.

Before you begin, you must identify the following:

- IP addressing and network connectivity for all controllers being deployed: Cisco DNA Center must have Internet access for system updates from the Cisco cloud repository.
- A network-reachable Network Time Protocol (NTP) server, used during Cisco DNA Center installation to help ensure reliable digital certificate operation for securing connections.
- Certificate server information, when self-signed digital certificates are not used.

Process

Installing Cisco DNA Center

1. Connect and configure the Cisco DNA Center hardware appliance
2. Check the Cisco DNA Center version
3. Migrate the Cisco DNA Center platform to Release 1.2
4. Upgrade the Cisco DNA Center 1.2 packages

The Cisco DNA Center appliance has 10-Gbps SFP+ modular LAN on motherboard (mLOM) interfaces and integrated copper interfaces available for network connectivity. Use the following table to assist with IP address assignment and connections. The validation shows a single-node cluster that uses a virtual IP (VIP) configured on a single Cisco DNA Center appliance, easing future migration to a three-node cluster. You do not need to physically connect the intra-cluster communications port for a single-node cluster configuration. For provisioning and assurance communication efficiency, Cisco DNA Center should be installed in close network proximity to the greatest number of devices being managed.

Figure 3. Rear view of the Cisco DNA Center appliance — DN1-HW-APL

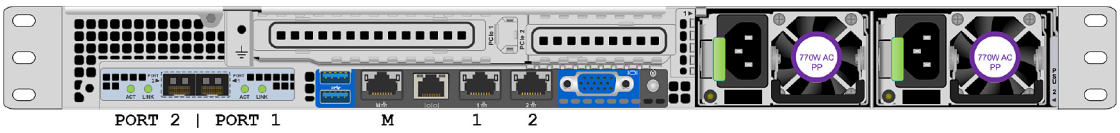


Table 1. Cisco DNA Center server LAN Ethernet interface assignments (left to right, from rear)

	PORT 2 mLOM SFP+ 10 Gbps	PORT 1 mLOM SFP+ 10 Gbps	M Integrated RJ-45	1 Integrated RJ-45	2 Integrated RJ-45
Wizard name	enp10s0	enp9s0	–	enp1s0f0	enp1s0f1
Use	Intra-cluster communications	Enterprise network infrastructure	Cisco Integrated Management Controller out-of-band server appliance management	Optional dedicated management network for web access	Optional isolated enterprise network
Example cluster VIP address	–	10.4.49.25 255.255.255.0	–	–	–
Example interface address	192.168.127.1 255.255.255.248	10.4.49.26 255.255.255.0	10.204.49.25 255.255.255.0	Unused in this example	Unused in this example

Tech tip

Connecting Cisco DNA Center to your network using a single network interface (enterprise network infrastructure, mLOM PORT1) simplifies the configuration by requiring only a default gateway and by avoiding the need to maintain a list of static routes for any additional interfaces connected. When you use additional optional interfaces (for example, to separate the networks for infrastructure provisioning and administrative access to Cisco DNA Center), the network route changes may require that you reconfigure the appliance. To update static routes in Cisco DNA Center after the installation, follow the procedure to reconfigure the appliance in the Cisco Digital Network Architecture Center Appliance Installation Guide for your installed version.

Reserve an arbitrary private IP space at least 20 bits of netmask in size that is not used elsewhere in the network. Divide the /20 address space into two /21 address spaces and use them in a later setup step for services communication among the processes running in a Cisco DNA Center instance. Both single-node cluster and three-node cluster configurations require the reserved IP address space.

The Cisco DNA Center appliance also must have Internet connectivity, either directly or via a web proxy, to obtain software updates from the Cisco cloud repository. Internet access requirements and optional proxy server setup requirements are detailed in the applicable version of the Cisco Digital Network Architecture Center Appliance Installation Guide.

Caution

The installation described assumes a new installation of Cisco DNA Center. If you already have Cisco DNA Center deployed and managing devices in your network, do not use the steps in this **Install Cisco DNA Center** process. Instead, you must refer to the release notes on Cisco.com for the correct procedure for a successful upgrade to your desired release.

https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-release-notes-list.html

Procedure 1 Connect and configure the Cisco DNA Center hardware appliance

Step 1: Connect the Cisco DNA Center hardware appliance to a Layer 2 access switch port in your network, by:

- Using the 10Gb port labeled PORT 1 on the mLOM card (named enp9s0 in the wizard)
- Using the Cisco Integrated Management Controller (IMC) port (labeled M on the embedded Ethernet ports)

Step 2: Connect any other ports needed for the deployment, such as the dedicated web management port, an isolated enterprise network port, or a cluster configuration port. These optional ports are not used for the deployment described.

The following example steps are described in detail with all options within the Installation Guide for the appliance software version. Use the guide to configure Cisco IMC on the appliance during first boot, along with the credentials required for Cisco IMC access. The Installation Guide describes the complete set of options, including joining a host to another host to create a cluster and configuring the left port (labeled PORT 2 on the mLOM card, and named enp10s0 in the wizard) for intra-cluster communications. The example that follows configures a single appliance for a single-node cluster or the first appliance for a three-node cluster deployment, without configuring a network proxy.

Step 3: Boot the Cisco DNA Center hardware appliance. A welcome message appears.

```
Welcome to the Maglev Configuration Wizard!
```

Step 4: Press **Enter** to accept the default choice, **Start a Cisco DNA-C Cluster**.

Step 5: Continue by accepting the wizard default choices, while supplying information for the following steps within the wizard (the wizard steps are in order but are not sequential):

- In wizard **STEP #4**, selection for **NETWORK ADAPTER #1 (enp10s0)**:
  This interface is used for clustering—configure clustering to easily allow for the future capability, even if you don't need clustering initially. Fill in the information for the **Host IP Address** and **Netmask** (a /29 size network or larger covers a three-member cluster), use the spacebar to select **Cluster Link**, do not fill in any other fields, and then select **next >>** to continue.

```
Host IP Address:
  192.168.127.1
Netmask:
  255.255.255.248
Default Gateway IP Address:
  [blank]
DNS Servers:
  [blank]
Static Routes:
  [blank]
Cluster Link
  [use spacebar to select]
Configure IPv6 address
  [blank]
```

- In wizard **STEP #4**, selection for **OPTIONAL - NETWORK ADAPTER #2 (enp1s0f0)**:
  This interface can be used as a dedicated management interface for administrative web access to Cisco DNA Center. If you are using this option (which requires static route configuration), fill in the information; otherwise leave all selections blank, and then select **next >>** to continue.
- In wizard **STEP #4**, selection for **OPTIONAL - NETWORK ADAPTER #3 (enp1s0f1)**:
  This interface is available for use with a separated network to the Internet cloud repository with a static route. Unless you require this connectivity, leave all selections blank, and select **next >>** to continue.
- In wizard **STEP #4**, selection for **OPTIONAL - NETWORK ADAPTER #4 (enp9s0)**:
  Use this interface for communications with your network infrastructure. Supply at least the **Host IP Address**, **Netmask**, **Default Gateway IP Address**, and **DNS Servers**, if you are not using the single interface with default gateway, supply **Static Routes**, and then select **next >>** to continue.

```
Host IP Address:
  10.4.49.26
Netmask:
  255.255.255.0
Default Gateway IP Address:
  10.4.49.1
DNS Servers:
  10.4.49.10
Static Routes:
  [blank for single interface installation]
Cluster Link
  [blank]
Configure IPv6 address
  [blank]
```

The wizard displays an informational message.

```
The wizard will need to shutdown the controller in order to validate…
```

Step 6: Select **proceed >>** to continue with the network validation. The installation validates gateway reachability.

```
Please wait while we validate and configure host networking...
```

Step 7: After the wizard network validation completes, continue entering initial configuration values. For all installations, create a cluster configuration to facilitate future migration. To add appliances into a cluster configuration, refer to the Installation Guide.

- In wizard **STEP #11** , **MAGLEV CLUSTER DETAILS**:

```
Cluster Virtual IP address
    10.4.49.25
```

- In wizard **STEP #13** , **USER ACCOUNT SETTINGS**:

```
Linux Password: *
  [linux password]
Re-enter Linux Password: *
  [linux password]
Password Generation Seed:
  [skip this entry]
Auto Generated Password:
  [skip this entry]
Administrator Passphrase: *
  [DNAC administrator password]
Re-enter Administrator Passphrase: *
  [DNAC administrator password]
```

Step 8: In wizard **STEP #14**, **NTP SEVER SETTINGS**, you must supply at least one active NTP server, which is tested before the installation can proceed.

```
NTP Servers: *
  10.4.0.1 10.4.0.2
```

Step 9: Select **next >>**. The installation validates connectivity to the NTP servers.

```
Validating NTP Server: 10.4.0.1
```

Step 10: In wizard **STEP #16** , **MAGLEV ADVANCED SETTINGS**, you assign unique IP networks that are not part of the enterprise network, which are used by Cisco DNA Center to manage its own API services and cluster services. The minimum recommended size for each is a network with a 21-bit netmask to accommodate the large numbers of different services with unique IP addresses that communicate with one another.

```
Services Subnet: *
  192.168.240.0/21
Cluster Services Subnet: *
  192.168.248.0/21
```

Select **next >>**. The wizard displays an informational message.

```
The wizard is now ready to apply the configuration on the controller.
```

Step 11: Disregard any additional warning messages about existing disk partitions. Select **proceed >>** to apply the configuration and complete the installation. You should not interact with the system until the installation is complete.

A number of status messages scroll by during the installation, the platform boots the installed image and configures the base processes for the first time, which can take multiple hours. When installation and configuration is complete, a login message is displayed.

```
Welcome to the Maglev Appliance (tty1)
```

Step 12: Log in with the maglev user from the Cisco IMC console, or alternatively from an SSH session on port 2222 to the host IP address as assigned during the installation.

```
maglev-master-1 login: maglev
Password: [password assigned during installation]
```

Step 13: Verify that processes are deployed.

```
$ maglev package status
```

For the validated version, all packages are DEPLOYED initially, except for any NOT_DEPLOYED packages listed, including the following, which vary depending on your installation version:

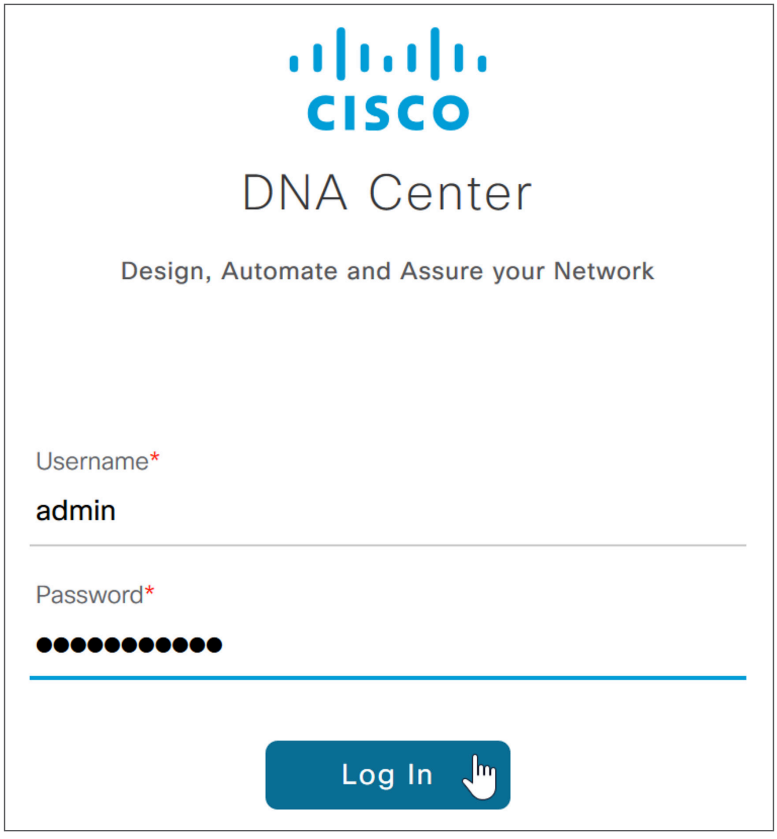
```
application-policy
sd-access
sensor-automation
```

You install other required components in later steps.

Procedure 2 Check the Cisco DNA Center version

Step 1: Connect to the Cisco DNA Center web UI by directing a web browser to the **Cluster Virtual IP address** you supplied in the previous procedure (example: https://10.4.49.25/). While processes are launched after installation, you may have to wait for some time before the web server is available to serve your first request.

Step 2: At the **Username** line enter **admin**, at the **Password** line enter the Cisco DNA Center administrator password that you assigned using the Maglev Configuration Wizard, and then click **Log In**.



Step 3: At the prompt to reset the password, choose a new password or skip to the next step.

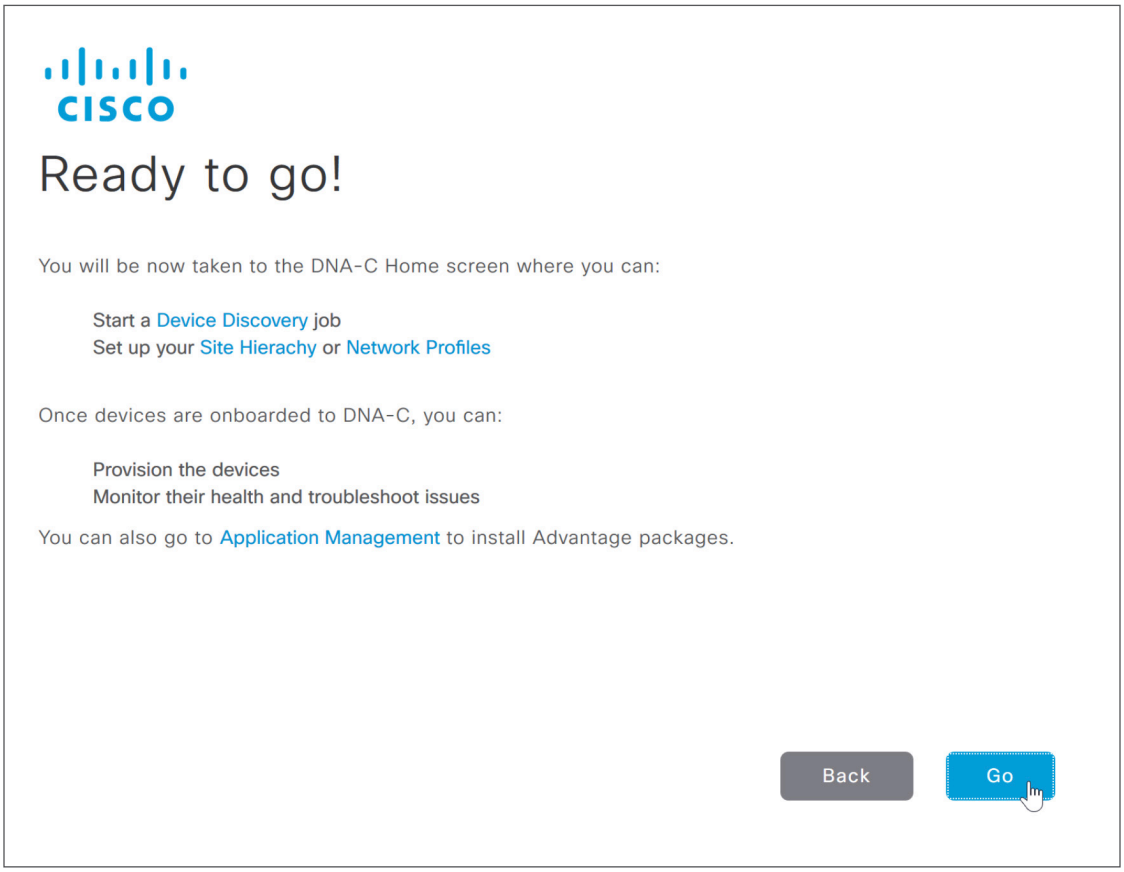
Step 4: At the **Welcome to Cisco DNA Center** prompt, provide a Cisco.com ID and password. The ID is used to register software downloads and receive system communications.

If you skip this step because you do not have an ID or plan to add one later by using **Settings** (gear) **> System Settings > Settings > Cisco Credentials**, features such as SWIM, Telemetry, and Licensing will be unable to function properly. Additionally, credentials are required for downloading software packages as described in the software migration and update procedures.

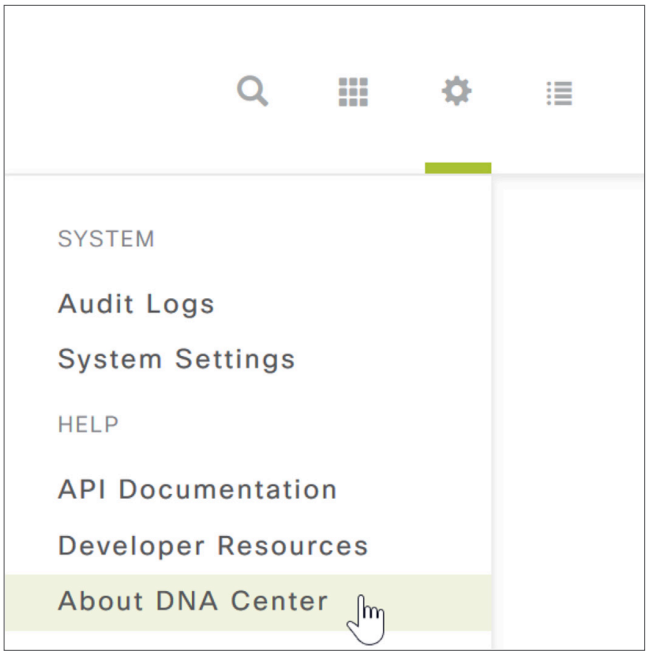
Step 5: In the previous step, if you did not enter an ID with Smart Account access with privileges for managing Cisco software licenses for your organization, a **Smart Account** prompt displays. Enter a Cisco.com ID associated with a Smart Account or click **Skip**.

Step 6: If you have an Infoblox or Bluecat IPAM server, enter the details at the **IP Address Manager** prompt and click **Next**. Otherwise, click **Skip**.

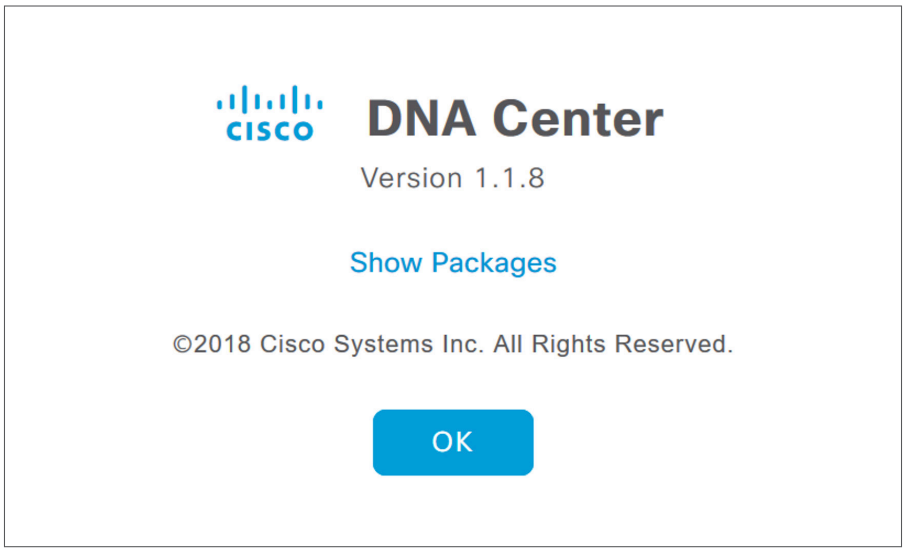
Step 7: At the **Terms and Conditions** display, click **Next**, and then at the **Ready to go!** display, click **Go**.



Step 8: At the main Cisco DNA Center dashboard, click the settings (gear) icon, and then click **About Cisco DNA Center**.



Step 9: Check that the version is at least 1.1.6. If your version is earlier than 1.1.6, contact support to reimage your Cisco DNA Center appliance to version 1.1.6 or later before continuing. Version 1.1.6 is the minimum software requirement to upgrade to version 1.2.3, shown in a later step.



Procedure 3 Migrate the Cisco DNA Center platform to Release 1.2

Optional

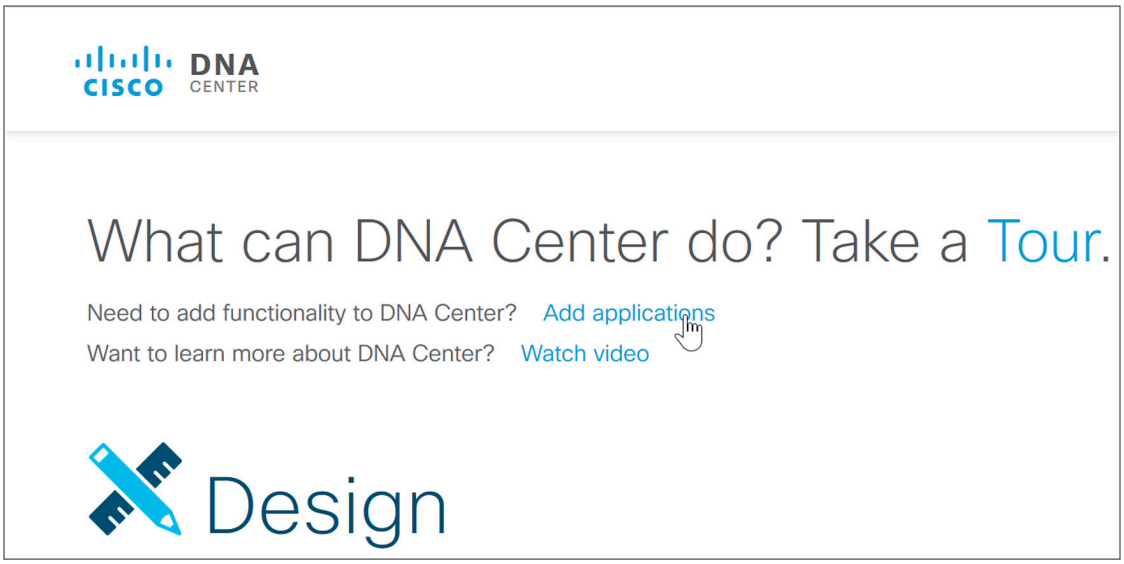
If you are running at least version 1.1.6, but are not running the desired 1.2.3 version of Cisco DNA Center, use the Cisco cloud repository to upgrade the Cisco DNA Center appliance to the required version.

Tech tip

This procedure shows the upgrade for Cisco DNA Center release 1.1 versions (minimum of 1.1.6) to version 1.2.3. For other software versions, refer to the release notes on Cisco.com for the correct procedure for a successful upgrade to the target version from the installed version.

https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-release-notes-list.html

Step 1: At the main Cisco DNA Center dashboard, click **Add applications**.



The **Application Management – Packages and Updates** screen displays. This screen is used to install packages, adding functionality to the controller, including SD-Access.

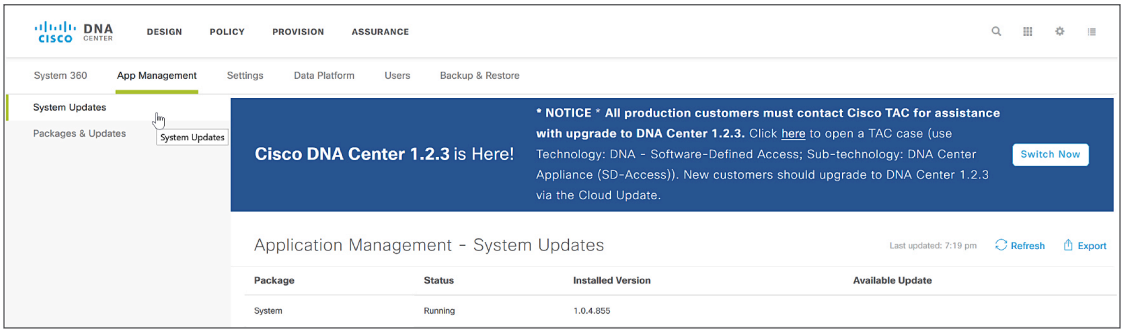
Tech tip

The Cisco DNA Center release notes include access requirements for connecting Cisco DNA Center to the Internet behind a firewall to download packages from the cloud catalog server. The release notes are on Cisco.com at:

https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-release-notes-list.html

Cisco DNA Center automatically connects to the Cisco cloud repository to find the latest updates. You can use the **Refresh** button to reveal any updates that are found over time.

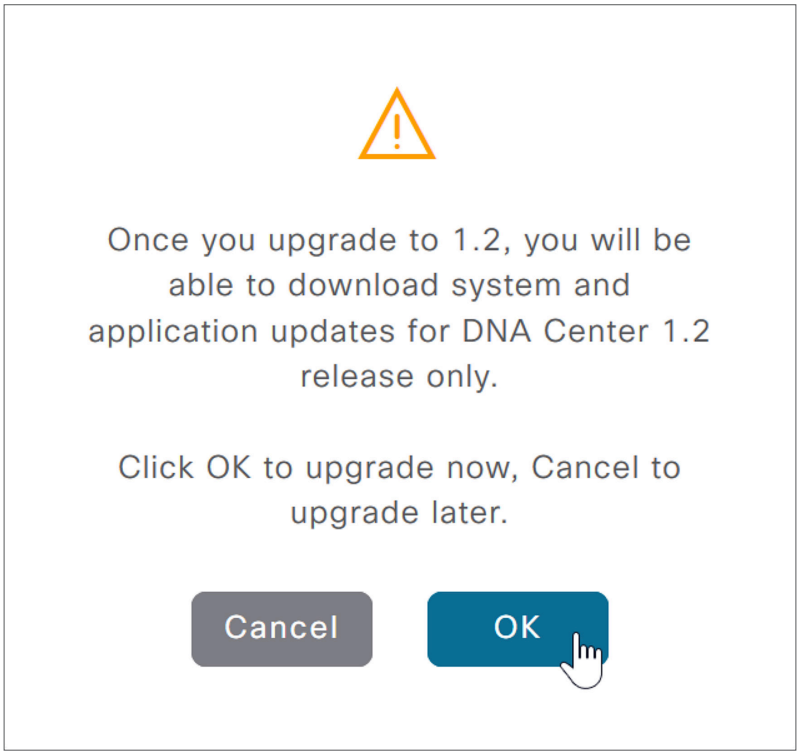
Step 2: Click the settings (gear) icon, click **System Settings**, and then navigate to **App Management > System Updates**. The **Application Management – System Updates** screen is displayed.



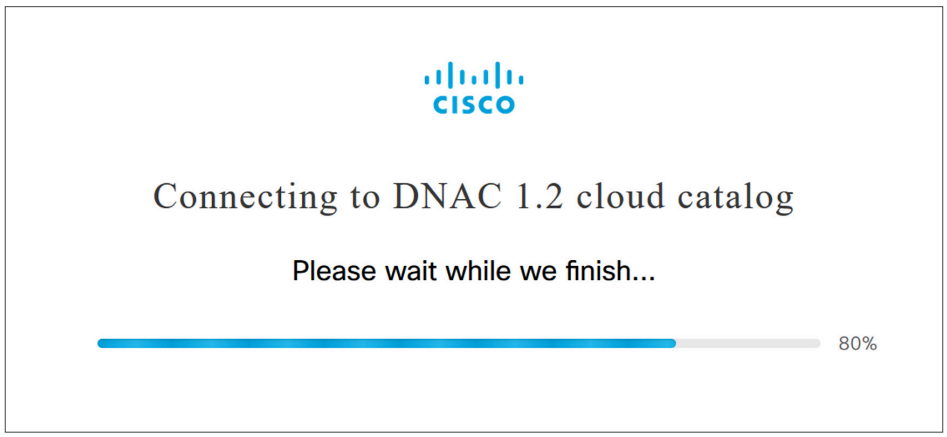
Tech tip

Illustrations are installation examples. Software versions used for validation are listed in Appendix A: Product list.

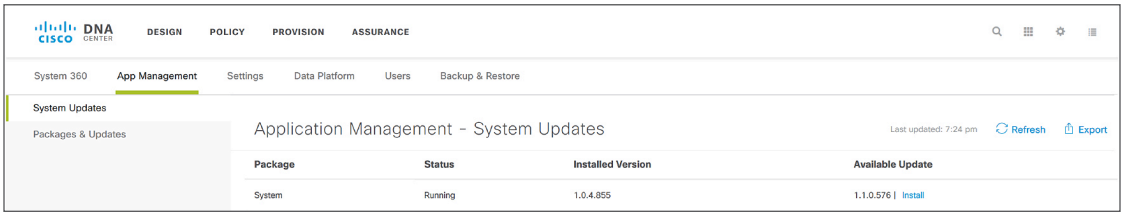
Step 3: Click the **Switch Now** button, and then acknowledge that the migration to 1.2 versions is irreversible by clicking **OK**.



Cisco DNA Center connects to the cloud catalog server.



After Cisco DNA Center finishes connecting to the 1.2 cloud catalog server, the page is refreshed with the 1.2 release option. You may use the **Refresh** button to manually update the screen. The system package **Available Update** version displayed is at least 1.1.0.576, which corresponds to release 1.2 of the Cisco DNA Center platform.



Step 4: To the right of the available update version number, click the **Install** button.

Caution

The **System** package within the **System Updates** section is the only package you download or update during the initial system update. After the installation of the system is complete, you then download and install the application package updates.

A message appears stating that the system update download has initiated. The **Status** shows **DOWNLOADING_UPDATES** for many minutes. After the download completes, the installation starts automatically with a status showing **INSTALLING_UPDATES**, which can take more than an hour. Use the **Refresh** button to check the status.

At the end of the installation, refresh the browser to view the new UI.

Procedure 4 Upgrade the Cisco DNA Center 1.2 packages

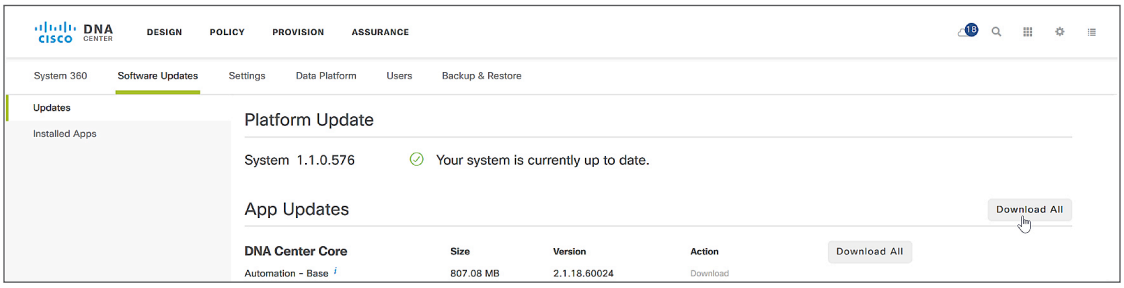
After the Cisco DNA Center platform is converted to release 1.2, you upgrade the system to the latest packages. The release 1.2 UI has some improvements that are used during the upgrades.

Step 1: Connect to the Cisco DNA Center web UI, and navigate to the main dashboard.

Step 2: In the top-right of the Cisco DNA Center release 1.2 dashboard, select the software updates cloud, and then click **Go to Software Updates**.

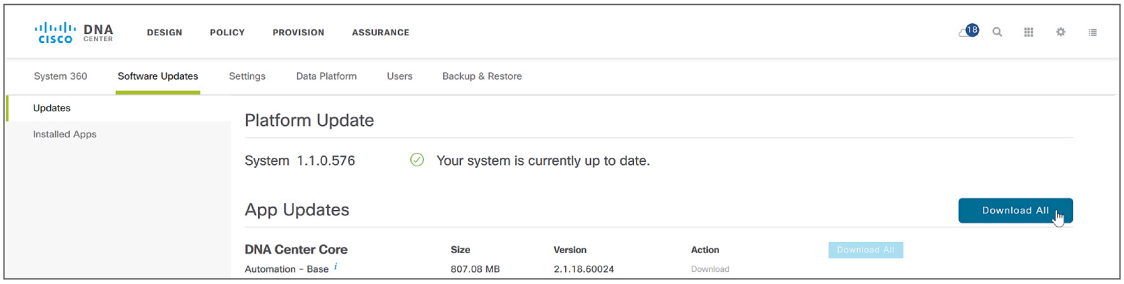
Release 1.2 displays an enhanced Platform Update screen.

Step 3: Check the top right of the **Platform Update** screen, on the same row as **App Updates**, to see if the **Download All** button is grayed out.

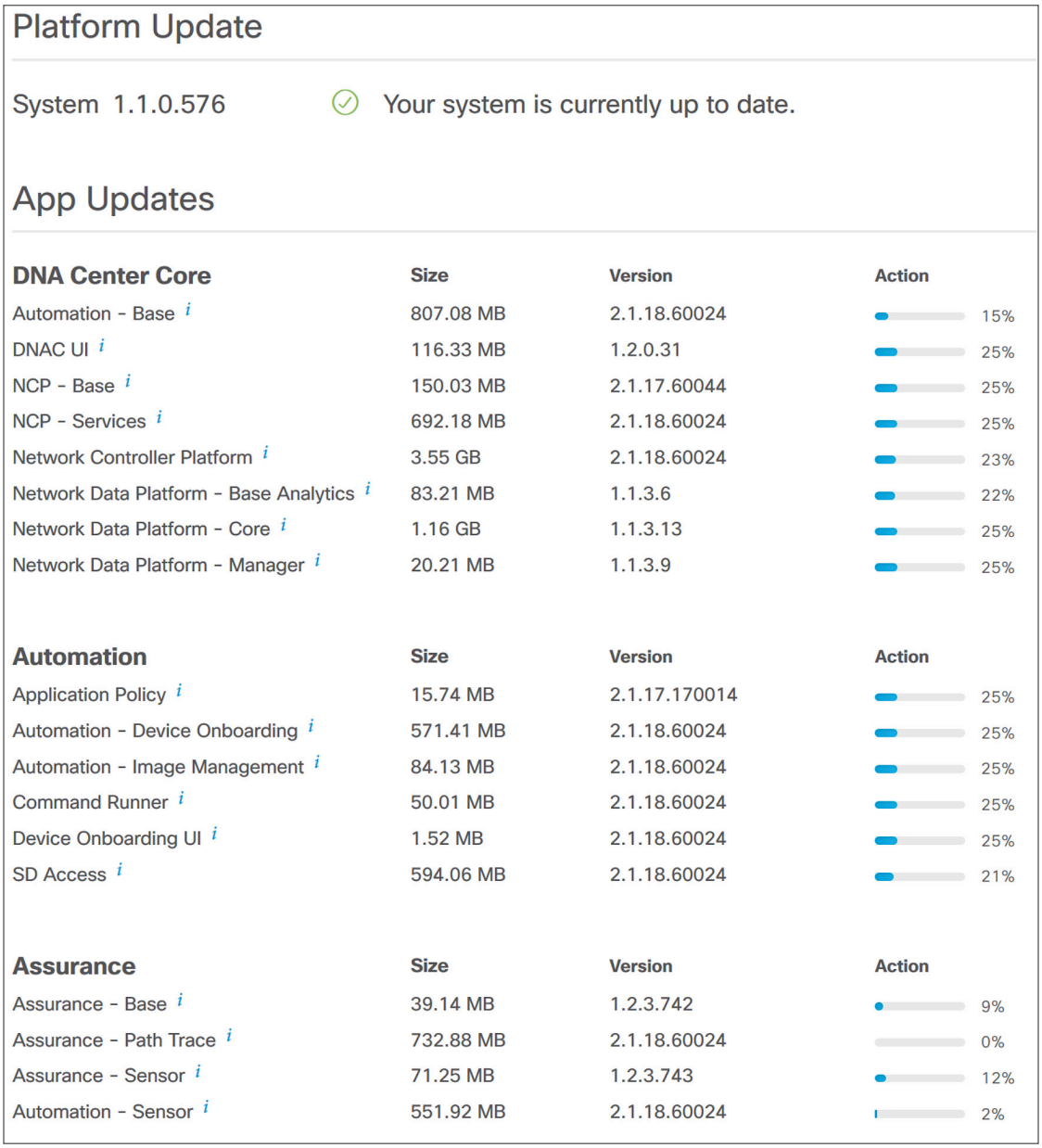


If the button is grayed out, enable your browser to display the new UI by either clearing your browser cache and reloading the browser window or using a private or incognito mode browser instance before continuing to the next step.

Step 4: At the top right of the **Platform Update** screen, on the same row as **App Updates**, click **Download All**. Do not select any of the other **Download All** buttons on the screen.



Step 5: At the popup, select **Continue** to confirm the update operation. At the second **System Readiness Check** popup, select Continue. The screen updates, showing all of the packages that are being downloaded.



Platform Update

System 1.1.0.576 Your system is currently up to date.

App Updates

DNA Center Core	Size	Version	Action
Automation - Base	807.08 MB	2.1.18.60024	15%
DNAC UI	116.33 MB	1.2.0.31	25%
NCP - Base	150.03 MB	2.1.17.60044	25%
NCP - Services	692.18 MB	2.1.18.60024	25%
Network Controller Platform	3.55 GB	2.1.18.60024	23%
Network Data Platform - Base Analytics	83.21 MB	1.1.3.6	22%
Network Data Platform - Core	1.16 GB	1.1.3.13	25%
Network Data Platform - Manager	20.21 MB	1.1.3.9	25%

Automation	Size	Version	Action
Application Policy	15.74 MB	2.1.17.170014	25%
Automation - Device Onboarding	571.41 MB	2.1.18.60024	25%
Automation - Image Management	84.13 MB	2.1.18.60024	25%
Command Runner	50.01 MB	2.1.18.60024	25%
Device Onboarding UI	1.52 MB	2.1.18.60024	25%
SD Access	594.06 MB	2.1.18.60024	21%

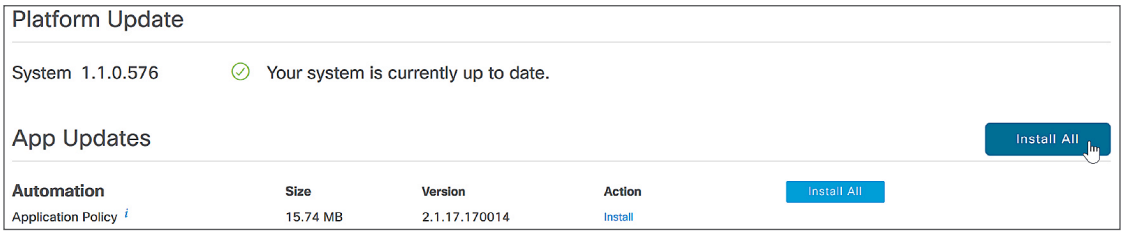
Assurance	Size	Version	Action
Assurance - Base	39.14 MB	1.2.3.742	9%
Assurance - Path Trace	732.88 MB	2.1.18.60024	0%
Assurance - Sensor	71.25 MB	1.2.3.743	12%
Automation - Sensor	551.92 MB	2.1.18.60024	2%

The interface updates with the package installation status, and at the top of the screen the cloud icon also informs users navigating to any screen of the status.

Before proceeding to the next step, refresh the screen until there are no longer any packages that are downloading. The download and associated package dependency download and installation can take over an hour to complete. If there are still package dependencies for updates, the **Download All** button is displayed again.

Step 6: After the downloads complete, if any additional packages are listed for updates, repeat the previous two steps until the **Download All** button is replaced with an **Install All** button that is not grayed out.

Step 7: After the new versions of the packages are downloaded, at the top right of the **Platform Update** screen, on the same row as **App Updates**, click **Install All**, on the popup click **Continue**, and then, on the **System Readiness Check** popup, click **Continue**. An informational message appears stating that the **Packages installation will start soon...**, and the installation begins.



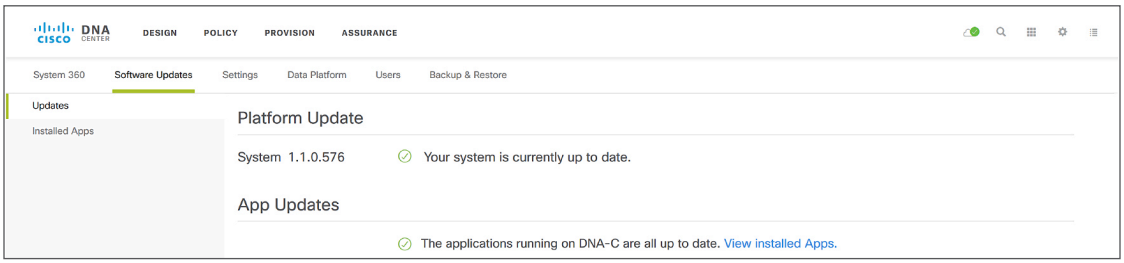
The remaining package updates begin. The browser refreshes automatically, showing the updated status for each package. The update process can take over an hour to complete.

Tech tip

Packages must be updated in a specific order to appropriately address package interdependencies. Allow Cisco DNA Center to handle dependencies by selecting and updating all package updates at once. The Installation Guide explains how to use the Maglev CLI to force a download retry for any stalled download.

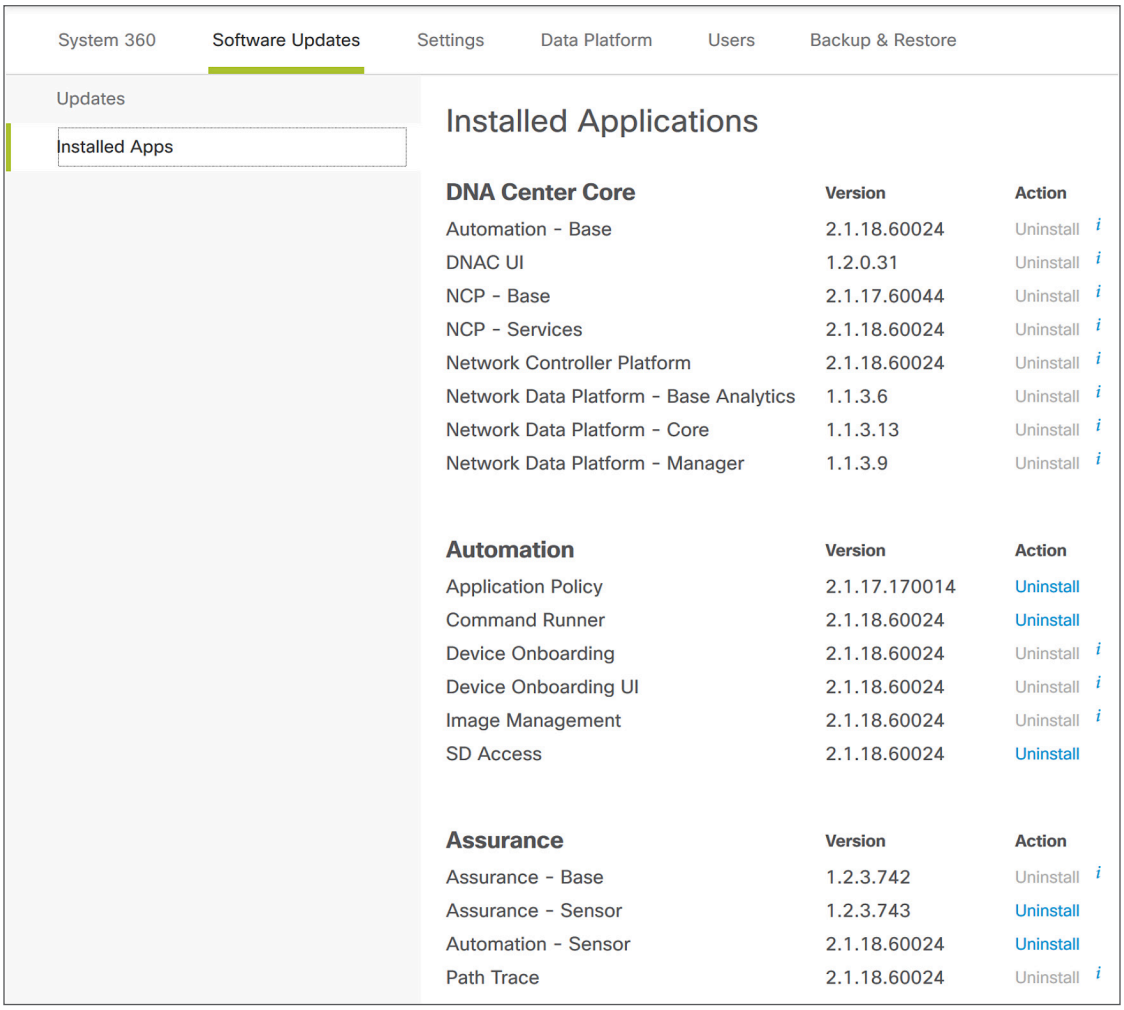
While the packages are installing, which takes some time, you may work in parallel on the next process for installing the Identity Services Engine nodes.

All of the application package updates are installed when the **Software Updates > Updates** screen no longer shows any available packages listed under **App Updates** and the cloud icon in the top right of the screen displays a green checkmark.

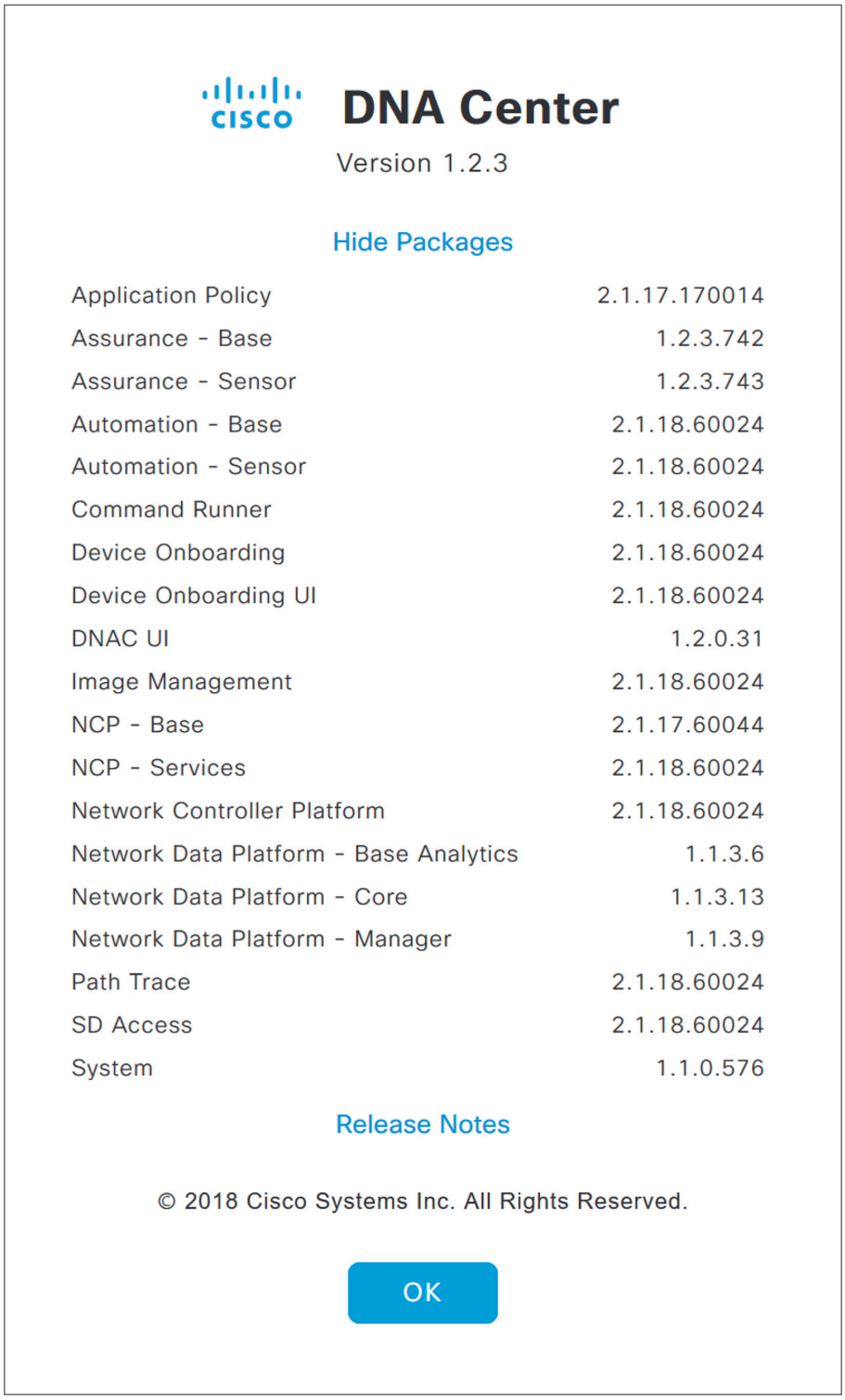


Do not continue to the next step until all packages are installed.

Step 8: Navigate to **Software Updates > Installed Apps** to see that all packages are installed. The packages are grouped by package type.



Step 9: At the main Cisco DNA Center dashboard, click the settings (gear) icon, click **About Cisco DNA Center**, and then click **Show Packages**. This view is useful for comparing to the release notes, which are available by clicking on the **Release Notes** text.



With all application packages installed, the SD-Access functionality is available to use, and integration with the installed ISE nodes can proceed.

Process

Installing Identity Services Engine nodes

1. Install ISE server images
2. Configure roles for ISE nodes
3. Register ISE node 2 and configure roles

The SD-Access solution described in this guide uses two ISE nodes in a high-availability standalone configuration dedicated to the SD-Access network and integrated into Cisco DNA Center management. The first ISE node has the primary policy administration node (PAN) persona configuration and the secondary monitoring and troubleshooting (MnT) persona configuration. The second ISE node has the secondary PAN persona configuration and the primary MnT persona configuration. Both nodes include policy services node (PSN) persona configurations. You must also enable pxGrid and External RESTful Services (ERS) on the ISE nodes.

Table 2. ISE node configurations

ISE Node 1	ISE Node 2
Primary PAN	Secondary PAN
Secondary MnT	Primary MnT
PSN	PSN
pxGrid	pxGrid
ERS Services	ERS Services

Tech tip

There are specific ISE software versions required for compatibility with Cisco DNA Center. To be able to integrate with an existing ISE installation, you must first ensure that the existing ISE is running at least the minimum supported version. An ISE integration option, which is not included in this validation, is to stand up a new ISE instance as a proxy to earlier versions of ISE.

The versions of ISE and Cisco DNA Center validated in HA standalone mode for this guide are listed in Appendix A: Product list. You may find alternative recommended images by searching Cisco.com for SD-Access Hardware and Software Compatibility Matrix.

Procedure 1 Install ISE server images

Step 1: On both ISE nodes, boot and install the ISE image.

Step 2: On the console of the first ISE node, at the login prompt, type **setup**, and then press **Enter**.

```
**********************************************
Please type 'setup' to configure the appliance
**********************************************

localhost login: setup
```

Step 3: Enter the platform configuration parameters.

```
Press 'Ctrl-C' to abort setup
Enter hostname[]: m29-ise1
Enter IP address []: 10.4.49.30
Enter IP netmask[]: 255.255.255.0
Enter IP default gateway[]: 10.4.49.1
Enter default DNS domain[]: ciscodna.net
Enter Primary nameserver[]: 10.4.49.10
Add secondary nameserver? Y/N [N]: N
Enter NTP server[time.nist.gov]: 10.4.0.1
Add another NTP server? Y/N [N]: Y
Enter NTP server[time.nist.gov]: 10.4.0.2
Add another NTP server? Y/N [N]: N
Enter system timezone[UTC]: UTC
Enable SSH service? Y/N [N]: Y
Enter username[admin]: admin
Enter password: [admin password]
Enter password again: [admin password]
Copying first CLI user to be first ISE admin GUI user…
Bringing up network interface...
Pinging the gateway...
Pinging the primary nameserver...

Do not use 'Ctrl-C' from this point on...

Installing Applications...
 === Initial Setup for Application: ISE ===
```

Additional installation messages appear, and then the server reboots.

```
Rebooting...
```

Step 4: Repeat steps 2 and 3 on the second ISE node, using the appropriate parameters for it.

The systems reboot automatically and display the Cisco ISE login prompt.

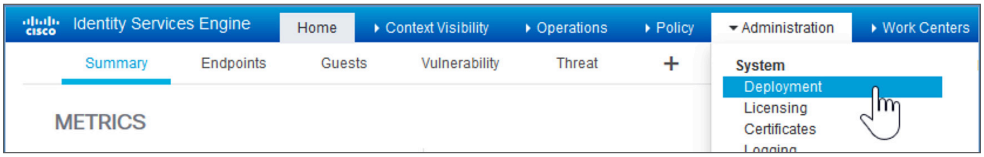
```
localhost login:
```

Procedure 2 Configure roles for ISE nodes

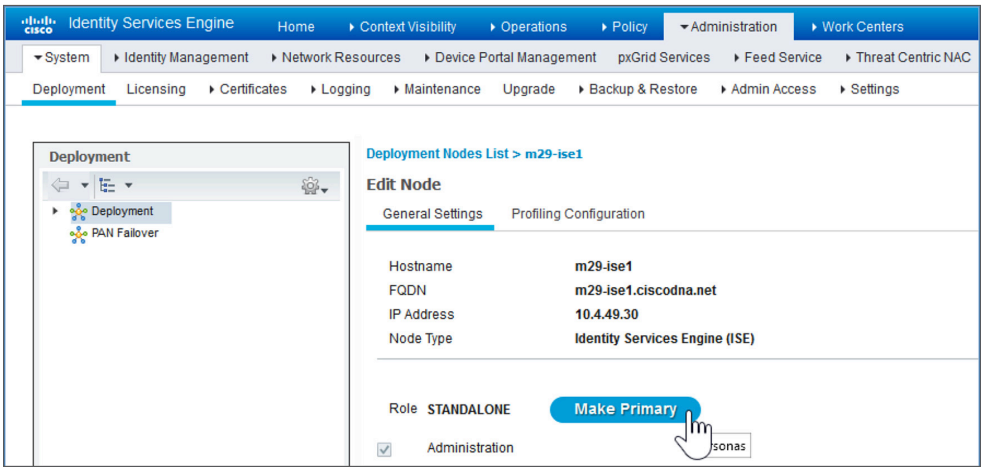
Step 1: On the first ISE node, login using a web browser and the configured username and password, and then accept any informational messages.

https://m29-ise1.ciscodna.net/

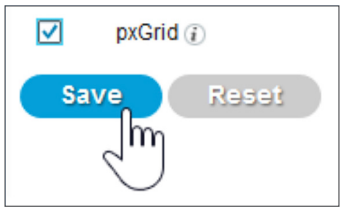
Step 2: Navigate to **Administration > System > Deployment**, and then click **OK** to the informational message.



Step 3: Click on the ISE node hostname, and then under Role, click **Make Primary**.



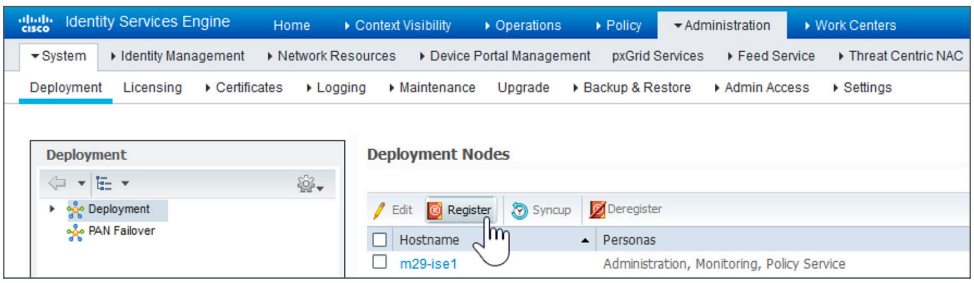
Step 4: Select **pxGrid**, and then click **Save**.



Procedure 3 Register ISE node 2 and configure roles

Integrate the additional ISE node by using the same ISE administration session started on the first node.

Step 1: Refresh the view by navigating again to **Administration > System > Deployment**, and then under the **Deployment Nodes** section, click **Register**.

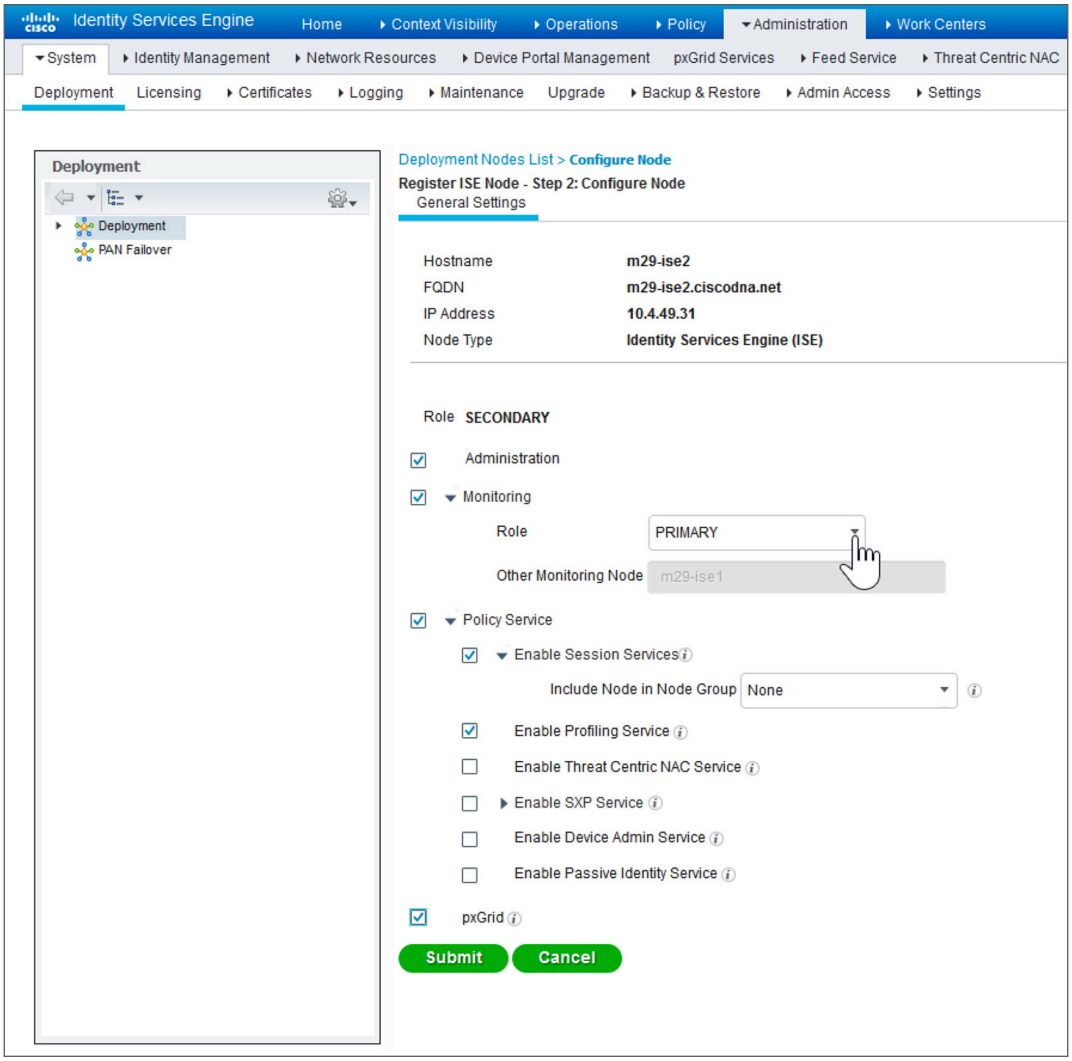


A screen displays allowing registration of the second ISE node into the deployment.

Step 2: Enter the ISE fully-qualified domain name **Host FQDN** (**m29-ise2.ciscodna.net**), **User Name** (**admin**), and **Password** (**[admin password]**), and then click **Next**.

Step 3: If you are using self-signed certificates, click **Import Certificate and Proceed**. If you are not using self-signed certificates, follow the instructions for importing certificates and canceling this registration, and then return to the previous step.

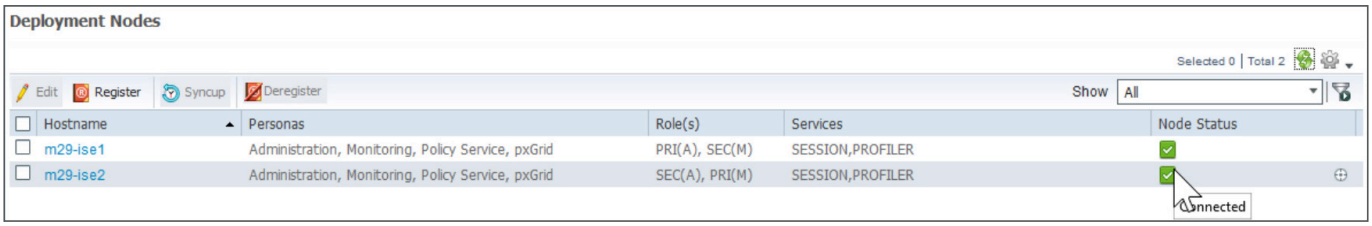
Step 4: On the **Register ISE Node - Step 2: Configure Node** screen, under **Monitoring**, change the role for this second ISE node to **PRIMARY**, at the bottom check **pxGrid**, and then click **Submit**.



The node configuration is saved.

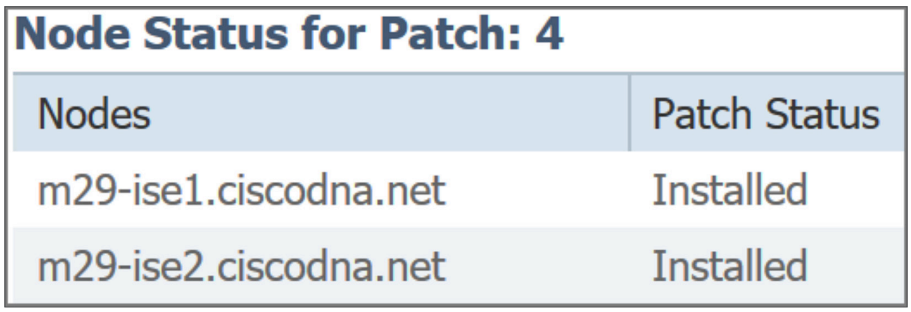
Step 5: Click **OK** to the notification that the data is to be synchronized to the node and the application server on the second node will restart.

The synchronization and restart of the second node can take more than ten minutes to complete. You can use the refresh button on the screen to observe when the node returns from **In Progress** to a **Connected** state to proceed to the next step.



Step 6: Check Cisco.com for ISE release notes, download any patch required for your installation, and install the patch by navigating in ISE to **Administration > System > Maintenance > Patch Management**, click **Install**, click **Browse**, browse for the patch image, and then click **Install**. The patch installs node-by-node to the cluster, and each cluster node reboots.

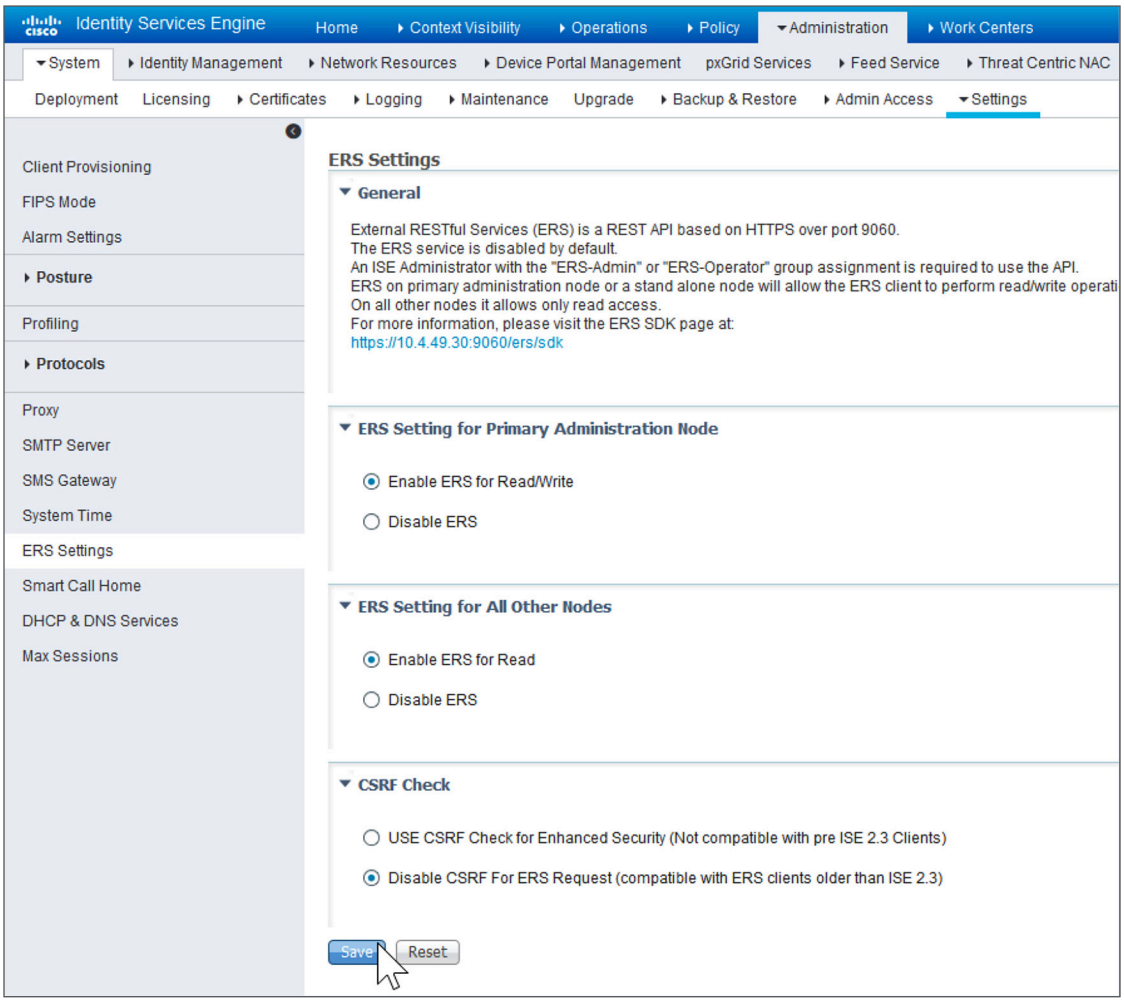
Step 7: After the ISE web interface is active again, check progress of the patch installation by navigating to **Administration > System > Maintenance > Patch Management**, select the patch, and then select **Show Node Status**. Use the **Refresh** button to update status until all nodes are in **Installed** status, and then proceed to the next step.



Node Status for Patch: 4

Nodes	Patch Status
m29-ise1.ciscodna.net	Installed
m29-ise2.ciscodna.net	Installed

Step 8: Navigate to **Administration > System > Settings**, on the left pane navigate to **ERS Settings**, under **ERS Setting for Primary Administration Node** select **Enable ERS for Read/Write**, accept any dialog box that appears, under **ERS Setting for All Other Nodes** select **Enable ERS for Read**, under **CRSF Check** select **Disable CSRF for ERS Request**, and then click **Save**. Accept any additional dialog box that appears.



The ERS settings are updated, and ISE is ready to be integrated with Cisco DNA Center.

Process

Integrating Identity Services Engines with Cisco DNA Center

1. Configure Cisco DNA Center authentication and policy servers

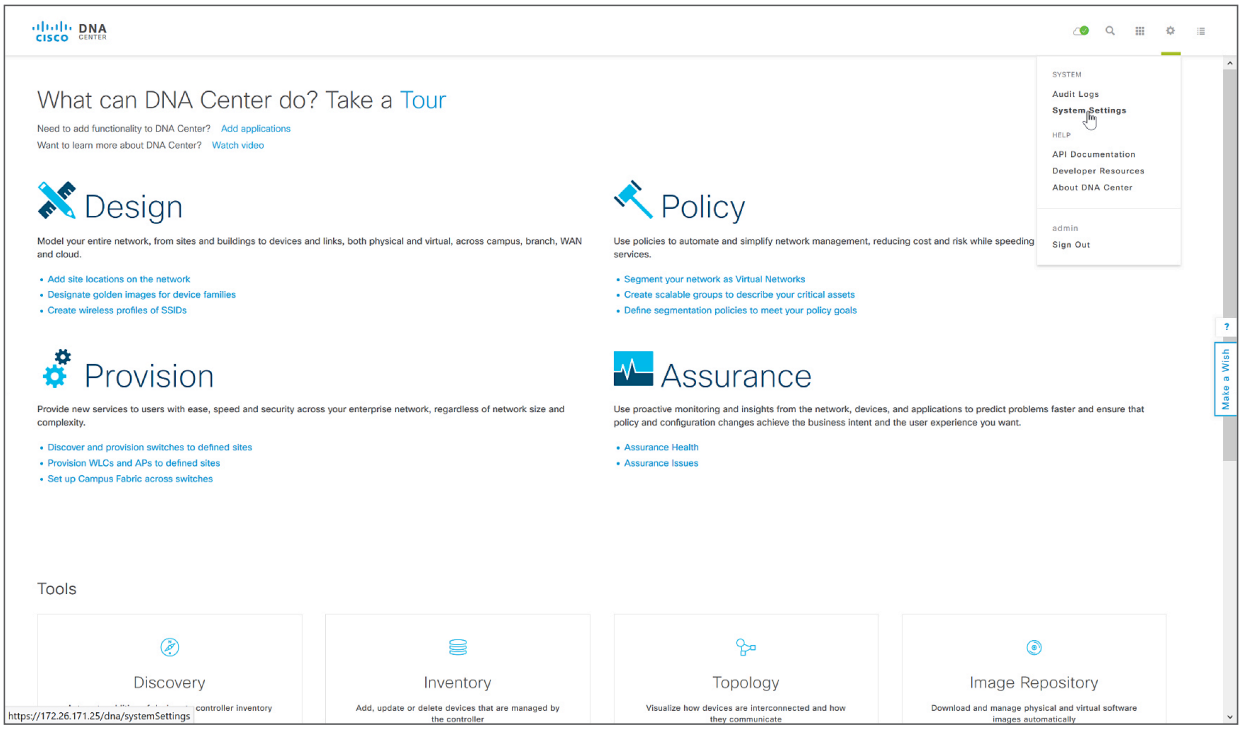
Integrate ISE with Cisco DNA Center by defining ISE as an authentication and policy server to Cisco DNA Center and permitting pxGrid connectivity from Cisco DNA Center into ISE. Integration enables information sharing between the two platforms, including device information and group information, and allows Cisco DNA Center to define policies to be rendered into the network infrastructure by ISE.

Tech tip

The validation includes Cisco DNA Center integration with ISE servers as a requirement for automation of the assignment of edge ports to VNs and policy configuration, including the deployment of scalable group tags and group-based policies.

Procedure 1 Configure Cisco DNA Center authentication and policy servers

Step 1: Log in to the Cisco DNA Center web interface, at the top-right corner select the gear icon, and then navigate to **System Settings**.

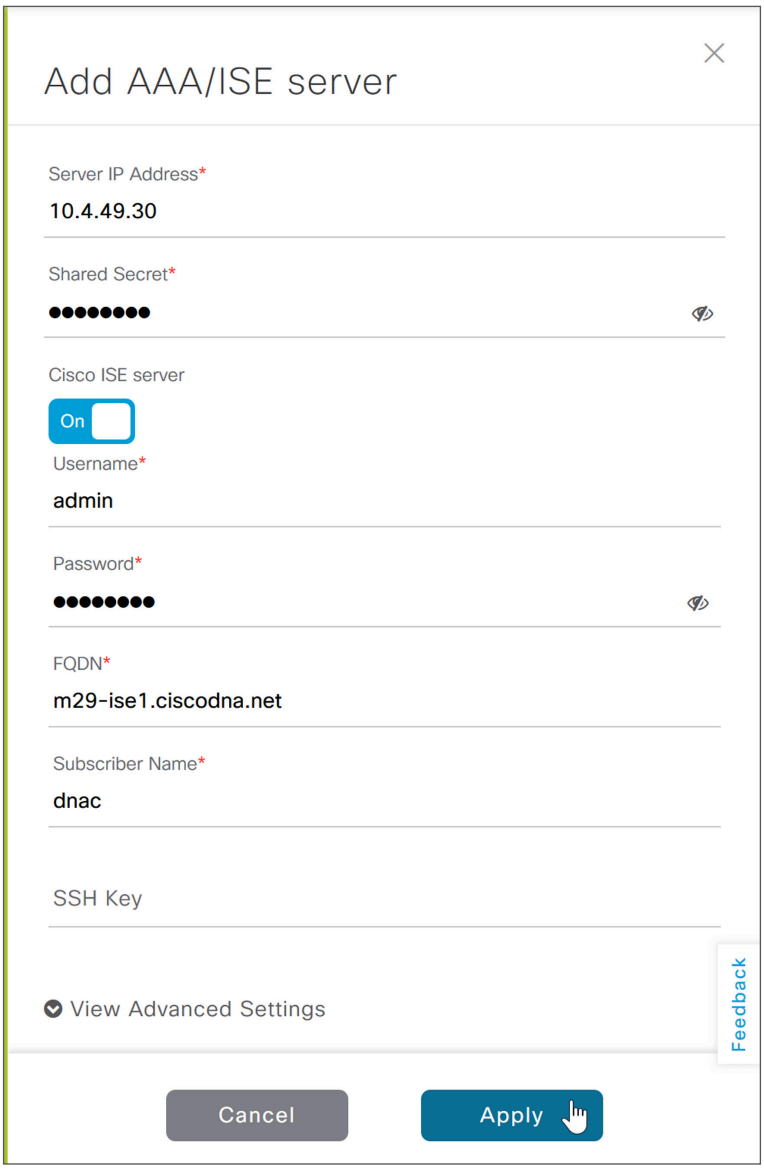


Step 2: Navigate to **Settings > Authentication and Policy Servers**, and then click the **+ Add** button.

Tech tip

The next step for integrating an ISE installation is the same whether you use a high-availability standalone ISE deployment, as validated, or a distributed ISE deployment. The shared secret chosen needs to be consistent with the shared secret used across the devices in the network for communicating with the authentication, authorization, and accounting (AAA) server. The username and password are used for Cisco DNA Center to communicate with ISE using SSH, and must be the default super admin account that was created during the ISE installation.

Step 3: In the **Add AAA/ISE SERVER** display, enter the ISE node 1 (primary PAN) **Server IP Address** (example: **10.4.49.30**) and **Shared Secret**, toggle the **Cisco ISE** selector, enter the ISE **Username** (example: **admin**), enter the ISE **Password**, enter the ISE fully qualified domain name for **FQDN**, enter **Subscriber Name** (example: **dnac**), leave the SSH Key blank, and then click **Apply**.



Tech tip

Many organizations use TACACS for management authentication to network devices, which is not covered in this validation. 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. ISE configuration information for enabling TACACS integration is found within ISE by navigating to **Work Centers > Device Administration > Overview**.

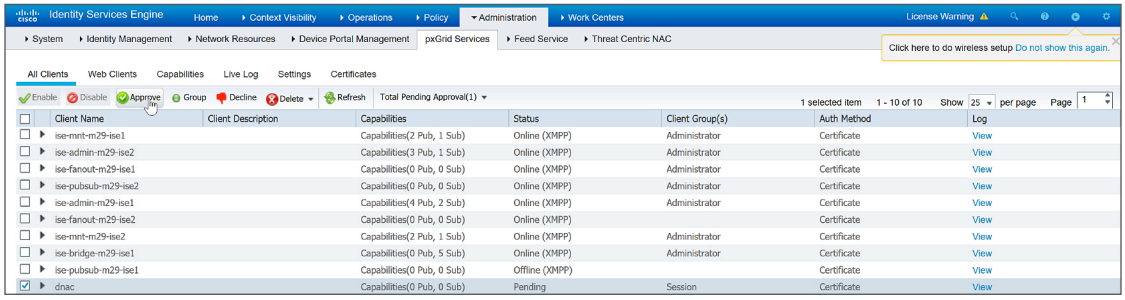
During communication establishment, status from Cisco DNA Center displays **Creating AAA server...** and then **Status** displays **INPROGRESS**. Use the **Refresh** button until communication establishes with ISE and the server displays **ACTIVE** status. If communication is not established, an error message displays with information reported from ISE regarding the problem to be addressed before continuing. You can also see the communication status by navigating from the gear icon to **System Settings > System 360**. Under **External Network Services**, the Cisco ISE server shows in **Available** status.

With communications established, Cisco DNA Center requests a pxGrid session with ISE.

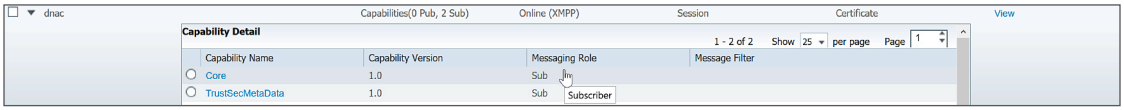
Step 4: Log in to ISE, and then navigate to **Administration > pxGrid Services**.

The client named **dnac** is now showing **Pending** in the **Status** column.

Step 5: Check the box next to **dnac**, above the list click **Approve**, and then click **Yes** to confirm.



A success message displays, and the **Pending** status changes to **Online (XMPP)**. You can additionally verify that the integration is active by expanding the view for the client and observing two subscribers, **Core** and **TrustSecMetaData**.



If ISE is integrated with Cisco DNA Center after scalable groups are already created in ISE, in addition to the default groups available, any existing ISE groups are also visible by logging in to Cisco DNA Center and navigating to **Policy > Registry > Scalable Groups**. Existing ISE policies are not migrated to Cisco DNA Center.

Process

Installing SD-Access wireless LAN controllers

1. Configure the WLC Cisco AireOS platforms using the startup wizard

For this deployment, dedicate the WLCs to SD-Access Wireless connectivity by integrating them natively with the fabric. The WLCs use link aggregation to connect to a redundant Layer 2 shared services distribution outside of the SD-Access fabric, as described in the Campus LAN and Wireless LAN Design Guide. Configure a pair of Cisco WLCs with high availability stateful switchover (HA SSO) resiliency, and all of the network connectivity should be in place before starting the configuration procedure.

Redundant WLCs should be connected to a set of devices configured to support the Layer 2 redundancy suitable for the HA SSO WLCs, such as a switch stack, Cisco Virtual Switching System, or Cisco StackWise® Virtual, which may exist in a data center or shared services network. For maximum resiliency, redundant WLCs should not be directly connected to the Layer 3 border nodes.

Tech tip

The SD-Access solution described supports transport of only IP frames in the Layer 2 overlays that are used for WLAN, without Layer 2 flooding of broadcast and unknown multicast traffic. Without broadcasts from the fabric edge, Address Resolution Protocol (ARP) functions by using the fabric control plane for MAC-to-IP address table lookups. For transport of non-IP frames and Layer 2 flooding, see the release notes for your software version in order to verify updated support.

Tech tip

Adding WLAN as part of the SD-Access solution while using Cisco Catalyst® 6800 Series fabric border devices requires the software releases listed in Appendix A: Product list. If the devices do not have software supporting the wireless control plane, you must use separate control plane devices that do include wireless support. See the release notes for any changes to WLAN Layer 2 control plane support when using the Cisco Catalyst 6800 Series.

Procedure 1 Configure the WLC Cisco AireOS platforms using the startup wizard

Perform the initial configuration using the CLI startup wizard.

After powering up the WLC, you should see the following on the WLC console. If not, type **-** (dash) followed by **Enter** repeatedly until the startup wizard displays the first question.

```
Welcome to the Cisco Wizard Configuration Tool

Use the '-' character to backup
```

Step 1: Terminate the auto-install process.

```
Would you like to terminate autoinstall? [yes]: YES
```

Step 2: Enter a system name. Do not use colons in the system name, and do not leave the default name.

```
System Name [Cisco_7e:8e:43] (31 characters max): SDA-WLC-1
```

Step 3: Enter an administrator username and password.

Tech tip

Use at least three of the following character classes in the password: lowercase letters, uppercase letters, digits, and special characters.

```
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): [password]
Re-enter Administrative Password                 : [password]
```

Step 4: Use DHCP for the service port interface address.

```
Service Interface IP address Configuration [static] [DHCP]: DHCP
```

Step 5: Enable Link Aggregation (LAG).

```
Enable Link Aggregation (LAG) [yes][NO]: YES
```

Step 6: Enter the management interface IP address, mask, and default router. The IP address for the secondary controller of an HA SSO pair is used only temporarily until the secondary WLC downloads the configuration from the primary and becomes a member of the HA controller pair.

```
Management Interface IP Address: 10.4.174.26
Management Interface Netmask: 255.255.255.0
Management interface Default Router: 10.4.174.1
```

Step 7: Configure the Management Interface VLAN Identifier.

```
Management Interface VLAN Identifier (0 = untagged): 174
```

Step 8: Configure the Management Interface Port Number. The displayed range varies by WLC model. This number is arbitrary after enabling LAG, because all management ports are automatically configured and participate as one LAG, and any functional physical port in the group can pass management traffic.

```
Management Interface Port Num [1 to 2]: 1
```

Step 9: Enter the DHCP server for clients. (Example: 10.4.48.10)

```
Management Interface DHCP Server IP Address: 10.4.48.10
```

Step 10: You do not need to enable HA SSO in this step. Cisco DNA Center automates the HA SSO controller configuration during device provisioning.

```
Enable HA (Dedicated Redundancy Port is used by Default)[yes][NO]: NO
```

Step 11: The WLC uses the virtual interface for mobility DHCP relay, guest web authentication, and inter-controller communication. Enter an IP address that is not used in your organization's network.

```
Virtual Gateway IP Address: 192.0.2.1
```

Step 12: Enter a multicast address that will be used by each AP to subscribe to IP multicast flows coming from the WLC. This address will be used only when configuring the IP multicast delivery method called ***multicast-multicast***.

```
Multicast IP Address: 239.1.1.1
```

Tech tip

The multicast address must be unique for each controller or HA pair in the network. The multicast address entered is used as the source multicast address, which the access points registered to the controller use for receiving wireless user-based multicast streams.

Step 13: Enter a name for the default mobility and RF group.

```
Mobility/RF Group Name: SDA-Campus
```

Step 14: Enter an SSID for the data WLAN. This is used later in the deployment process.

```
Network Name (SSID): SDA-Data
```

Step 15: Disable DHCP Bridging Mode.

```
Configure DHCP Bridging Mode [yes][NO]: NO
```

Step 16: Enable DHCP snooping.

```
Allow Static IP Addresses [YES][no]: NO
```

Step 17: Do not configure the RADIUS server now. You will configure the RADIUS server later using the GUI.

```
Configure a RADIUS Server now? [YES][no]: NO
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.
```

Step 18: Enter the country code where you are deploying the WLC.

```
Enter Country Code list (enter 'help' for a list of countries) [US]: US
```

Step 19: Enable all of the required wireless networks.

```
Enable 802.11b network [YES][no]: YES
Enable 802.11a network [YES][no]: YES
Enable 802.11g network [YES][no]: YES
```

Step 20: Enable the radio resource management (RRM) auto-RF feature.

```
Enable Auto-RF [YES][no]: YES
```

Step 21: Synchronize the WLC clock to your organization's NTP server.

```
Configure a NTP server now? [YES][no]:YES
Enter the NTP server's IP address: 10.4.0.1
Enter a polling interval between 3600 and 604800 secs: 86400
```

Step 22: Do not configure IPv6.

```
Would you like to configure IPv6 parameters[YES][no]:NO
```

Step 23: Confirm that the configuration is correct. The WLC saves the configuration and resets automatically.

```
Configuration correct? If yes, system will save it and reset. [yes][NO]: YES

…

Configuration saved!

Resetting system with new configuration…
```

If you press Enter or respond with **no**, the system resets without saving the configuration, and you will have to complete this procedure again.

The WLC resets and displays a **User:** login prompt.

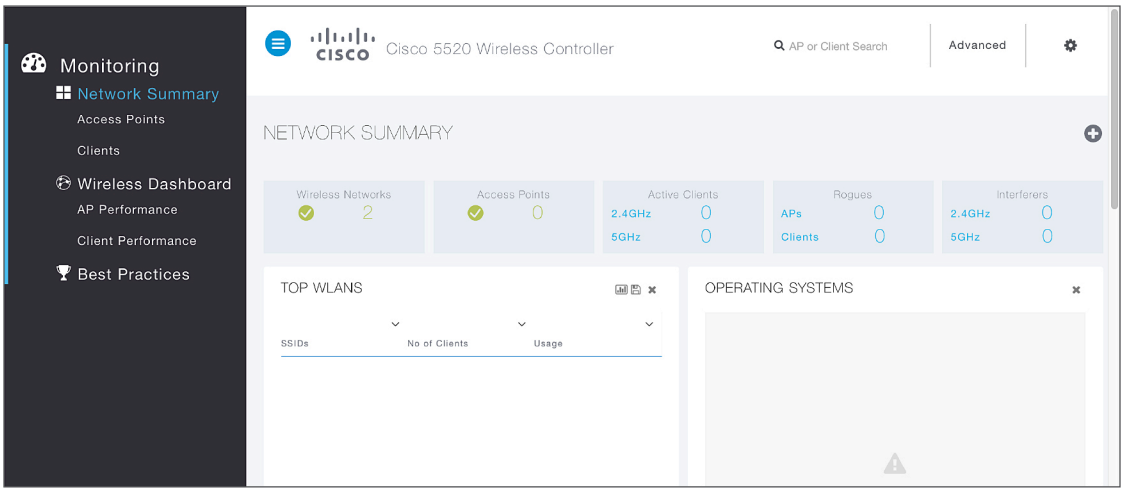
```
(Cisco Controller)

Enter User Name (or 'Recover-Config' this one-time only to reset configuration
to factory defaults)

User:
```

Step 24: Repeat Step 1 through Step 23 for the secondary WLC, using the appropriate parameters for it.

Step 25: Use a web browser to verify connectivity by logging in to each of the Cisco WLC administration web pages using the credentials created in Step 3 of Procedure 1. (Example: https://10.4.174.26)



Step 26: Navigate to **Commands > Set Time**. Verify that the date and time agree with the NTP server. If the time appears to be significantly different, manually correct it, and, if your network infrastructure devices use something other than the default time zone, also choose a time zone. The correct date and time are important for certificate validation and successful AP registration with the WLC.

The controllers are ready for discovery and integration into the Cisco DNA Center setup. Additional controller reachability requirements, such as a specific route at the edge nodes to the WLC, are addressed in later integration procedures.

Deploying SD-Access

Process

Using Cisco DNA Center for initial network design and discovery

1. Create network sites
2. Configure network services for sites
3. Add device credentials for discovery and management
4. Define global IP address pools
5. Reserve IP address pools

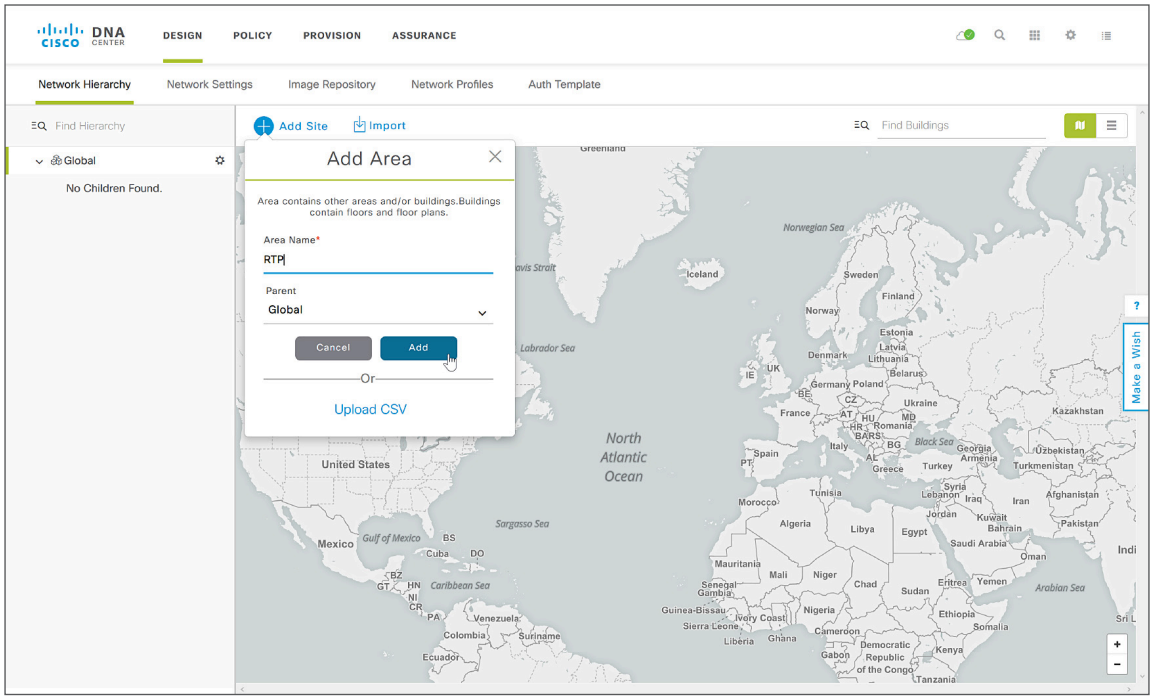
Cisco DNA Center provides a robust Design Application to allow customers of varying sizes and scales to easily define their physical sites and common resources. Using a hierarchical format that is intuitive to use, the Design Application removes the need to redefine the same resources, such as DHCP, 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 areas or buildings and floors within areas. Devices map into the buildings and floors for service provisioning.

Procedure 1 Create network sites

Step 1: Log in to Cisco DNA Center. Navigate to the main Cisco DNA Center dashboard, under the **Design** category, select **Add site locations on the network**.

Step 2: Click **Add Site** to start a network design using the tool, in the drop-down menu select **Add Area**, supply an appropriate **Area Name**, and then click **Add**.



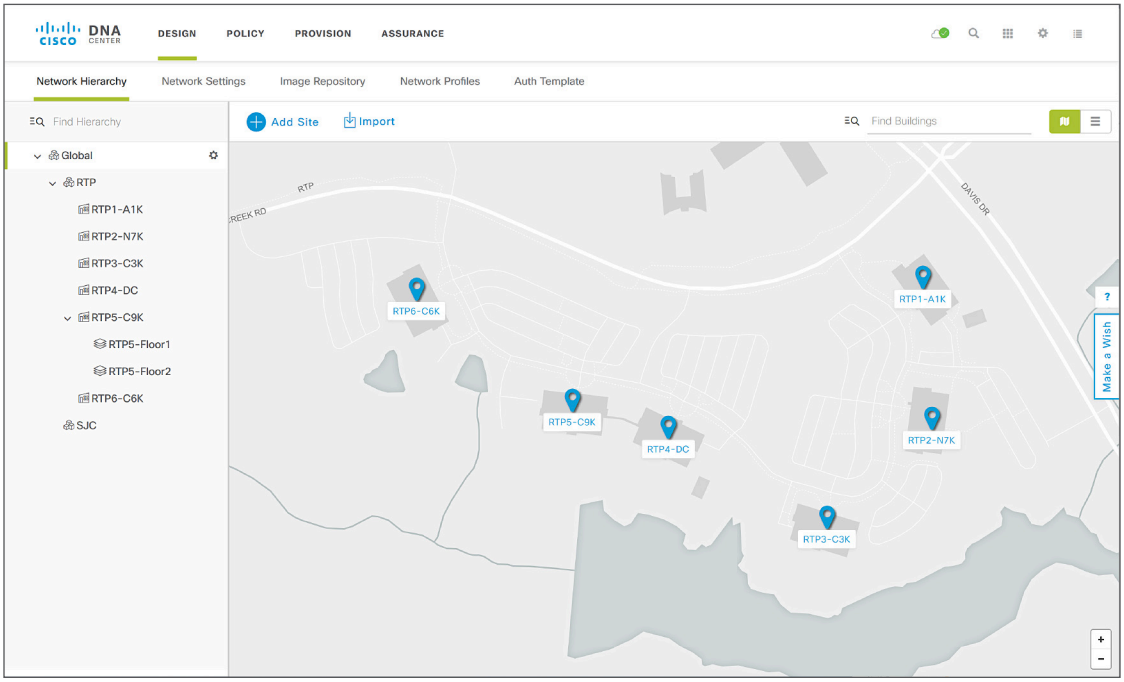
Step 3: Click **Add Site**, in the drop-down menu select the **Add Building** button, supply an appropriate **Building Name**, select the site created in the previous step as the **Parent**, complete the wizard to assign a location, and then click **Add**.

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 steps as required to add sites and buildings, creating a hierarchy that makes sense for your organization.

Step 5: If you are integrating wireless to a building, or want 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.

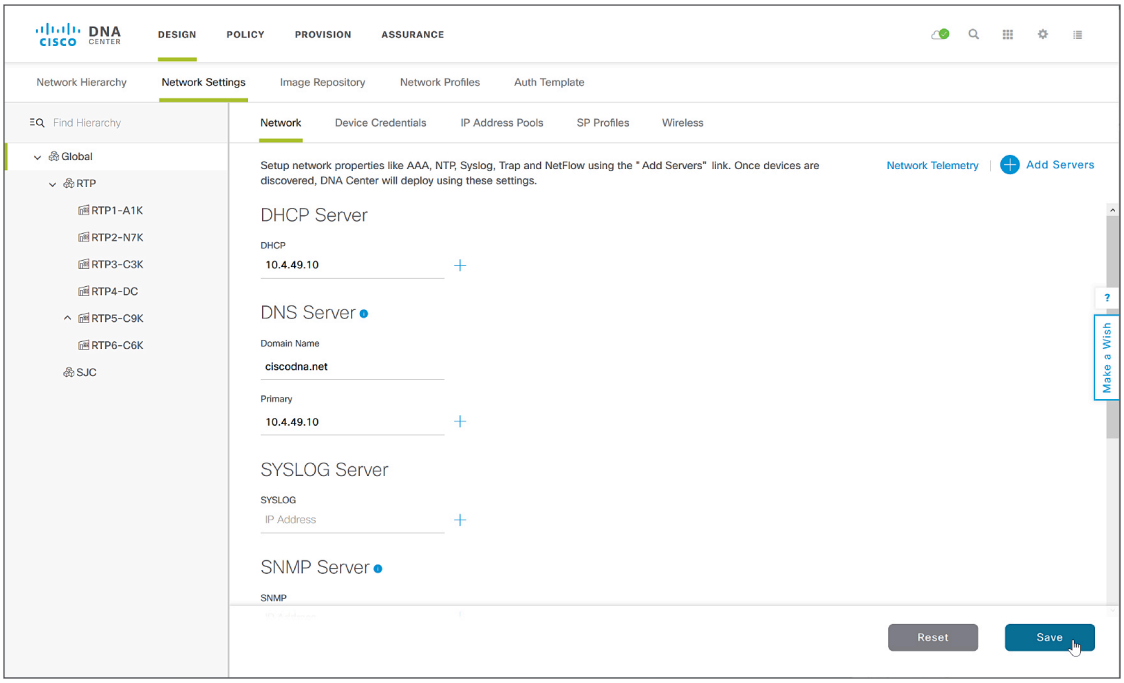
Floors are referenced during the wireless provisioning. If you have floor map diagrams in DXF, DWG, JPG, GIF, or PNG formats, add them to any defined floors as a useful component for wireless deployments to show AP locations and coverage. You can add hundreds of sites up to the limits listed in the Software-Defined Access Design Guide.



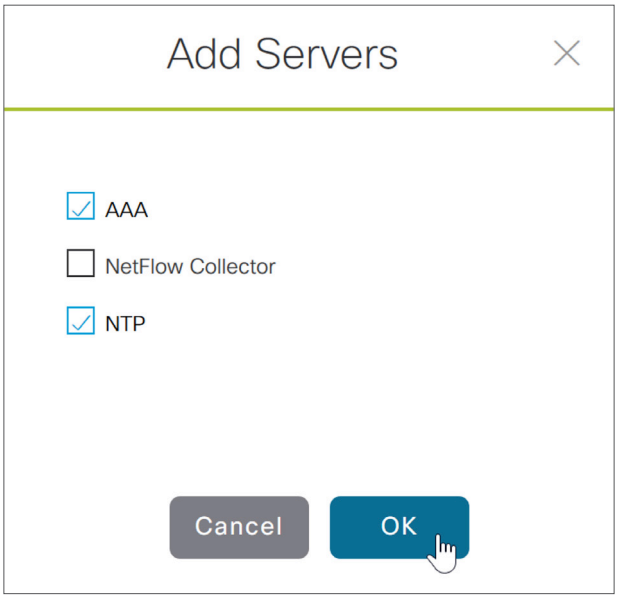
Procedure 2 Configure network services for sites

Configure AAA, DHCP, and DNS services that align to the hierarchy in Cisco DNA Center. If the services use the same servers across all of the hierarchy, 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, 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 management and the client endpoints connecting to the infrastructure. For validation, the high-availability standalone ISE nodes are used with RADIUS for both the network infrastructure and the client endpoint authentication.

Tech tip

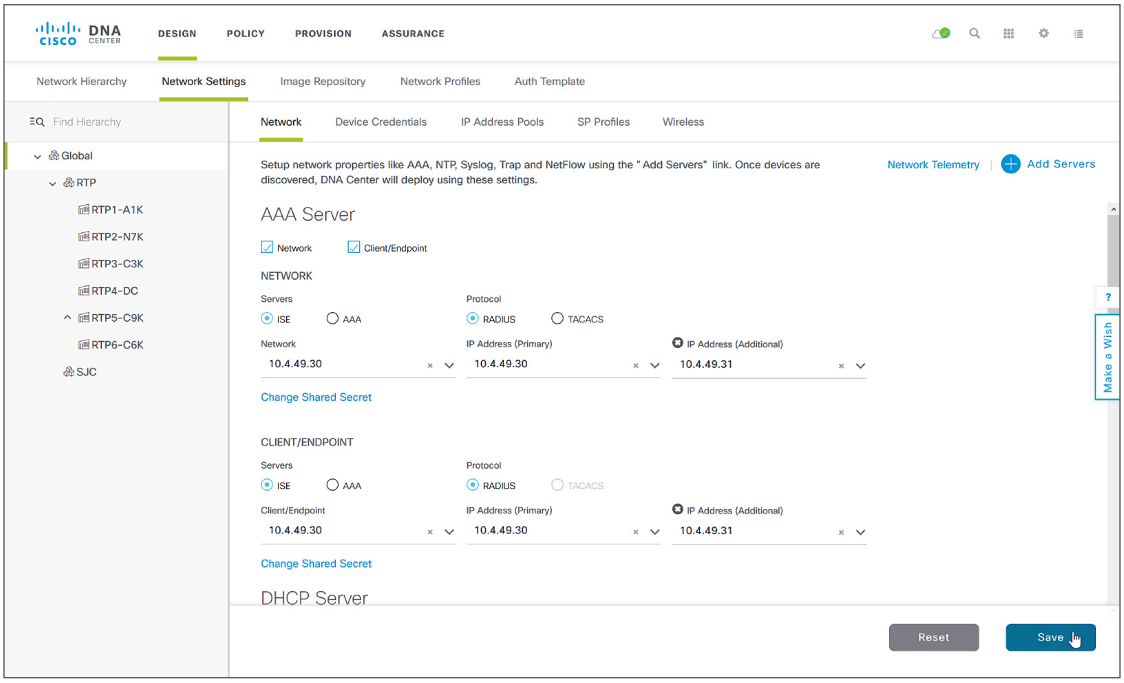
Many organizations use TACACS for management authentication to network devices, which is not covered in this validation. If you intend to enable TACACS on the same ISE server being used for RADIUS client authentication, then you add the Cisco DNA Center TACACS information during these steps. ISE configuration information for enabling TACACS integration is found within ISE by navigating to **Work Centers > Device Administration > Overview**.

Step 3: Under **AAA Server** select the **Network** and **Client/Endpoint** check boxes, under **NETWORK** and **Servers**, select the **ISE** radio button, use the pull-down to select the prepopulated ISE server, under **Protocol**, select the **RADIUS** radio button, use the second pull-down to select the device-reachable **IP Address (Primary)** of the ISE server, select the plus sign (**+**) button, and then in the **IP Address (Additional)** pull-down select the redundant ISE server node.

Tech tip

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, use the pull-down to select the device-reachable **IP Address (Primary)** of the ISE server, select the plus sign (**+**) button, and then in the **IP Address (Additional)** pull-down select the redundant ISE server node, and then click **Save**.



Step 5: Under **NTP Server**, add the **IP Address** of the NTP server, 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, 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.

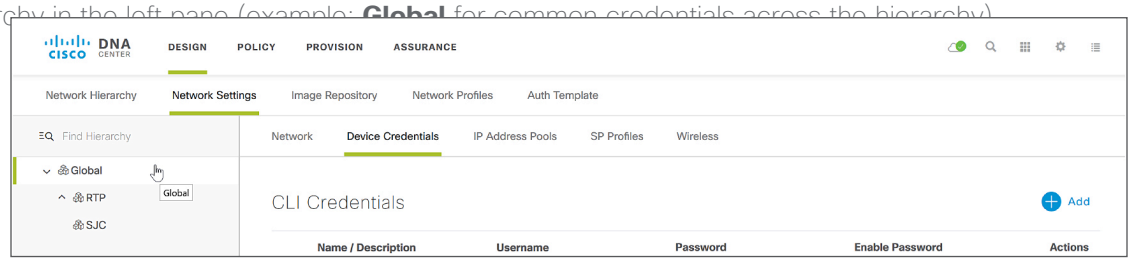
Procedure 3 Add device credentials for discovery and management

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.

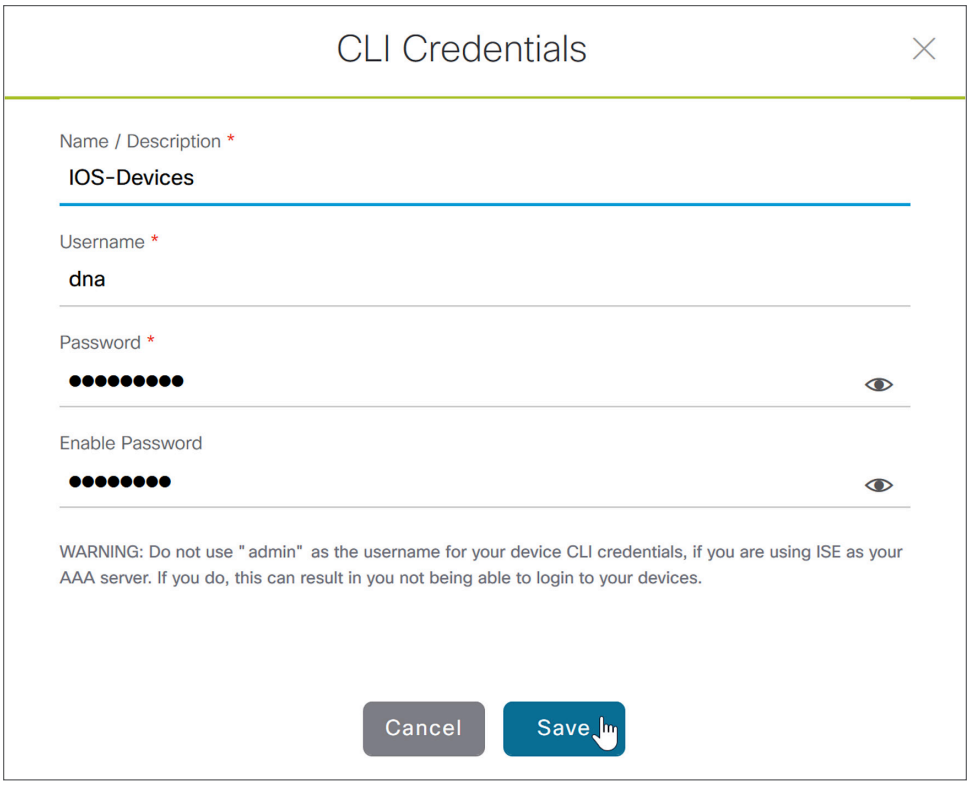
As an option, you can deploy LAN switches without existing configurations into the underlay by using the Cisco DNA Center LAN Automation capabilities. Cisco Network Plug and Play (PnP) is the mechanism enabling connectivity and initial configuration for supported switches. For LAN Automation deployments, 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.

Add device credentials to manage scopes of the site hierarchy created in the design. These credentials enable discovery and management for the network.

Step 1: 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**.



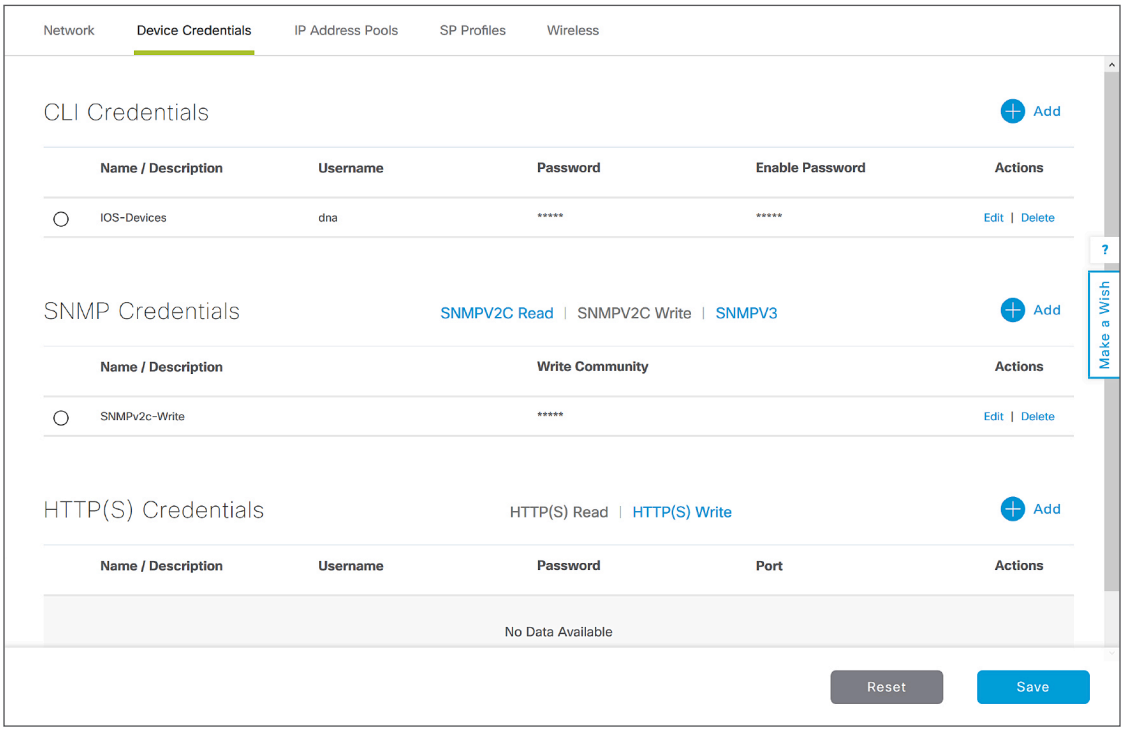
Caution

If you are using ISE as your AAA server, you should 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: SNMPv2c Read). 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, and click **Save**.

Step 4: Repeat steps 2 and 3 for any additional credentials required in the hierarchy. **CLI Credentials** and both **SNMPV2C Read** and **SNMPV2C Write** are the most common requirements.

Step 5: For each of the CLI and SNMP credentials assigned, click all radio buttons next to each assignment created, including ones where you toggle among the options (example: SNMPV2C Write). After each selection, at the bottom of the Device Credentials screen, 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. The assignments can be pushed to an IP address manager (IPAM) (examples: Infoblox, Bluecat) by integrating the IPAMs through APIs. You optionally 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. If you are not integrating with an IPAM, you manually configure IP addressing and DHCP scopes on your IPAM 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 150 for configuration by TFTP server). Check the product documentation to accommodate the requirements for your deployment.

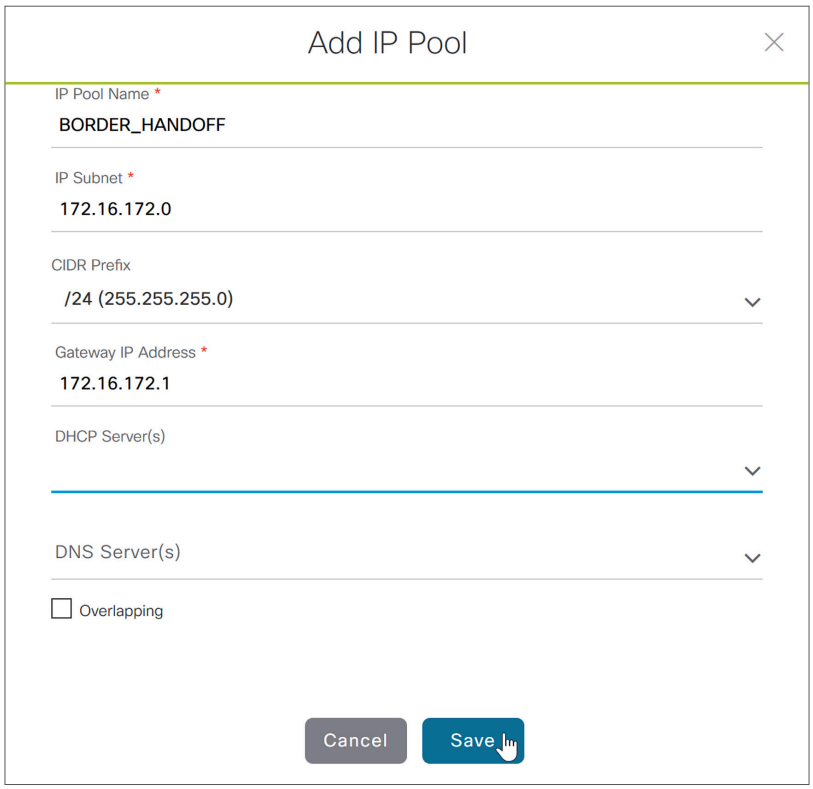
This procedure shows how to manually define the IP address pools that will be used during the pool reservation process. These pools are assigned to the sites in your network, and the assignment steps are required for both manual and integrated IPAM deployments. You have the flexibility to create a larger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

Validation of the deployment described in this guide uses the set of global address pools listed in the table.

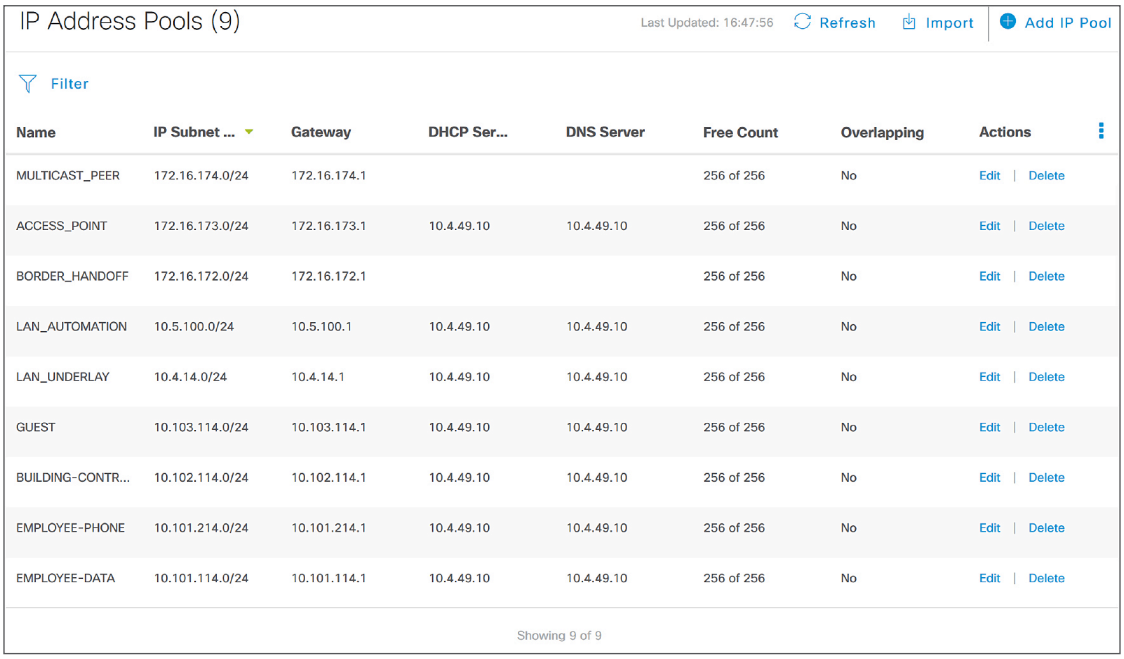
Table 3. Global address pools used during validation

Pool name	Network/mask	IP gateway	DHCP server	DNS server
Border-Handoff	172.16.172.0/24	172.16.172.1	–	–
Multicast-Peer	172.16.174.0/24	172.1 6.174.1	–	–
Access-Point	172.16.173.0/24	172.16.173.1	10.4.49.10	10.4.49.10
Lan-Underlay	10.4.14.0/24	10.4.14.1	10.4.49.10	10.4.49.10
Employee-Data	10.101.114.0/24	10.101.114.1	10.4.49.10	10.4.49.10
Employee-Phone	10.101.214.0/24	10.101.214.1	10.4.49.10	10.4.49.10
Building-Control	10.102.114.0/24	10.102.114.1	10.4.49.10	10.4.49.10
Guest	10.103.114.0/24	10.103.114.1	10.4.49.10	10.4.49.10
LAN-Automation	10.5.100.0/24	10.5.100.1	10.4.49.10	10.4.49.10

Step 1: Add a global pool in Cisco DNA Center that is dedicated to fabric border node connectivity provisioning. Navigate 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. If the pool has endpoint clients, assign 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.



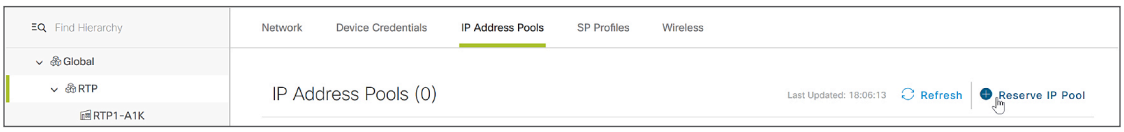
Procedure 5 Reserve IP address pools

Use the defined global IP address pools to reserve IP addresses for sites in your design using the network hierarchy. For single-site deployments, the entire set of global IP address pools can be reserved for that site. 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.

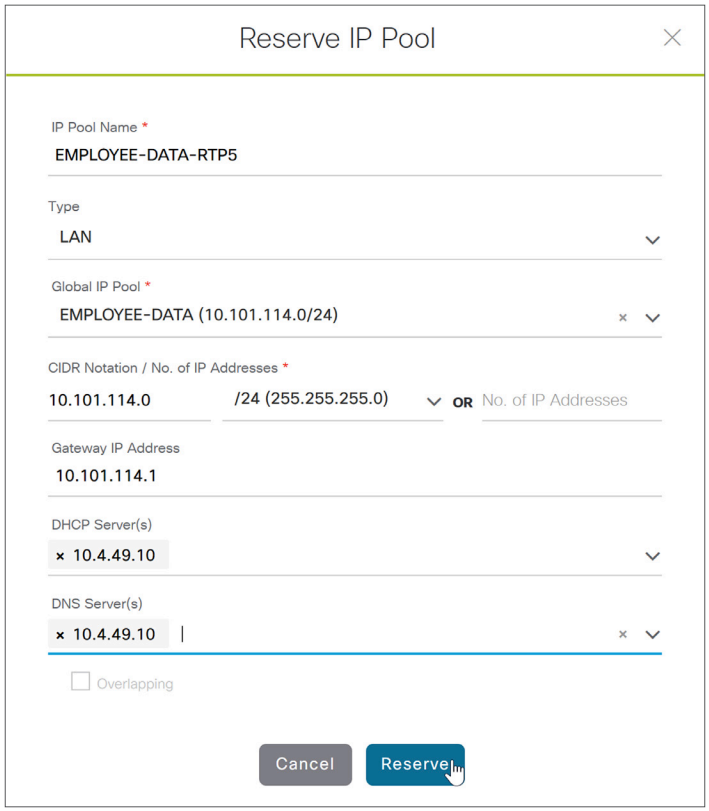
Tech tip

Reserving IP address pools at the site is an enhancement to the capabilities previously available in the SD-Access 1.1 solution, and is available using the Cisco DNA Center software listed in the appendix.

Step 1: 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: RTP5-C9K), and then in the top right click **Reserve IP Pool**.

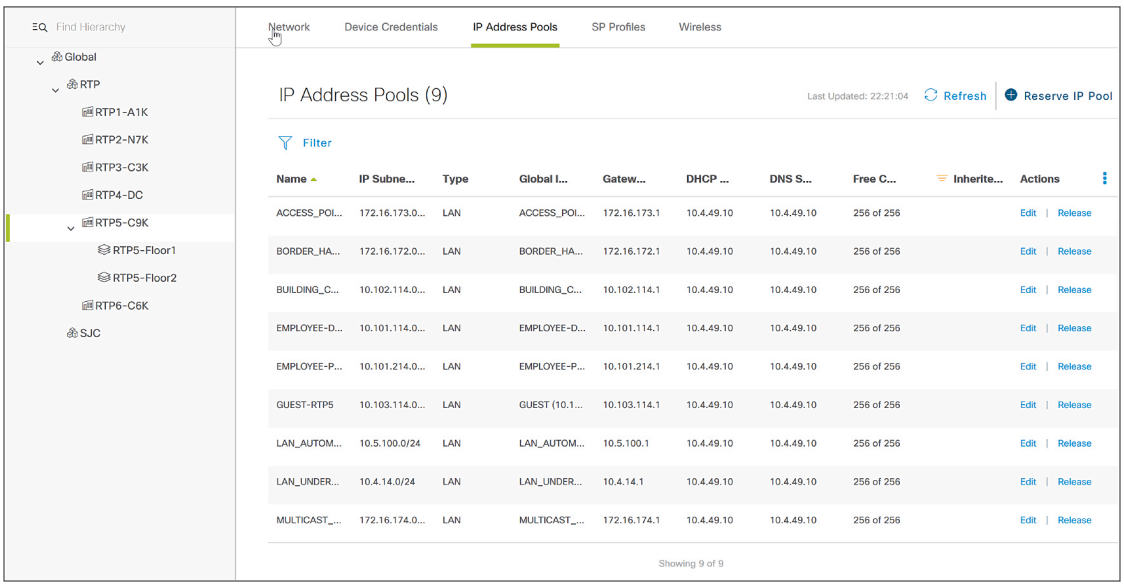


Step 2: Fill in the **IP Pool Name** (example: EMPLOYEE-DATA-RTP5), under **Type** select **LAN**, select the **Global IP Pool** source for the reservation (example: EMPLOYEE-DATA), under **CIDR Notation/No. of IP Addresses** select the portion of the address space to use (example: 10.101.114.0/24), assign a **Gateway IP Address**, **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 a site.

The hierarchy shows the assigned address pools.



Process

Creating segmentation and policy for the SD-Access network

1. Add an overlay VN to the SD-Access network
2. Create a micro-segmentation policy using SGTs

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

The desired outcomes of policy application using segmentation may be easily accommodated with group policies. In a university example, students and faculty machines may both 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.

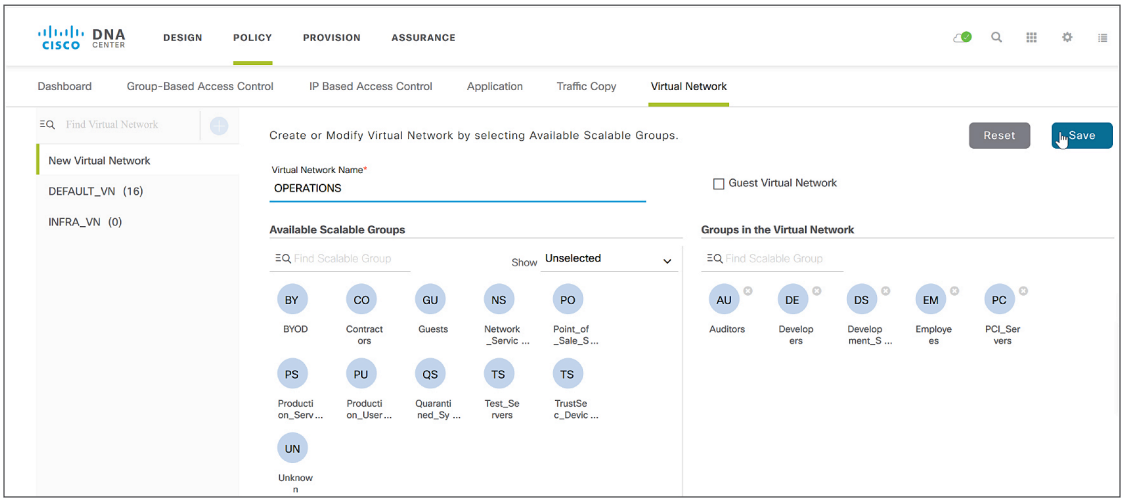
In other cases, a higher degree of isolation is required. In a retail store example, the point-of-sale machines should never be in communication with the video surveillance network infrastructure, which in turn should never communicate with the building HVAC system. In cases where the isolation need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

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

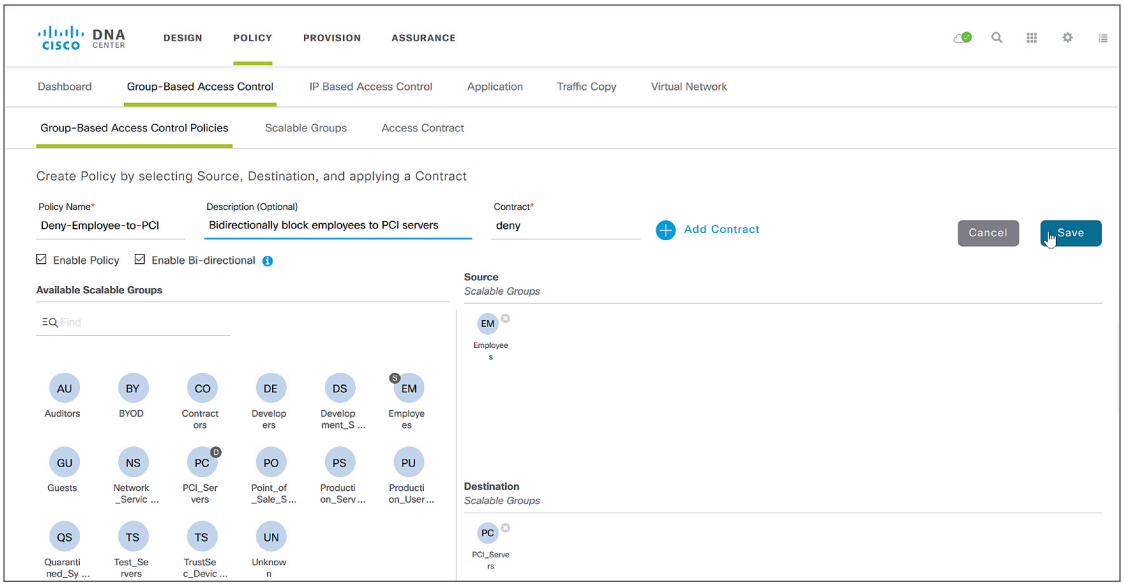
If you don't see any groups, likely the pxGrid connectivity between Cisco DNA Center and ISE is not fully operational. In this case, review the integration procedures for ISE with Cisco DNA Center and be sure to approve the pxGrid connection request in ISE from Cisco DNA Center.

Repeat this step for each overlay network. You can also return to this step after the fabric is provisioned to create more overlay networks.

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. The policy intent that is created here is used when authentication profiles appropriately assign an SGT to an endpoint or user, as rendered into the network by ISE.

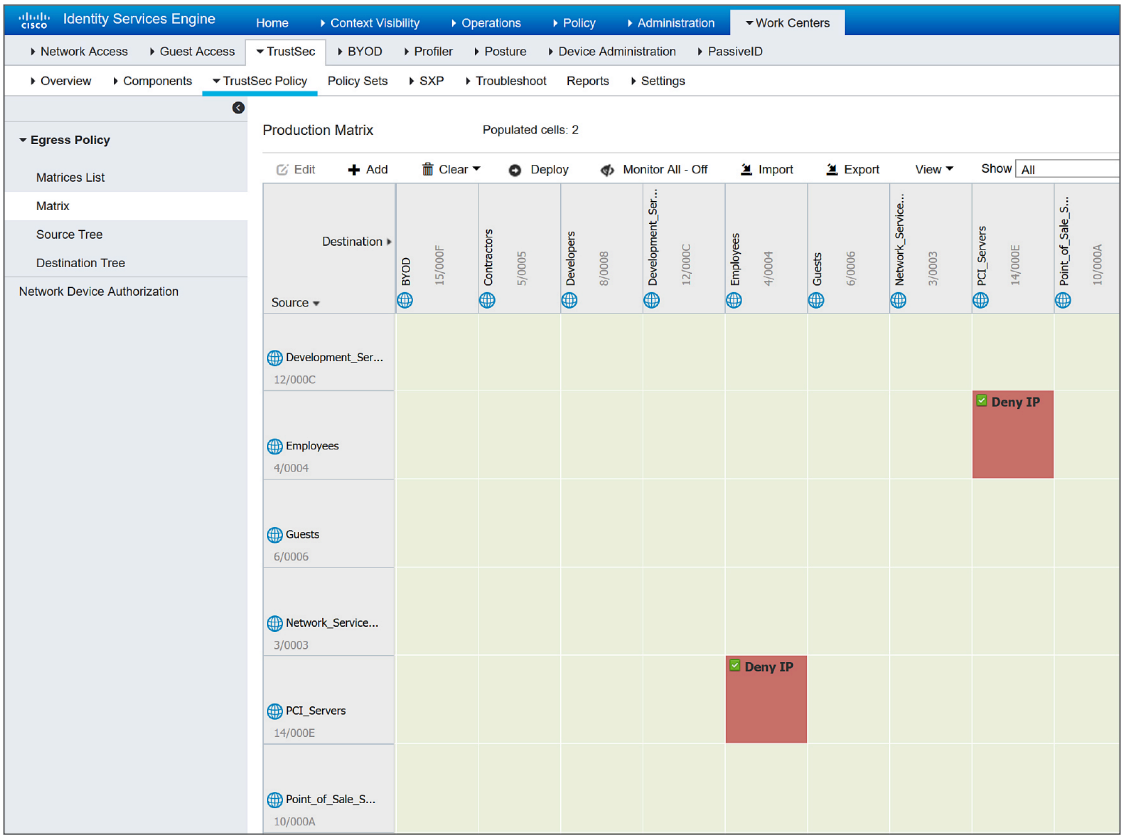
Step 1: From the main Cisco DNA Center dashboard, navigate to **POLICY > Group-Based Access Control > Group-Based Access Control Policies**, click **+ Add Policy**, from the **Available Scalable Groups** pane drag the **Employees** group and drop it into the **Source** pane, drag the **PCI_Servers** 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 **DEPLOYED**. The reverse policy is also created and deployed, as a result of the bidirectional option selection. The policies are now available to be applied to fabrics that are created in Cisco DNA Center and are also available in ISE, viewable using the Cisco TrustSec policy matrix.

Step 2: At the top right, click **Advanced Options**. You are redirected to log in to ISE, which then displays the TrustSec policy matrix. Verify that the policy has been updated to ISE for rendering into the network.

This step is a shortcut to logging in to ISE, navigating to **Work Centers > TrustSec > TrustSec Policy**, and then on the left side, selecting **Matrix**.



Process

Preparing the network for automation

1. Configure underlay network device management using the Cisco IOS XE CLI
2. Configure underlay network links for routed access connectivity
3. Enable routing connectivity at border toward external router neighbor
4. Redistribute shared services subnets into underlay IGP
5. Enable connectivity at external fusion router towards border neighbor
6. Configure MTU on unmanaged intermediate devices
7. Discover and manage network devices
8. Configure underlay switches using LAN Automation
9. Manage software images for devices in inventory
10. Use software image management to update device software

To be able to deploy the network designs and policies created, a functioning network underlay must exist with working management connectivity.

Procedure 1 Configure underlay network device management using the Cisco IOS XE CLI

For maximum resiliency and bandwidth, use a loopback interface on each device and enable Layer 3 connectivity 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 with SNMPv2c for device configuration to the device loopback interfaces.

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.

```
hostname [hostname]
```

Step 2: Configure local login and password.

```
username dna privilege 15 secret [user password]
enable secret [enable password]
service password-encryption
```

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

```
ip ssh version 2
line vty 0 15
  login local
  transport input ssh
  transport preferred none
```

Step 4: Enable Simple Network Management Protocol (SNMP) and configure SNMPv2c with both a read-only and a read-write community string, which match the credentials input into Cisco DNA Center.

```
snmp-server community [SNMP read-only name] ro
snmp-server community [SNMP read-write name] rw
```

Step 5: 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 6: Configure the switch loopback address.

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

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. Most deployments require this procedure.

Do not add a configuration to any devices that you intend to discover and configure using LAN Automation. Devices with existing configurations cannot be configured using the LAN Automation onboarding.

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 device will be provisioned as a fabric border node and the connection is to be used as a handoff from the fabric to the rest of the infrastructure, use the next procedure instead.

```
interface TenGigabitEthernet1/0/1
 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 for many switches
ip routing
router isis
 net 49.0000.0100.0400.0001.00
 domain-password [domain password]
 ispf level-1-2
```

```
 metric-style wide
 nsf ietf
 log-adjacency-changes
 bfd all-interfaces
```

Tech tip

A common convention in IS-IS is to embed the loopback IP address into the unique NET, or system ID. For example, a loopback IP address **10.4.32.1** (**010.004.032.001**) becomes **0100.0403.2001**, and it is appended with **.00** and prepended with an area ID (example: **49.0000**), resulting in NET **49.0000.0100.0403.2001.00**.

Step 3: Enable IS-IS routing on all of the 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 [ip address] [netmask]
 ip router isis
interface range TenGigabitEthernet1/0/1-2 , TenGigabitEthernet2/0/1-2
 no switchport
 dampening
 ip address [ip address] [netmask]
 ip router isis
 logging event link-status
 load-interval 30
 bfd interval 100 min_rx 100 multiplier 3
 no bfd echo
 isis network point-to-point
```

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 a 802.1Q handoff, skip this procedure. Most deployments require this procedure.

To connect border node devices into your network, you establish connectivity across interfaces configured using VRF-lite, which uses 802.1Q VLAN tagging to separate the VRFs. Connect common network services available outside of the border nodes such as DNS, DHCP, and WLCs, and for Cisco DNA Center management when it is not directly connected to the SD-Access network nodes, by extending your existing enterprise network to the underlay at the border. Connectivity to Cisco DNA Center is required for additional provisioning.

The external device handling routing among multiple virtual networks and a global routing instance acts as a ***fusion router*** for those networks, and the separation of connectivity is maintained by using VRFs connected using interfaces with 802.1Q tagging to the border, 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 link augmented with additional tags and BGP sessions as needed for overlay VN connectivity.

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]
 no shutdown
interface FortyGigabitEthernet1/0/24
 switchport
 switchport mode trunk
 switchport trunk allowed vlan add 100
 no shutdown
```

Step 2: For each border node, if you are configuring a device such as an ASR or ISR router that supports 802.1Q VLAN tagging, use an alternative subinterface configuration instead of a switch trunk interface 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]
 no shutdown
```

Step 3: Connect the redundant border nodes together with at least one routed interface for underlay communication and later BGP peering. The configuration for integrating into the IS-IS protocol is shown. Repeat this step for each interface connecting border nodes.

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

Step 4: Enable BGP routing to the fusion router for connectivity to networks external to the fabric, and activate BGP on the connecting interfaces. You use BGP to allow Cisco DNA Center management access to the underlay network devices, while allowing further provisioning for virtual networks on the interfaces and minimizing disruption to network connectivity. Repeat this step for each border node.

```
router bgp [underlay AS number]
 bgp router-id [loopback 0 IP address]
 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
  maximum-paths 2
 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 connect to establish connectivity. 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 by 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 the 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.

The example fusion router is configured with route peering between a VRF containing the enterprise-wide global routes and the global routing table on the border for the fabric underlay reachability, without using the fusion router global routing table.

Alternatively, peer between the fusion router enterprise-wide global routing table and the global routing table on the 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 connection from the external fusion router to the SD-Access 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 requiring trunk port configurations, match the other side that was previously configured.

```
interface TenGigabitEthernet0/1/7
 description to 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 [external 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
  maximum-paths 2
  default-information originate
 exit-address-family
```

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

```
router eigrp LAN
 !
 address-family ipv4 unicast vrf VRF-GLOBAL_ROUTES autonomous-system 100
  topology base
   redistribute bgp [external AS number] metric 1000000 1 255 1 9100 route-map RM-BGP-TO-EIGRP
  exit-af-topology
  network [external IP network address] [netmask]
  eigrp router-id [loopback IP address]
 exit-address-family
```

Procedure 6 Configure MTU on unmanaged 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 that will not be managed by Cisco DNA Center (example: hardware or software support isn't available in Cisco DNA Center), then the devices must still meet the requirements for transporting SD-Access traffic through those transit fabric intermediate nodes. 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 unmanaged 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.

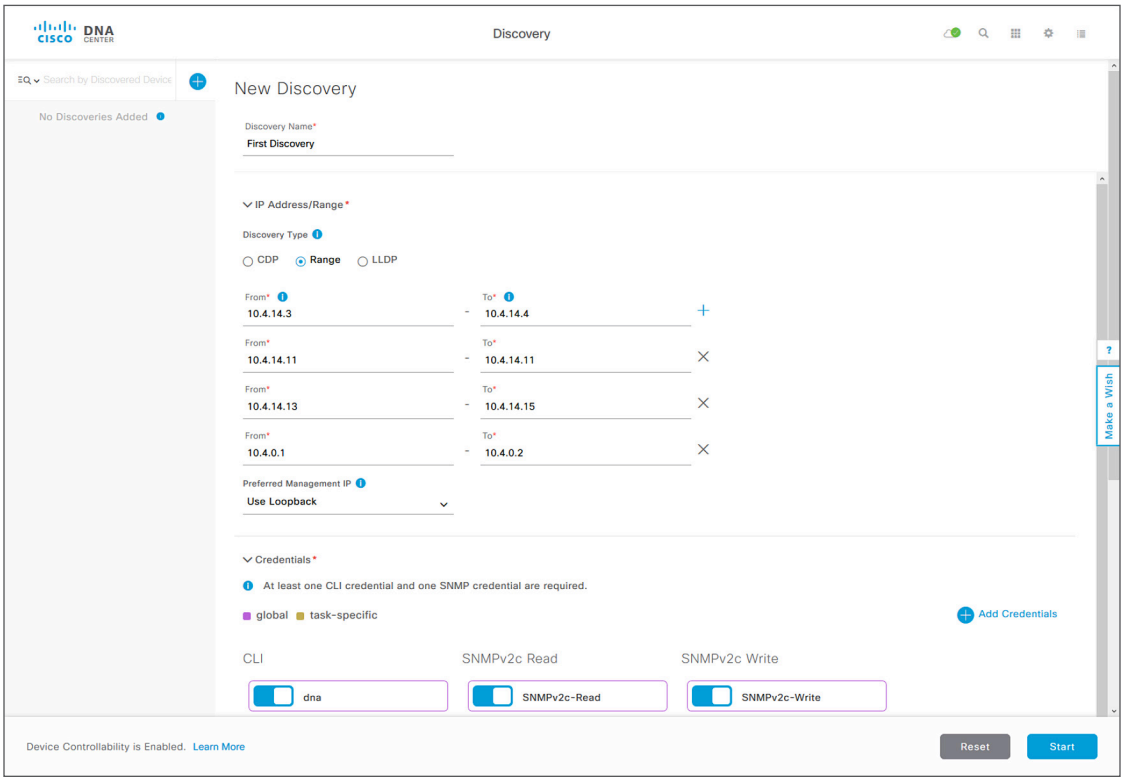
Procedure 7 Discover and manage network devices

You use Cisco DNA Center to discover and manage the SD-Access underlay network devices by enabling IP connectivity to the devices and supplying Cisco DNA Center with the CLI and SNMP 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,

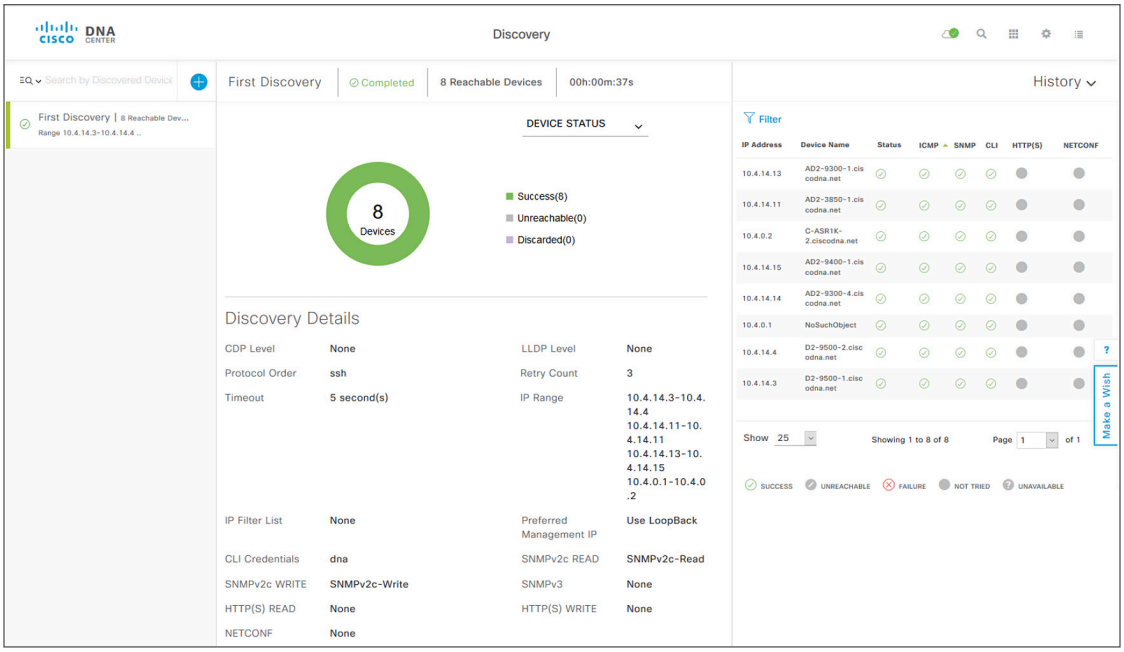
These steps show how to initiate discovery by supplying an IP address range or multiple ranges for scanning network devices, which constrains the discovery and potentially saves time. Alternatively, for the devices not using LAN Automation onboarding, you can supply an initial device for discovery and 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, and at the bottom, within the **Tools** section, click **Discovery** and supply a **Discovery Name**. Click **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, use the drop-down to select **Use Loopback**.

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. Verify the credentials to be used for the discovery, and then at the bottom click **Start**.



The discovery details are displayed while the discovery runs.



Step 3: If there are any discovery failures, inspect the devices list, resolve the problem, and restart the discovery for those devices.

Tech tip

If you are using a Cisco Catalyst 6800 Series switch with a large configuration, you can avoid discovery timeouts by adding the following command in configuration mode:

```
snmp mib flash cache
```

Step 4: After the discovery process finishes successfully, 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, the devices show a status **of Managed**.

Device Name	IP Address	Reachability Status	Uptime	Last Updated	Resync Interval	Last Sync Status	Site
AD2-3850-1.ciscodna.net	10.4.14.11	Reachable	127 days 4 hrs 34 mins	3 minutes ago	00:25:00	Managed	Unassigned
AD2-9300-1.ciscodna.net	10.4.14.13	Reachable	127 days 5 hrs 04 mins	a minute ago	00:25:00	Managed	Unassigned
AD2-9300-4.ciscodna.net	10.4.14.14	Reachable	127 days 4 hrs 00 mins	2 minutes ago	00:25:00	Managed	Unassigned
AD2-9400-1.ciscodna.net	10.4.14.15	Reachable	127 days 3 hrs 51 mins	a minute ago	00:25:00	Managed	Unassigned
C-ASR1K-1.ciscodna.net	10.4.0.1	Reachable	127 days 3 hrs 38 mins	4 minutes ago	00:25:00	Managed	Unassigned
C-ASR1K-2.ciscodna.net	10.4.0.2	Reachable	127 days 3 hrs 39 mins	4 minutes ago	00:25:00	Managed	Unassigned
D2-9500-1.ciscodna.net	10.4.14.3	Reachable	23 days 5 hrs 34 mins	3 minutes ago	00:25:00	Managed	Unassigned
D2-9500-2.ciscodna.net	10.4.14.4	Reachable	127 days 4 hrs 59 mins	3 minutes ago	00:25:00	Managed	Unassigned

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

Tech tip

At the right side of the title row for the Inventory table, you can temporarily adjust which columns are displayed. Adding the **Device Role** column enables the ability 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 8 Configure underlay switches using LAN Automation

Optional

Use this procedure if you are deploying LAN switches without existing configurations into the underlay by using Cisco DNA Center's LAN Automation capabilities. The device CLI and SNMP credentials to be pushed by PnP, the network-reachable IP address pool used for connectivity, and the seed devices (typically border switches) have been configured as part of previous procedures. Each seed device is expected to 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 (validated switches are listed in the appendix). Discovered switches are directly connected to chosen seed device interfaces (OOB management ports are not supported) 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 all of 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 and should be in install mode (not bundle mode). 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
```

Step 1: Verify that the seed devices are in the inventory, managed by Cisco DNA Center, and assigned to a site.

Step 2: If you are using a Catalyst 6800 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

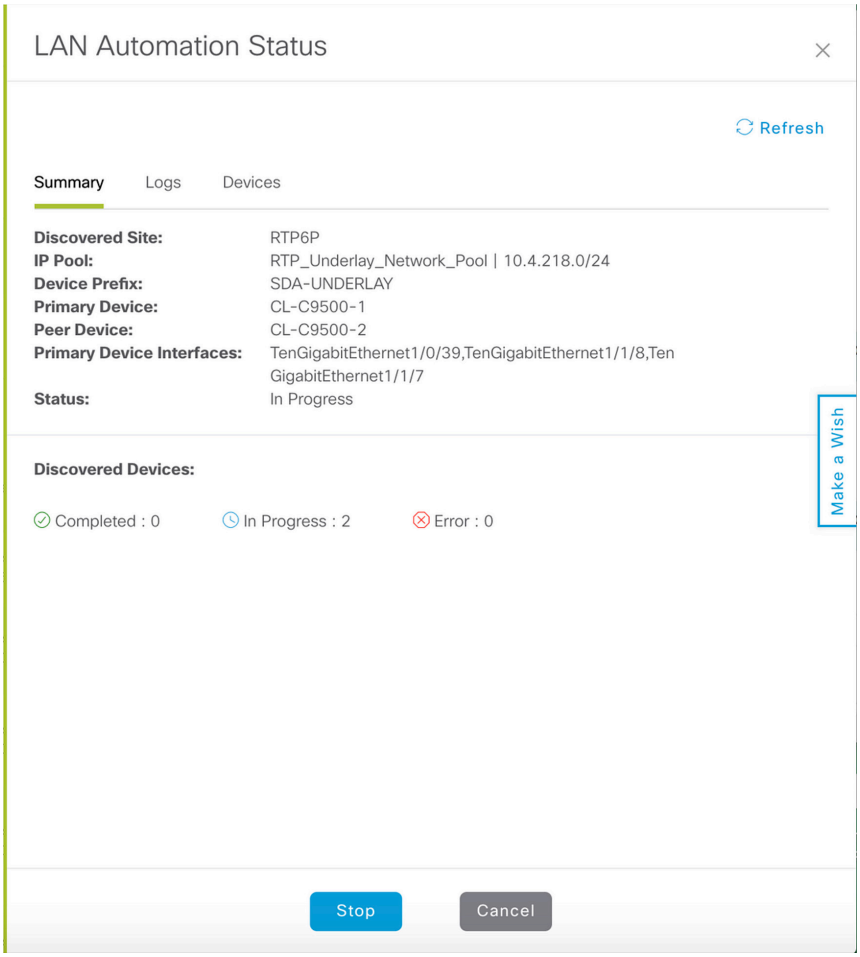
The IP pool used for LAN Automation should be sized significantly larger than the number of devices to be discovered. The pool is divided in half, with one half used for VLAN 1 DHCP services provided by the seed devices. The second half of the pool is divided in half again, leaving a quarter of the total address space for point-to-point link addressing, and a quarter for loopback addressing. Endpoints should not be plugged into the switches, as they can exhaust the IP pool DHCP uses for PnP provisioning.

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. If your Cisco DNA Center uses the optional dedicated management network for web access port instead of a single port with a default route, then 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.

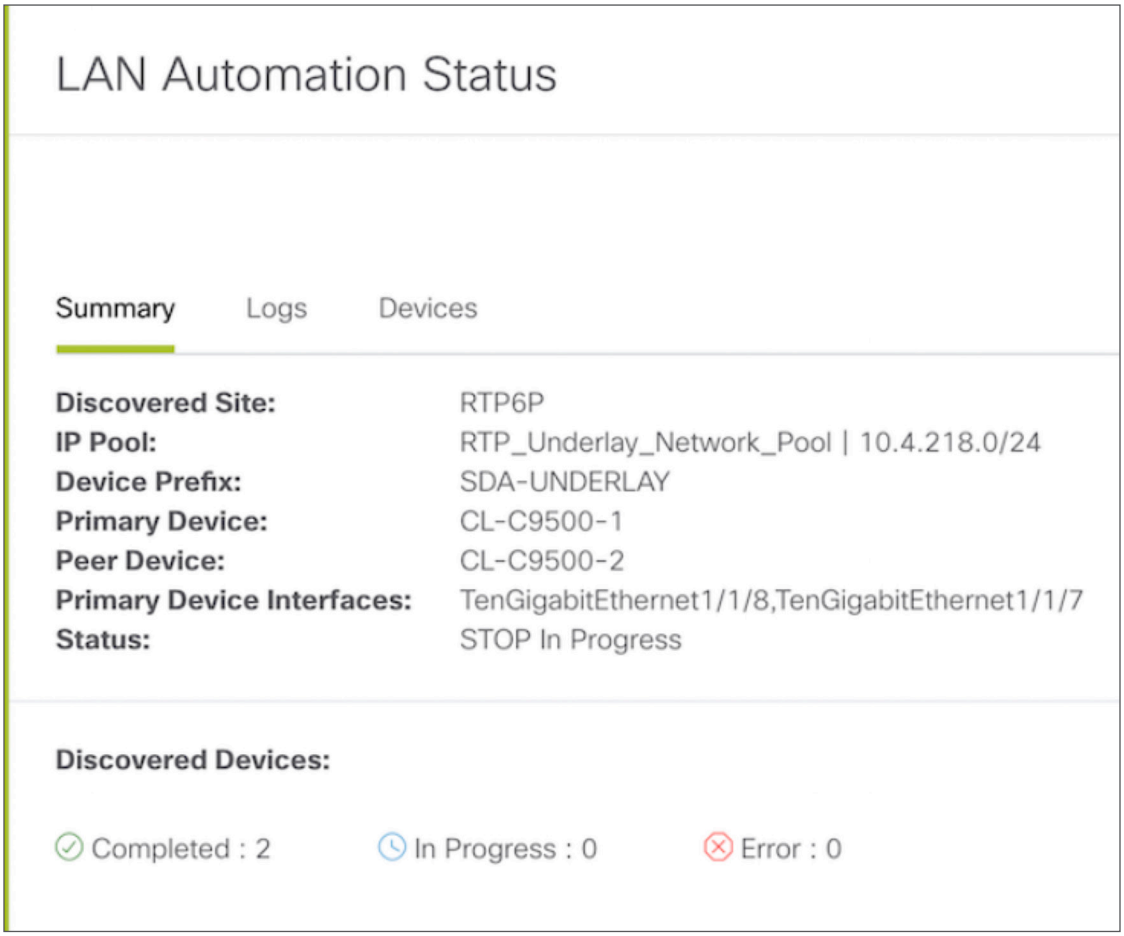
Step 3: Navigate to **PROVISION > Devices > Inventory**. At the top, click the **LAN Automation** drop-down, click **LAN Automation**, on the right in the LAN Automation slide-out, fill in all of the parameters for the supported seed device. Select the interfaces connected to the devices to be discovered, and then click **Start**.



Step 4: 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 PnP process will leave the discovery in a state needing manual intervention for recovery. Discovering devices an additional hop away from the seed can take significantly more time to reach completion.

Step 5: 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, then under **Tools** select **Inventory**, for each seed device switch, at the top, in the **Actions** pull-down, select **Resync**. Wait for the devices to change to managed state, and then proceed to the next step.

Step 6: 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 routed network, and devices are managed in the inventory.

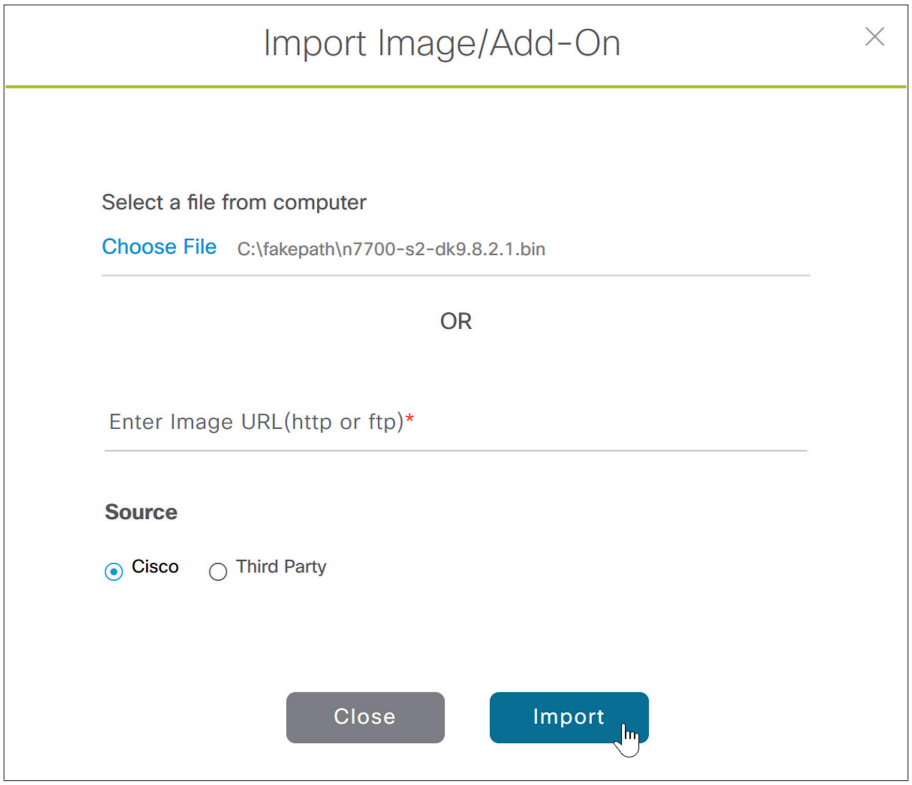


Procedure 9 Manage software images for devices in inventory

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 recommended images by searching Cisco.com for SD-Access Hardware and Software Compatibility Matrix. The images used for validation are listed in Appendix A: Product list.

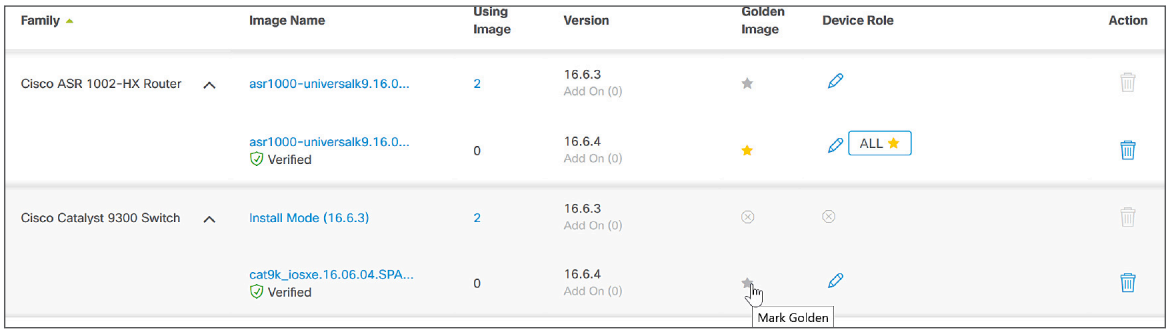
Use the following steps to apply software updates of images and software maintenance updates (SMUs) to the devices, by importing the required images, marking images as golden, and applying images to devices.

Step 1: Navigate to the main Cisco DNA Center dashboard, click **Design**, click **Image Repository**, 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. Repeat this step for all images that you wish to deploy using Cisco DNA Center. Images to be used for device families not yet available in Cisco DNA Center will be listed under the **Unassigned** category. You can verify an import is in the image repository ready to deploy by clicking **Show Tasks** until the image import task is listed as green with a checkmark next to it.

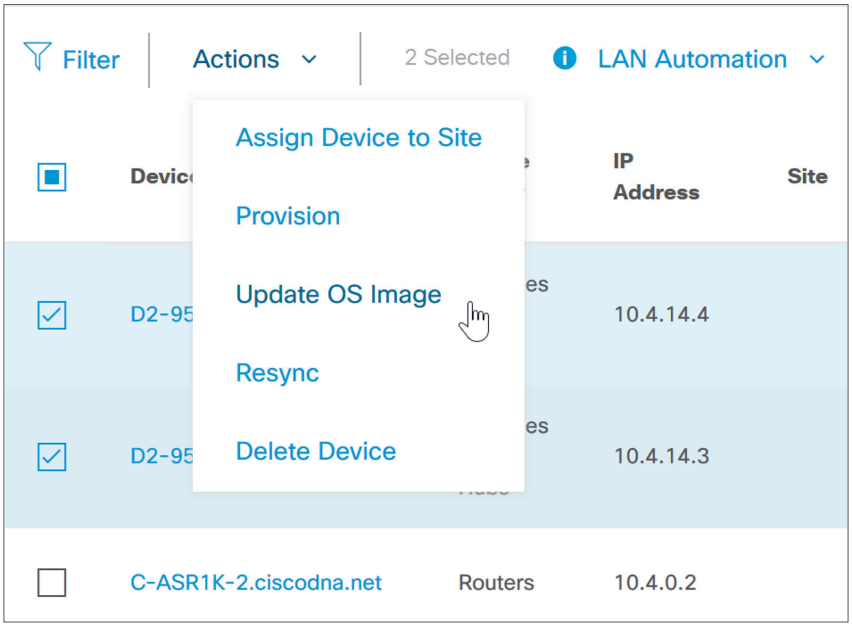
Step 2: After the image is successfully imported, use the **Refresh** button to update available device families that have the imported image available, under the **Image Name** column click the down arrow next to the image listed for a device family, and then click the star for **Golden Image** to mark the appropriate image as the preferred one for the platform. Repeat the importing and tagging images as golden until all devices are marked for an appropriate image.



Procedure 10 Use software image management to update device software

Cisco DNA Center runs a compliance check of devices in inventory compared to images marked 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. When you update device software, the software image copy and upgrade happen in a single step.

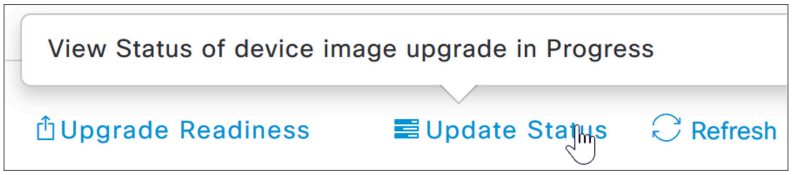
Step 1: Navigate to **PROVISION > Devices > Inventory**, select all devices marked **Outdated** that do not have a connectivity dependency among the selection (to avoid losing connectivity during upgrade while devices reboot), and then in the **Actions** menu, select **Update OS Image**.



Step 2: Confirm the selection of devices 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 devices, and then the devices reboot to activate the new images immediately after the image distribution is complete. Use the **Refresh** button to see when the **In Progress** status is removed.

Step 3: If a device upgrade fails and the **OS Image** status returns to **Outdated**, at the top right of the Device Inventory page click **Update Status** to find the reason the upgrade was unsuccessful.



Address any failures, based on the task status messages displayed.

Step 4: Repeat this procedure as needed to update the device software to the required versions for the network deployment.

Process

Provisioning the SD-Access underlay network

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

After devices have management connectivity with Cisco DNA Center and are running the appropriate software versions for SD-Access, use Cisco DNA Center to provision the devices with their roles as part of an SD-Access network

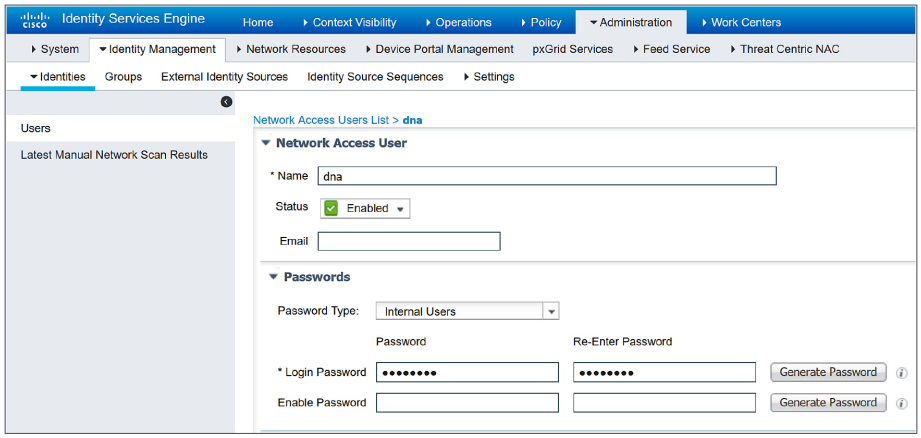
Procedure 1 Provision devices and assign to sites to prepare for SD-Access

Provision the network devices, and then assign the devices to a site for integration into an SD-Access network. Update the ISE configuration with credentials to support the provisioning as part of this procedure.

Tech tip

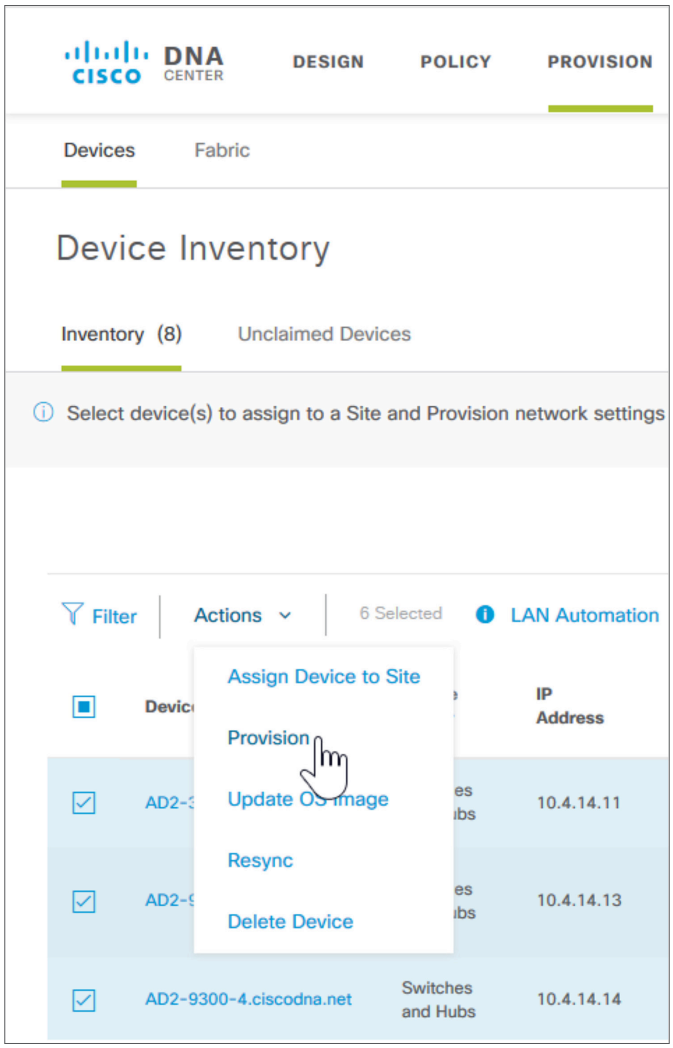
When devices are provisioned, the devices receive a number of configurations appropriate for the assigned site, including the centralized AAA server configuration using ISE, which is preferred over local login credentials. To maintain the ability to manage the devices after provisioning, the credentials you use for provisioning must be available from the ISE server, either directly or as the means to an external identity source such as Active Directory.

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, in addition to the same user ID stored on each device.

Step 2: In Cisco DNA Center, navigate to **PROVISION > Devices > Inventory**, select the devices to provision into an SD-Access network, click **Actions**, and then click **Provision**.

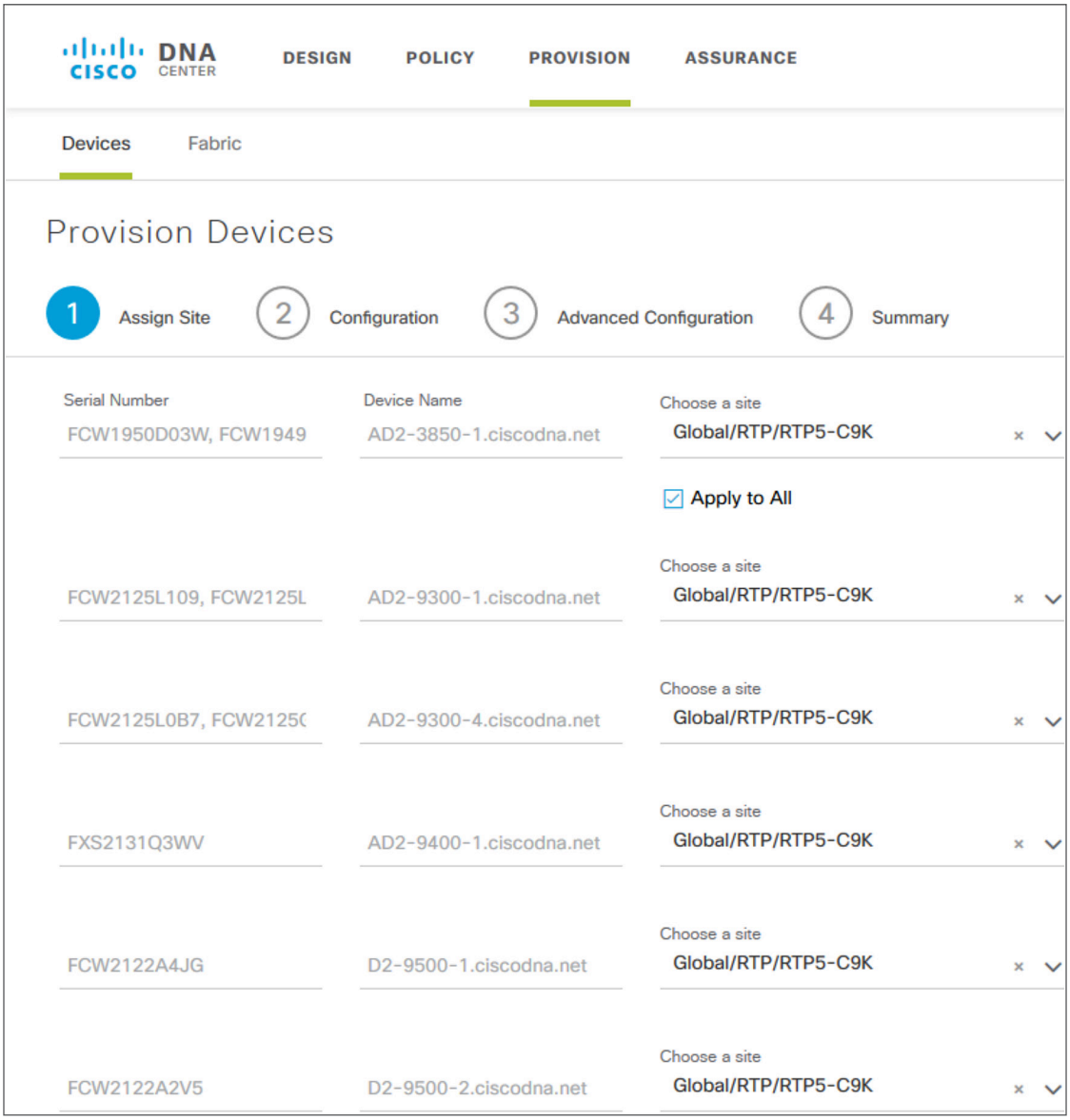


A **Provision Devices** wizard screen appears.

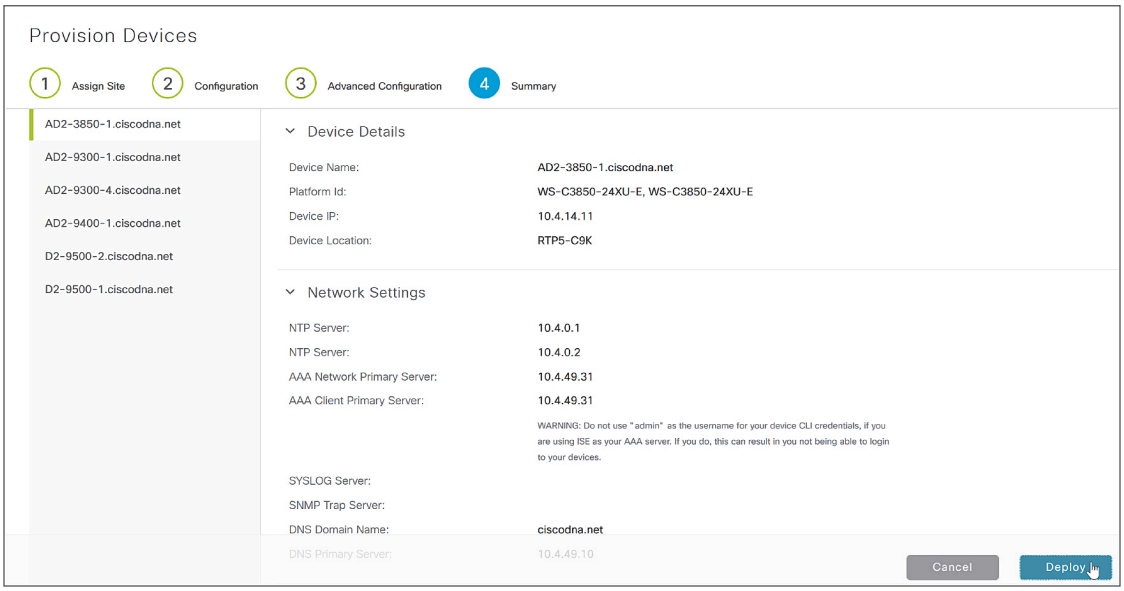
Tech tip

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

Step 3: Within the first wizard screen, select the site assignments for the devices, and then at the bottom of the screen click **Next**.



Step 4: Use **Next** to skip the **Configuration** and **Advanced Configuration** screens, in the **Summary** screen review the details for each device, and then click **Deploy**.

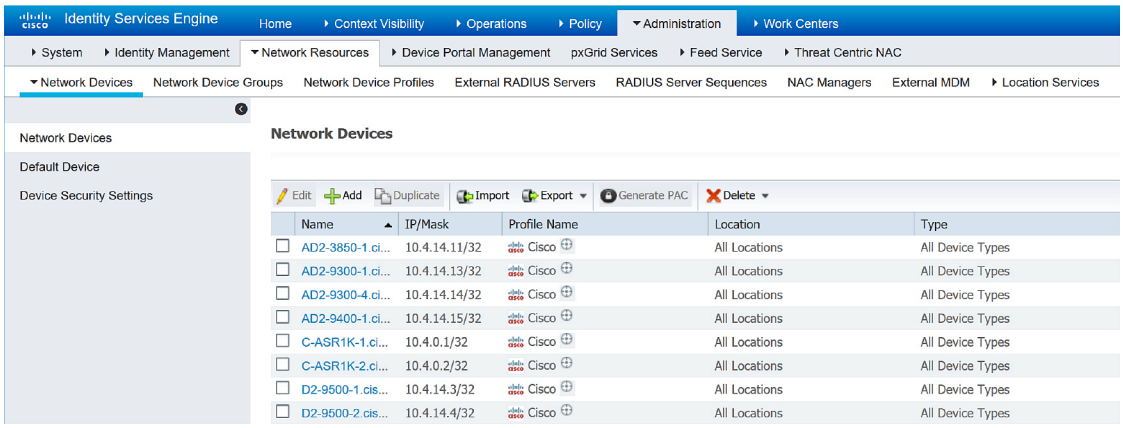


Step 5: At the popup screen, leave the default selection of **Now**, and click **Apply**.

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 final status.

Step 6: Repeat the Cisco DNA Center provisioning steps for each batch of devices being added. As a result of the Cisco DNA Center pxGrid integration with ISE, the network devices also appear in ISE.

Step 7: Verify the ISE integration function by logging in to ISE and navigating to **Administration > Network Resources > Network Devices**. The provisioned devices appear.



Process

Provisioning an SD-Access overlay network

1. Create an IP-based transit site
2. Create a fabric domain and add sites
3. Create a fabric overlay
4. Enable eBGP connectivity for VN at neighbor (fusion) to border router
5. Assign wired clients to VN and enable connectivity
6. Enable fabric edge ports for client onboarding
7. Enable multicast for fabric

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 1.2 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 either an external network (IP-based transit) or to one or more fabric sites (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.

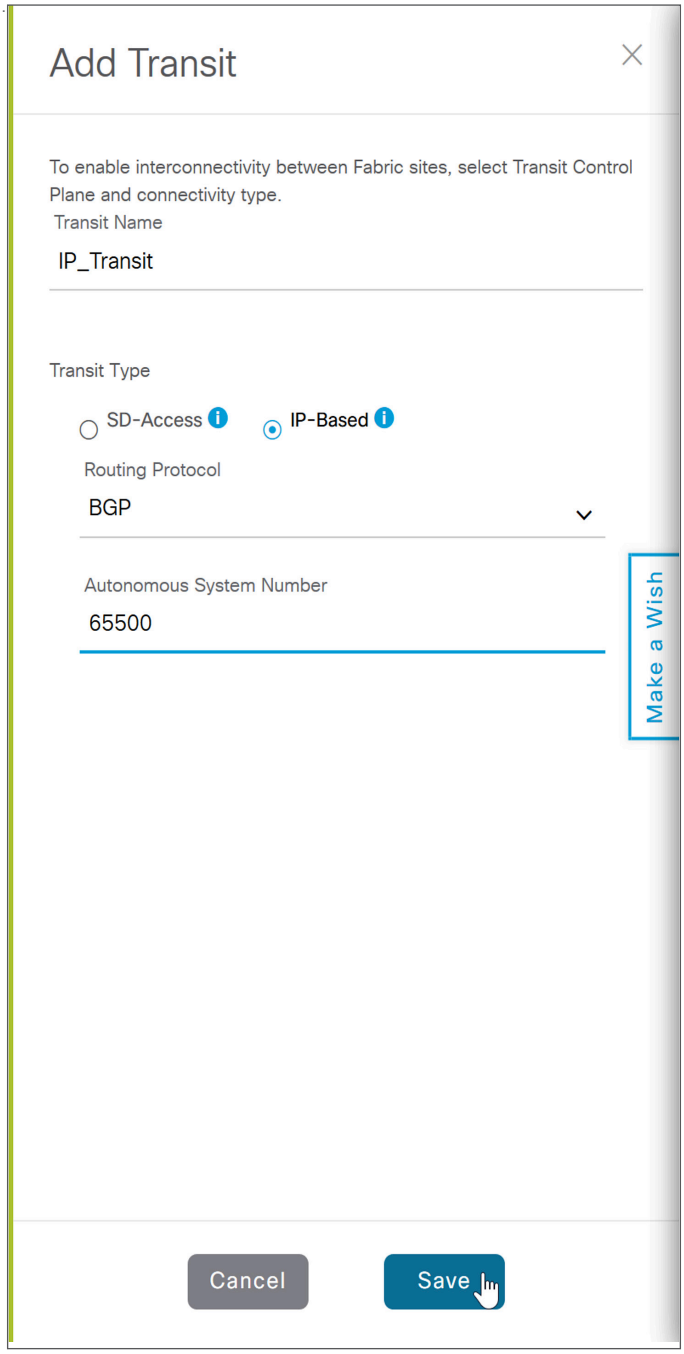
Tech tip

Cisco DNA Center software and Cisco IOS software listed in the appendix does not include validation of SD-Access transit. 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

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.

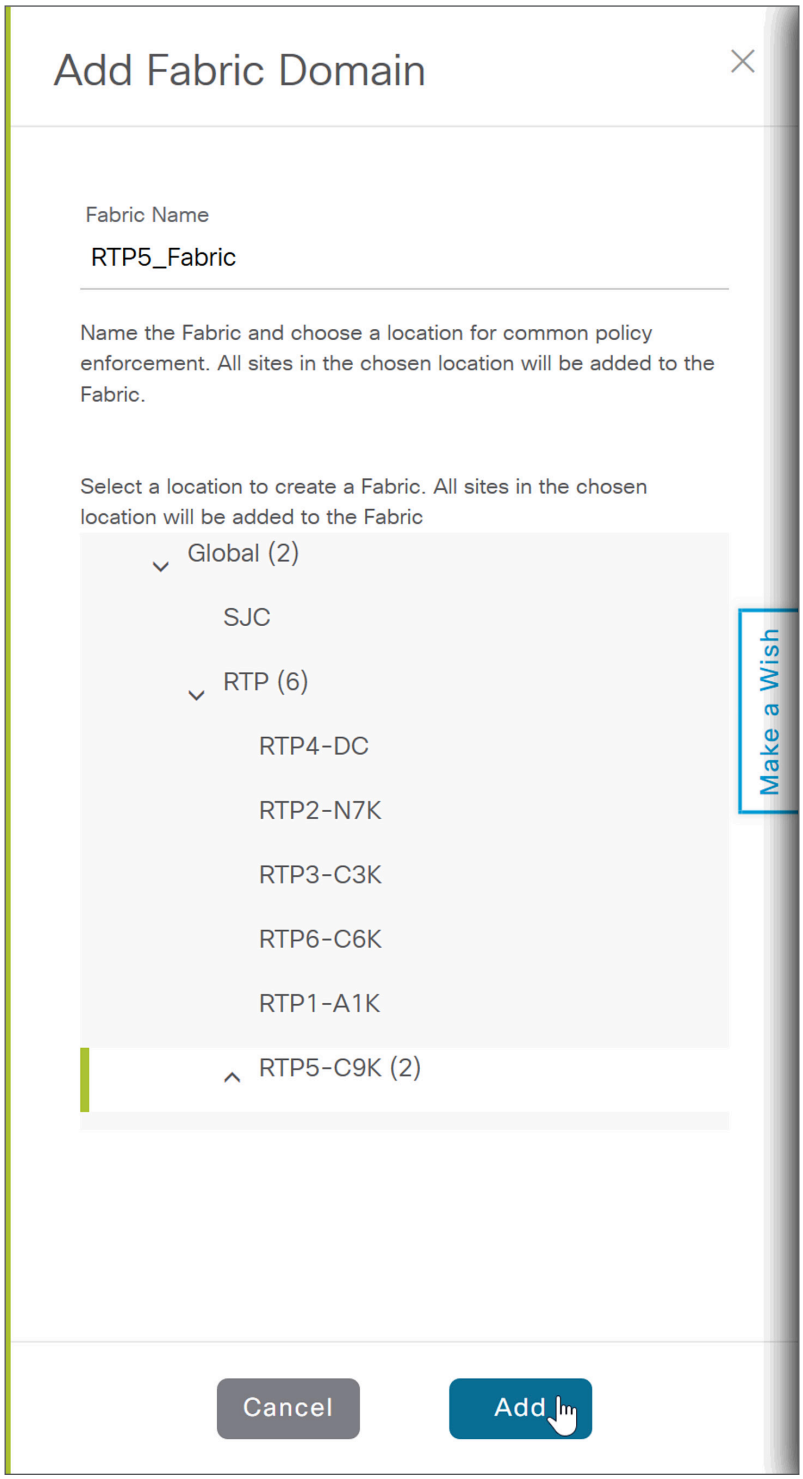
Step 1: Using Cisco DNA Center, navigate to **PROVISION > Fabric**, at the top right click **+ Add Fabric Domain or Transit**, click **Add Transit**, in the slide-out supply a **Transit Name** (example: IP_Transit), select **IP-Based**,
for **Routing Protocol** select **BGP**, enter an **Autonomous System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



A status message appears, and the transit is created.

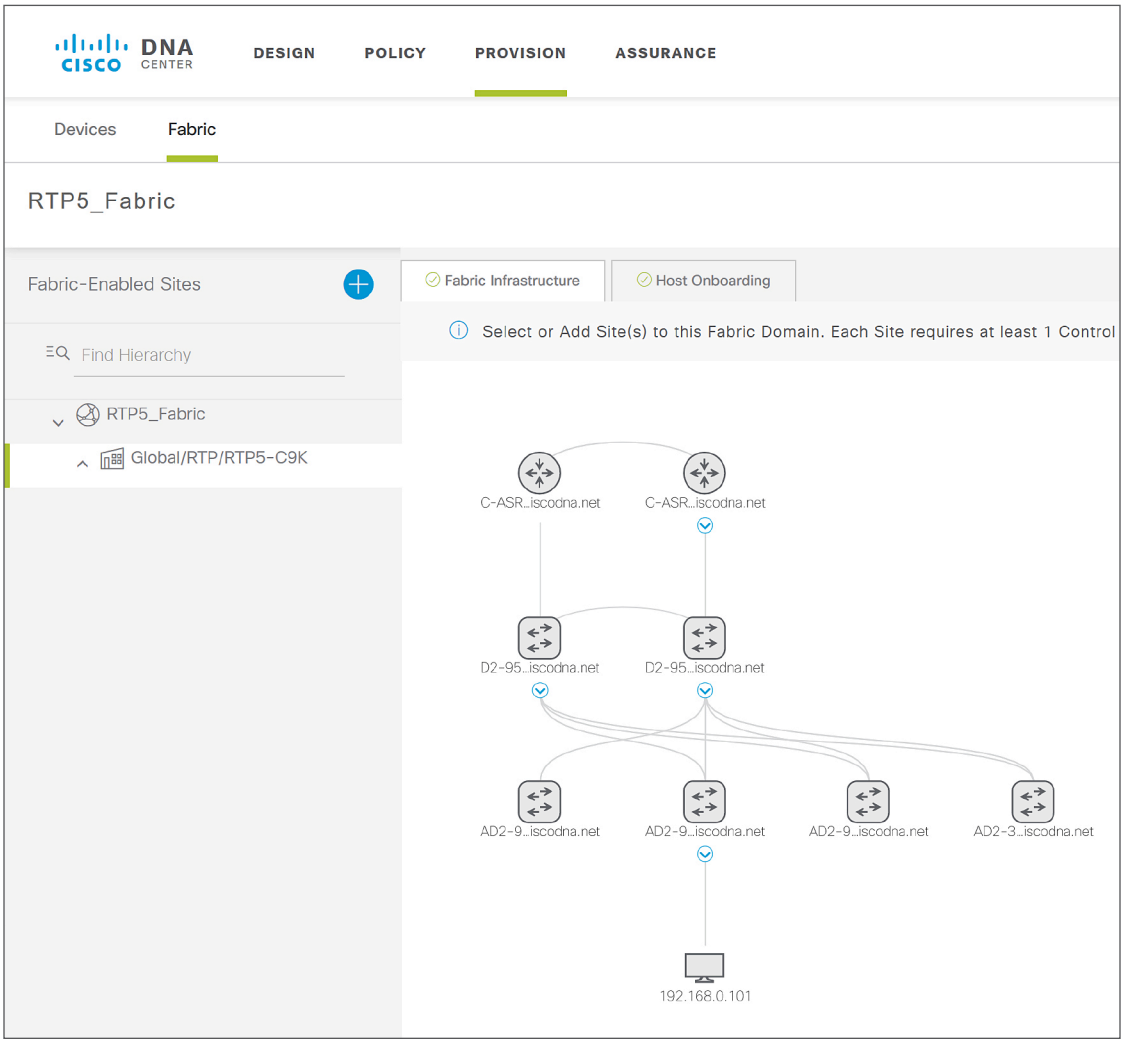
Procedure 2 Create a fabric domain and add sites

Step 1: Using Cisco DNA Center, navigate to **PROVISION > Fabric**, at the top right click **+ Add Fabric Domain 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**.



The new campus fabric domain is created.

Step 2: 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: Global/RTP/RTP5-C9K). A view of the fabric and related sites is displayed.



Step 3: 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.

Procedure 3 Create a fabric overlay

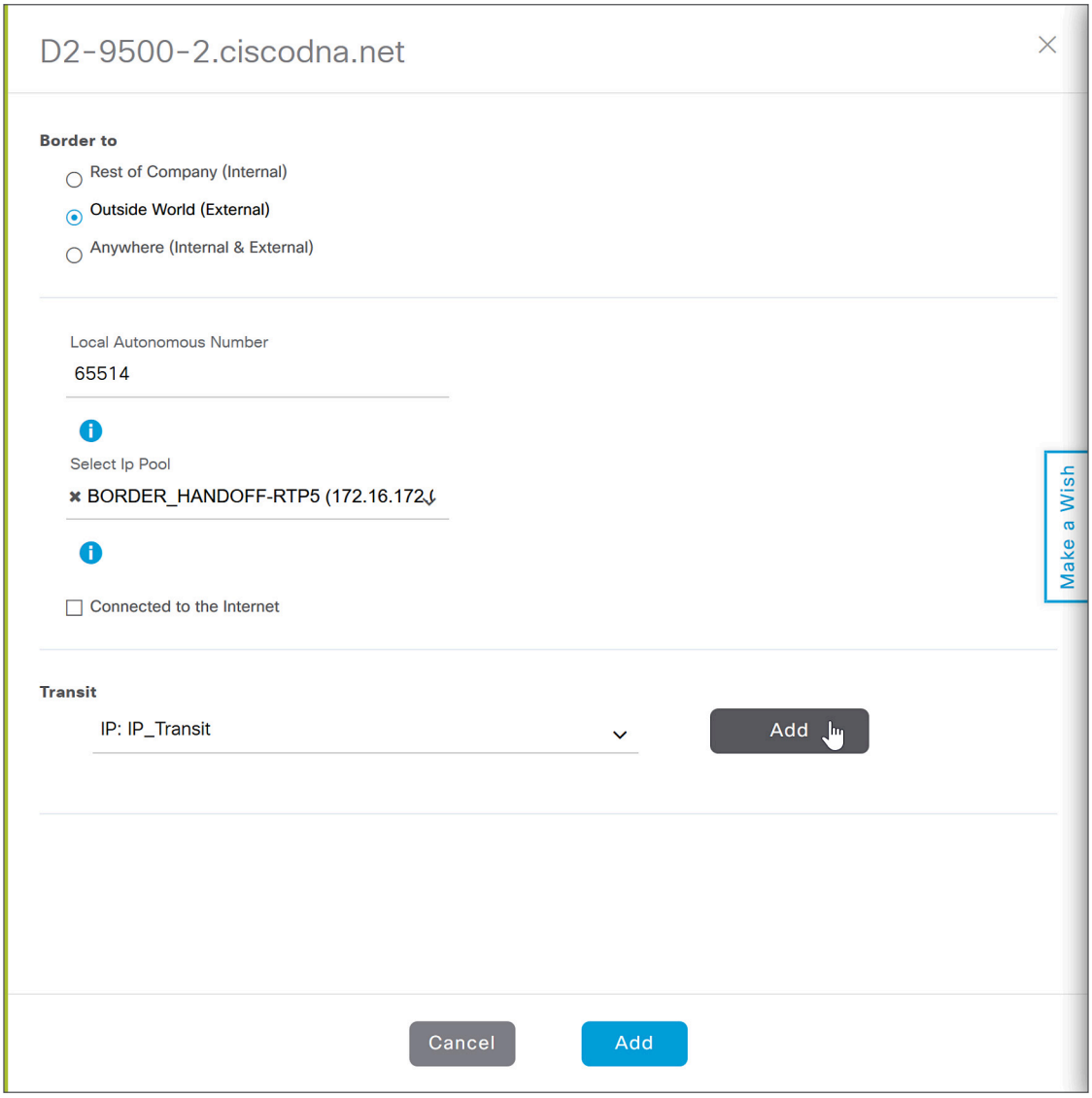
Step 1: In the fabric domain topology view, hold the Shift key, click all of the nodes that are fabric edge nodes, and then in the popup box, click **Add to Fabric**.

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. Additionally, enable the MPLS license and configure MPLS LDP on the physical links to the control plane nodes to support the control plane connectivity.

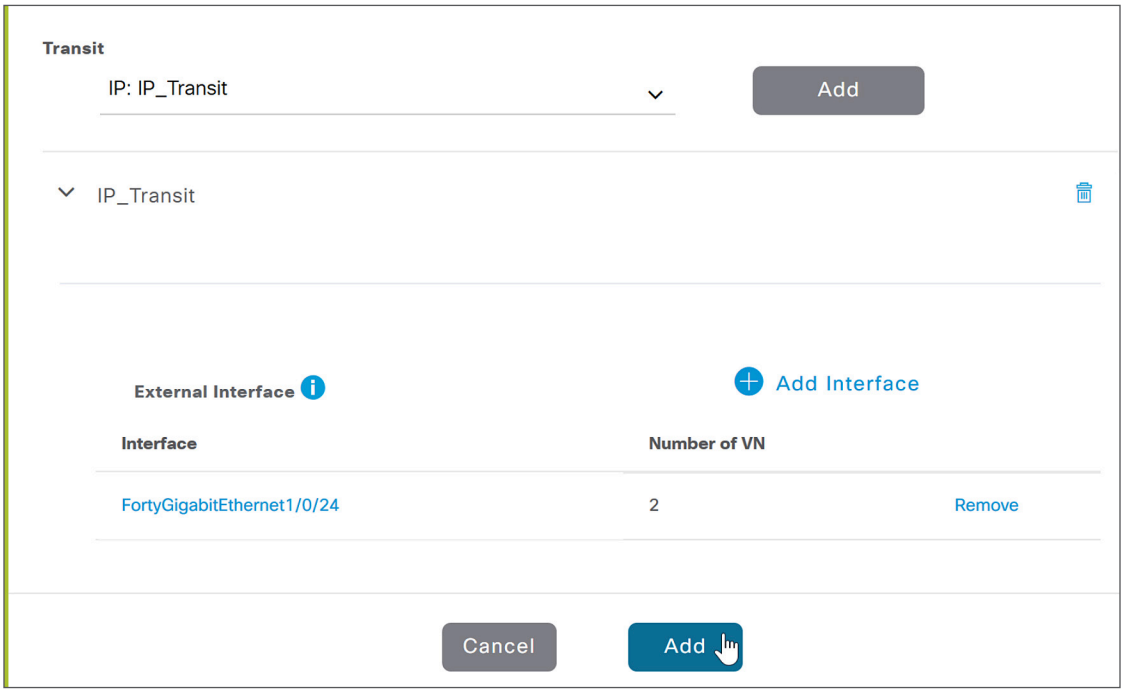
Step 3: Click a device to perform the fabric border role, in the popup box click either **Add as Border** or **Add as CP+Border** (if skipping the previous step), fill in the additional dialog for the type of border (example: Outside World (External)), supply the BGP **Local AS Number** (example: 65514), under **Border Handoff > Layer 3** use the **Select Ip Pool** drop-down to select the global pool configured previously for border connectivity functionality, leave **Connected to the Internet** unchecked, in the **Transit** menu select the transit (example: IP_Transit), and then next to the transit click the gray **Add** button.



Tech tip

If the border is the only path to exit 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, 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, select **Virtual Network** and select all VNs to include in the Layer 3 handoff outside the fabric, click **Save**, and then click **Add**.

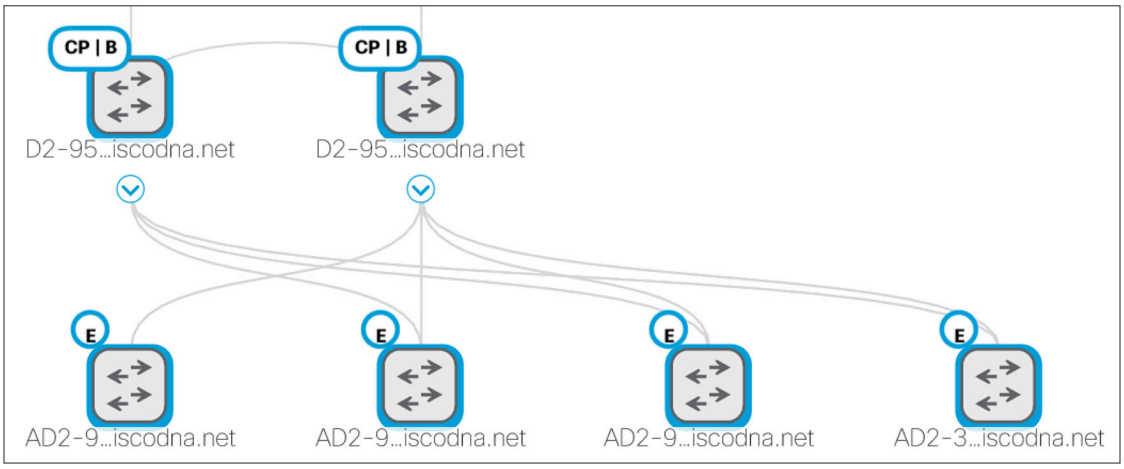


Step 5: If you have an additional fabric border node, repeat the previous two steps for it.

Tech tip

To configure a VRF-Lite handoff interface from the border to the rest of the network requires an 802.1Q-tagged interface. If you are managing the border using in-band connectivity over the redundant links to be converted, you first make the connection over a tagged interface, as described in the processes to setup management to a border device for network discovery. When using the version of SD-Access validated in this guide, provisioning is unsuccessful if the interface already includes a non-tagged configuration.

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 4 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 validated, you manually configure the external network peers of the border devices with the compatible VRF-Lite and BGP peering information.

Step 1: Log in to border devices and use the CLI to observe the automated configurations created by the SD-Access Cisco DNA Center application for IP connectivity outside of the border. 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 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, configure VRFs as required by virtual networks created on the border. 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
```

Repeat this step for each virtual network context, consistent with the border node configuration.

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

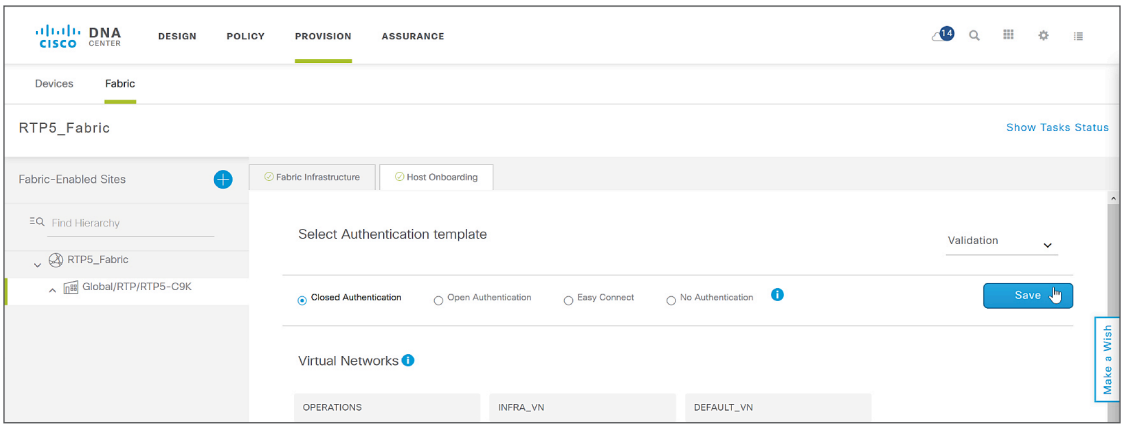
```
interface [Peer interface]
```

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 IP Address] remote-as [Fabric BGP AS]
 !repeat for any additional neighbors
 !
 address-family ipv4
  network [Loopback IP Address] mask 255.255.255.255
  neighbor [Border 1 IP Address] activate
  neighbor [Border 2 IP Address] activate
  maximum-paths 2
 exit-address-family
```

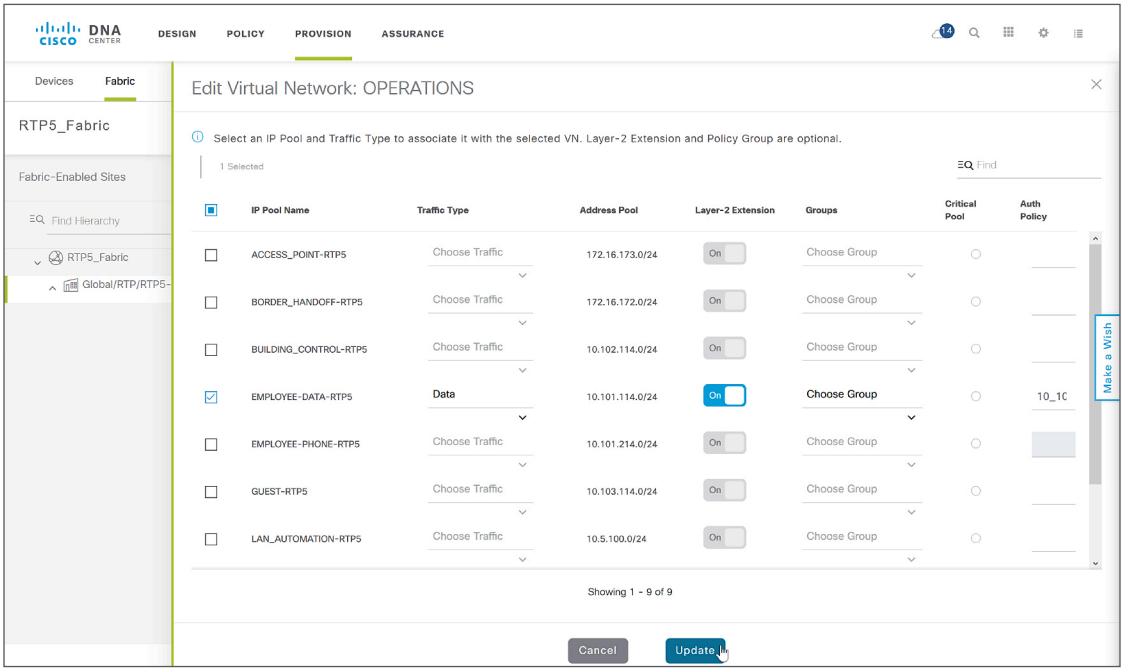
Procedure 5 Assign wired clients to VN and enable connectivity

Step 1: From the Cisco DNA Center dashboard, navigate to **PROVISION > Fabric**, under **Fabric Domains** click the created fabric site (example: RTP5_Fabric), 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 the ports; this setting can be overridden for other purposes.

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-RTP5), select a **Traffic Type** of **Data**, verify that **Layer 2 Extension** is **On**, and then click **Update**.



Step 3: At the **Modify Authentication Template** slide-out, keep the default **Now** selection, and then click **Apply**.

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

Procedure 6 Enable fabric edge ports for client onboarding

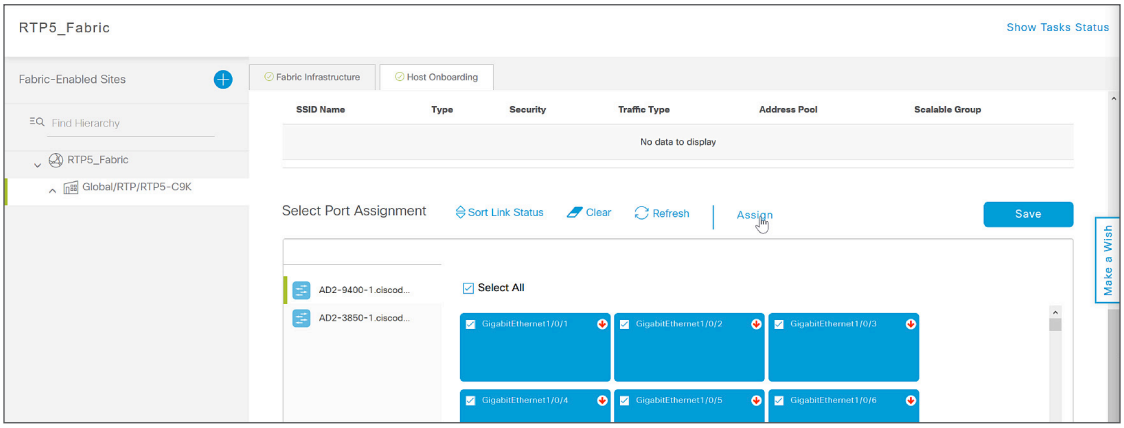
Optional

Overwrite the default authentication template (closed authentication) assigned in the previous procedure, when you have devices connected that do not support 802.1x such as APs, 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.

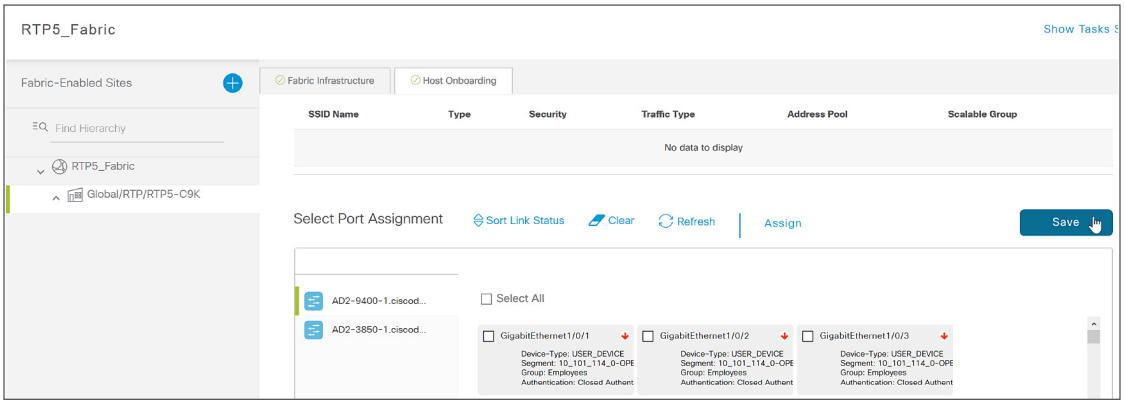
Step 1: Navigate to **PROVISION > Fabric**, under **Fabric Domains** click the created fabric site (example: RTP5_Fabric), click the **Host Onboarding** tab, and under the **Select Port Assignment** section, in the left column, select a switch.

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: 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**.

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.

Tech tip

The group assignment is used to statically assign a group if the fabric edge port does not receive its assignment dynamically using an authentication server, which is useful for some types of devices used in an organization. If "No Authentication" is selected as an authentication method, Cisco DNA Center pushes the global default authentication template chosen in the "Select Authentication template" section at the top of the screen. Cisco DNA Center pushes a port configuration when you choose "Closed Authentication", and also when you choose "Open Authentication".

Procedure 7 Enable multicast for fabric

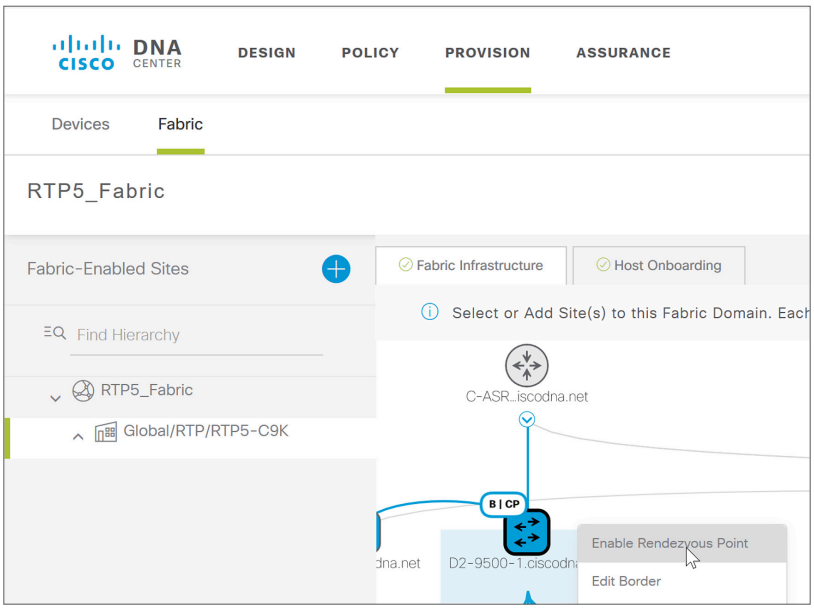
Optional

Use this procedure to configure 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 fabric or outside of the fabric, and Rendezvous Point configuration is available only at the 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 **Fabric Domains** click the created fabric site (example: RTP5_Fabric), in the **Fabric-Enabled Sites** navigation click the specific site (example: Global/RTP/RTP5-C9K), 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-RTP5), click **Next**, 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 pushes 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 device.

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
```

Process

Integrating wireless into SD-Access

1. Add the wireless controllers into inventory and create an HA SSO pair
2. Create IP address pools for access points
3. Design fabric enterprise wireless SSIDs
4. Design a fabric guest wireless SSID
5. Provision the WLC for SD-Access Wireless fabric integration
6. Enable onboarding of access points into the wireless fabric
7. Assign wireless clients to VN and enable connectivity

The process to install wireless LAN controllers for SD-Access is completed as part of previous procedures and the controllers are available to integrate into the fabric using Cisco DNA Center.

Procedure 1 Add the wireless controllers into inventory and create an HA SSO pair

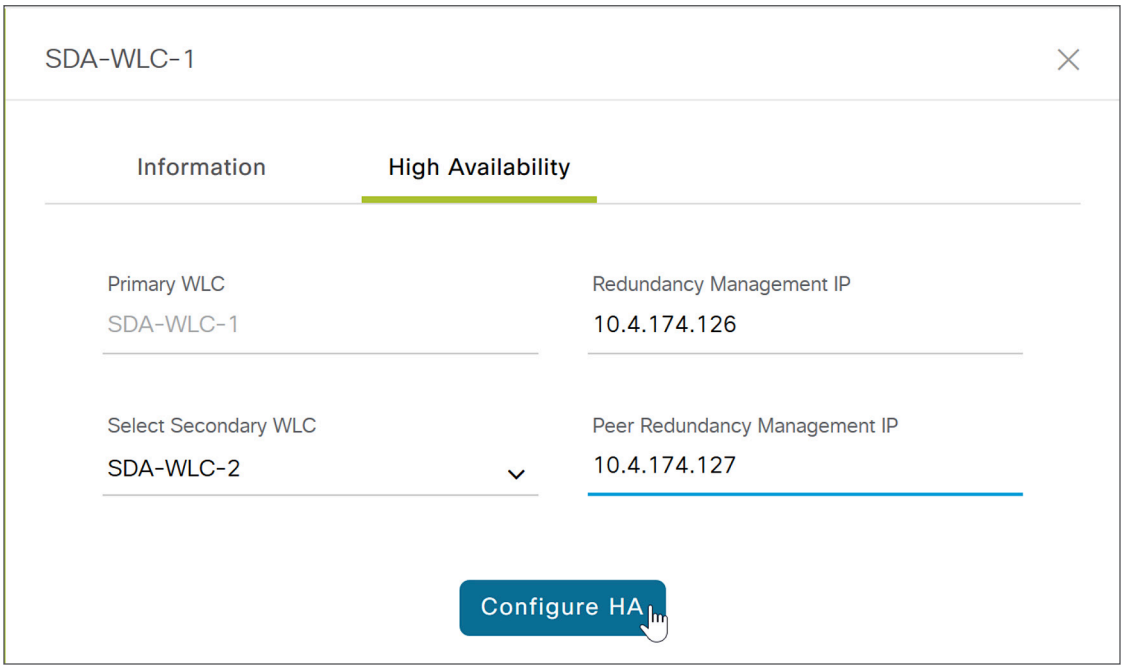
If the wireless LAN controllers are not in the Cisco DNA Center inventory, you must add them before the wireless integration, and create an HA SSO pair.

Step 1: Navigate to the main Cisco DNA Center dashboard, under the **Tools** section click **Discovery**, fill out a **Discovery Name**, click **Range**, in both the start and end IP loopback address for **IP Ranges** enter the IP address of the WLC (example: 10.4.174.26), click **+** (plus sign) to include the range, add a range for the second WLC (example: 10.4.174.27) , click **+** (plus sign) to include the additional range, leave the default **Preferred Management IP** of **None**, if you have unique credentials for the device click **+ Add Credentials** add each new credential (examples: public/private SNMP communities and admin user) and save them, and then click **Start**.

The inventory discovery starts. When it is complete the device count increments and **Complete** is displayed.

Step 2: Navigate to the main Cisco DNA Center dashboard under the **Tools** section click **Inventory**, and find the added WLCs. Before proceeding, use the **Refresh** button to update the **Last Inventory Collection Status** until it is in **Managed** status.

Step 3: 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**, select 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), and then click **Con igure HA**.



Warning messages display.

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

```
Configuring HA for Secondary...
```

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

Step 4: Go to the main Cisco DNA Center dashboard, navigate to **DESIGN > Image Repository**. If the WLC image is the correct version, then mark the image golden. If the image needs to be updated, 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 5: Navigate to **PROVISION > Devices > Inventory**, select the WLC marked **Outdated**, and then in the **Actions** menu, select **Update OS Image**.

Step 6: 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**.

Step 7: 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.

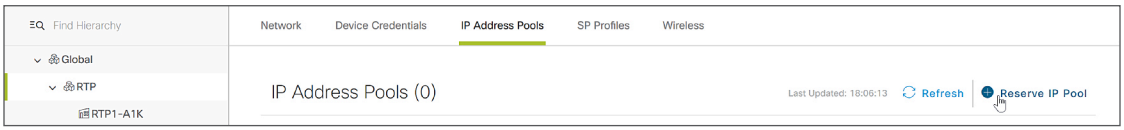
Procedure 2 Create IP address pools for access points

Verify that a global pool in Cisco DNA Center is available for address assignment for the APs to be managed by the network.

Step 1: Navigate to **DESIGN > Network Settings > IP Address Pools**. In the site hierarchy on the left, select **Global**, and inspect the list of IP address Pools for a pool dedicated to the AP infrastructure (example: ACCESS_POINT).

Step 2: If a pool for the APs does not exist, click **+ Add IP Pool**, fill in the IP Pool Name, IP Subnet, CIDR Prefix, and Gateway IP address (examples: ACCESS_POINT, 172.16.173.0, /24, 172.16.173.1), select the **DHCP Server** and **DNS Server**, and then click **Save**.

Step 3: 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: RTP5-C9K), and then in the top right click **Reserve IP Pool**.



Step 4: Fill in the **IP Pool Name** (example: ACCESS_POINT-RTP5), under **Type** select **LAN**, select the **Global IP Pool** source for the reservation, under **CIDR Notation/No. of IP Addresses** select the portion of the address space to use, assign a **Gateway IP Address**, **DHCP Server(s)**, and **DNS Servers(s)**, and then click **Reserve**.

Procedure 3 Design fabric enterprise wireless SSIDs

Step 1: From the main Cisco DNA Center dashboard, navigate to **DESIGN > Network Settings> Wireless**, in the **Enterprise Wireless** section click **+ Add**, in the **Create an Enterprise Wireless Network** wizard, and 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 **WPA2 Enterprise**
- Under **ADVANCED SECURITY OPTIONS** select **Adaptive**

Step 2: 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 will broadcast (example: Global/RTP/RTP5-C9K), and include floors to include in SSID coverage (example: Global/RTP/RTP5-C9K/Floor 1)

Step 3: Click **Add** to create the wireless profile and associate it with a site, then click **Finish** to continue. The **DESIGN > Network Settings> Wireless** screen is displayed.

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

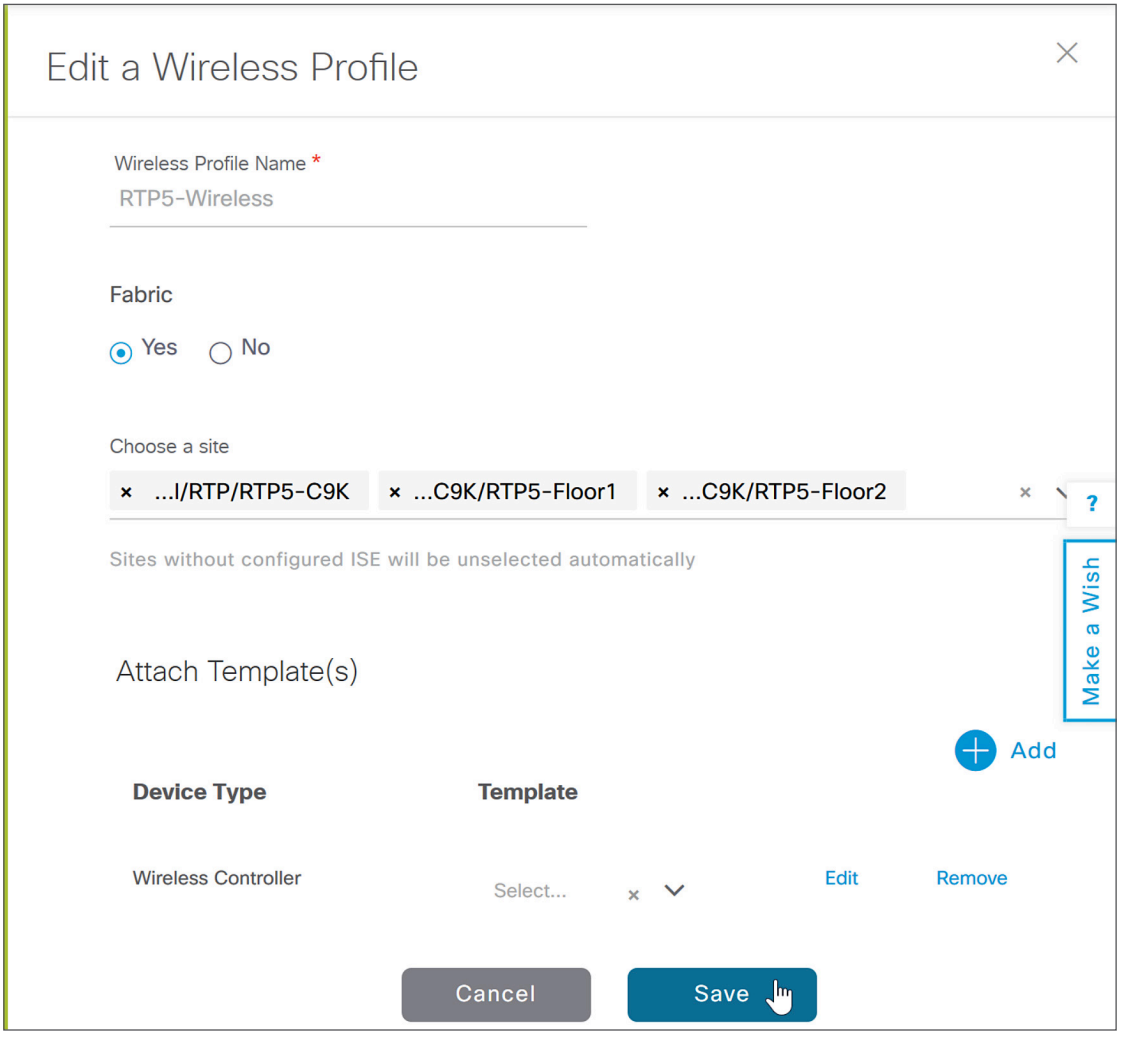
Procedure 4 Design a fabric guest wireless SSID

Step 1: 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.

Step 2: In the **Wireless Profiles** section, 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 3: In the **Portals** screen, click **+ Add**. The **Portal Builder** screen appears.

Step 4: 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 5: Click **Finish**. The wireless LAN design is created and is ready to deploy.

Procedure 5 Provision the WLC for SD-Access Wireless fabric integration

After completing the SD-Access Wireless design, push the configuration from the Design Application to the WLC.

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

Tech tip

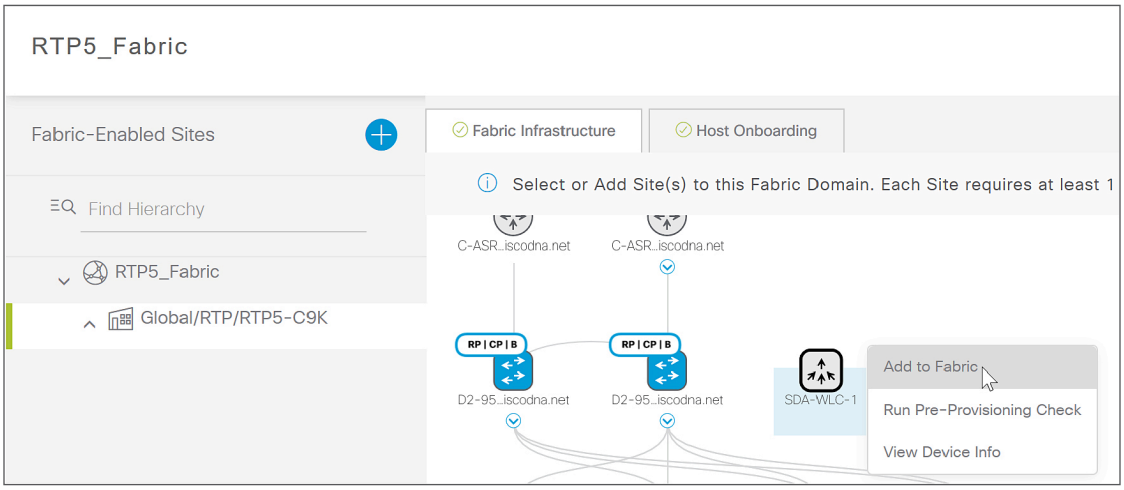
When a pair of WLCs is configured in HA SSO mode, a single WLC appears in the Cisco DNA Center inventory. You can verify that an HA SSO pair is configured by clicking the device name and then clicking the **High Availability** tab.

Step 2: Assign the site (example: Global/RTP/RTP5-C9K), click **Next**, at the **Configuration** screen 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** screen click **Next**.

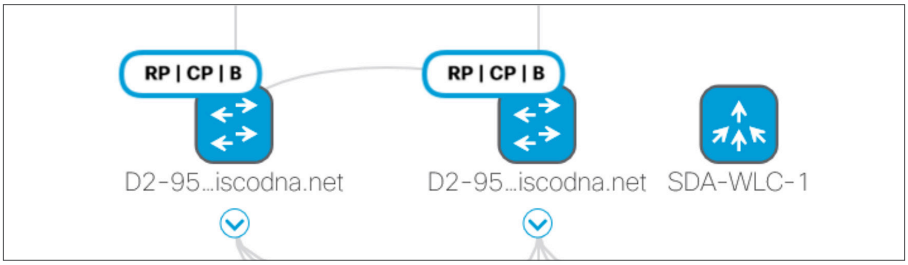
Step 3: At the **Summary** screen review the configurations, click **Deploy**, at the slide-out panel keep the default selection **Now,** and then click **Apply**.

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

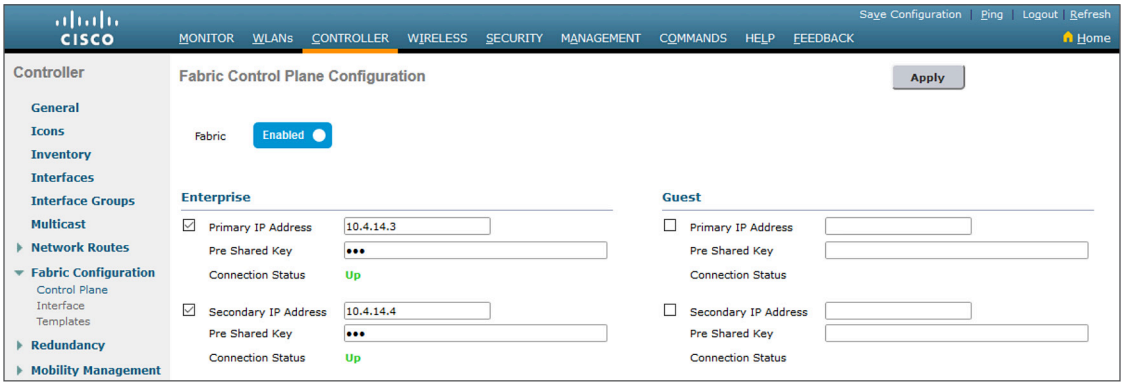
Step 4: From the Cisco DNA Center dashboard, navigate to **PROVISION > Fabric**, under **Fabric Domains** click the created fabric site (example: RTP5_Fabric), on the left in the **Fabric-Enabled Sites** navigation click the associated site (example: Global/RTP/RTP5-C9K), click the WLC, and then in the popup box click **Add to Fabric**.



Step 5: 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.



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.



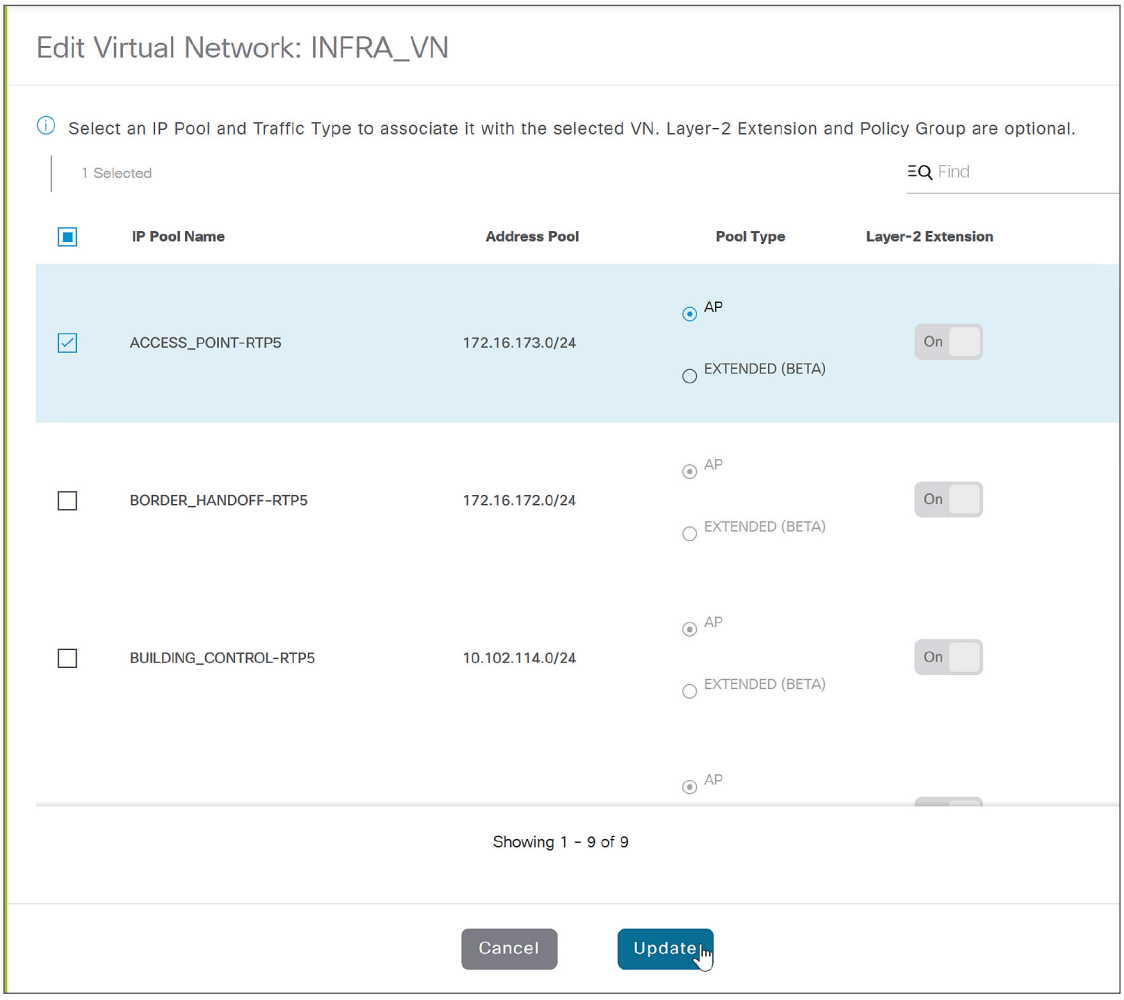
Procedure 6 Enable onboarding of access points into the wireless fabric

The APs are hosts that join the fabric and are assigned into a 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.

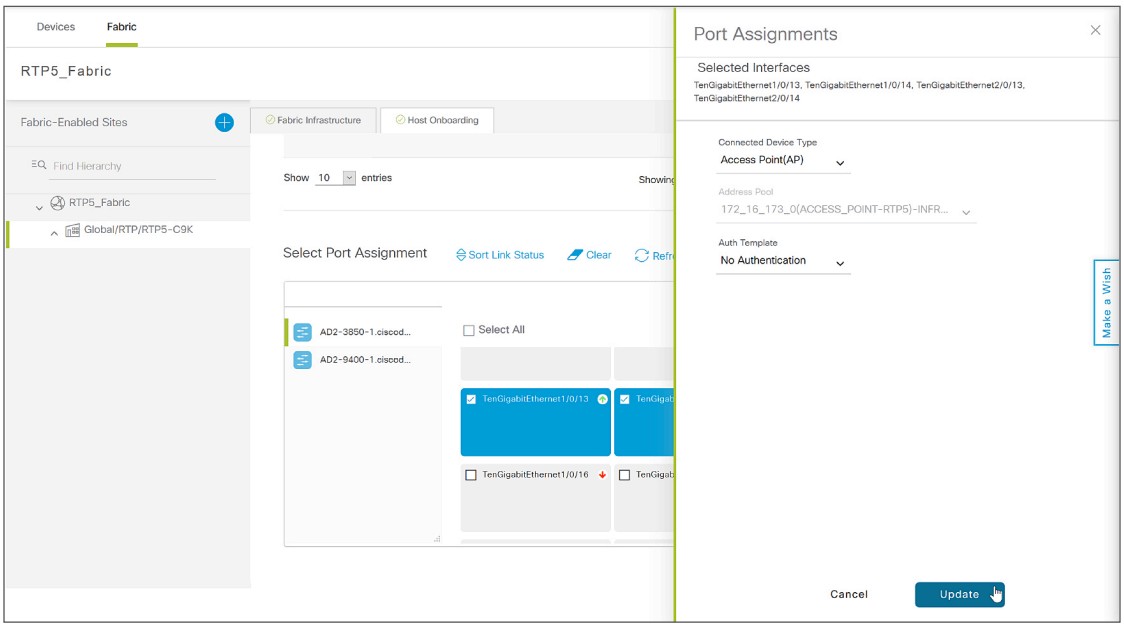
Step 2: From the Cisco DNA Center dashboard, navigate to **PROVISION > Fabric**, under **Fabric Domains** click the created fabric site (example: RTP5_Fabric), on the left in the **Fabric-Enabled Sites** navigation click the associated site (example: Global/RTP/RTP5-C9K), and then click **Host Onboarding**.

Step 3: Under **Virtual Networks**, select **INFRA_VN**, click 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 4: In the Modify Virtual Network slide-out panel, keep the default selection **Now,** and then click **Apply**.

Step 5: 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 authentication template to be set to **No Authentication**. Alternatively, you use the switch port configurations in Cisco DNA Center to assign a port to the IP address pool for the APs.

Step 6: Repeat the previous step for any additional switches that have ports used for APs.

Step 7: After all ports supporting APs have been selected, at the top of the **Select Port Assignment** section, click **Save**, keep the default **Now** selection, and then click **Apply**.

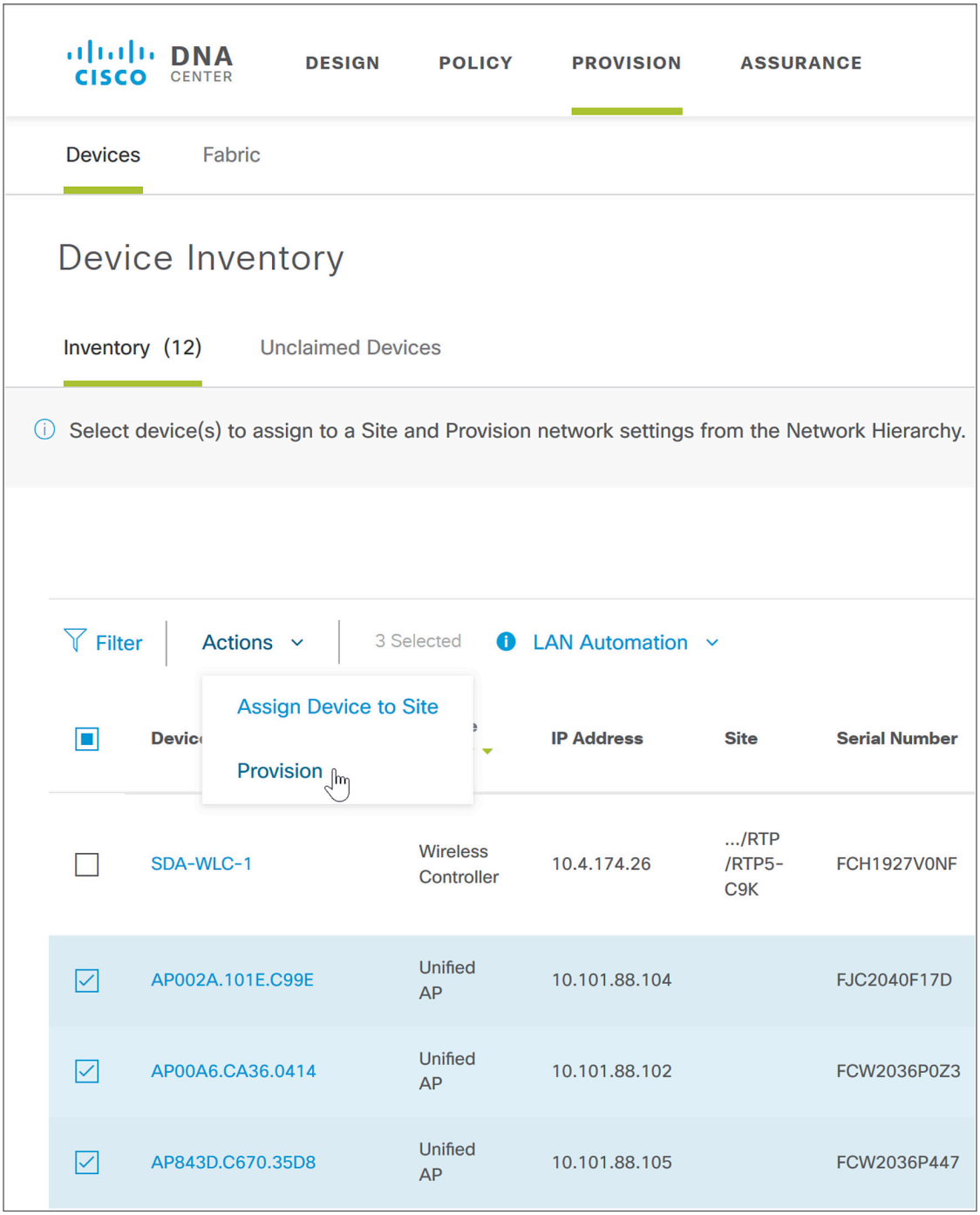
After the update is complete, the edge node switch ports connected to the APs are enabled with a device tracking configuration recognizing APs and permitting the APs to get network connectivity.

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. Redistribute the WLC route at the border into the underlay IGP routing process for efficiency. Alternatively, you can create static entries at each edge node supporting APs.

Step 8: Navigate to the main Cisco DNA Center dashboard, under **Tools** select **Inventory**, select the WLC being added, and then at the top, in the **Actions** pull-down, select **Resync**. The APs associated with the WLC are added to the inventory without waiting for an inventory refresh.

Step 9: 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**.

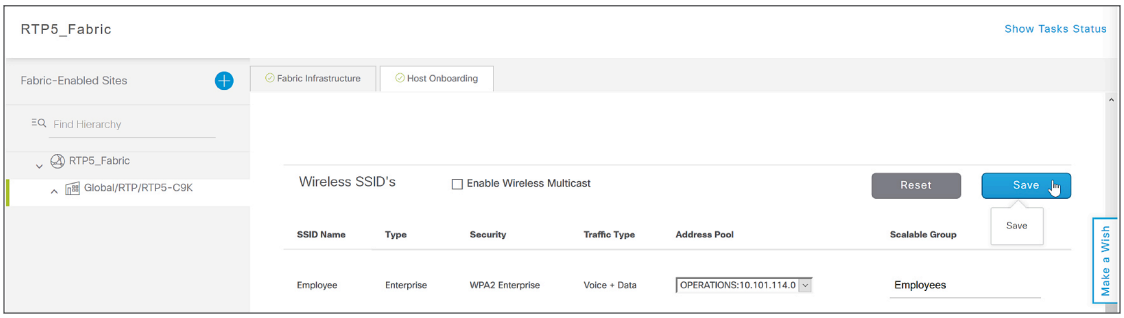


Step 10: On the **Provision Devices** screen, assign the APs to a floor (example: Global/RTP/RTP5-C9K/ Floor 1), click **Next**, for **RF Profile** select **TYPICAL**, click **Next**, at the **Summary** page click **Deploy**, and in the slide-out panel, leave the default selection of **Now**, and then click **Apply** and acknowledge any warnings about reboots.

Procedure 7 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 is not inclusive of all possibilities. Additional hardware options are listed in the associated Software-Defined Access Design Guide, and the SD-Access Product Compatibility Matrix 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.

Additional Cisco DNA Center information is on Cisco.com here:

Install and Upgrade Guides

Maintain and Operate Guides

End-User Guides

Cisco DNA Center

Functional area	Product	Part number	Software version
Network Automation	Cisco DNA Center Appliance	DN1-HW-APL	1.2.3 (System Update 1.1.0.576)

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	2.1.17.1700014
Assurance - Base	1.2.3.742
Assurance – Sensor	1. 2.3.743
Automation – Base	2.1.18.60024
Automation – Sensor	2.1.18.60024
Command Runner	2.1.18.60024
Device Onboarding	2.1.18.60024
Device Onboarding UI	2.1.18.60024
DNAC UI	1.2.0.31
Image Management	2.1.18.60024
NCP – Base	2.1.17.60044
NCP – Services	2.1.18.60024

Package	Version
Network Controller Platform	2.1.18.60024
Network Data Platform – Base Analytics	1.1.3.6
Network Data Platform – Core	1.1.3.13
Network Data Platform – Manager	1.1.3.9
Path Trace	2.1.18.60024
SD-Access	2.1.18.60024

Identity management

Functional area	Product	Software version
Cisco ISE Server	Cisco Identity Services Engine	2.3 Patch 4

SD-Access fabric border and control plane

Functional area	Product	Software version
Border and control plane	Cisco Catalyst 9500 Series Switches	16.6.4
Border and control plane – small site	Cisco Catalyst 3850 XS switches (10-Gbps fiber)	16.6.4
Border and control plane	Cisco 4000 Series Integrated Services Routers	16.6.4
Border and control plane – large scale	Cisco ASR 1000-X and 1000-HX Series Aggregation Services Routers	16.6.4
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)SY1
Border	Cisco Catalyst 6880-X and 6840-X switches	15.5(1)SY1
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	8.2(2) + SMU CSCvg39911, CSCvh87828, CSCvg09282, and CSCvh32898
Control plane	Cisco Cloud Services Router 1000V Series	16.6.3

SD-Access fabric edge

Functional area	Product	Software version
Fabric edge	Cisco Catalyst 9300 Series – stackable	16.6.4
Fabric edge	Cisco Catalyst 9400 Series with Supervisor Engine-1 – modular chassis	16.6.4
Fabric edge	Cisco Catalyst 3850 Series – stackable	16.6.4
Fabric edge	Cisco Catalyst 3650 Series – standalone with optional stacking	16.6.4
Fabric edge	Cisco Catalyst 4500E Series with Supervisor 8-E – modular chassis	3.10.1E

SD-Access Wireless

Functional area	Product	Software version
Wireless LAN controller	Cisco 8540, 5520, and 3504 Series Wireless Controllers	8.5.131.0 (8.5 MR3)
Fabric mode access points	Cisco Aironet® 1800, 2800, and 3800 Series (Wave 2)	8.5.131.0 (8.5 MR3)

LAN Automation switches

Product-CVD verified (not inclusive of all possibilities)	PnP roles tested (discovered devices directly attached to seeds)
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
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

Glossary

AAA authentication, authorization, and accounting

ACL access control list

AD Active Directory

AP access point

ARP address resolution protocol

BGP border gateway protocol

BPDU bridge protocol data unit

CAPWAP control and provisioning of wireless access points protocol

CLI command-line interface

DHCP dynamic host configuration protocol

DMVPN dynamic multipoint virtual private network

DNS domain name system

ECMP equal-cost multipath

FHRP first-hop redundancy protocols

GLBP gateway load-balancing protocol

GRE generic routing encapsulation

GUI graphical user interface

HSRP hot standby router protocol

IGMP Internet Group Management Protocol

IoT Internet of Things

IS-IS intermediate system to intermediate system routing protocol

IGP interior gateway protocol

ISE Cisco Identity Services Engine

LISP locator/ID separation protocol

MnT Monitoring and Troubleshooting Node

MPLS multiprotocol label switching

MSDP multicast source discovery protocol

MTU maximum transmission unit

PAN Policy Administration Node

PSN Policy Service Node

RP rendezvous point

SD-Access Software-Defined Access

SGACL scalable group access control list

SGT scalable group tag or security group tag

SVI switched virtual interface

SXP scalable group tag exchange protocol

VLAN virtual local area network

VN virtual network

VRF virtual routing and forwarding

Please use the feedback form to send comments and suggestions about this guide.

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 www.cisco.com/go/offices.