

CISCO VALIDATED DESIGN

Software-Defined Access Deployment Guide

September 2018
Solution 1.1



Table of Contents

Software-Defined Access introduction	1
Implementation overview.....	2
Design considerations	3
Additional information.....	4
Deployment details.....	5
Installing controllers for an SD-Access network.....	5
Install Identity Services Engine nodes	15
Integrate Identity Services Engines with DNA Center	21
Install SD-Access wireless LAN controllers.....	23
Deploying SD-Access	27
Using DNA Center for initial network design and discovery.....	27
Creating segmentation and policy for the SD-Access network.....	35
Preparing the network for automation	38
Provisioning the SD-Access underlay network.....	50
Provisioning an SD-Access overlay network	53
Optional.....	63
Integrating wireless into SD-Access	64
Appendix A: Product list.....	71
DNA Center.....	71
DNA Center packages.....	71
Identity management.....	72
SD-Access fabric border and control plane	72
SD-Access fabric edge.....	72
SD-Access Wireless	73
LAN Automation switches—Cisco Validated Design verified (not inclusive of all possibilities).....	73
Glossary	74

Software-Defined Access introduction

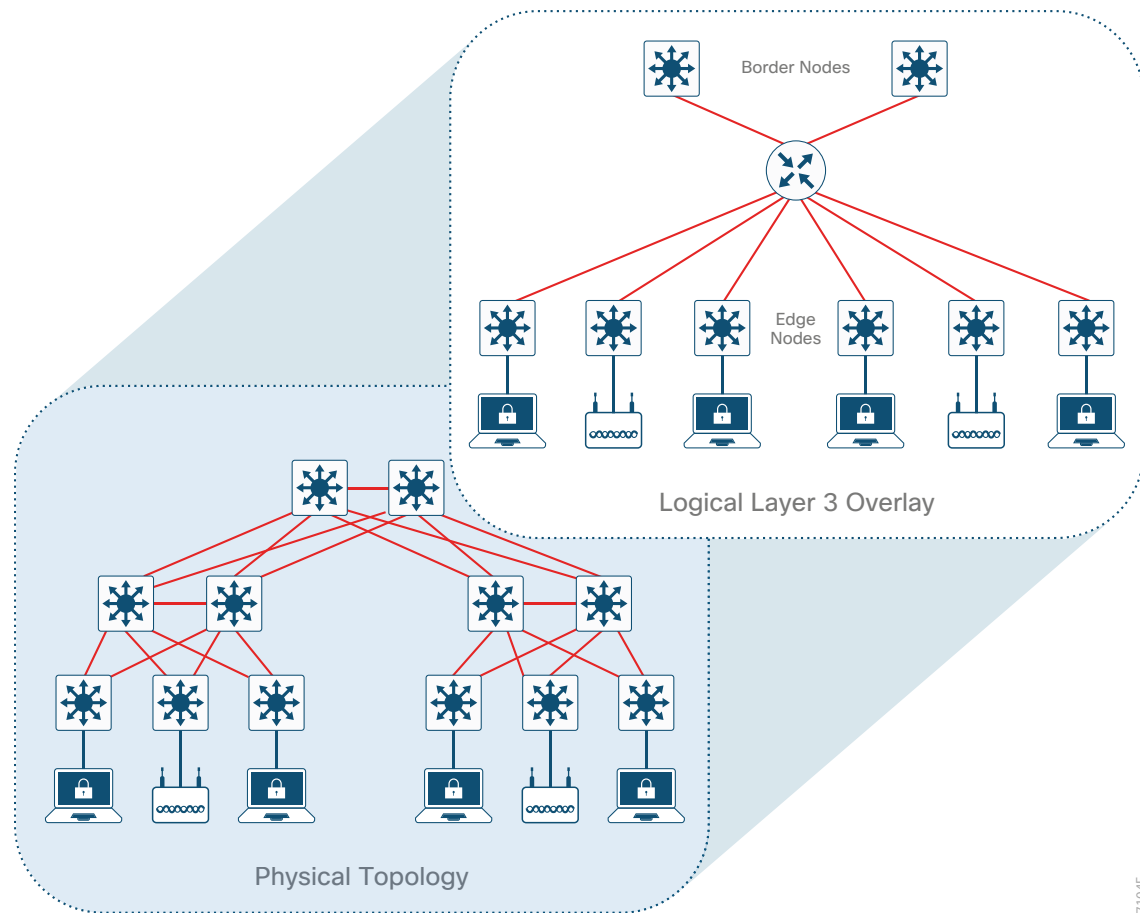
Cisco® Software-Defined Access (SD-Access) is an application package that runs on the Cisco DNA Center™ controller for designing, provisioning, applying policy, and facilitating the creation of an intelligent campus wired and wireless network with assurance. Fabric technology for the campus, an integral part of SD-Access, introduces programmable overlays enabling easy-to-deploy network virtualization across the wired and wireless campus. In addition to network virtualization, fabric technology for campus provides 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 DNA Center to automate the creation of virtual networks provides reduction in operational expenses, coupled with the advantage of reduced risk with integrated security and improved network performance provided by the assurance and analytics capabilities.

This guide describes an implementation for deploying an SD-Access network using DNA Center, integrated into 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, 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 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 part of the campus fabric. All network elements of the underlay must establish IP connectivity via the use of a routing protocol, just as when building a traditional campus network. Instead of using arbitrary network topologies and protocols, this implementation uses a well-designed Layer 3 foundation inclusive of the campus edge switches (also known as a **routed access** design), ensuring performance, scalability, and high availability of the network. In the campus fabric, end-user subnets are not part of the underlay network, even though the underlay infrastructure equipment supports the end-user physical connectivity.

You use the underlay as the supporting infrastructure when creating one or more overlay networks, which run across a set of the underlay network devices. The data plane traffic and control plane signaling is contained within each virtualized network, maintaining isolation among the networks in addition to isolation from the underlay network. The SD-Access fabric implements virtualization by encapsulating user traffic over IP packets that are sourced and terminated at the boundaries of the fabric, extending all the way to 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. In multi-tenant style deployments where you relinquish control of the addressing for each tenant's Layer 3 overlay, you likely have to allow for some non-unique IP address space appearing in more than one overlay. You can support the overlapping IP address space requirement by preserving the traffic separation beyond the fabric border using typical virtualization techniques—including adding devices to remediate addressing conflicts (typically using network address translation) and provisioning to enable communication with permitted common external IP services such as DNS and the Internet.

Figure 1. Layer 3 overlay—connectivity logically routed

7104F

In addition to network virtualization, the campus fabric integrates Cisco TrustSec technology to enable software-defined segmentation and policy enforcement based on user identity and group membership. In this deployment, security policy management uses Cisco Identity Services Engine (ISE). Scalable group tags (SGTs), also known as security group tags, are integrated into the campus fabric headers. For group policies that extend outside of the campus, you configure the propagation of the SGT information from the fabric border node outside of the campus by either transporting the tags to TrustSec-aware devices using SGT exchange protocol (SXP) or by directly mapping SGTs to Cisco Meta Data using inline tagging capabilities implemented for connections to the border.

Implementation overview

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

Within this guide, the deployment of the underlay network is a Layer 3 routed access topology using the Intermediate System to Intermediate System (IS-IS) routing protocol with fast network convergence properties available using equal-cost multipath (ECMP) routing. Underlay topologies for the fabric should not use the classic Layer 2 access design components, such as EtherChannel, in a fabric implementation for the SD-Access 1.1 solution. The overlay networks deployed are IP-only and connect with the rest of the enterprise network at the fabric border nodes as a function enabled on the campus core devices. Network virtualization extending outside of the fabric is preserved using VRF-lite, a virtualization technology commonly used to enable multiple separated Layer 3 routing and forwarding functions within a device.

Outside of the fabric, you enable any required connectivity among virtual routing and forwarding instances (VRFs) and to services (typically residing within either the global routing table or a dedicated VRF) using classic virtualization techniques, which preserve the separation while allowing communication on an as-needed basis. When you consider integrating the campus fabric into an existing enterprise network, there are two key network design considerations, and each drives unique requirements for the integration:

- **Virtualized network:** If the network is already virtualized, the VRFs at the campus fabric border extend into that virtualization technique of choice by using VRF-lite as a handoff into the existing virtualized infrastructure, whether it is MPLS, Multi-VRF, or some other technique.
- **Non-virtualized network:** If the existing network is not virtualized, the recommended, validated interconnection between the fabric border and the non-virtualized network uses an intermediate device (*fusion router*) to enable route exchange between the domains and enabling shared services across all the virtual networks. Dual fusion routers are deployed for increased availability and use Border Gateway Protocol (BGP) as an exterior gateway protocol to the fabric border, which easily accommodates loop avoidance.

In the deployment described, the campus core layer hosts the border functionality. An alternative border for smaller networks using a collapsed core/distribution using stackable switches is also described. Using the core as the border offers the overlay benefits across the entire campus LAN at the common campus exit point. The location where traffic exits the fabric as the default path is the *external border*. There are alternative choices for the external border, such as extending the border further into the enterprise, perhaps by extending the fabric all the way to the Internet edge. For trial deployments, the entire fabric could consist of a pair of distribution switches (or a collapsed core/distribution at a smaller site) performing the fabric external border role along with associated access switches at the fabric edge. When implementing this, recognize that the fabric benefits are limited to the devices covered by the extent of the border-to-edge fabric domains.

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 Layer 3 access 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. To achieve this goal for underlay deployments not manually created, the DNA Center LAN Automation feature deploys new networks using an IS-IS routed access design. Though there are many alternatives, the 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 to a routed access layer. All the same, SD-Access introduces the flexibility to remove traditional routed access layer restrictions associating client subnets to the closest Layer 3 gateway and allows subnets to stretch through the SD-Access fabric to support a specific function, such as connectivity for computers, unified communications, or wireless LAN access points.

- Do you plan to deploy the underlay manually in a custom configuration as an extension to the routing protocol already used throughout an organization, or do you intend to use a dedicated interior gateway protocol (IGP) for the fabric underlay? This deployment shows a separate IGP using IS-IS for the underlay, which has a well-defined scope that is useful in automating new 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 stretched subnets meet the requirements? The deployment accommodates both types of deployments by supporting one or multiple VRFs extended outside the fabric domain. Nevertheless, consider that multiple overlays require additional planning for integration of common services into the multi-VRF environment. In both scenarios, you need to plan for and document all overlay subnets and VRFs for the host pools and be 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 trial deployment, a production deployment will present operational challenges if you deploy the border in one location and later decide to relocate it to another location, so careful consideration of the future fabric coverage scope 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.

Process

Installing controllers for an SD-Access network

1. Install DNA Center

The Cisco SD-Access 1.1 solution described in this guide uses a single DNA Center controller hardware appliance, prepared for inclusion as part of a cluster in the future. For this solution, DNA Center 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: DNA Center must have Internet access for system updates from the Cisco cloud repository.
- A network-reachable Network Time Protocol (NTP) server, used during DNA Center installation to help ensure reliable digital certificate operation for securing connections.
- Certificate server information, if you choose not to use self-signed digital certificates for a single node: For three-node cluster configurations, certificates generated by a certificate authority are required.

Procedure 1 Install DNA Center

The 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. Validation is shown using a virtual IP (VIP) configured on a standalone DNA Center appliance, making it easier to migrate to a three-appliance cluster in the future. You do not need to physically connect the intra-cluster communications port for a standalone configuration. For provisioning and assurance communication efficiency, DNA Center should be installed in close network proximity to the greatest number of devices being managed.

Figure 2. Rear view of the DNA Center Appliance – DN1-HW-APL

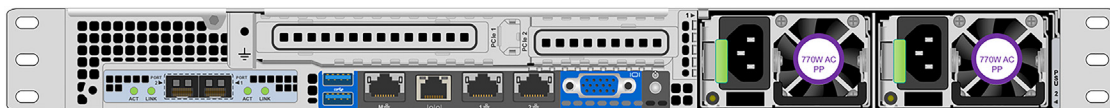


Table 1. DNA Center server LAN Ethernet interface assignments (left to right, from rear)

	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

To avoid the need to maintain a list of static routes on an additional interface, you can connect DNA Center to your network using a single network interface configured with a default gateway. For deployments requiring multiple interfaces separating administrative access and network infrastructure provisioning, static route changes after installation may require reconfiguration. If reconfiguration is required, follow the procedure to reconfigure the appliance using the wizard in the [Cisco Digital Network Architecture Center Appliance Installation Guide](#).

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 DNA Center instance. The address space is required for both a single-server configuration and a three-server configuration.

The 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 [Cisco Digital Network Architecture Center Appliance Installation Guide](#).

Step 1: Connect the DNA Center server 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)
- Optionally using any other ports required for the installation, such as the dedicated web management port, an isolated enterprise network port, or cluster configuration port.

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 standalone host or the first host in a cluster deployment, without a network proxy.

Step 2: Boot the DNA Center hardware appliance. A welcome message appears.

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

Step 3: Press **Enter** to accept the default choice, **Start a DNA-C Cluster**.

Step 4: 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 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 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 is available for use with an isolated network 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**, optionally 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 5: Select **proceed >>** to continue with the network validation. The installation validates gateway reachability.

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

Step 6: After the wizard network validation completes, continue entering initial configuration values. For a standalone appliance, you 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 7: In wizard **STEP #14, NTP SEVER SETTINGS**, you must supply at least one active NTP server.

NTP Servers: *

10.4.0.1 10.4.0.2

Step 8: Select **next >>**. The installation validates connectivity to the NTP servers.

Validating NTP Server: **10.4.0.1**

Step 9: In wizard **STEP #16 , MAGLEV ADVANCED SETTINGS**, you assign unique IP networks that are not part of the enterprise network, which are used by 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 10: 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 11: Log in with the maglev user from the 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 12: Verify that processes are deployed.

```
$ maglev package status
```

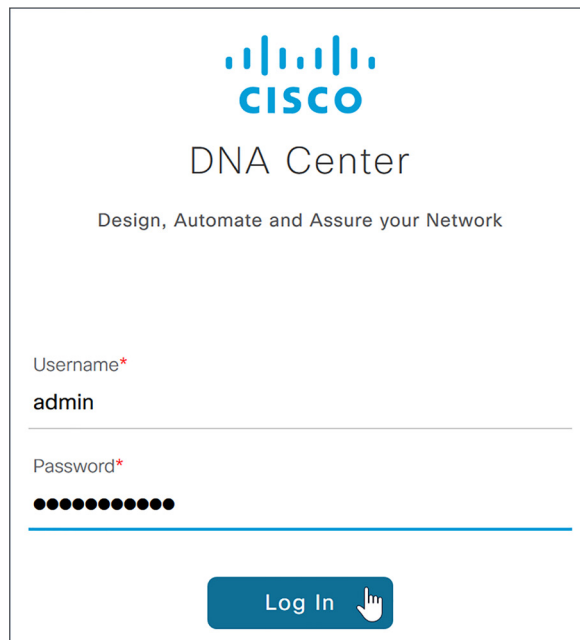
For the validated version, all packages are DEPLOYED initially, except for any NOT_DEPLOYED packages listed, including the following, which vary depending on your installation version:

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

You install other required components in later steps.

Step 13: Connect to the DNA Center Web UI by directing a web browser to the **Cluster Virtual IP address** you supplied in the first step of the installation (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 14: At the **Username** line enter **admin**, at the **Password** line enter the DNA Center administrator password that you assigned using the Maglev Configuration Wizard, and then click **Log In**.



Step 15: At the prompt, choose a new password or skip to the next step.

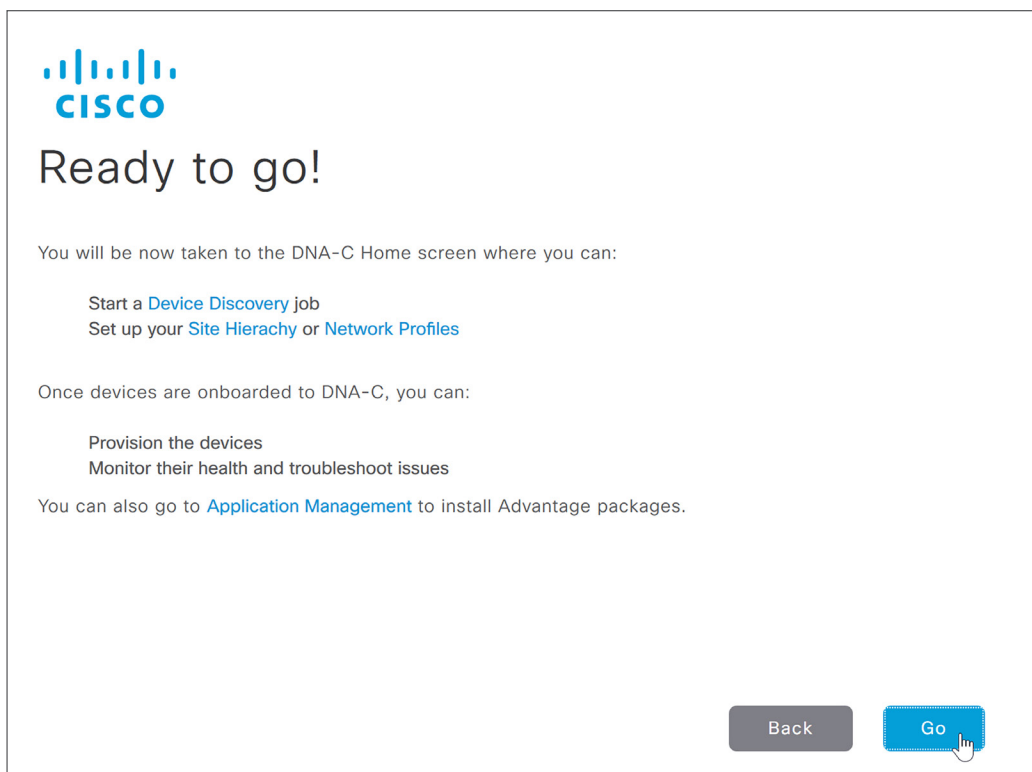
Step 16: At the **Welcome to DNA Center** prompt, provide a Cisco.com ID and password. The ID is used to register software downloads and receive system communications.

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.

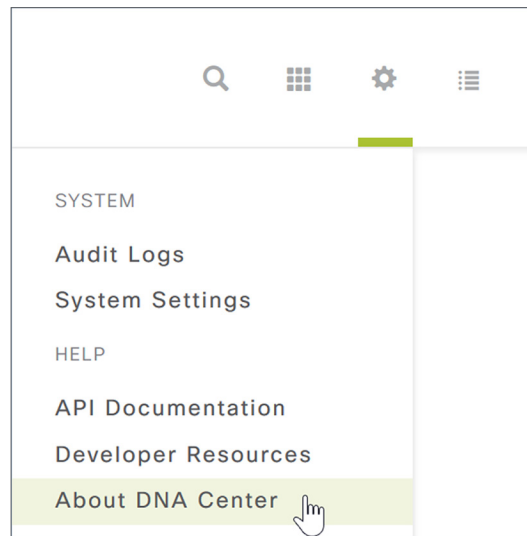
Step 17: In the previous step, if you did not enter an ID with Smart Account access with privileges for managing Cisco software licenses for your organization, a **Smart Account** prompt displays. Enter a Cisco.com ID associated with a Smart Account or click **Skip**.

Step 18: 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 19: At the **Terms and Conditions** display, click **Next**, and then at the **Ready to go!** display, click **Go**.



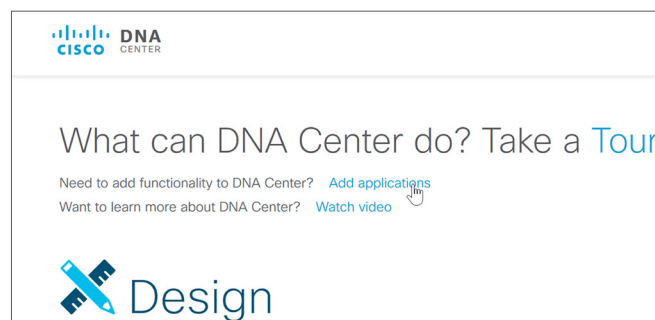
Step 20: At the main DNA Center dashboard, click the settings (gear) icon, and then click **About DNA Center**.



Step 21: Check that the version is at least 1.1.6. If your version is earlier than 1.1.6, contact support to reimage your 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 1.1.8, shown in a later step.



Step 22: At the main 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

For the validated version of DNA Center and SD-Access listed in Appendix A: Product List, a system update from the Internet is required. Check the release notes for your target software version for the appropriate procedures and dependencies.

DNA Center release notes are found at:

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

The release notes include firewall access requirements for connecting DNA Center to the Internet to download packages from the cloud catalog server.

DNA Center software newer than the version used for this validation may also support additional platform images, which can be found by searching Cisco.com for [SD-Access Hardware and Software Compatibility Matrix](#).

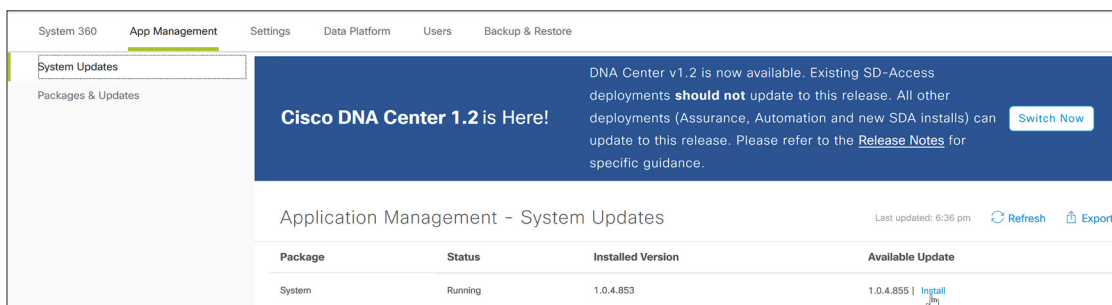
DNA Center automatically connects to the Cisco cloud repository to find the latest updates. You can use the **Refresh** button to reveal any updates that are found over time.

Tech tip

When deploying with this guide, do not use the DNA Center 1.2 **Switch Now** button, if it appears. This guide covers SD-Access using only DNA Center 1.1 versions of the software.

Step 23: Click the settings (gear) icon, click **System Settings**, and then navigate to **App Management > System Updates**. The **Application Management – System Updates** screen is displayed.

Step 24: Under the **Available Update** column, in the row showing **System**, if there is an available update, click **Install**.



The screenshot shows the 'System Updates' page in the Cisco DNA Center interface. At the top, there is a navigation bar with 'System 360', 'App Management', 'Settings', 'Data Platform', 'Users', and 'Backup & Restore'. The 'App Management' section is active, and 'System Updates' is selected in the left sidebar. A prominent blue notification banner reads 'Cisco DNA Center 1.2 is Here!' and states that DNA Center v1.2 is now available, warning that existing SD-Access deployments should not update to this release. A 'Switch Now' button is present in the banner. Below the banner, the page title is 'Application Management – System Updates' with a 'Last updated: 6:36 pm' timestamp and 'Refresh' and 'Export' buttons. A table lists the available updates:

Package	Status	Installed Version	Available Update
System	Running	1.0.4.853	1.0.4.855 Install

A download of the new system update begins, which can take many minutes. Then the installation starts automatically, which can take more than an hour. Use the **Refresh** button to check the status until the updated **Installed Version** is displayed with a **Running** status.

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.

Tech tip

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

Step 25: Click the settings (gear) icon, click **System Settings**, and navigate to **App Management > Packages and Updates**. At the top of the list, select all packages by selecting the box next to **Package**, click the **Actions** pull-down menu, and then select **Download**.

Package	Status	Installed Version	Downloaded Version	Available Version
<input checked="" type="checkbox"/> Assurance - Base	Running	1.1.5.259		1.1.8.1205
<input checked="" type="checkbox"/> Assurance - Path Trace	Running	2.1.11.60011		2.1.12.60016
<input checked="" type="checkbox"/> Assurance - Sensor	Running	1.1.5.40		

Step 26: At the popup, select **OK** to confirm the download operation. The screen updates, showing all of the packages that are being downloaded.

Before proceeding to the next step, refresh the screen until there are no longer any packages showing a status of **Downloading**. The download can take many minutes to complete.

Step 27: After the new versions of the packages are downloaded, install the packages, including the latest version of the SD-Access package. Select all packages in common that have a new **Downloaded Version** available, at the top of the window click the **Actions** pull-down menu, select **Update**, and then click **OK**.

Package	Status	Installed Version	Downloaded Version	Available Version
<input checked="" type="checkbox"/> Assurance - Base	Running	1.1.5.259	1.1.8.1205	
<input checked="" type="checkbox"/> Assurance - Path Trace	Running	2.1.11.60011	2.1.12.60016	
<input type="checkbox"/> Assurance - Sensor	Running	1.1.5.40		

The package updates begin. Use the browser refresh button to see the updated status for each package. The update process can take over an hour to complete.

Tech tip

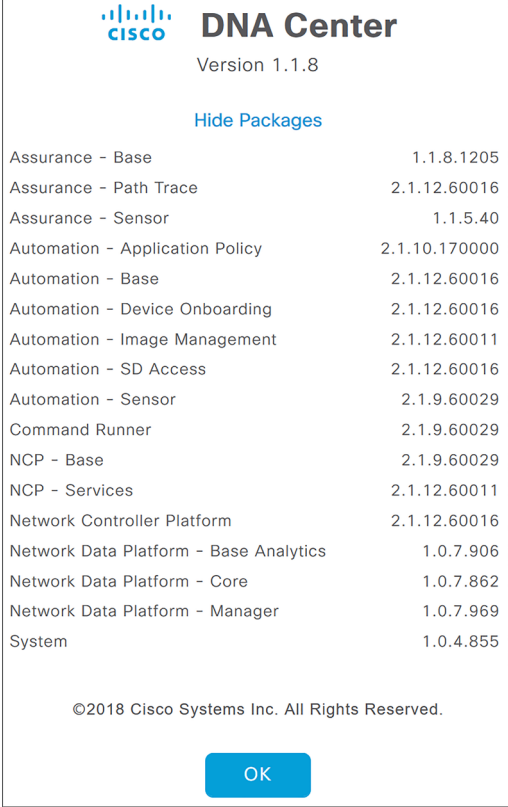
Packages must be updated in a specific order to appropriately address package interdependencies and should be updated only after the system updates have completed. Allow DNA Center to handle dependencies by selecting and updating all package updates at once; otherwise refer to the [Installation Guide](#) for the correct package update sequence. The Installation Guide also explains how to use the Maglev CLI to force a download retry for any stalled download.

The **Actions** menu is unavailable until package tasks are complete. Wait until packages no longer show a **Status** of **Pending Update**, **Preparing Update**, or **Updating** before proceeding.

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.

After the **Automation - SD Access** package is in **Running** status, along with any other updated packages, the functionality is available to use, and integration with the installed ISE nodes can proceed.

Step 28: Validate that the correct versions of DNA Center and all packages are now installed. At the main DNA Center dashboard, click the settings (gear) icon, click **About DNA Center**, and then click **Show Packages**.



DNA Center	
Version 1.1.8	
Hide Packages	
Assurance - Base	1.1.8.1205
Assurance - Path Trace	2.1.12.60016
Assurance - Sensor	1.1.5.40
Automation - Application Policy	2.1.10.170000
Automation - Base	2.1.12.60016
Automation - Device Onboarding	2.1.12.60016
Automation - Image Management	2.1.12.60011
Automation - SD Access	2.1.12.60016
Automation - Sensor	2.1.9.60029
Command Runner	2.1.9.60029
NCP - Base	2.1.9.60029
NCP - Services	2.1.12.60011
Network Controller Platform	2.1.12.60016
Network Data Platform - Base Analytics	1.0.7.906
Network Data Platform - Core	1.0.7.862
Network Data Platform - Manager	1.0.7.969
System	1.0.4.855

©2018 Cisco Systems Inc. All Rights Reserved.

OK

Process

Install 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 1.1 solution described in this guide uses two ISE nodes in a high-availability standalone configuration dedicated to the SD-Access network and integrated into 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 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 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 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.

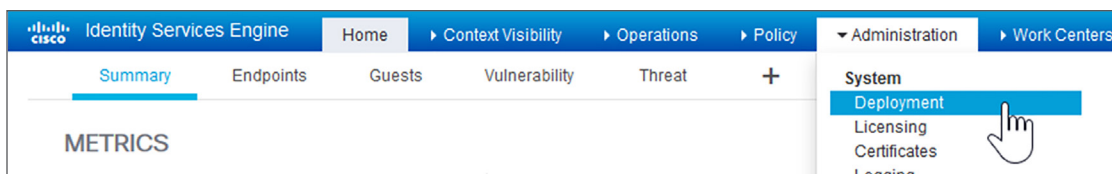
localhost login:

Procedure 2 Configure roles for ISE nodes

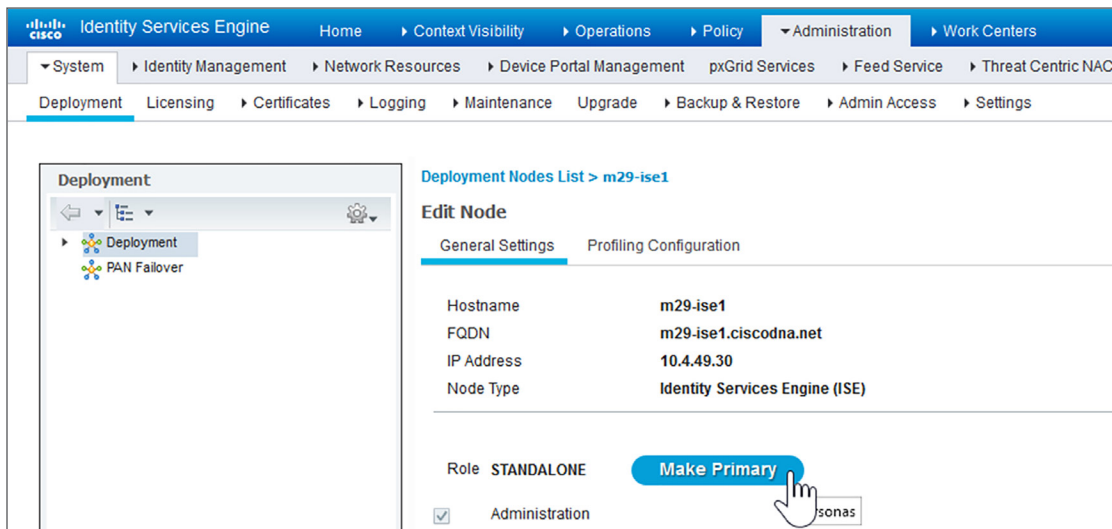
Step 1: On the first ISE node, login using a web browser and the configured username and password, and then accept any informational messages.

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

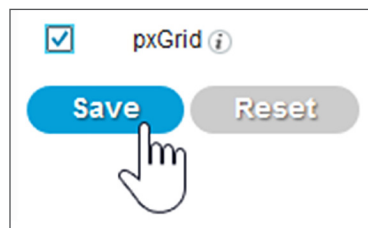
Step 2: Navigate to **Administration > System > Deployment**, and then click **OK** to the informational message.



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



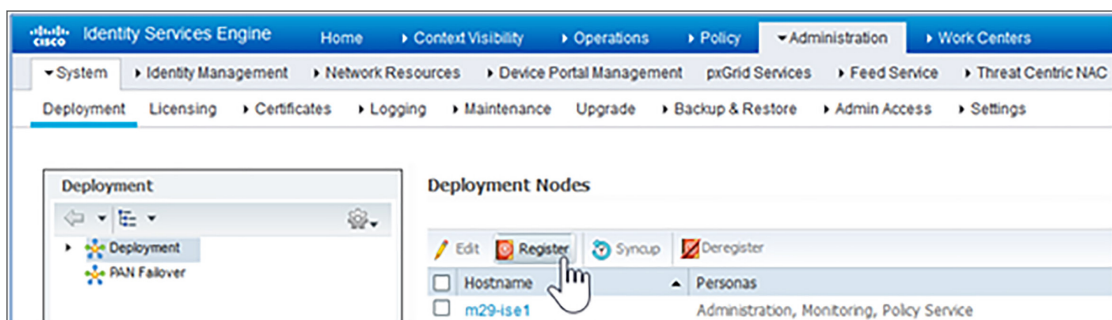
Step 4: Select **pxGrid**, and then click **Save**.



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 screenshot shows the 'Register ISE Node - Step 2: Configure Node' configuration page. The 'Monitoring' section is expanded, and the 'Role' dropdown is set to 'PRIMARY'. The 'pxGrid' checkbox is checked. The 'Submit' button is highlighted in green.

Deployment Nodes List > Configure Node
Register ISE Node - Step 2: Configure Node
 General Settings

Hostname: m29-ise2
 FQDN: m29-ise2.ciscodna.net
 IP Address: 10.4.49.31
 Node Type: Identity Services Engine (ISE)

Role: **SECONDARY**

Administration

Monitoring

Role: PRIMARY

Other Monitoring Node: m29-ise1

Policy Service

Enable Session Services *i*

Include Node in Node Group: None *i*

Enable Profiling Service *i*

Enable Threat Centric NAC Service *i*

Enable SXP Service *i*

Enable Device Admin Service *i*

Enable Passive Identity Service *i*

pxGrid *i*

Submit **Cancel**

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.

Deployment Nodes				
Hostname	Personas	Role(s)	Services	Node Status
<input type="checkbox"/> m29-ise1	Administration, Monitoring, Policy Service, pxGrid	PRI(A), SEC(M)	SESSION, PROFILER	<input checked="" type="checkbox"/>
<input type="checkbox"/> m29-ise2	Administration, Monitoring, Policy Service, pxGrid	SEC(A), PRI(M)	SESSION, PROFILER	<input checked="" type="checkbox"/>

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**, and then click **Save**. Accept any additional dialog box that appears.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The left-hand navigation pane shows the following menu items: System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, Threat Centric NAC, Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Backup & Restore, Admin Access, and Settings. The 'Settings' menu item is selected. The main content area displays the 'ERS Settings' configuration page. The page is divided into three sections: 'ERS General', 'ERS Setting for Primary Administration Node', and 'ERS Setting for All Other Nodes'. The 'ERS General' section contains a description of ERS and a link to the SDK page. The 'ERS Setting for Primary Administration Node' section has two radio button options: 'Enable ERS for Read/Write' (selected) and 'Disable ERS'. The 'ERS Setting for All Other Nodes' section has two radio button options: 'Enable ERS for Read' (selected) and 'Disable ERS'. At the bottom of the page, there are 'Save' and 'Reset' buttons. A mouse cursor is pointing at the 'Save' button.

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

Integrate Identity Services Engines with DNA Center

1. Configure DNA Center authentication and policy servers

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

Tech tip

Validation shows DNA Center integrated with ISE servers. Although it is possible to avoid the integration of ISE, policy configuration such as using scalable group tags and group-based policies will not be possible and there will be a loss of automation, resulting in the requirement to manually assign edge ports to VNs, which is not a part of the validation shown.

Procedure 1

Configure DNA Center authentication and policy servers

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

The screenshot displays the Cisco DNA Center web interface. At the top right, a gear icon is clicked, opening a dropdown menu. The menu items are: SYSTEM, Audit Logs, System Settings (highlighted with a mouse cursor), HELP, API Documentation, Developer Resources, About DNA Center, and a separator line. Below the menu, the main content area features a header with the text "What can DNA Center do? Take a Tour." and several sections: Design, Policy, Provision, and Assurance. Each section includes a brief description and a list of key features. At the bottom, there is a "Tools" section with eight tiles: Discovery, Inventory, Topology, Image Repository, Command Runner, License Manager, Template Editor, and Telemetry. A "Feedback" link is visible in the bottom right corner.

Step 2: Navigate to **Settings > Authentication and Policy Servers**, and then click on 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 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** (verified with a DNS lookup at submission—cut-and-paste from a browsing session to ISE aids with entry accuracy), enter **Subscriber Name** (example: **dnac**), leave the SSH Key blank, and then click **Apply**.

The screenshot shows a configuration window titled "Add AAA/ISE server". The fields are as follows:

- Server IP Address*: 10.4.49.30
- Shared Secret*: [masked]
- Cisco ISE server: On
- Username*: admin
- Password*: [masked]
- FQDN*: m29-ise1.ciscodna.net
- Subscriber Name*: dnac
- SSH Key: [empty]

At the bottom, there are "Cancel" and "Apply" buttons. A "View Advanced Settings" link is also present. A "Feedback" button is visible on the right side of the dialog.

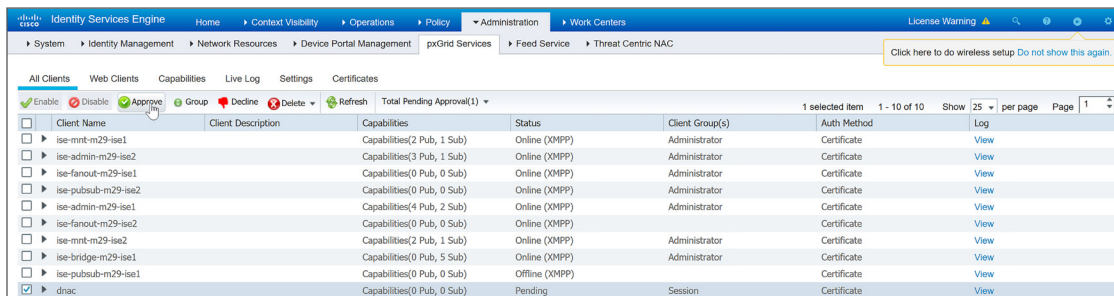
During communication establishment, status from DNA Center displays **IN PROGRESS**. Use the **Refresh** button until communication establishes with ISE and the server displays **ACTIVE** status. If communication is not established, an error message displays with information reported from ISE regarding 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, DNA Center requests a pxGrid session with ISE.

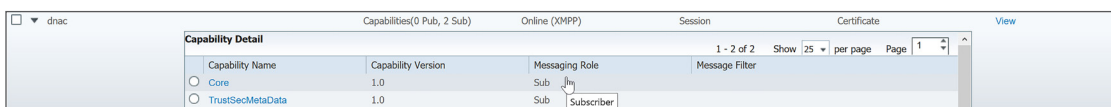
Step 4: Log in to ISE, and then navigate to **Administration > pxGrid Services**.

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 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 DNA Center and navigating to **Policy > Registry > Scalable Groups**. Existing ISE policies are not migrated to DNA Center.

Process

Install 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](#). Use this guide to 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.

Because each fabric border node is an independent routed device, redundant WLCs should not be connected at the border, but rather 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.

Tech tip

The SD-Access 1.1 solution 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

To add WLAN as part of SD-Access 1.1 with the software releases listed in Appendix A: Product List, while using Cisco Catalyst® 6800 Series fabric border devices not 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: Do not enable HA SSO. 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.

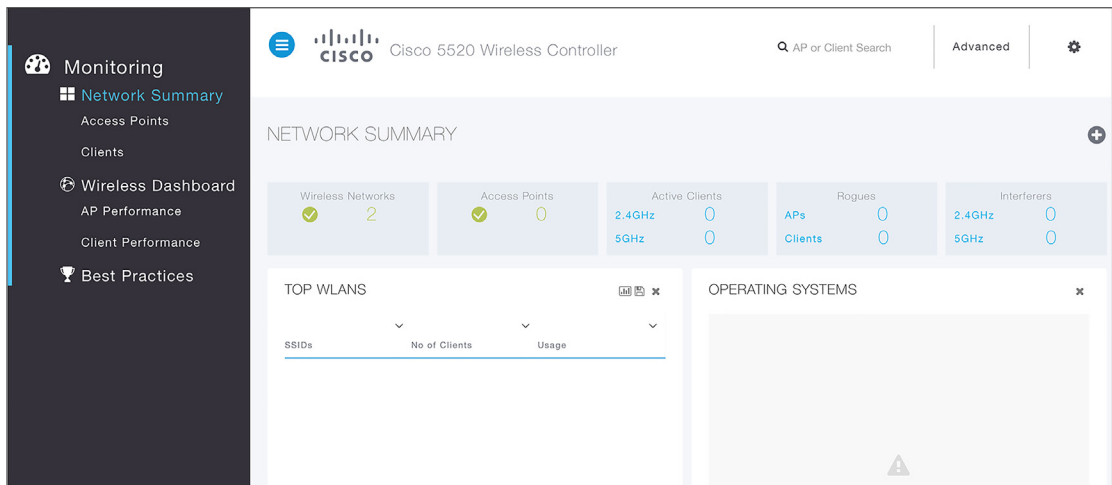
```
(Cisco Controller)
```

```
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 also choose a time zone, if you commonly use something other than the default in the network infrastructure. 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 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

Using DNA Center for initial network design and discovery

Process

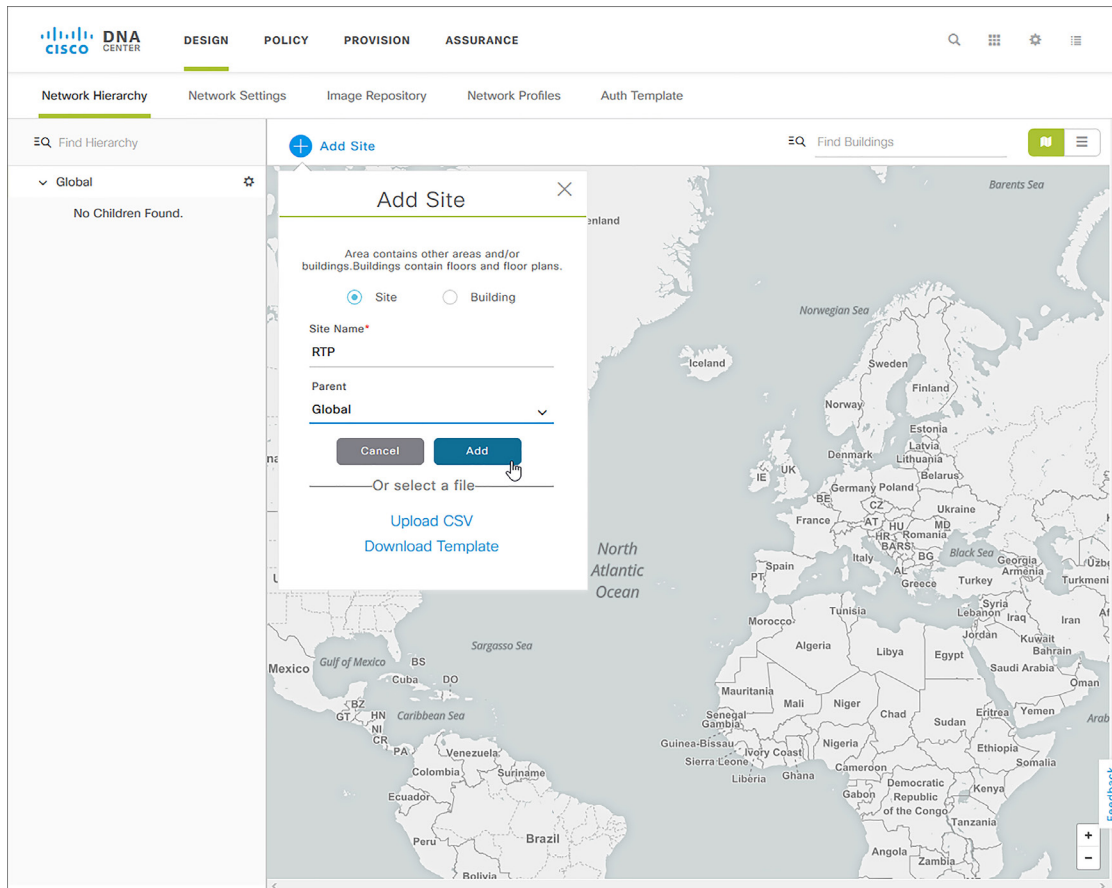
1. Create network sites
2. Configure network services for sites
3. Add device credentials for discovery and management
4. Reserve IP address pools for network provisioning

Using DNA Center, you create a network hierarchy of sites that can contain additional sites or buildings and floors within sites. Devices map into buildings for configuration.

Procedure 1 Create network sites

Step 1: Log in to DNA Center. Navigate to the main 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, supply an appropriate **Site Name**, and then click **Add**.



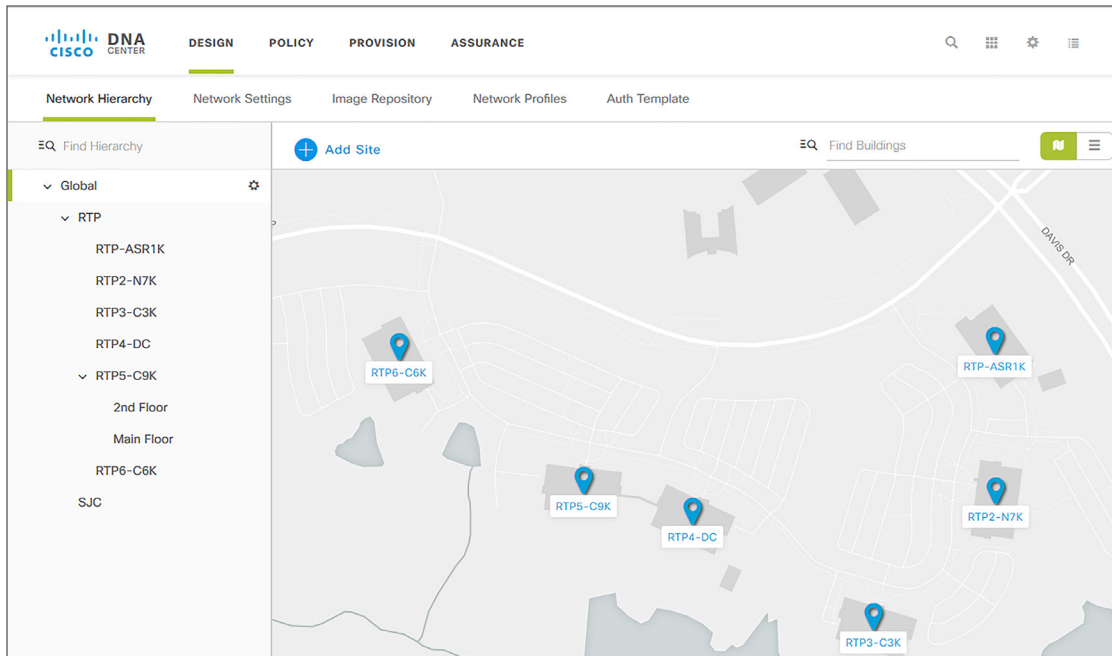
Step 3: Click **Add Site**, select the **Building** button, supply an appropriate **Building Name**, select the site previously created as the **Parent**, complete the wizard to assign a location, and then click **Add**.

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.

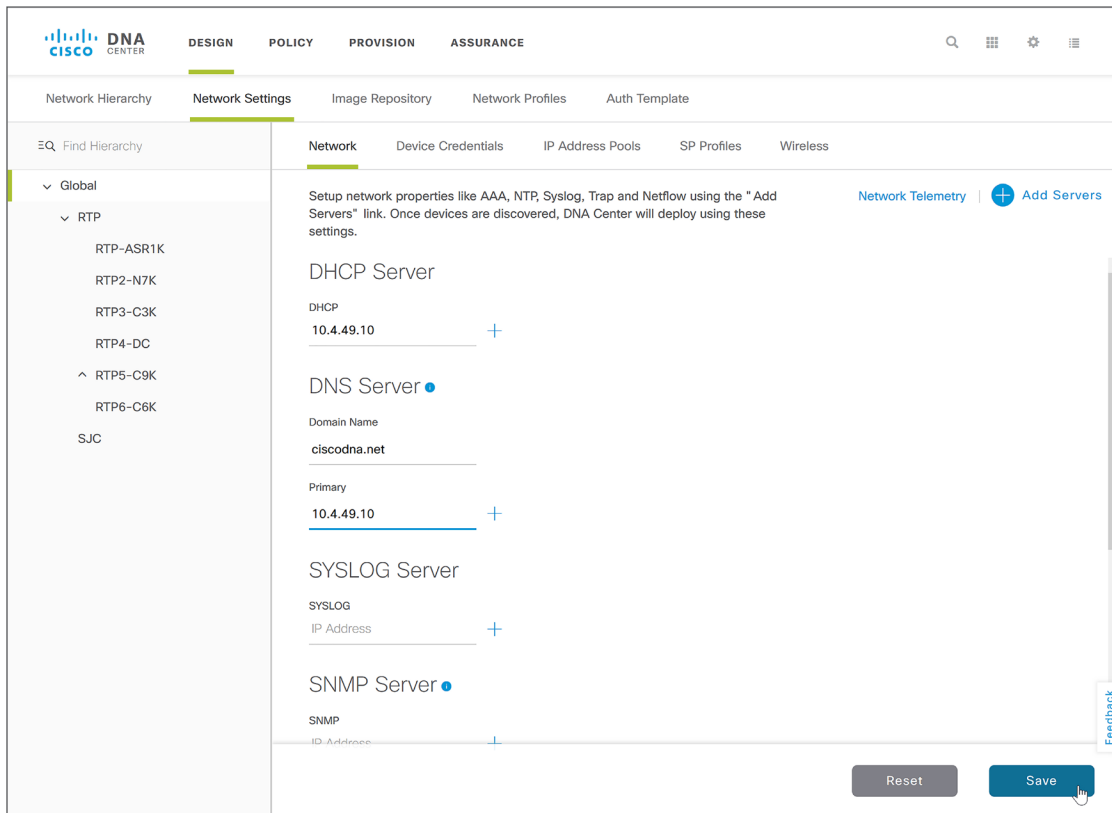
Floors are referenced during the wireless provisioning. If you have floor map diagrams in DXF, DWG, JPG, GIF, or PNG formats, add them to any defined floors as a useful component for wireless deployments to show access point locations and coverage. You can add hundreds of sites up to the limits listed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



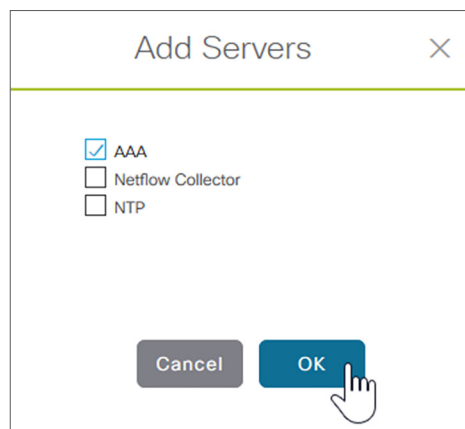
Procedure 2 Configure network services for sites

Configure AAA, DHCP, and DNS services as required for the sites in DNA Center. If the services use the same servers across all of your sites, you can configure them globally, and the inheritance properties of the hierarchy make 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 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** check box, and then click **OK**.



The configuration pane is updated with **AAA Server** as an available configuration section, ready for configuring 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.

Step 3: Select the **Network** checkbox, and select both the **ISE** and **RADIUS** radio buttons. Under **Network**, use the pull-down to select the prepopulated ISE server. Use the second pull-down that appears to select the **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.

Step 4: Select the **Client/Endpoint** checkbox, and select both the **ISE** and **RADIUS** radio buttons. Under **Client/Endpoint**, use the pull-down to select the prepopulated ISE server. Use the second pulldown that appears to select the **IP Address (Primary)** of the ISE server, and then click **Save**.

The screenshot shows the Cisco DNA Center interface for configuring an AAA Server. The left sidebar shows a hierarchy: Global > RTP > RTP5-C9K. The main content area is titled 'AAA Server' and has two sections: 'NETWORK' and 'CLIENT/ENDPOINT'. Both sections have checkboxes for 'Network' and 'Client/Endpoint', and radio buttons for 'ISE' and 'RADIUS'. In the 'NETWORK' section, the 'Network' dropdown is set to '10.4.49.30', the 'IP Address (Primary)' dropdown is '10.4.49.30', and the 'IP Address (Additional)' dropdown is '10.4.49.31'. In the 'CLIENT/ENDPOINT' section, the 'Client/Endpoint' dropdown is '10.4.49.30' and the 'IP Address (Primary)' dropdown is '10.4.49.30'. There are 'Reset' and 'Save' buttons at the bottom right.

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

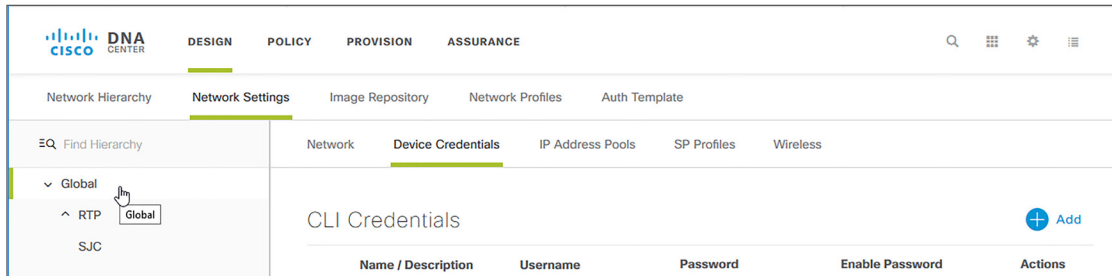
Procedure 3 Add device credentials for discovery and management

When you deploy the SD-Access underlay using devices that are already configured and which are network reachable by 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 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 up to one additional hop of connected switches, all of which must be running the PnP agent and have no previous configuration. The credentials supplied allow 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**, select an appropriate level of the site hierarchy in the left pane (example: **Global** for common credentials across the hierarchy), and acknowledge any pop-up alerts.



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 **OK**.

×

Name / Description *

Username *

Password *

Show

Enable Password

Show

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

Cancel
Save

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**.

The screenshot shows the 'Device Credentials' configuration page. It is divided into three sections: CLI Credentials, SNMP Credentials, and HTTP(S) Credentials. Each section has a table of credentials and an 'Add' button. The 'Save' button is highlighted at the bottom right.

CLI Credentials				
Name / Description	Username	Password	Enable Password	Actions
<input checked="" type="radio"/> IOS Devices	dna	*****	*****	Edit Delete

SNMP Credentials		
Name / Description	Write Community	Actions
<input checked="" type="radio"/> SNMPv2c Write	*****	Edit Delete

HTTP(S) Credentials	
Name / Description	Actions
<input type="radio"/> HTTP(S) Read	Edit Delete
<input type="radio"/> HTTP(S) Write	Edit Delete

Buttons: Reset, Save

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

Procedure 4 Reserve IP address pools for network provisioning

Reserve IP addresses for your networks by manually assigning them in 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.

This procedure shows how to manually define the IP address pools that will be used later and then assign pools to be used by the sites in your network, which you do for both manual and IPAM configurations. You have the flexibility to create a larger global pool and then later reserve a subset of a pool at lower levels, such as for a specific site in the site hierarchy. When using the validated version of DNA Center listed in Appendix A: Product List, you use the global level only to create IP address pools.

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 be configured to enable their devices to function correctly, which can be checked in product documentation.

The global address pools in the table are added as part of the validation.

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	–	–
Access-Point	172.16.173.0/24	172.16.173.1	10.4.49.10	10.4.49.10
14-Underlay	10.4.14.0/24	10.4.14.1	10.4.49.10	10.4.49.10
14-Employee	10.101.114.0/24	10.101.114.1	10.4.49.10	10.4.49.10
14-Phone	10.101.214.0/24	10.101.214.1	10.4.49.10	10.4.49.10
14-Things	10.102.114.0/24	10.102.114.1	10.4.49.10	10.4.49.10
14-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 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**.

Add IP Pool ✕

IP Pool Name *
Border-Handoff

IP Subnet *
172.16.172.0

CIDR Prefix
/24 (255.255.255.0) ▼

Gateway IP Address *
172.16.172.1

DHCP Server(s) ▼

DNS Server(s) ▼

Overlapping

Cancel
Save

Repeat this 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.

IP Address Pools (8)							Last Updated: 02:20:32	Refresh	Import	+ Add IP Pool
Filter										
Name ▲	IP Subne...	Gate...	DHCP ...	DNS S...	Free ...	Overl...	Actions			
14-Employee	10.101.114....	10.101.114.1	10.4.49.10	10.4.49.10	256 of 256	No	Edit		Delete	
14-Guest	10.103.114....	10.103.114.1	10.4.49.10	10.4.49.10	256 of 256	No	Edit		Delete	
14-Phone	10.101.214....	10.101.214.1	10.4.49.10	10.4.49.10	256 of 256	No	Edit		Delete	
14-Things	10.102.114....	10.102.114.1	10.4.49.10	10.4.49.10	256 of 256	No	Edit		Delete	
14-Underlay	10.4.14.0/24	10.4.14.1	10.4.49.10	10.4.49.10	256 of 256	No	Edit		Delete	
Access-Point	172.16.173....	172.16.173.1	10.4.49.10	10.4.49.10	256 of 256	No	Edit		Delete	
Border-Hand...	172.16.172....	172.16.172.1			256 of 256	No	Edit		Delete	
LAN-Automa...	10.5.100.0/24	10.5.100.1	10.4.49.10	10.4.49.10	256 of 256	No	Edit		Delete	

Showing 8 of 8

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.

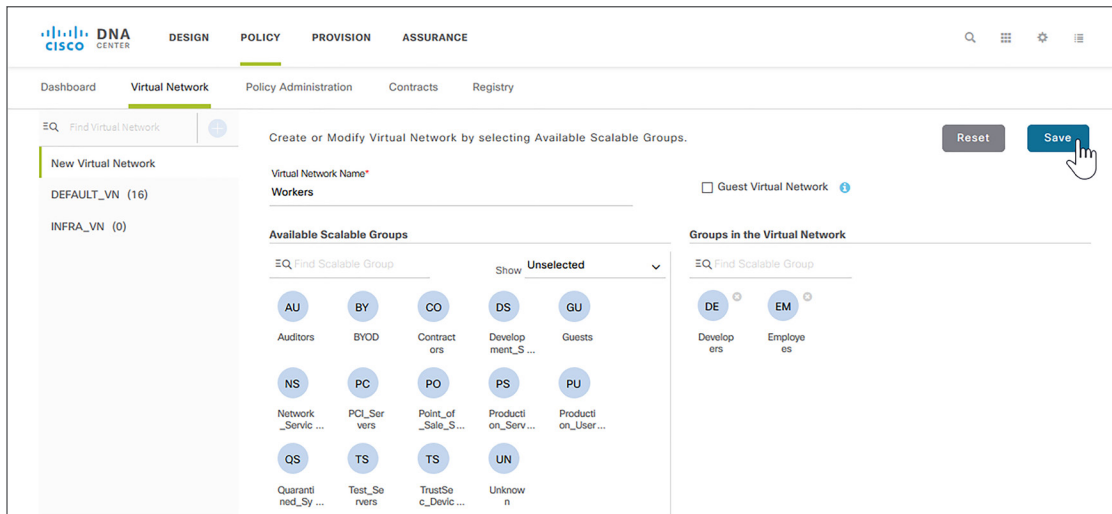
The desired outcomes of policy application using segmentation may be easily accommodated with group policies. In a university example, students and faculty machines may both be permitted to access printing resources, but student machines should not communicate directly with faculty machines, and printing 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 VNs.

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 2: From the main DNA Center dashboard, navigate to **POLICY > Virtual Network**, click the + (plus sign) to create a new virtual network, enter a **Virtual Network Name** (example: Workers), drag scalable groups from the Available Scalable Groups pool into the Groups in the Virtual Network pool (examples: Employees and Developers), 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 DNA Center and ISE is not fully operational. In this case, review the integration procedures for ISE with DNA Center and be sure to approve the pxGrid connection request in ISE from DNA Center.

Repeat this step for each overlay network, either guest or non-guest, as required. 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 within a VN from communicating with other employee devices and also from one another when a group called Quarantined_System is applied.

Step 3: From the main DNA Center dashboard, navigate to **POLICY > Policy Administration > Group-Based Access Control (Fabric)**, click **+ Add Policy**, from the **Available Scalable Groups** pane drag the **Quarantined_System** group and drop it into both the **Source** and the **Destination** panes, drag the **Employees** group into the **Destination** pane, input a **Policy Name** (example: Quarantine), enter a **Description**, select **Enable Policy**, leave **Enable Bi-directional** unselected, click **+ Add Contract**, select **deny**, click **OK**, and then click **Save**.

The policy is created and listed with a status of **DEPLOYED**. This policy is now available to be applied to fabrics that are created and is available in ISE.

<input type="checkbox"/>	Policy Name	Status	Description
<input type="checkbox"/>	Quarantine	DEPLOYED	Isolate quarantined from employees and themselves

Step 4: Log in to ISE, navigate to **Work Centers > TrustSec > TrustSec Policy**, on the left side select **Matrix**, and verify that the policy has been updated to ISE for rendering into the network.

Source	Development_Ser... 12/000C	Employees 4/0004	Guests 6/0006	Network_Serv... 3/0003	PCI_Servers 1-4/000E	Point_of_Sale_S... 10/000A	Production_Serv... 11/000B	Production_User... 7/0007	Quarantined_Sys... 255/00FF	Test_Servers 13/000D	TrustSec_Devic... 2/0002	Unknown
Destination	Development_Ser... 12/000C	Employees 4/0004	Guests 6/0006	Network_Serv... 3/0003	PCI_Servers 1-4/000E	Point_of_Sale_S... 10/000A	Production_Serv... 11/000B	Production_User... 7/0007	Quarantined_Sys... 255/00FF	Test_Servers 13/000D	TrustSec_Devic... 2/0002	Unknown
Source	Production_Serv... 11/000B	Production_User... 7/0007	Quarantined_Sys... 255/00FF	Test_Servers								

Preparing the network for automation

1. Configure underlay network device management using the 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 CLI

For maximum resiliency and bandwidth, use a loopback interface on each device and enable Layer 3 connectivity for 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 PnP onboarding.

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 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
```

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

Optional

If your underlay network is already configured as a routed access network, skip this procedure.

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 PnP 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] 255.255.255.254
```

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 49.0001.0100.0400.0001.00
metric-style wide
nsf ietf
ispf level-1-2
passive-interface loopback0
log-adjacency-changes
```

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 the area ID (**49.0001**), resulting in NET **49.0001.0100.0403.2001.00**.

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 router isis
interface range TenGigabitEthernet1/0/1-2 , TenGigabitEthernet2/0/1-2
  ip router isis
```

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, skip 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 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 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 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 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: If you skipped the procedure to interconnect the underlay devices, 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] 255.255.255.254
  ip router isis
  no shutdown
```

Step 4: Enable BGP routing to the fusion router in order to connect networks external to the fabric, and activate BGP for the connecting interfaces. You use BGP to allow 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 addresses 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 SD-Access fabric border routers require CLI configuration for BGP connectivity consistent with the border routers configured in the previous procedure. Follow this procedure at each external fusion router device that is connected to your border.

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
  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
interface TenGigabitEthernet0/1/7.100
  encapsulation dot1Q 100
  vrf forwarding VRF-GLOBAL
  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
  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 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 DNA Center manage all devices in a fabric domain. 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 DNA Center (example: hardware or software support isn't available in 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:

- Are Layer 3 devices that must be actively participating in routing within the other fabric underlay domain 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 PnP onboarding.

Procedure 7 Discover and manage network devices

You discover and manage devices in a network to be used as the underlay for an SD-Access network when DNA Center has IP connectivity to the devices and has the CLI and SNMP credentials required to manage the devices. These steps show how to initiate discovery by supplying an IP address range or multiple ranges to use to scan for network devices, which constrains the discovery and potentially saves time. Alternatively, you can supply an initial device for discovery and direct DNA Center to use Cisco Discovery Protocol to find connected neighbors.

Step 1: Navigate to the main DNA Center dashboard, and at the bottom, under the **Tools** section, click **Discovery** and fill out 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**, click + (plus sign), and then select **Use Loopback**.

Step 2: If you have any additional ranges, in the **IP Ranges** section, enter the additional range, and then click + (plus sign). Verify the credentials to be used for the discovery, and then click **Start**.

The screenshot shows the 'Discovery' configuration page in DNA Center. The 'New Discovery' form is active, showing the following details:

- Discovery Name:** First Discovery
- IP ADDRESS/RANGE:**
 - Type: Range
 - IP Ranges: 10.4.14.3 to 10.4.14.4, 10.4.14.11 to 10.4.14.11, 10.4.14.13 to 10.4.14.15, 10.4.0.1 to 10.4.0.2
 - Preferred Management IP: Use Loopback
- CREDENTIALS:**
 - CLI: dna
 - SNMPV2C READ: SNMP v2c WLAN P...
 - SNMPV2C WRITE: SNMPv2c Write

The discovery details are displayed and the discovery begins. A progress bar shows the status. During the discovery you can click the device count icon at the top of the page to see devices as they are discovered.

The screenshot shows the 'Discovery' page during an 'Initial Discovery' process. The 'Initial Discovery' card is in 'In Progress' status, showing a device count of 1. The 'DISCOVERY DETAILS' section shows CDP LEVEL: None and PROTOCOL ORDER: ssh. The 'Devices' table shows one discovered device:

IP Address	Device Name	Status	ICMP	SNMP	CLI	HTTP(S)	NETCONF
10.4.14.11	AD3-3850-1-clis	SUCCESS	✓	✓	✓	✓	✓

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

Step 4: After the discovery process finishes successfully, navigate to the main 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**.

<input type="checkbox"/>	Device Name <small>↕</small>	IP Address	Reachability Status	Up Time	Last Updated Time	Resync Interval	Last Inventory Collection Status	Location	<small>⋮</small>
<input type="checkbox"/>	AD2-3850-1.ciscodna.net <small>↗</small>	10.4.14.11	✔ Reachable	64 days, 12:15:18.24	a few seconds ago	00:25:00	Managed	Unassigned	
<input type="checkbox"/>	AD2-9300-1.ciscodna.net <small>↗</small>	10.4.14.13	✔ Reachable	56 days, 13:48:59.36	a few seconds ago	00:25:00	Managed	Unassigned	
<input type="checkbox"/>	AD2-9300-4.ciscodna.net <small>↗</small>	10.4.14.14	✔ Reachable	56 days, 9:05:05.45	a few seconds ago	00:25:00	Managed	Unassigned	
<input type="checkbox"/>	AD2-9400-1.ciscodna.net <small>↗</small>	10.4.14.15	✔ Reachable	72 days, 7:43:18.07	a minute ago	00:25:00	Managed	Unassigned	
<input type="checkbox"/>	C-ASR1K-1.ciscodna.net <small>↗</small>	10.4.0.1	✔ Reachable	57 days, 7:14:29.55	2 minutes ago	00:25:00	Managed	Unassigned	
<input type="checkbox"/>	C-ASR1K-2.ciscodna.net <small>↗</small>	10.4.0.2	✔ Reachable	57 days, 7:14:40.97	2 minutes ago	00:25:00	Managed	Unassigned	
<input type="checkbox"/>	D2-9500-1.ciscodna.net <small>↗</small>	10.4.14.3	✔ Reachable	56 days, 14:02:36.91	2 minutes ago	00:25:00	Managed	Unassigned	
<input type="checkbox"/>	D2-9500-2.ciscodna.net <small>↗</small>	10.4.14.4	✔ Reachable	56 days, 14:02:41.58	2 minutes ago	00:25:00	Managed	Unassigned	

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

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 DNA Center's LAN Automation capabilities. The device CLI and SNMP credentials to be pushed by Cisco Network Plug and Play (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 connected to devices to be discovered must be in layer-2 mode, and cannot be dedicated out-of-band (OOB) management ports on a switch.

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 away. The credentials supplied allow 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 commands:

```
crypto key zeroize
no crypto pki cert 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 systemswrite erase
reload
```

Do not save the configurations for the reload process.

Step 1: Verify that the seed devices are in the inventory and managed by DNA Center.

Step 2: Navigate to **PROVISION > Devices > Inventory**. At the top right, click **LAN Automation**, and 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 3: Click **LAN Auto Status** to view progress. Do not click **Stop** until all devices show a state of **Completed**. 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.

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 all pools need to be reachable by DNA Center to successfully complete provisioning.

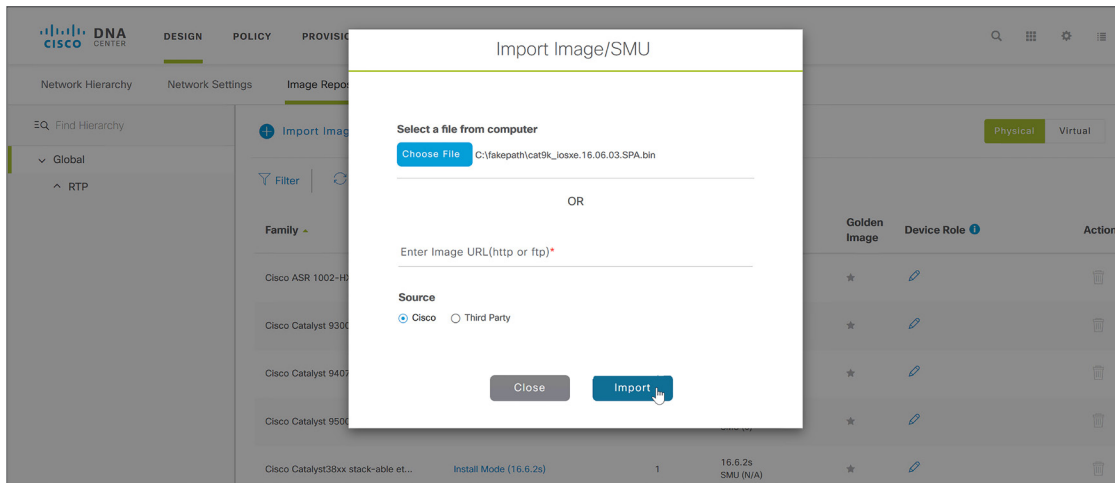
Step 4: After the devices discovered all reach **Completed** state, click **Stop**. LAN Automation tears down all Layer 2 connectivity on VLAN 1 and the underlay IS-IS routing process is used for reachability to the routed network, and devices can be managed just like other devices in the inventory.

Procedure 9 Manage software images for devices in inventory

To achieve the full capabilities of SD-Access, the SD-Access package in DNA Center has minimum software version requirements for the devices that it provisions. The software image management capability built into 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 DNA Center dashboard, click **Design**, click **Image Repository**, click **+ Import Image/SMU**, choose a file location, and then click **Import**.



The image import into DNA Center starts. Repeat this step for all images that you wish to deploy using DNA Center. Images to be used for device families not yet available in 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.

Family	Image Name	Using Image	Version	Golden Image	Device Role	Action
Cisco ASR 1002-HX Router	asr1000-universalk9.16.06.03.SP... Verified	0	16.6.3 SMU (0)	★	ALL ★	🗑️
Cisco Catalyst 9300 Switch	Install Mode (16.6.2s) cat9k_losxe.16.06.03.SPA.bin Verified	2 0	16.6.2s SMU (0) 16.6.3 SMU (0)	★ 👆	🔗 🔗	🗑️ 🗑️

Procedure 10 Use software image management to update device software

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**, select **Actions**, and then select **Update OS Image**.

The screenshot shows the Cisco DNA Center interface. The top navigation bar includes 'DESIGN', 'POLICY', 'PROVISION', and 'ASSURANCE'. The 'PROVISION' tab is active. Below the navigation, there are buttons for 'LAN Automation', 'LAN Auto Status', and a menu icon. The main content area is titled 'Device Inventory' and shows 'Inventory (8)' and 'Unclaimed Devices (0)'. A table lists devices with columns for IP Address, Site, Serial Number, Uptime, OS Version, OS Image, Sync Status, Last Provision, and Provision Status. Two devices are highlighted: AD2-38 and AD2-93. A dropdown menu is open over the 'Update OS Image' action for the first device.

Device	IP Address	Site	Serial Number	Uptime	OS Version	OS Image	Sync Status	Last Provision	Provision Status
AD2-38	10.4.14.11		FCW1950D03W, FCW1949D0AD	65 days, 4:45:35.04	16.6.2s	CAT3K_CAA[16.6.2s... Outdated	In Progress	-	Not Provisioned
AD2-93	10.4.14.13		FCW2125L109, FCW2125L12D, FCW2125L13Q	57 days, 6:25:51.78	16.6.2s	CAT9K[16.6.2s... Outdated	Managed	-	Not Provisioned

Step 2: Inspect the list of devices to be updated. If any devices do not have the appropriate resources for an upgrade, they are flagged. Fix any problems before continuing.

Figure 3. Example device with insufficient flash memory available for update

The screenshot shows the 'Update Devices' dialog box. It contains a table with the following columns: Device, Device Type, Target Image, Target Version, Target Image Size, Flash, RAM, and Reboot. One device is listed: AD2-3850-1.ciscodna.net, Switches and Hubs, cat3k_caa-universalk9..., 16.6.2s, 391 MB. The 'Flash' column has a red dot, indicating insufficient flash memory. The 'RAM' column has a green dot, and the 'Reboot' column has 'Yes'.

Device	Device Type	Target Image	Target Version	Target Image Size	Flash	RAM	Reboot
AD2-3850-1.ciscodna.net	Switches and Hubs	cat3k_caa-universalk9...	16.6.2s	391 MB	●	●	Yes

Step 3: Select all devices to update, use the default selection of **Run Now**, click **Apply**, and then at the popup warning about devices being rebooted click **OK**.

The screenshot shows the 'Update Devices' dialog box. It contains a table with the following columns: Device, Device Type, Target Image, Target Version, Target Image Size, Flash, RAM, and Reboot. Two devices are listed: AD2-3850-1.ciscodna.net and AD2-9300-1.ciscodna.net. Both have 'Flash' and 'RAM' columns with green dots, and 'Reboot' column with 'Yes'. Below the table, there is a 'When' section with 'Now' selected and 'Later' unselected. At the bottom, there are 'Cancel' and 'Apply' buttons.

Device	Device Type	Target Image	Target Version	Target Image Size	Flash	RAM	Reboot
AD2-3850-1.ciscodna.net	Switches and Hubs	cat3k_caa-universalk9...	16.6.3	391 MB	●	●	Yes
AD2-9300-1.ciscodna.net	Switches and Hubs	cat9k_iosxe.16.06.03...	16.6.3	569 MB	●	●	Yes

When
 Now Later

Cancel Apply

Images are distributed to the selected devices, and then the devices reboot to activate the new images immediately after the image distribution is complete.

Step 4: In **Inventory**, click **Refresh** to see overall upgrade status and click **Upgrade Status** to see the details for each task.

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 DNA Center and are running the appropriate software versions for SD-Access, use 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 devices and assign devices to a site for integration into an SD-Access network. ISE is updated to support the provisioning.

Tech tip

When devices are provisioned, the devices receive a number of configurations appropriate for the assigned site, including the centralized AAA server configuration, 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 centralized AAA 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 DNA Center discovery), enter the associated **Login Password** and **Re-Enter Password**, and then at the bottom of the screen click **Submit**.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The main navigation bar includes: System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, and Threat Centric NAC. The sub-navigation bar includes: Identities, Groups, External Identity Sources, Identity Source Sequences, and Settings. The left sidebar shows 'Users' and 'Latest Manual Network Scan Results'. The main content area is titled 'Network Access Users List > dna'. Under the 'Network Access User' section, the following fields are visible:

- * Name: dna
- Status: Enabled
- Email: [Empty field]

 Under the 'Passwords' section:

- Password Type: Internal Users
- Password: [Masked field]
- Re-Enter Password: [Masked field]
- * Login Password: [Masked field] with a 'Generate Password' button and an information icon.
- Enable Password: [Empty field] with a 'Generate Password' button and an information icon.

The network administrative user login is now available from ISE, in addition to the same user ID stored on each device.

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

The screenshot shows the Cisco DNA Center interface with the 'PROVISION' tab selected. The 'Device Inventory' section displays a table of devices. The 'Actions' menu is open, and the 'Provision' option is highlighted. The table contains the following data:

Device	IP Address	Site	Serial Number	Uptime	OS Version	OS Image	Sync Status	Last Provision	Provision Status
AD2-38	10.4.14.11		FCW1950D03W, FCW1949D0AD	4:58:03.90	16.6.3	CAT3K_CAA[16...	Managed	-	Not Provisioned
AD2-93	10.4.14.13		FCW2125L109, FCW2125L12D, FCW2125L13Q	5:18:35.42	16.6.3	CAT9K[16.6.3]	Managed	-	Not Provisioned

A **Provision Devices** wizard screen appears.

Tech tip

Devices must be of the same type (example: all switches) 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**.

The screenshot shows the 'Assign Site' step of the provisioning wizard. The screen displays a list of devices with their serial numbers and site assignments. The 'Apply to All' checkbox is checked. The table contains the following data:

Serial Number	Devices	Choose a site
FCW2122A2V5	D2-9500-2.ciscodna.net	...TP/RTP5-C9K x v
FCW2122A4JG	D2-9500-1.ciscodna.net	...TP/RTP5-C9K x v
FXS2131Q3WV	AD2-9400-1.ciscodna.net	...TP/RTP5-C9K x v
FCW2125L0B7, FCW2125L	AD2-9300-4.ciscodna.net	...TP/RTP5-C9K x v
FCW2125L109, FCW2125L	AD2-9300-1.ciscodna.net	...TP/RTP5-C9K x v
FCW1950D03W, FCW1949	AD2-3850-1.ciscodna.net	...TP/RTP5-C9K x v

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 pop-up 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**. As a result of the DNA Center pxGrid integration with ISE, the network devices also appear in ISE.

Step 6: Verify the ISE integration function by logging into ISE and navigating to **Administration > Network Resources > Network Devices**. The provisioned devices appear.

Name	IP/Mask	Profile Name	Location	Type
AD2-3850-1.ci...	10.4.14.11/32	Cisco	All Locations	All Device Types
AD2-9300-1	10.4.14.13/32	Cisco	All Locations	All Device Types
AD2-9300-4	10.4.14.14/32	Cisco	All Locations	All Device Types
AD2-9400-1	10.4.14.15/32	Cisco	All Locations	All Device Types
D2-9500-1.cis...	10.4.14.3/32	Cisco	All Locations	All Device Types
D2-9500-2.cis...	10.4.14.4/32	Cisco	All Locations	All Device Types

Process

Provisioning an SD-Access overlay network

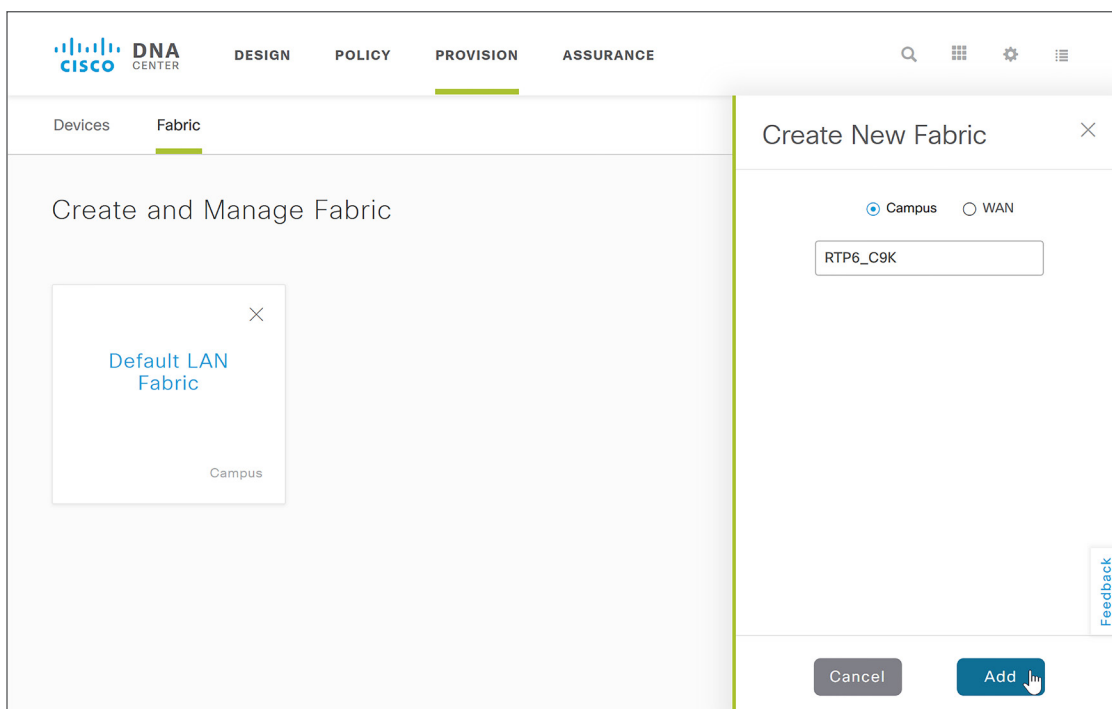
1. Create a fabric domain and add provisioned network devices
2. Enable eBGP connectivity for VN at neighbor (fusion) to border router
3. Assign wired clients to VN and enable connectivity
4. Enable fabric edge ports for client onboarding
5. Enable multicast for fabric

Create a fabric overlay network using the provisioned SD-Access underlay network devices.

Procedure 1 Create a fabric domain and add provisioned network devices

A fabric domain called **Default LAN Fabric** is automatically created by DNA Center, containing provisioned devices ready to be assigned to a fabric. Create a new campus fabric domain and assign the appropriate devices to it. Campus fabric domains are used in the SD-Access 1.1 solution, enabling client endpoints to connect to wired and wireless LAN networks.

Step 1: Using DNA Center, navigate to **PROVISION > Fabric**, click **+ Add**, leave the default **Campus** selection, supply a fabric name (example: RTP6_C9K), and then click **Add**.



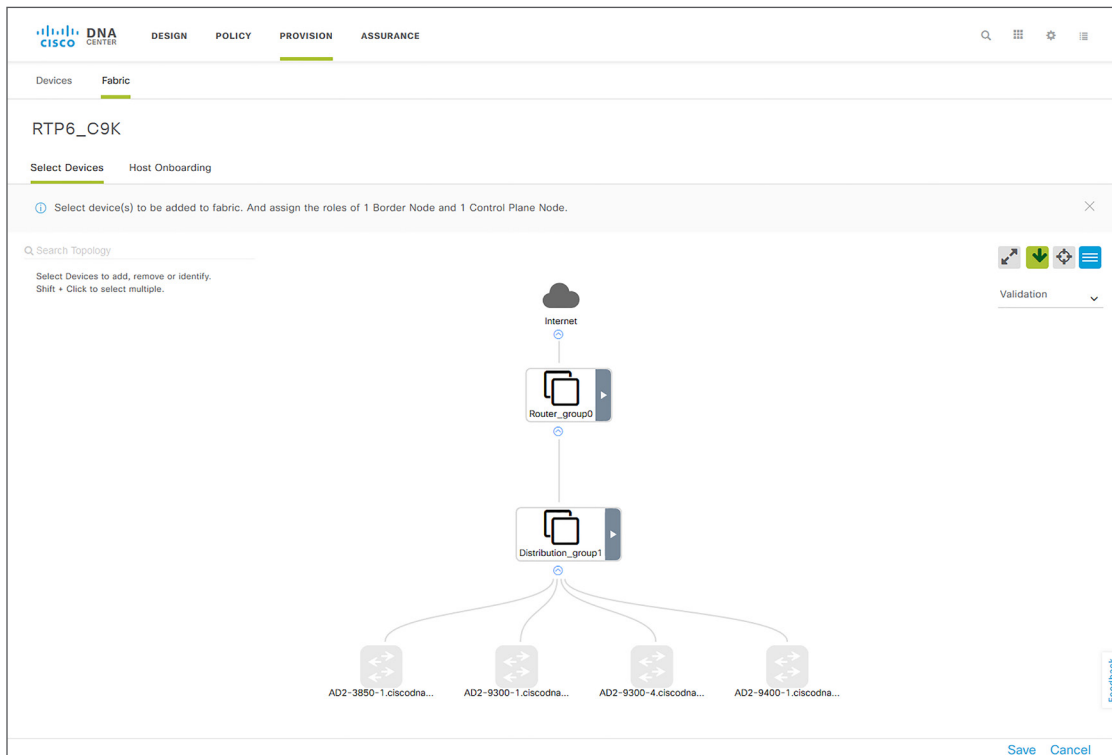
The new campus fabric domain is created.

Tech tip

All devices appear across all fabric domains. The fabric is defined within a domain by assigning fabric functionality to devices and requires at least one instance of each of the fabric functions: edge node, border node, and control plane. The roles may be combined (example: control plane and border node) as permitted by the SD-Access solution being deployed.

Step 2: Click the icon for the fabric domain you just created (example: RTP6_C9K). The fabric **Select Devices** wizard starts.

Step 3: If the 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 clicking each device, on the pop-up menu select **Device Role**, inspect its network role, and then either change the role and click **Save**, or if the role is correct select **Cancel**. When the device roles are complete an appropriate topology is displayed. The topology can be reoriented by clicking the green arrow button.



Step 4: Hold the shift key and click all of the nodes that are fabric edge nodes, and then in the pop-up box, click **Add to Fabric**.

Step 5: 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 pop-up 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 Nexus 7700 Series 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 6: Click a device to perform the fabric border role, in the pop-up 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** dropdown to select the Global pool configured previously in the guide for border connectivity functionality, and then next to **External Interface** click **+ Add Interface**.

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 7: Select the interface for the connection to the fusion router outside of the fabric, fill in the BGP **Remote AS Number** for the device outside of the fabric (example: 65500), select **Virtual Network** and all VNs to include in the Layer 3 handoff outside the fabric, click **Save**, and then click **Add**.

The screenshot displays the Cisco DNA Center Provisioning interface. On the left, a network topology diagram shows a central 'Router_group0' connected to an 'Internet' cloud. Below it, two border nodes 'D2-9500-1.ciscodna...' and 'D2-9500-2.ciscodna...' are connected to four leaf nodes: 'AD2-3850-1.ciscodna...', 'AD2-9300-1.ciscodna...', 'AD2-9300-4.ciscodna...', and 'AD2-9400-1.ciscodna...'. On the right, a configuration dialog for 'D2-9500-1.ciscodna.net' is open. The dialog includes the following fields and options:

- Border to:** Radio buttons for 'Rest of Company (Internal)', 'Outside World (External)' (selected), and 'Anywhere (Internal & External)'.
- BGP:** A dropdown menu.
- Local AS Number:** A text field containing '65514'.
- Border Handoff:** A dropdown menu set to 'Layer 3'.
- VRF-Lite:** A dropdown menu.
- Border-Handoff (172.16.172.0/24):** A dropdown menu.
- External Interface:** A section with a '+ Add Interface' button.
- Interface:** A table with columns 'Interface' and 'Number of VN'. The table contains one row: 'FortyGigabitEthernet1/0/24' with a value of '3' in the 'Number of VN' column. A 'Remove' button is next to the row.

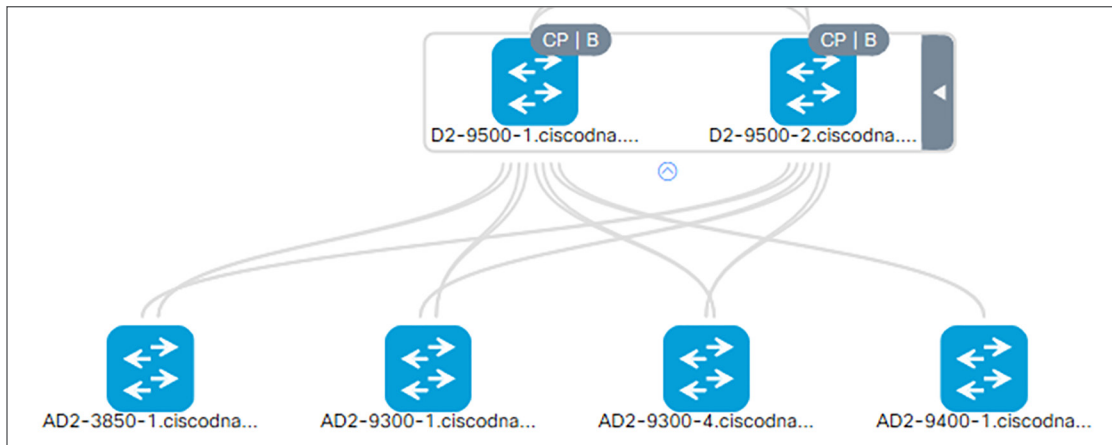
At the bottom of the dialog, there are 'Cancel!' and 'Add' buttons. A mouse cursor is pointing at the 'Add' button.

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 8: 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.



Procedure 2 Enable eBGP connectivity for VN at neighbor (fusion) to border router

The SD-Access application in 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. For AP and other infrastructure onboarding, you use the routing information from the BGP peer for the DEFAULT_VN, highlighted in the example below.

Example subset of border node configuration pushed by DNA Center SD-Access application

```
vrf definition DEFAULT_VN
  rd 1:4098
  !
  address-family ipv4
    route-target export 1:4098
    route-target import 1:4098
  exit-address-family
  !
vrf definition Workers
  rd 1:4099
  !
  address-family ipv4
    route-target export 1:4099
    route-target import 1:4099
  exit-address-family
```

```
!  
interface Vlan3001  
  description vrf interface to External router  
  ip address 172.16.172.1 255.255.255.252  
  no ip redirects  
  ip route-cache same-interface  
!  
interface Vlan3002  
  description vrf interface to External router  
  vrf forwarding Workers  
  ip address 172.16.172.5 255.255.255.252  
  no ip redirects  
  ip route-cache same-interface  
!  
interface Vlan3003  
  description vrf interface to External router  
  vrf forwarding DEFAULT_VN  
  ip address 172.16.172.9 255.255.255.252  
  no ip redirects  
  ip route-cache same-interface  
!  
router bgp 65514  
  bgp router-id interface Loopback0  
  bgp log-neighbor-changes  
  neighbor 10.4.2.65 remote-as 65500  
  neighbor 10.4.14.4 remote-as 65514  
  neighbor 10.4.14.4 update-source Loopback0  
  neighbor 172.16.172.2 remote-as 65500  
  neighbor 172.16.172.2 update-source Vlan3001
```

```
!  
address-family ipv4  
  network 10.4.14.3 mask 255.255.255.255  
  aggregate-address 10.4.14.0 255.255.255.0 summary-only  
  redistribute isis level-2  
  redistribute lisp metric 10  
  neighbor 10.4.2.65 activate  
  neighbor 10.4.14.4 activate  
  neighbor 172.16.172.2 activate  
  neighbor 172.16.172.2 weight 65535  
exit-address-family  
!  
address-family ipv4 vrf DEFAULT_VN  
  redistribute lisp metric 10  
  neighbor 172.16.172.10 remote-as 65500  
  neighbor 172.16.172.10 update-source Vlan3003  
  neighbor 172.16.172.10 activate  
  neighbor 172.16.172.10 weight 65535  
exit-address-family  
!  
address-family ipv4 vrf Workers  
  redistribute lisp metric 10  
  neighbor 172.16.172.6 remote-as 65500  
  neighbor 172.16.172.6 update-source Vlan3002  
  neighbor 172.16.172.6 activate  
  neighbor 172.16.172.6 weight 65535  
exit-address-family  
!
```

The deployed configuration includes VRF, VLAN, and BGP elements similar to the ones shown in the above configuration example; however, the VLANs deployed will likely be different.

Step 9: Login to border devices and use the CLI to observe the automated configurations created by the SD-Access 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

There are other important additions to the configuration, which are handled completely by the automation. If you are interested in observing additional LISP fabric control plane changes, use the following command:

```
show running-config | section LISP|lisp|site
```

Step 10: Login to the fusion devices external to the fabric that are 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.

Step 11: Configure each interface to the neighbor. Some devices support VLAN subinterface configuration directly on trunks, and other devices require VLAN interfaces to be created and associated with a trunk. Repeat the neighbor interface configuration for each neighbor on each peer to the border.

```
interface [Peer interface]
```

Step 12: Configure BGP IPv4 unicast routing towards the fusion router 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
```

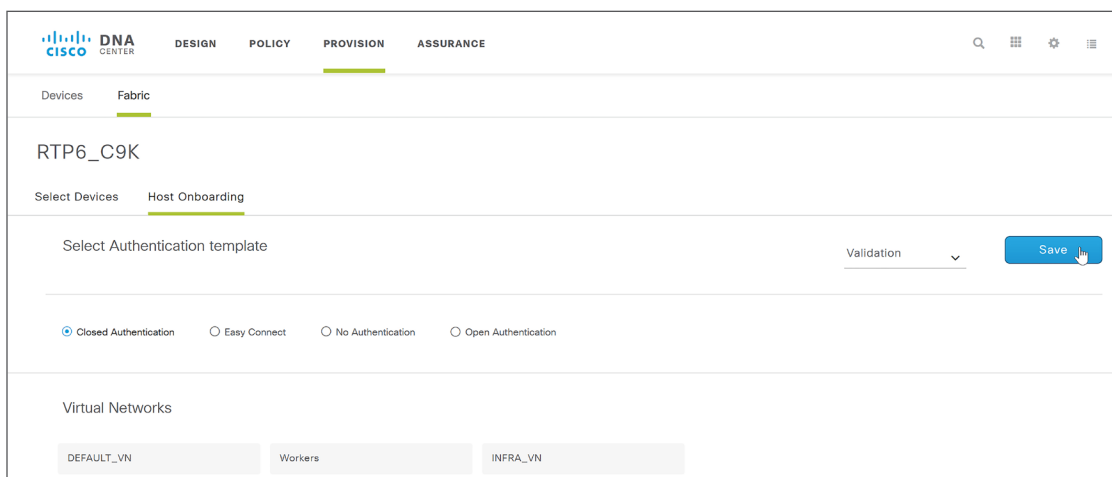
```

!
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 3 Assign wired clients to VN and enable connectivity

Step 1: From the DNA Center dashboard, navigate to **PROVISION > Fabric > Host Onboarding**, under **Select Authentication template** select **Closed Authentication**, at the top of the section click **Save**, and then click **Apply**.



Step 2: Under **Virtual Networks**, select a VN to be used for wired clients (example: Workers), in the **Edit Virtual Network:Workers** slide-out pane, select the names of **IP Pools** to add to the VN (example: 14-Employee), select **Traffic Type** of **Data**, change **Layer 2 Extension** to **Off**, and then click **Update**.

Layer 2 extension is only supported with wireless in SD-Access solution 1.1.

IP Pool Name	Traffic Type	Address Pool	Layer-2 Extension
<input checked="" type="checkbox"/> 14-Employee	Data	10.101.114.0/24	<input type="checkbox"/> Off
<input type="checkbox"/> 14-Guest	Choose Traffic	10.103.114.0/24	<input type="checkbox"/> On
<input type="checkbox"/> 14-Phone	Choose Traffic	10.101.214.0/24	<input type="checkbox"/> On
<input type="checkbox"/> 14-Things	Choose Traffic	10.102.114.0/24	<input type="checkbox"/> On
<input type="checkbox"/> 14-Underlay	Choose Traffic	10.4.14.0/24	<input type="checkbox"/> On
<input type="checkbox"/> Access-Point	Choose Traffic	172.16.173.0/24	<input type="checkbox"/> On

Step 3: At the **Modify Authentication Template** slideout, keep the default **Run Now** selection, and then click **Apply**.

Procedure 4 Enable fabric edge ports for client onboarding

Repeat this procedure for each fabric edge switch where clients are connecting.

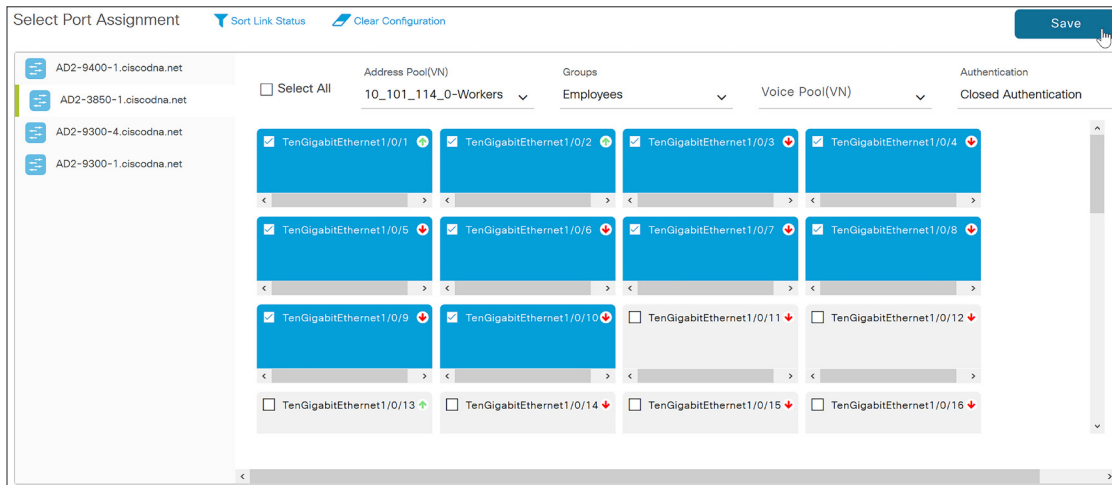
Step 1: Navigate to **PROVISION > Fabric > Host Onboarding**. Under **Select Port Assignment** in the left column, select a switch.

Step 2: At the top of the list of switch ports on the right, select the **Address Pool(VN)** (example: 10_101_114_0-Workers). Optionally select an appropriate group from **Groups** (example: Employees), optionally select a Voice Pool(VN) to use for IP telephones, and then select the **Authentication** (example: Closed Authentication).

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, DNA Center pushes the global default authentication template chosen in the “Select Authentication template” section at the top of the screen. DNA Center pushes a port configuration when “Closed Authentication” is configured.

Step 3: Within the list of switch ports, select every wired fabric edge port to participate in the fabric VN, click **Save**, and then click **Apply**.



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

Example port configuration pushed by DNA Center using closed authentication

```
interface GigabitEthernet1/0/23
  switchport access vlan 1032
  switchport mode access
  switchport voice vlan 1030
  load-interval 30
  authentication control-direction in
  authentication event server dead action authorize vlan 3999
  authentication event server dead action authorize voice
  authentication host-mode multi-auth
  authentication order dot1x mab
  authentication priority dot1x mab
  authentication port-control auto
  authentication periodic
  authentication timer reauthenticate server
  authentication timer inactivity server dynamic
  mab
  no macro auto processing
  dot1x pae authenticator
  dot1x timeout tx-period 10
  spanning-tree portfast
```


Procedure 5 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: Add a global pool in DNA Center that is dedicated for unicast IP interfaces used to enable multicast for each VN where multicast is enabled. Navigate to **DESIGN > Network Settings > IP Address Pools**. In the site hierarchy on the left, select **Global**. Click **+ Add IP Pool**, and fill in the IP Pool Name, IP Subnet, CIDR Prefix, and Gateway IP address. Assign DHCP Server(s) and DNS Server(s). Do not select **Overlapping**. When you are done, click **Save**.

Step 2: Using DNA Center, navigate to **PROVISION > Fabric**, and click the icon for the fabric domain. The fabric **Select Devices** wizard starts.

Step 3: Right-click on a fabric border node and select **Enable Rendezvous Point**. Within the **Associate Multicast Pools to VNs** popup window at the right, under **Associate Virtual Networks**, choose the VN. Under **Select IP Pools**, choose the pool created for multicast, and click the plus sign to add the pool to the list. 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**.

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
```

Integrating wireless into SD-Access

1. Add the wireless controllers into inventory and create an HA SSO pair
2. Create IP 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 SD-Access wireless LAN controllers is completed as part of previous procedures and the controllers are available to integrate into the fabric using DNA Center.

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

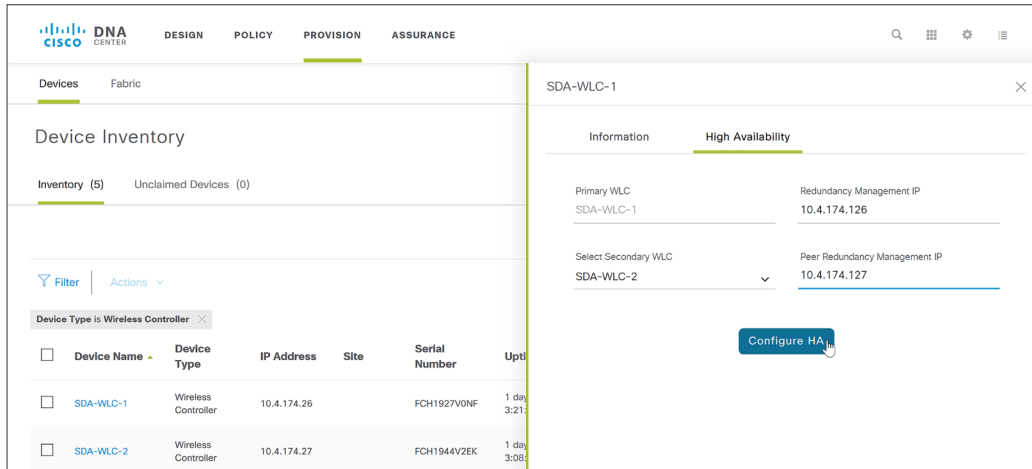
If the wireless LAN controllers are not in the DNA Center inventory, you must add them before the wireless integration, and create an HA SSO pair.

Step 1: Navigate to the main 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, 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 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, go to the main 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 **Configure 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 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 dropdown for the device to mark the image golden.

In the validated version, an external SFTP server is required for upgrading WLC devices directly from the DNA Center Image Repository. For expediency, the next step shows an easy alternative to upgrade without an available SFTP server.

Step 5: Use a web browser to view the WLC main page (example: <https://10.4.174.26>), navigate to **COMMANDS > Download File**, select **File Type**, **Transfer Mode**, and **File Name** (example: Code, HTTP, AIR-CT5520-K9-8-5-131-0.aes), click **DOWNLOAD**, and then click **OK**. A progress status notification appears. Follow the instructions displayed to complete the upgrade.

Procedure 2 Create IP pools for access points

Verify that a global pool in 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**.

Procedure 3 Design fabric enterprise wireless SSIDs

Step 1: From the main 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**
- 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/Main Floor)

Step 3: 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 to the WLC.

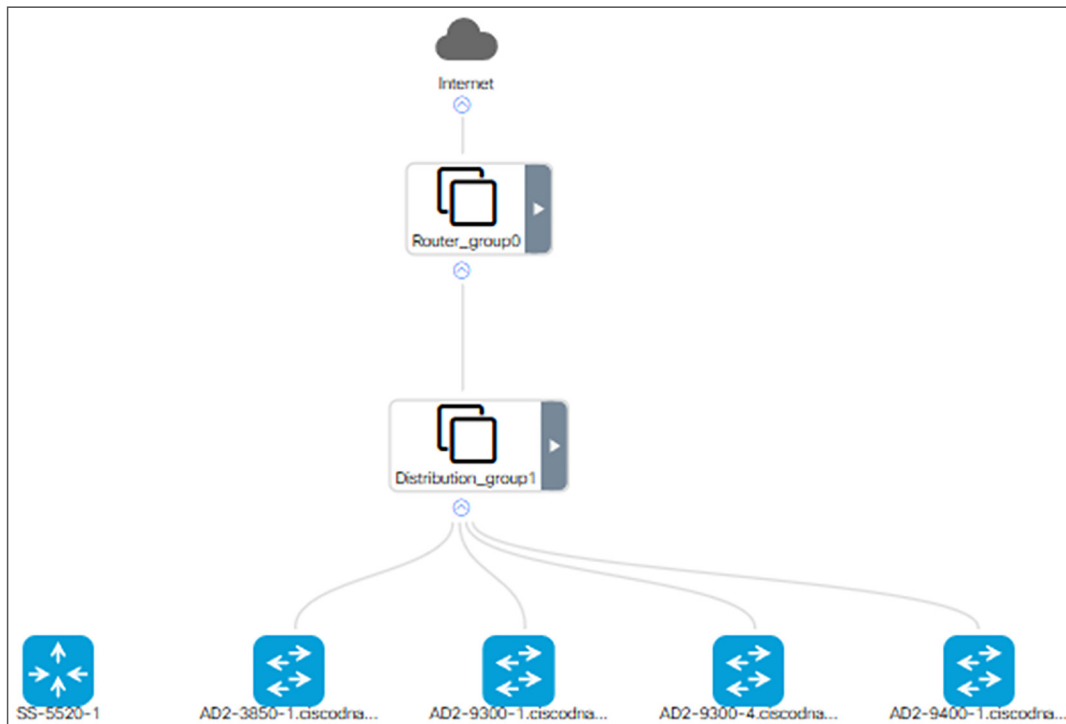
Step 1: Navigate to **PROVISION > Devices**, find the WLC and select the checkbox next to it, and then at the top of the screen under the **Actions** pull-down, select **Provision**. The **Provision Devices** wizard opens.

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/Main Floor), 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 **Run 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: Navigate to **PROVISION > Fabric**, click the fabric domain where the WLC is to be added (example: RTP6_C9K), click the WLC, in the popup box select **Add to Fabric**, click **Save**, in the slide-out menu keep the default selection **Run 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.

The screenshot shows the Cisco WLC management console interface. The top navigation bar includes 'MONITOR', 'WLANS', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The left sidebar shows the 'Controller' menu with options like 'General', 'Icons', 'Inventory', 'Interfaces', 'Interface Groups', 'Multicast', 'Network Routes', 'Fabric Configuration', 'Redundancy', and 'Mobility Management'. The main content area is titled 'Fabric Control Plane Configuration' and features an 'Apply' button. The 'Fabric' status is 'Enabled'. Under the 'Enterprise' section, the 'Primary IP Address' is 10.4.14.3 and the 'Secondary IP Address' is 10.4.14.4, both with 'Up' connection status. Under the 'Guest' section, the 'Primary IP Address' and 'Secondary IP Address' fields are empty, and the connection status is not shown.

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: Navigate to **PROVISION > Fabric**, select the fabric, and then click **Host Onboarding**.

Step 3: Under **Select Authentication template**, select **No Authentication**, click **Save**, in the slide-out panel keep the default selection **Run Now** and then click **Apply**.

The authentication template is applied to the fabric, and automatic onboarding of APs is enabled.

Tech tip

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 DNA Center to assign a port to the IP address pool for the APs.

Step 4: Under **Virtual Networks**, select **INFRA_VN**, click the check box next to the IP Pool Name for the APs (example: Access-Point), click Update, in the slide-out panel keep the default selection **Run Now**, and then click **Apply**.

The screenshot shows the Cisco DNA Center interface with the 'Edit Virtual Network: INFRA_VN' panel open. The panel displays a table of IP Pool Names and their associated configurations. The 'Access-Point' entry is selected, and the 'Update' button is highlighted.

IP Pool Name	Address Pool	AP Provision Pool	Layer-2 Extension
<input type="checkbox"/> 14-Employee	10.101.114.0/24	<input type="checkbox"/> On	<input type="checkbox"/> On
<input type="checkbox"/> 14-Guest	10.103.114.0/24	<input type="checkbox"/> On	<input type="checkbox"/> On
<input type="checkbox"/> 14-Things	10.102.114.0/24	<input type="checkbox"/> On	<input type="checkbox"/> On
<input type="checkbox"/> 14-Underlay	10.4.14.0/24	<input type="checkbox"/> On	<input type="checkbox"/> On
<input checked="" type="checkbox"/> Access-Point	172.16.173.0/24	<input type="checkbox"/> On	<input type="checkbox"/> On
<input type="checkbox"/> Border-Handoff	172.16.172.0/24	<input type="checkbox"/> On	<input type="checkbox"/> On

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

Step 6: Navigate to the main DNA Center dashboard, **PROVISION > Devices > Inventory**, select the APs being added, at the top in the **Actions** pulldown menu, select **Provision**, assign the APs to a floor (example: Global/RTP/RTP5-C9K/Main Floor), click **Next**, for **RF Profile** select **TYPICAL**, click **Next**, at the **Summary** page click **Deploy**, and then in the slide-out panel, click **Apply** and acknowledge any warnings about reboots.

Procedure 7 Assign wireless clients to VN and enable connectivity

Step 1: Navigate to **PROVISION > Fabric > Host Onboarding**, select a VN to be used for clients (example: Guest), in the **Edit Virtual Network: Guest** slide-out pane, select the names of **IP Pools** to add to the VN (example: 14-Guest), select **Traffic Type** of **Data**, verify **Layer-2 Extension** is **On**, and then click **Update**.

Tech tip

Selecting **Layer-2 Extension** enables the SD-Access LISP control plane to learn MAC addresses, which is required for wireless clients.

IP Pool Name	Traffic Type	Address Pool	Layer-2 Extension
<input type="checkbox"/> 14-Employee	Choose Traffic	10.101.114.0/24	<input type="button" value="Off"/>
<input checked="" type="checkbox"/> 14-Guest	Data	10.103.114.0/24	<input checked="" type="button" value="On"/>
<input type="checkbox"/> 14-Things	Choose Traffic	10.102.114.0/24	<input type="button" value="Off"/>
<input type="checkbox"/> 14-Underlay	Choose Traffic	10.4.14.0/24	<input type="button" value="Off"/>
<input type="checkbox"/> Access-Point	Choose Traffic	172.16.173.0/24	<input type="button" value="Off"/>
<input type="checkbox"/> Border-Handoff	Choose Traffic	172.16.172.0/24	<input type="button" value="Off"/>

Step 2: Under the **Modify Authentication Template** slideout, keep the default **Run Now** selection, and then click **Apply**.

Step 3: In the **Wireless SSID's** section, for each **SSID Name**, under **Address Pool**, select the appropriate **IP Address Pool**, click **Save**, 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. Additional hardware options are listed in the associated [Software-Defined Access Design Guide](#), and updated DNA Center package files are regularly released and available within the packages and updates listings.

DNA Center

Functional area	Product	Part number	Software version
Network Automation	Cisco DNA Center Appliance	DN1-HW-APL	1.1.8 (System Update 1.0.4.855)

DNA Center packages

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

Package	Version
Assurance - Base	1.1.8.1205
Assurance - Path Trace	2.1.12.60016
Assurance - Sensor	1.1.5.40
Automation - Application Policy	2.1.10.170000
Automation - Base	2.1.12.60016
Automation - Device Onboarding	2.1.12.60016
Automation - Image Management	2.1.12.60011
Automation - SD-Access	2.1.12.60016
Automation - Sensor	2.1.9.60029
Command Runner	2.1.9.60029
NCP - Base	2.1.9.60029
NCP - Services	2.1.12.60011
Network Controller Platform	2.1.12.60011
Network Data Platform - Base Analytics	1.0.7.906
Network Data Platform - Core	1.0.7.862
Network Data Platform - Manager	1.0.7.969

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 3850XSswitches (10-Gbpsfiber)	16.6.4
Border and control plane	Cisco 4000 Series Integrated Services Routers	16.6.3
Border and control plane–large scale	Cisco ASR 1000-X and 1000-HX Series Aggregation Services Routers	16.6.3
Border (wired-only control plane option)	Cisco Catalyst 68077–slot chassis with Supervisor Engine 6T or Supervisor Engine 2T and 6800 32–port 10GE with dual integrated DFC4	15.5(1)SY1
Border (wired-only control plane option)	Cisco Catalyst 6880-X and 6840-X switches	15.5(1)SY1
Border	Cisco Nexus 7700 switches 2–slot chassis with Supervisor2 Enhanced module and Cisco Nexus 7700 M3–Series 48–port 1/10 Gigabit Ethernet module	8.2(1) + SMU
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

Functional area	Product	Software version
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–Cisco Validated Design verified (not inclusive of all possibilities)

Product	PnP roles tested (discovered devices directly attached to seeds)
Cisco Catalyst 9500 Series (standard performance versions)	Seed device
Cisco Catalyst 3850XSswitches(10Gbpsfiber)	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.

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2018 Cisco Systems, Inc. All rights reserved.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)