Software-Defined Access & Cisco DNA Center Management Infrastructure

Solution Adoption Prescriptive Reference Deployment Guide

October, 2019

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

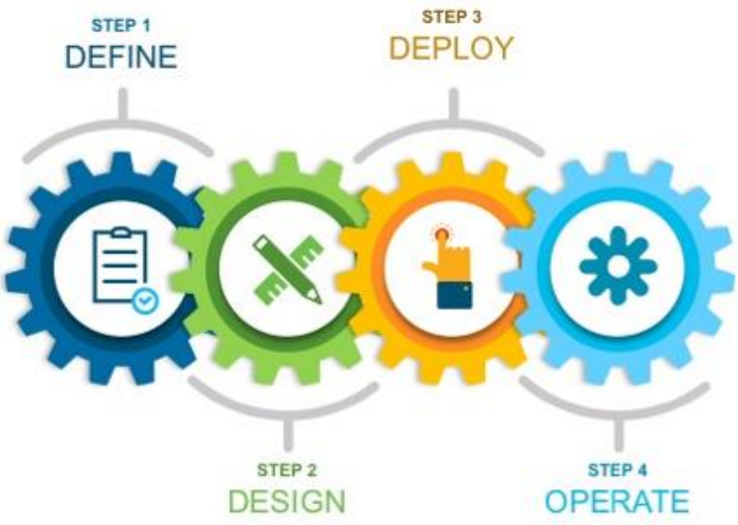
Contents

Hardware and Software Version Summary

Table 1. Hardware and software version summary

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

About this Guide



This guide contains four major sections:

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

The **DESIGN** section shows the deployment topology and discusses additional network planning items needed in advance of the deployment.

The **DEPLOY** section provides information and steps for the various workflows to install and bootstrap Cisco DNA Center, an AireOS Wireless LAN Controller, and Cisco Identity Services Engine.

The **OPERATE** section demonstrates the steps necessary to integrate Cisco DNA Center and Cisco Identify Services Engine once both have been installed and have basic network configuration.

Define

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

About SD-Access & Cisco DNA Center

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

This guide is used to deploy the management infrastructure, including Cisco DNA Center, Cisco Identity Services Engine (ISE), and Cisco Wireless LAN Controllers (WLC), described in the companion Software-Defined Access Solution Design Guide. The deployment described in this guide is used in advance of deploying a Cisco Software-Defined Access fabric, as described in the companion Software Defined Access Fabric Deployment Guide.

Companion Resources

Find the companion Software-Defined Access Solution Design Guide, Software-Defined Access Medium and Large Site Fabric Provisioning Prescriptive Deployment Guide, Software-Defined Access for Distributed Campus Prescriptive Deployment Guide, related deployment guides, design guides, and white papers, at the following pages:

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

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

Scale Metrics and Latency Information

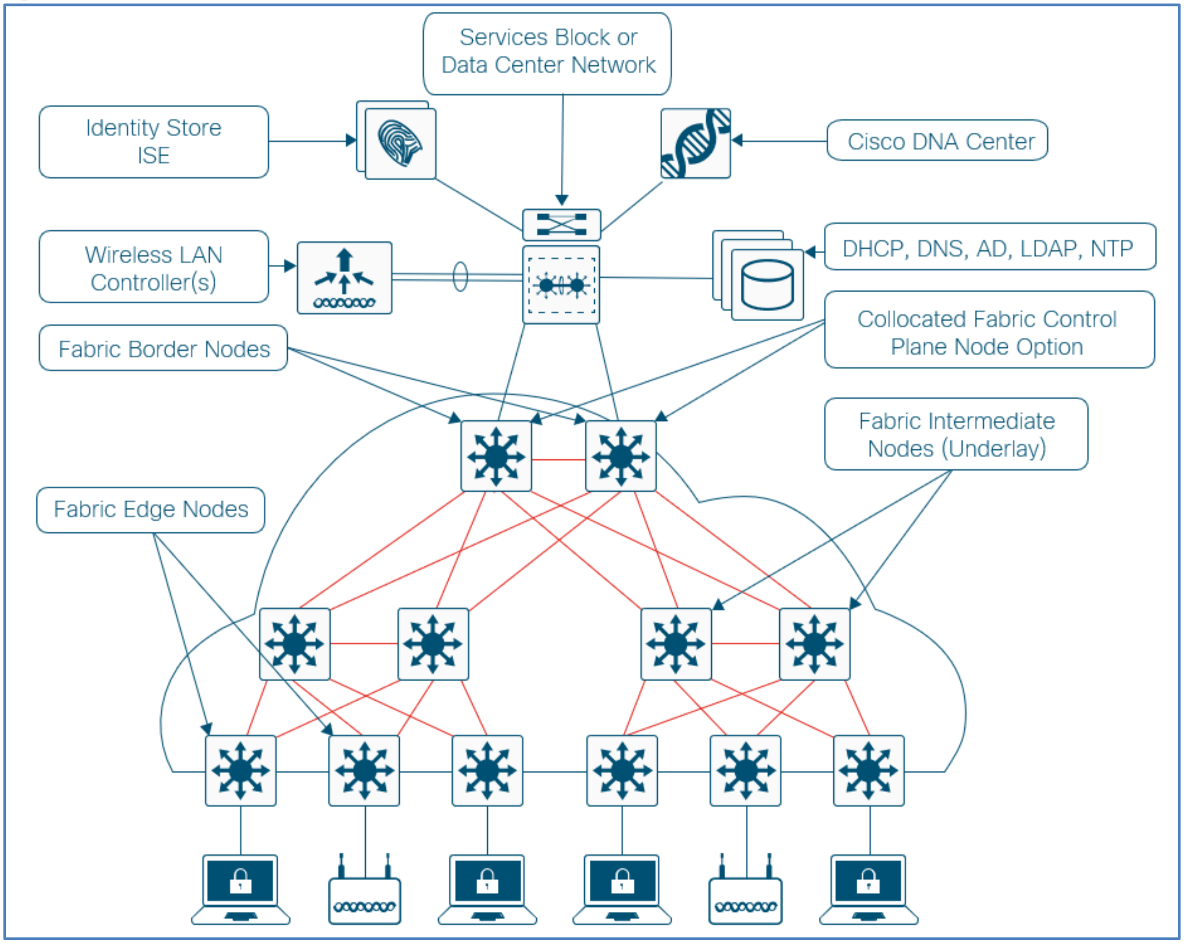
For scale metrics and latency information, please see the SD-Access Resources and Latency Design Guidance on Cisco Communities.

Design

This section provides an overview of the topology used throughout this guide. Additional network planning items for Cisco DNA Center and for the management infrastructure are discussed.

Topology Overview

Figure 1. Design topology


Services Block or Data Center Network
Identity Store ISE
Cisco DNA Center
Wireless LAN Controller(s)
DHCP, DNS, AD, LDAP, NTP
Collocated Fabric Control Plane Node Option
Fabric Border Nodes
Fabric Intermediate Nodes (Underlay)
Fabric Edge Nodes

The Cisco SD-Access management infrastructure solution described uses a single Cisco DNA Center hardware appliance, installed initially as a single-node cluster and then expanded into a three-node cluster as an option. For this solution, the Cisco DNA Center software integrates with two Cisco ISE nodes configured for redundancy and dedicated to the Cisco SD-Access deployment, as detailed in the installation. To support Cisco SD-Access Wireless, the solution includes two Cisco WLCs for controller redundancy

Network Planning Considerations and Requirements

Before you begin, you must identify the following:

- IP addressing and network connectivity for all controllers being deployed: Cisco DNA Center must have Internet access for system updates from the Cisco cloud catalog server.
- A network-reachable Network Time Protocol (NTP) server, used during Cisco DNA Center installation to help ensure reliable digital certificate operation for securing connections.

- Network-reachable Domain Name System (DNS) server used during installation and Day N operations. The configured DNS servers cannot be changed after installation.
- Certificate server information, when self-signed digital certificates are not used.

Deploy

This section provides the workflow to install Cisco DNA Center, Cisco Wireless LAN Controller, and Cisco Identity Services engine and configure basic IP connectivity for this infrastructure. The basically installation for Cisco DNA Center is shown for both a single-node and a three-node (HA) cluster. Finally, an example demonstrates how to cloud upgrade Cisco DNA Center.

How to read deployment commands

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

Commands to enter at a CLI prompt:

```
configure terminal
```

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

```
ntp server 10.4.0.1
```

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

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

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

```
Router# enable
```

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

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

Process 1: Installing Cisco DNA Center

The Cisco DNA Center appliance has 10-Gbps SFP+ modular LAN on motherboard (mLOM) interfaces and integrated copper interfaces, and available for network connectivity. The M5-based appliances uses PCIe interfaces rather than mLOM. Use the following table to assist with IP address assignment and connections. The validation starts with a single-node cluster that uses a virtual IP (VIP) configured on a single Cisco DNA Center appliance, easing future migration to a three-node cluster. The update from a single-node cluster to a three-node cluster is described.

For provisioning and assurance communication efficiency, Cisco DNA Center should be installed in close network proximity to the greatest number of devices being managed. The latency RTT (round-trip-time) between Cisco DNA Center and the network devices it manages must be taken into consideration. The optimal RTT should be less than 100 milliseconds to achieve optimal performance. Latency RTT of up to 200ms is support.

Both single-node cluster and three-node cluster configurations require the reserved IP address space for internal application services within the appliance and for communication among its internal infrastructure services. These are referred to in the installation wizard as the Cluster Services and Cluster Services Subnets. Reserve an arbitrary private IP space at least 20 bits of netmask in size that is not used elsewhere in the enterprise network (example: 192.168.240.0/20). Divide the /20 address space into two /21 address spaces (examples: 192.168.240.0/21, 192.168.248.0/21) and use them in a later setup step for services communication among the processes running in a Cisco DNA Center instance.

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

Caution

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

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

The validated installation process uses a DN2-HW-APL-L appliance. If you are using an appliance with a different physical interface structure, such as the DN1-HW-APL appliance, the Maglev Configuration wizard steps for interface configuration display with different names and in a different order. Details for other appliances are also shown in the release notes.

The 10-Gbps ports on the original M4-based appliance are reversed left-to-right from the more recent M5-based appliance, and the location of the on-board copper Ethernet ports are in different locations. The M4 appliance uses an 802.1q header tag with VLAN ID 0, requiring IOS-XE switches to use an interface configuration supporting the tagged configuration (switchport voice vlan dot1p) and operating as a trunk, whereas an M5-based appliance requires a basic interface access VLAN configuration for the Ethernet switch connection, as described in the associated installation guides.

Figure 2.
Figure 2 Rear view of the original Cisco DNA Center appliance — DN1-HW-APL (M4-based)

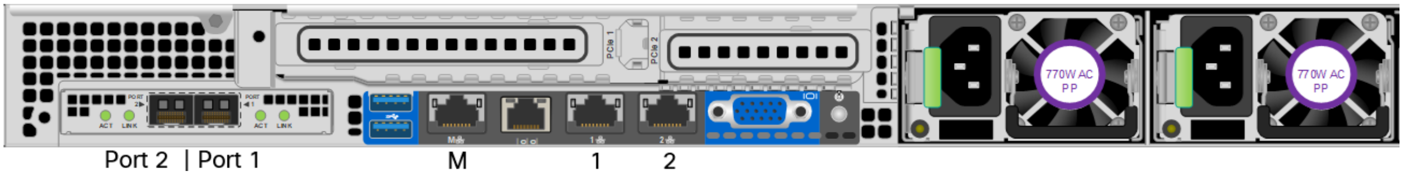


Figure 3.
Figure 3 Rear view of the Cisco DNA Center appliance — DN2-HW-APL (M5-based)

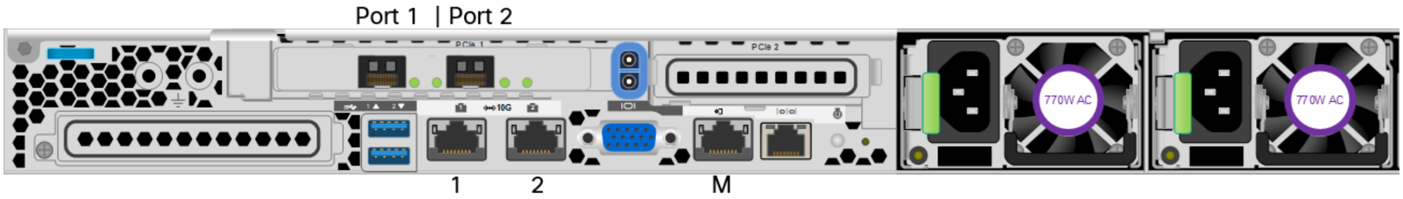


Table 2. Cisco DNA Center server LAN Ethernet interface assignments

	PORT 1 mLOM/PCIe SFP+ 10 Gbps	PORT 2 mLOM/PCIe SFP+ 10 Gbps	1 Integrated RJ-45 1 Gbps	2 Integrated RJ-45 1 Gbps	M (or "gear" label) RJ-45 1 Gbps
Wizard name when using DN2-HW-APL, DN2-HW-APL-L	`enp94s0f0`	`enp94s0f1`	`eno1`	`eno2`	—
Wizard name when using DN1-HW-APL	`enp9s0`	`enp10s0`	`enp1s0f0`	`enp1s0f1`	—
Use	Enterprise: Enterprise network infrastructure	Cluster: Intra-cluster communications	Management: Dedicated management network for web access	Cloud: Optional cloud network port for separated Internet connectivity	CIMC: Cisco Integrated Management Controller out-of-band server appliance management
Example cluster VIP address	*10.4.49.29* *255.255.255.0*	*192.168.127.1* *255.255.255.248*	—	—	—
Example interface address (node 1)	*10.4.49.34* *255.255.255.0*	*192.168.127.2* *255.255.255.248*	Unused in this example	Unused in this example	*10.204.49.34* *255.255.255.0*
Example interface address (node 2)	*10.4.49.35* *255.255.255.0*	*192.168.127.3* *255.255.255.248*	Unused in this example	Unused in this example	*10.204.49.35* *255.255.255.0*
Example interface address (node 3)	*10.4.49.36* *255.255.255.0*	*192.168.127.4* *255.255.255.248*	Unused in this example	Unused in this example	*10.204.49.36* *255.255.255.0*

Tech tip

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

Procedure 1. Connect and configure the Cisco DNA Center hardware appliance

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

- Using the 10 Gbps SFP+ port labeled PORT 1 on the mLOM/PCIe card (named enp94s0f1 or enp9s0 in the wizard).
- Using the 10 Gbps port SFP+ labeled PORT 2 on the mLOM/PCIe card (named enp94s0f0 or enp10s0 in the wizard). This port **must** be up for single-node cluster configurations and for each appliance in a 3-node cluster.
- Using the Cisco Integrated Management Controller (IMC) port (labeled with a gear symbol or letter M on the integrated copper Ethernet ports).

For maximum physical network resiliency in a three-node cluster, each cluster node should connect to a unique top-of-rack switch, with each node interface placed into a separate Layer 2 domain (VLAN) on that switch. Enable communication between the nodes by using trunks to between each switch. Typical designs aggregate top-of-rack switches to redundant switches at the aggregation layer for this purpose. This design enables at least two nodes of the three-node cluster to communicate during an outage of any single switch or link, meeting the minimum criteria for the cluster to survive those communication failures.

Step 2. The described deployment uses the required minimum three ports on Cisco DNA Center Appliance– Cisco IMC and both SFP+ ports. Connect any other ports needed for the deployment, such as the dedicated web management port or an isolated enterprise network port. These ports are not used for the deployment described.

The following example steps are described in detail with all options within the Installation Guide for the appliance software version. Use the Installation 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. The example procedure that follows configures a single appliance for a single-node cluster or the first appliance for a three-node cluster deployment, without configuring a network proxy.

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

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

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

Step 5. Continue by accepting the wizard default choices, while supplying information for the following steps within the wizard (the wizard steps are in order but are not sequential; different hardware appliances have different adapter names and may be in a different order):

- In wizard **STEP #4**, selection for **NETWORK ADAPTER #1 (eno1):**

This interface can be used as a dedicated management interface for administrative web access to Cisco DNA Center. If you are using this option (which may require static route configuration), fill in the information; otherwise leave all selections blank, and then select next >> to continue.

Tech tip

Only one interface can be configured with a default gateway. If a default gateway is not defined on the interface, static routes can be used. These take the form of 'Subnet/Subnet Mask/Gateway.' Multiple static routes can be entered using a space between each.

Example: `198.51.100.0/255.255.255.0/198.51.100.254 203.0.113.0/255.255.255.0/203.0.113.254`

- In wizard **STEP #4**, selection for **OPTIONAL - NETWORK ADAPTER #2 (eno2)**:

This interface is available for use with a separate network (example: firewall DMZ) to the Internet cloud catalog server. Unless you require this connectivity, leave all selections blank, and select **next >>** to continue.

- In wizard **STEP #4**, selection for **OPTIONAL - NETWORK ADAPTER #3 (enp94s0f0)**:

Use this interface for communications with your network infrastructure. Supply at least the **Host IP Address, Netmask, Default Gateway IP Address, and DNS Servers**. If you are not using the single interface with default gateway, supply **Static Routes**, and then select **next >>** to continue.

```
Host IP Address:
  10.4.49.34
Netmask:
  255.255.255.0
Default Gateway IP Address:
  10.4.49.1
DNS Servers:
  10.4.49.10
Static Routes:
  [blank for combined management/enterprise interface installation]
Cluster Link
  [blank]
Configure IPv6 address
  [blank]
```

- In wizard **STEP #4**, selection for **OPTIONAL - NETWORK ADAPTER #4 (enp94s0f1)**:

This interface is used for cluster communication, although this port must be configured and operational for both single-node and 3-node clusters. Fill in the information for the **Host IP Address** and **Netmask** (a /29 size network or larger covers a three-member cluster), use the spacebar to select **Cluster Link**, do not fill in any other fields, and then select **next >>** to continue.

```
Host IP Address:
  192.168.127.2
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]
```

Tech tip
Confirm that the cluster link configuration is correct before proceeding. Changing the cluster link configuration after it is applied will require initiating a fresh configuration. If the cluster link is down, the VIP addresses will become unavailable. For both single-node and three-node clusters, the cluster link must be in an operational state.

```
The wizard displays an informational message.
The wizard will need to shutdown the controller in order to validate…
```

Tech tip
The wizard validates the DNS Servers and NTP servers entry using ICMP. Do not restrict ICMP echo communication between the appliance and any configured DNS and NTP servers.

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

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

Step 7. If the wizard detects a network proxy server, then you are prompted to configure the proxy settings.

- In wizard **STEP #8**, selection for **NETWORK PROXY**:

Update the settings as required and select **next >>** to continue.

Step 8. Define VIPs (Virtual IPs) for each of the configured interfaces. The VIPs must have a different IP address, although be in the same subnet as the configured interfaces. These can be entered in an order, and each VIP must be separated with a space.

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

```
Cluster Virtual IP address(s):
    10.4.49.29 192.168.127.1
Cluster’s hostname:
    [cluster fully-qualified domain name]
```

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

```
Linux Password: *
  [Cisco DNA Center CLI password]
Re-enter Linux Password: *
  [Cisco DNA Center CLI password]
Password Generation Seed:
  [skip this entry]
Auto Generated Password:
  [skip this entry]
Administrator Passphrase: *
  [Cisco DNA Center GUI administrator password]
Re-enter Administrator Passphrase: *
  [Cisco DNA Center GUI administrator password]
```

Step 9. In wizard **STEP #14**, **NTP SERVER SETTINGS**, you must supply at least one active NTP server. Connectivity to the defined NTP servers is validated and must succeed before the installation can proceed. Multiple NTP servers can be defined using a space between them.

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

Step 10. Select **next >>**. The installation validates connectivity to the NTP servers.

```
Validating NTP Server: 10.4.0.1 ...
```

Step 11. In wizard **STEP #16**, **MAGLEV ADVANCED SETTINGS**, you assign unique IP networks for the Services and Cluster Services subnets. These subnets must not be present or in use anywhere else in the deployment. The minimum size for each is a network with a 21-bit netmask (/21).

```
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 12. 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.

Many 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 several hours. When installation and configuration are complete, a login message is displayed.

```
Welcome to the Maglev Appliance
```

Step 13. Log in with the maglev user from the CIMC console or connect using an SSH session to the host IP address as assigned during the installation and destination port 2222.

```
maglev-master-1 login: maglev
Password: [Cisco DNA Center CLI password assigned during installation]
```

Step 14. Verify that processes are deployed.

```
$ maglev package status
```

Tech tip

Do not proceed until all packages are listed as DEPLOYED or NOT_DEPLOYED with exception.The following three packages will, depending on version, show as NOT_DEPLOYED. This is an expected behavior.

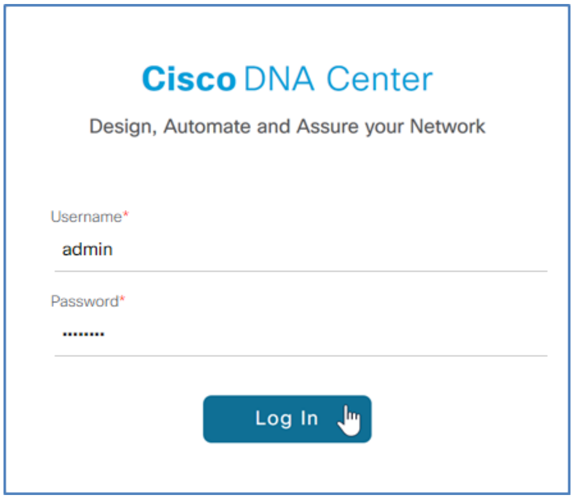
```
application-policy
sd-access
sensor-automation
```

This guide demonstrates how to upgrade Cisco DNA Center to the next version. Therefore, these packages will remain NOT_DEPLOYED at this point in the installation, as they will be upgraded and installed in later steps.

Procedure 2. Connect to Cisco DNA Center and verify the version

Step 1. Log in to the Cisco DNA Center web interface by directing a web browser to the **Cluster Virtual IP address** that you supplied in the previous procedure (example: https://10.4.49.29/).

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



Cisco DNA Center

Design, Automate and Assure your Network

Username* admin

Password* ••••••••

Tech tip

When logging into the GUI for the first time as the admin user, you will be asked to complete a first-time setup wizard. Although steps can be skipped in the Wizard, at minimum, the Cisco Credentials should be configured, and the Terms and Conditions must be accepted.

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

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

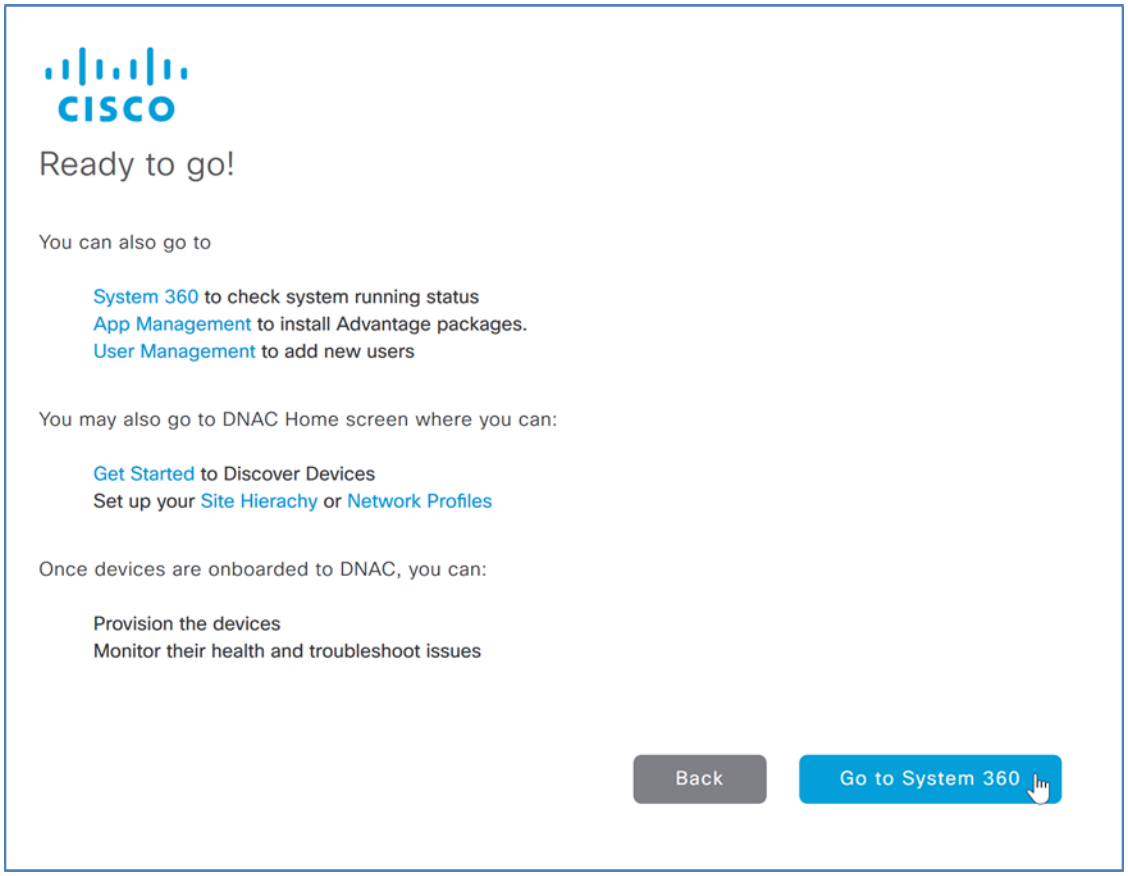
If you skip this step because you do not have an ID or plan to add one later by using **Settings (gear) > System Settings > Settings > Cisco Credentials**, features such as SWIM, Telemetry, and Licensing will be unable to function properly. Additionally, credentials are required for downloading software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

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

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

Step 7. If you are using a proxy server, enter the details at the Enter Proxy Server prompt and click Next. Otherwise, click Skip.

Step 8. At the **Terms and Conditions** display, click **Next**, and then at the **Ready to go!** display, click **Go to System 360**.



Ready to go!

You can also go to

System 360 to check system running status
App Management to install Advantage packages.
User Management to add new users

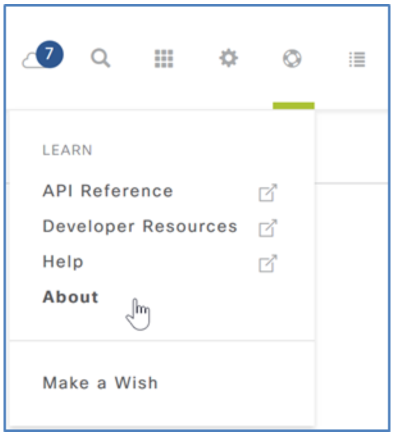
You may also go to DNAC Home screen where you can:

Get Started to Discover Devices
Set up your Site Hierachy or Network Profiles

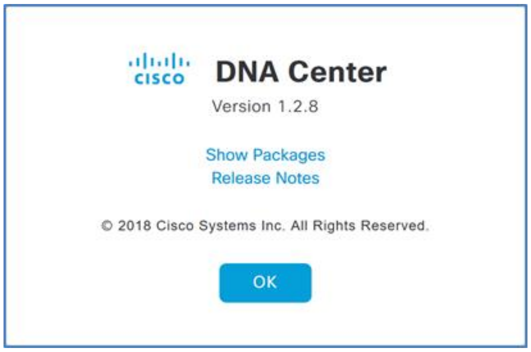
Once devices are onboarded to DNAC, you can:

Provision the devices
Monitor their health and troubleshoot issues

Step 9. At the main Cisco DNA Center dashboard, click the help (life preserver) icon, and then click **About**.



Step 10. Check the DNA Center version.



DNA Center

Version 1.2.8

© 2018 Cisco Systems Inc. All Rights Reserved.

If you are using an original M4-based DN1-HW-APL appliance, verify that the version is at least 1.2.6. If your version is earlier than 1.2.6 and you're creating a three-node cluster, or if your version is earlier than 1.1.6 and you're creating a single-node cluster, contact support to reimage your Cisco DNA Center appliances to your final target version before continuing. Version 1.2.6 is the minimum software requirement to cluster nodes in advance of upgrading the entire cluster to version 1.2.8 or later from the cloud catalog server. Newer M5-based appliances are preinstalled with 1.2.8 or a more recent version. For additional information, please see the Upgrade Paths in the Cisco Digital Network Architecture Center Upgrade Guide.

Procedure 3. Connect and configure the second and third add-on nodes to the cluster

Optional

If you are creating a three-node HA cluster configuration, complete this procedure.

Step 1. Connect the second and third add-on Cisco DNA Center hardware appliance nodes to a Layer 2 switchport in your network, by:

- Using the 10 Gbps SFP+ port labeled PORT 1 on the mLOM/PCIe card (named enp94s0f1 or enp9s0 in the wizard).
- Using the 10 Gbps port SFP+ labeled PORT 2 on the mLOM/PCIe card (named enp94s0f0 or enp10s0 in the wizard). This port **must** be up for single-node cluster configurations and for each appliance in a 3-node cluster.
- Using the Cisco Integrated Management Controller (IMC) port (labeled with a gear symbol or letter M on the integrated copper Ethernet ports).

The Cisco DNA Center nodes joining the cluster must boot from the same version of software as the first node.

Step 2. Connect any other ports needed for the deployment, such as the dedicated web management port or an isolated enterprise network port. All nodes should have the same interfaces connected.

The following example steps are described in detail with all options in the Installation Guide for the appliance software version. Use the Installation 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.

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

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

Step 4. Select Join a DNA-C Cluster (do not accept the default choice), and then press Enter.

Tech tip

Do this step only on the second node, and do not attempt to configure the third node in parallel. The second node must be joined into the cluster completely before you start the steps of joining the third node into the cluster.

Step 5. Continue by accepting the wizard default choices, while supplying information for the following steps within the wizard (the wizard steps are in order but are not sequential; different hardware appliances have different adapter names and may be in a different order):

- In wizard **STEP #4**, selection for **NETWORK ADAPTER #1 (eno1)**:

This interface can be used as a dedicated management interface for administrative web access to Cisco DNA Center. If you are using this option (which may require 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 #2 (eno2)**:

This interface is available for use with a separate network (example: firewall DMZ) to the Internet cloud catalog server. Unless you require this connectivity, leave all selections blank, and select **next >>** to continue.

- In wizard **STEP #4**, selection for **OPTIONAL - NETWORK ADAPTER #3 (enp94s0f0)**:

Use this interface for communications with your network infrastructure. Supply at least the Host IP Address, Netmask, Default Gateway IP Address, and DNS Servers. If you are not using the single interface with default gateway, supply Static Routes, and then select **next >>** to continue.

```
Host IP Address:
  10.4.49.35
Netmask:
  255.255.255.0
Default Gateway IP Address:
  10.4.49.1
DNS Servers:
  10.4.49.10
Static Routes:
  [blank for combined management/enterprise interface installation]
Cluster Link
  [blank]
Configure IPv6 address
  [blank]
```

- In wizard **STEP #4**, selection for **OPTIONAL - NETWORK ADAPTER #4 (enp94s0f1)**:

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

```
Host IP Address:
  192.168.127.3
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]
```

The wizard displays an informational message.

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

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

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

Step 7. If the wizard detects a network proxy server, then you are prompted to configure the proxy settings.

- In wizard **STEP #8**, selection for **NETWORK PROXY**:

Update the settings as required and select **next >>** to continue.

Step 8. After the wizard network validation completes, continue entering configuration values for the add-on node. The add-on node refers to the IP address of the cluster link on the first master node when joining the cluster.

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

```
Maglev Master Node: *
    192.168.127.2
Username: *
    maglev
Password: *
    [Cisco DNA Center CLI password assigned to first (master) node]
```

The wizard checks connectivity and uses the credentials to register to the master node.

Step 9. Continue entering the add-on node settings.

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

```
Linux Password: *
  [Cisco DNA Center CLI password]
Re-enter Linux Password: *
  [Cisco DNA Center CLI password]
Password Generation Seed:
  [skip this entry]
Auto Generated Password:
  [skip this entry]
```

Step 10. In wizard **STEP #14**, **NTP SERVER SETTINGS**, you must supply at least one active NTP server, which is tested before the installation can proceed.

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

Step 11. Select **next >>**.

The installation validates connectivity to the NTP servers.

```
Validating NTP Server: 10.4.0.1 ...
```

The wizard displays an informational message.

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

Disregard any additional warning messages about existing disk partitions.

Step 12. Select **proceed >>** to apply the configuration and complete the installation. You should not interact with the system until the installation is complete.

Many 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 over an hour. When installation and configuration are complete, a login message is displayed.

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

Step 13. Log in with the maglev user from the Cisco IMC console or connect using an SSH session to the host IP address as assigned during the installation and destination port 2222.

```
maglev-master-192 login: maglev
```

```
        Password: [password assigned during installation]
```

Step 14. Verify that the first two nodes are deployed.

```
        $ kubectl get nodes
```

The installed nodes appear, and the status is updated from **NotReady** to **Ready**:

```
        NAME            STATUS    AGE       VERSION
        192.168.127.2   Ready     15h       v1.7.3
        192.168.127.3   Ready     4m        v1.7.3
```

If the command returns an error instead of displaying the nodes, wait for the node process startup and communication establishment to complete and then try again. Do not proceed until the first two nodes in the cluster appear.

Step 15. Boot the third Cisco DNA Center hardware appliance. A welcome message appears.

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

Tech tip
Complete these steps on the third node only after the second node is verified as completely joined into the cluster.

Step 16. Select **Join a DNA-C Cluster** (do not accept the default choice), and then press **Enter**.

Step 17. 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; different hardware appliances have different adapter names and may be in a different order):

- In wizard **STEP #4**, selection for **NETWORK ADAPTER #1 (eno1)**:

This interface can be used as a dedicated management interface for administrative web access to Cisco DNA Center. If you are using this option (which requires static route configuration), fill in the information; otherwise leave all selections blank, and then select **next >>** to continue.

- In wizard **STEP #4**, selection for **OPTIONAL - NETWORK ADAPTER #2 (eno2)**:

This interface is available for use with a separate network (example: firewall DMZ) to the Internet cloud catalog server using 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 #3 (enp94s0f0)**:

Use this interface for communications with your network infrastructure. Supply at least the **Host IP Address**, **Netmask**, **Default Gateway IP Address**, and **DNS Servers**. If you are not using the single interface with default gateway, supply **Static Routes**, and then select **next >>** to continue.

```
        Host IP Address:
          10.4.49.36
        Netmask:
          255.255.255.0
        Default Gateway IP Address:
          10.4.49.1
        DNS Servers:
          10.4.49.10
        Static Routes:
          [blank for combined management/enterprise interface installation]
        Cluster Link
          [blank]
```

```
Configure IPv6 address
  [blank]
```

- In wizard **STEP #4**, selection for **OPTIONAL - NETWORK ADAPTER #4 (enp94s0f1)**:

This interface is used for cluster communication, although this port must be configured and operational for both single-node and 3-node clusters. Fill in the information for the Host IP Address and Netmask (a /29 size network or larger covers a three-member cluster), use the spacebar to select Cluster Link, do not fill in any other fields, and then select next >> to continue.

```
Host IP Address:
  192.168.127.4
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]
```

The wizard displays an informational message.

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

Step 18. Select **proceed >>** to continue with the network validation. The installation validates gateway reachability.

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

Step 19. If the wizard detects a network proxy server, then you are prompted to configure the proxy settings.

- In wizard **STEP #8**, selection for **NETWORK PROXY**:

Update the settings as required and select **next >>** to continue.

Step 20. After the wizard network validation completes, continue entering configuration values for the add-on node. The add-on node refers to the IP address of the cluster link on the first master node when joining the cluster.

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

```
Maglev Master Node: *
    192.168.127.2
Username: *
    maglev
Password: *
    [linux password assigned to first (master) node]
```

The wizard checks connectivity and uses the credentials to register to the master node.

Step 21. Continue entering the add-on node settings.

- 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]
```

Step 22. In wizard STEP #14, NTP SERVER SETTINGS, you must supply at least one active NTP server, which is tested before the installation can proceed. Multiple NTP servers can be defined using a space between them.

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

Step 23. Select **next >>**.

The installation validates connectivity to the NTP servers.

```
Validating NTP Server: 10.4.0.1 ...
```

The wizard displays an informational message.

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

Disregard any additional warning messages about existing disk partitions.

Step 24. Select **proceed >>** to apply the configuration and complete the installation. You should not interact with the system until the installation is complete.

Many status messages scroll by during the installation. The platform boots the installed image and configures the base processes for the first time, which can more than an hour. When installation and configuration are complete, a login message is displayed.

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

Step 25. Log in with the maglev user from the Cisco IMC console or connect using an SSH session to the host IP address as assigned during the installation and destination port 2222.

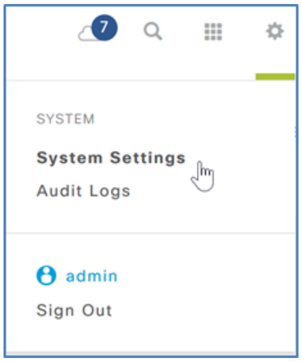
```
maglev-master-1 login: maglev
Password: [password assigned during installation]
```

Step 26. Verify that all three nodes are deployed.

```
$ kubectl get nodes
The installed nodes appear, and the status is updated from NotReady to Ready:
NAME            STATUS    AGE       VERSION
192.168.127.2   Ready     16h       v1.7.3
192.168.127.3   Ready     34m       v1.7.3
192.168.127.4   Ready     11m       v1.7.3
```

Step 27. Log in to the Cisco DNA Center web interface by directing a web browser to the cluster VIP address (example: https://10.4.49.29/).

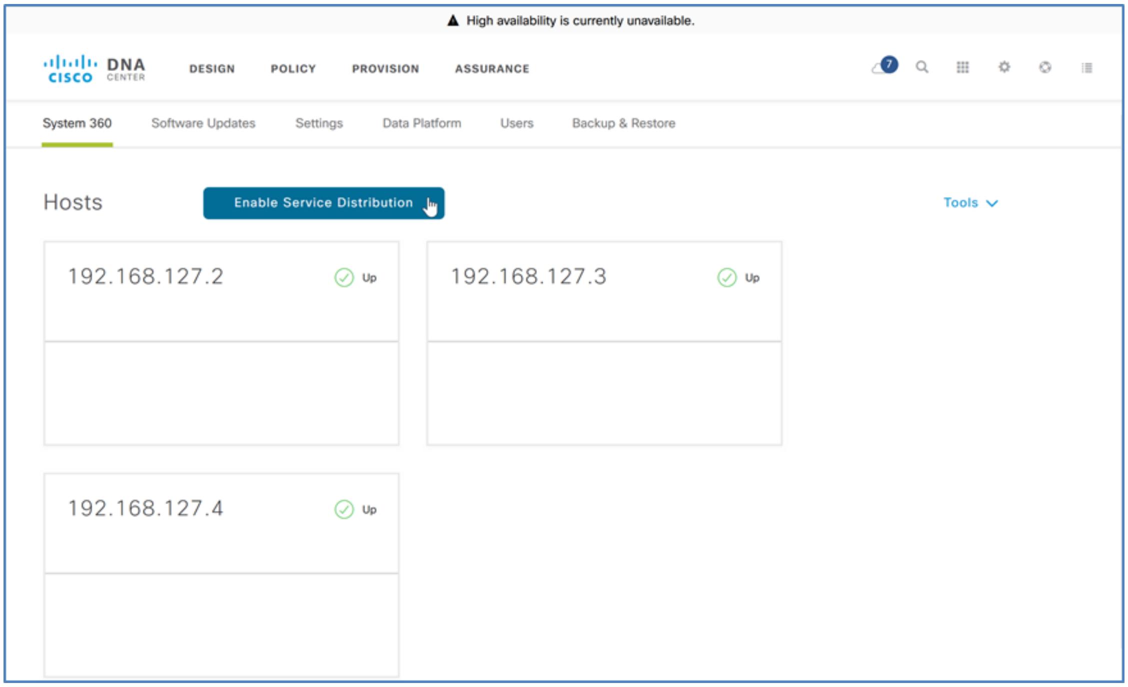
Step 28. At the main Cisco DNA Center dashboard, click the settings (gear) icon, and then click **System Settings**.



Tech tip

In 3-node HA deployment, running services are distributed across the appliance. Processes and services are redistributed from the master-node to the two other nodes. This process is completed in the GUI, and Cisco DNA Center enters maintenance mode while this completes.

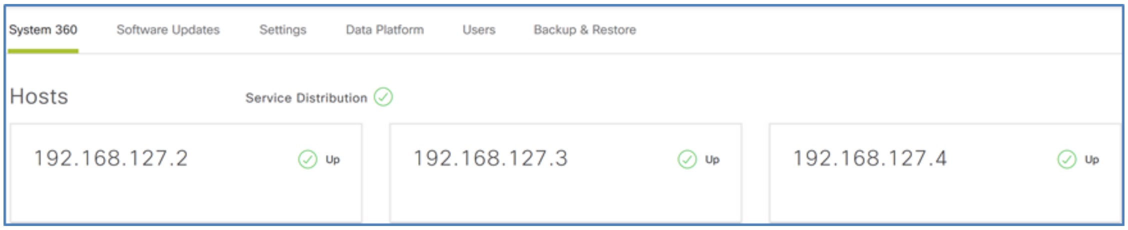
Step 29. Next to **Hosts**, click **Enable Service Distribution** (or, depending on the display for your version, toggle the **HIGH AVAILABILITY** switch on), and then at the warning message click **Continue**.



High availability is currently unavailable.

The button text changes to **Enabling Service Distribution…** and the services are distributed across the nodes in the cluster.

This process can take approximately an hour. Use the browser refresh button to verify the configuration status, which shows DNA Center is in maintenance mode until the process completes.



Procedure 4. Update the Cisco DNA Center software

Cisco DNA Center automatically connects to the Cisco cloud catalog server to find the latest updates. Update Cisco DNA Center to the required version using the Cisco cloud catalog server.

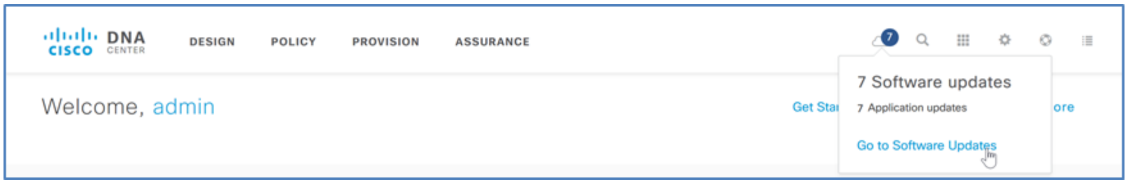
Tech tip

This procedure shows a Cisco DNA Center upgrade from release 1.2.8, and illustrations are installation examples. Software versions used for validation are listed in Appendix A: Product List. For upgrade requirements using other software versions, refer to the release notes on Cisco.com for the correct procedure for a successful upgrade to the target version from the installed version.

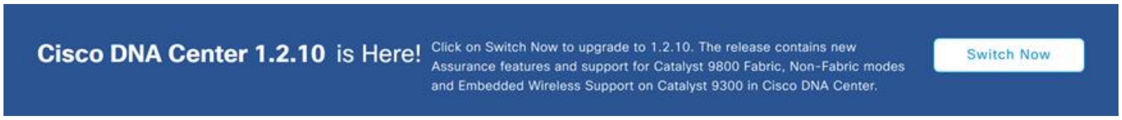
https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-release-notes-list.html

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

Step 1. At the main Cisco DNA Center dashboard, at the top right of the window, click the **Software Updates** (cloud) button, and then click **Go to Software Updates**.

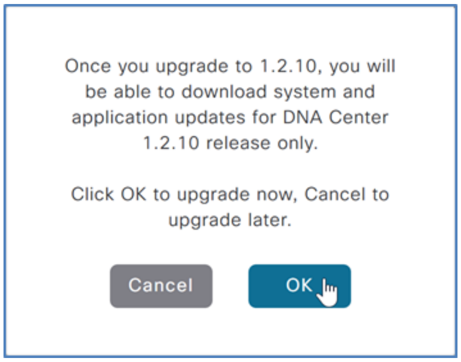


The **Settings > Software Updates > Updates** screen appears. This screen is used to install updates and packages that add functionality to the controller, including SD-Access. For significant system-wide updates, an announcement is displayed at the top of the updates window.



Cisco DNA Center 1.2.10 is Here! Click on Switch Now to upgrade to 1.2.10. The release contains new Assurance features and support for Catalyst 9800 Fabric, Non-Fabric modes and Embedded Wireless Support on Catalyst 9300 in Cisco DNA Center.

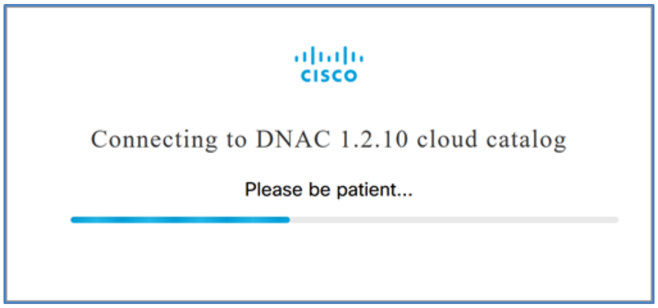
Step 2. Click the **Switch Now** button, and then acknowledge that the migration is irreversible by clicking OK.



Once you upgrade to 1.2.10, you will be able to download system and application updates for DNA Center 1.2.10 release only.

Click OK to upgrade now, Cancel to upgrade later.

Cisco DNA Center connects to the cloud catalog server.



Connecting to DNAC 1.2.10 cloud catalog

Please be patient...

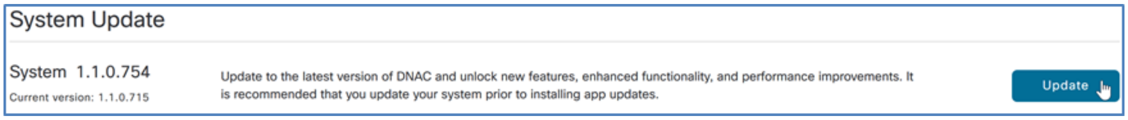
After Cisco DNA Center finishes connecting to the cloud catalog server, use the **Refresh** button to manually update the screen to display the available system update package.

Step 3. To the right of the available system update, click the **Update** button, click **Continue**, and then click **Continue**.

Caution

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

Do not switch to a new version of Cisco DNA Center until you have completely updated the system. Before switching, check the listing of permitted update paths in the Cisco Digital Network Architecture Center Upgrade Guide.


System Update

System 1.1.0.754

Current version: 1.1.0.715

Update to the latest version of DNAC and unlock new features, enhanced functionality, and performance improvements. It is recommended that you update your system prior to installing app updates.

The system goes into maintenance mode, and a message appears stating that there is a system update in progress. The download and installation can take more than an hour. Use the **Refresh** button to check the status.

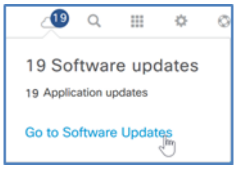
At the end of the installation, refresh the browser to view the web interface for the updated Cisco DNA Center.

Procedure 5. Upgrade the Cisco DNA Center application packages

When Cisco DNA Center is running the latest system update, you upgrade the packages to the versions associated with the updated system version.

Step 1. Log in to the Cisco DNA Center web interface and navigate to the main dashboard.

Step 2. In the top right of the Cisco DNA Center dashboard, click the **Software Updates** (cloud) button, and then click **Go to Software Updates**.

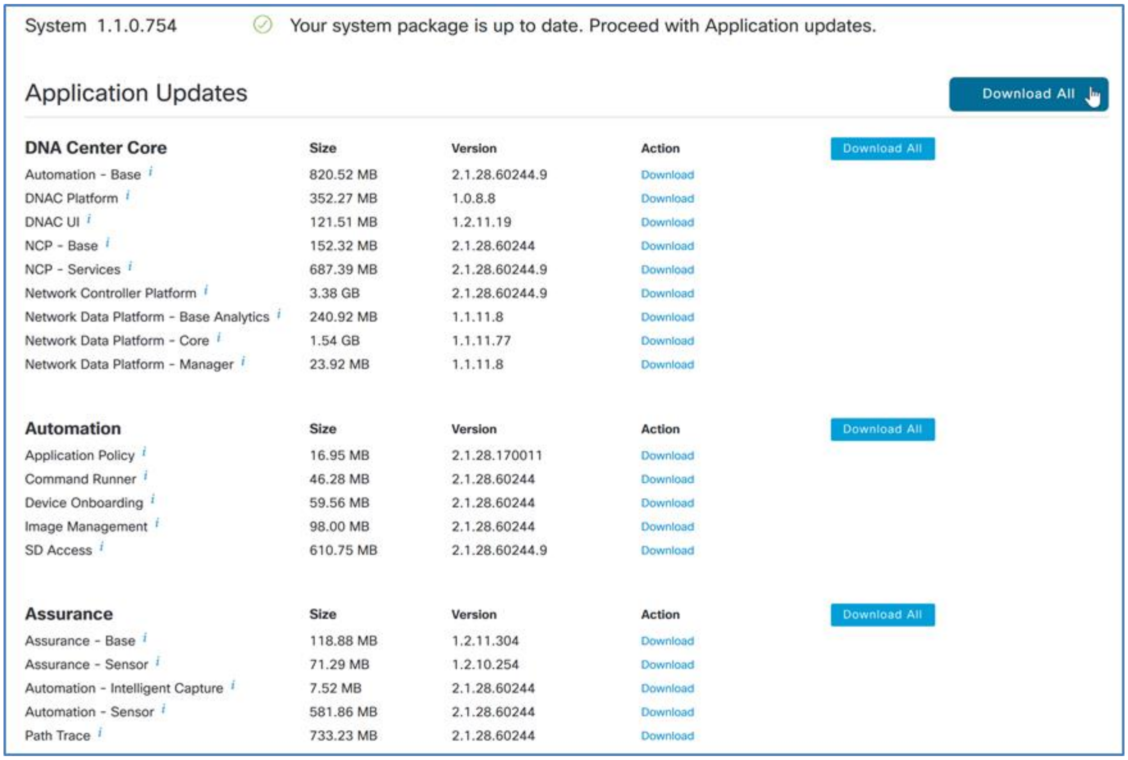


19 Software updates

19 Application updates

The system navigates to the **Software Updates > Updates > System Update** screen.

Step 3. At the top right of the **System Update screen**, on the same row as **Application Updates**, click the upper **Download All** button. At the pop-up window, click **Continue** to confirm the update operation, and then, at the second **System Readiness Check** pop-up window, click **Continue**.



System 1.1.0.754 ✓ Your system package is up to date. Proceed with Application updates.

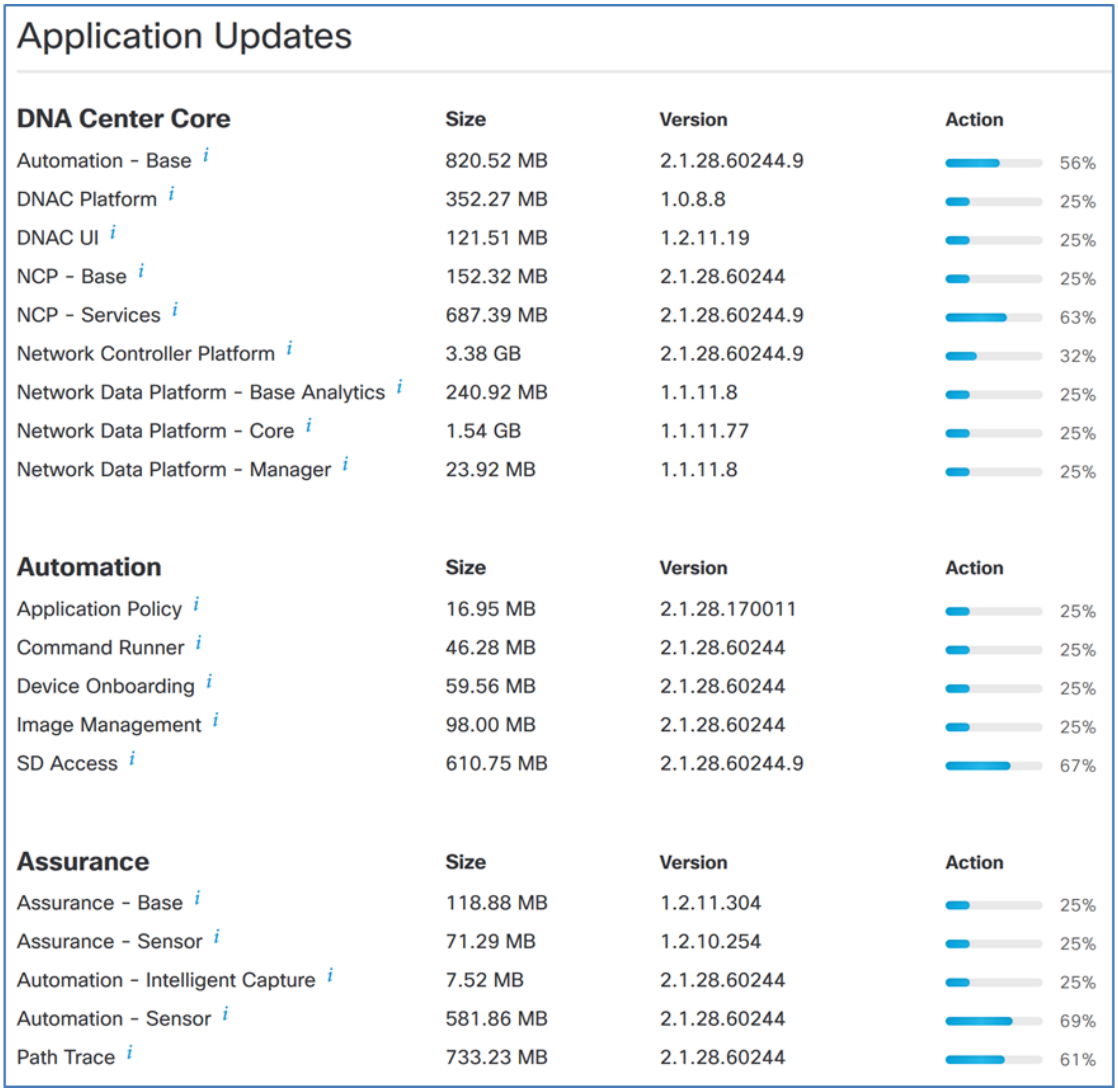
Application Updates

DNA Center Core	Size	Version	Action	Download All
Automation - Base	820.52 MB	2.1.28.60244.9	Download	
DNAC Platform	352.27 MB	1.0.8.8	Download	
DNAC UI	121.51 MB	1.2.11.19	Download	
NCP - Base	152.32 MB	2.1.28.60244	Download	
NCP - Services	687.39 MB	2.1.28.60244.9	Download	
Network Controller Platform	3.38 GB	2.1.28.60244.9	Download	
Network Data Platform - Base Analytics	240.92 MB	1.1.11.8	Download	
Network Data Platform - Core	1.54 GB	1.1.11.77	Download	
Network Data Platform - Manager	23.92 MB	1.1.11.8	Download	

Automation	Size	Version	Action	Download All
Application Policy	16.95 MB	2.1.28.170011	Download	
Command Runner	46.28 MB	2.1.28.60244	Download	
Device Onboarding	59.56 MB	2.1.28.60244	Download	
Image Management	98.00 MB	2.1.28.60244	Download	
SD Access	610.75 MB	2.1.28.60244.9	Download	

Assurance	Size	Version	Action	Download All
Assurance - Base	118.88 MB	1.2.11.304	Download	
Assurance - Sensor	71.29 MB	1.2.10.254	Download	
Automation - Intelligent Capture	7.52 MB	2.1.28.60244	Download	
Automation - Sensor	581.86 MB	2.1.28.60244	Download	
Path Trace	733.23 MB	2.1.28.60244	Download	

The browser interface updates, showing the package installation status. At the top of the screen, the cloud icon also offers status information to users navigating to any screen.



Application Updates

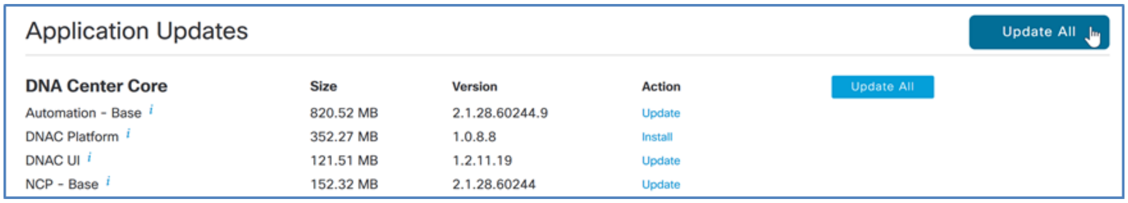
DNA Center Core	Size	Version	Action
Automation - Base *i*	820.52 MB	2.1.28.60244.9	56%
DNAC Platform *i*	352.27 MB	1.0.8.8	25%
DNAC UI *i*	121.51 MB	1.2.11.19	25%
NCP - Base *i*	152.32 MB	2.1.28.60244	25%
NCP - Services *i*	687.39 MB	2.1.28.60244.9	63%
Network Controller Platform *i*	3.38 GB	2.1.28.60244.9	32%
Network Data Platform - Base Analytics *i*	240.92 MB	1.1.11.8	25%
Network Data Platform - Core *i*	1.54 GB	1.1.11.77	25%
Network Data Platform - Manager *i*	23.92 MB	1.1.11.8	25%

Automation	Size	Version	Action
Application Policy *i*	16.95 MB	2.1.28.170011	25%
Command Runner *i*	46.28 MB	2.1.28.60244	25%
Device Onboarding *i*	59.56 MB	2.1.28.60244	25%
Image Management *i*	98.00 MB	2.1.28.60244	25%
SD Access *i*	610.75 MB	2.1.28.60244.9	67%

Assurance	Size	Version	Action
Assurance - Base *i*	118.88 MB	1.2.11.304	25%
Assurance - Sensor *i*	71.29 MB	1.2.10.254	25%
Automation - Intelligent Capture *i*	7.52 MB	2.1.28.60244	25%
Automation - Sensor *i*	581.86 MB	2.1.28.60244	69%
Path Trace *i*	733.23 MB	2.1.28.60244	61%

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

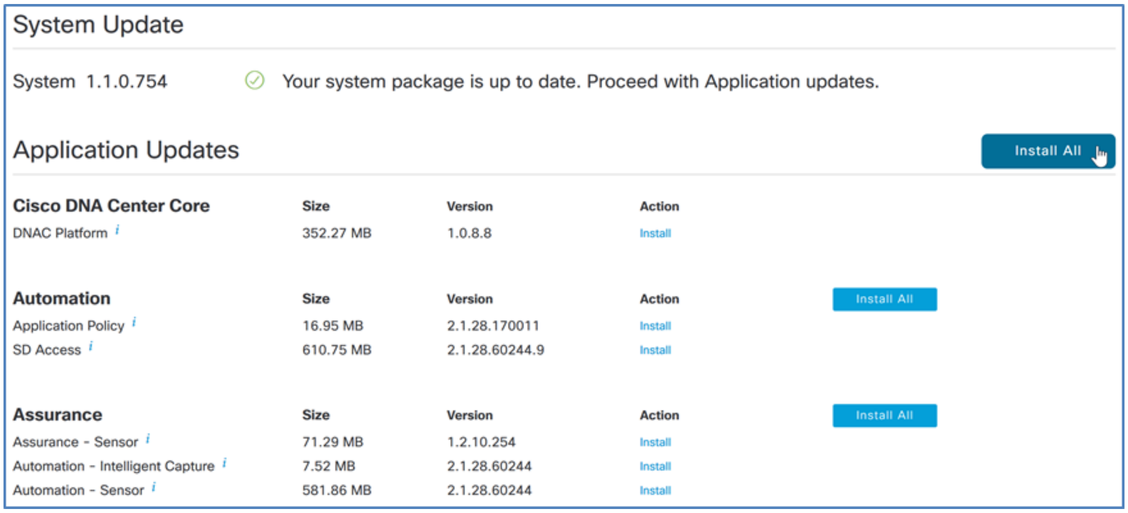
Step 4. After the downloads complete, if any additional packages are listed for updates, repeat the previous two steps until the **Download All** button is replaced with an **Update All** button that is not grayed out.



Application Updates

DNA Center Core	Size	Version	Action
Automation - Base *i*	820.52 MB	2.1.28.60244.9	Update
DNAC Platform *i*	352.27 MB	1.0.8.8	Install
DNAC UI *i*	121.51 MB	1.2.11.19	Update
NCP - Base *i*	152.32 MB	2.1.28.60244	Update

Step 5. After the new versions of the packages are downloaded, at the top right of the **System Update** screen, on the same row as **Application Updates**, click the upper **Install All** button. On the pop-up window, click **Continue**, and then, on the **System Readiness Check** pop-up window, click **Continue**. An informational message appears, and the installation begins.



System Update

System 1.1.0.754 ✓ Your system package is up to date. Proceed with Application updates.

Application Updates

Cisco DNA Center Core	Size	Version	Action	
DNAC Platform	352.27 MB	1.0.8.8	Install	

Automation	Size	Version	Action	Install All
Application Policy	16.95 MB	2.1.28.170011	Install	
SD Access	610.75 MB	2.1.28.60244.9	Install	

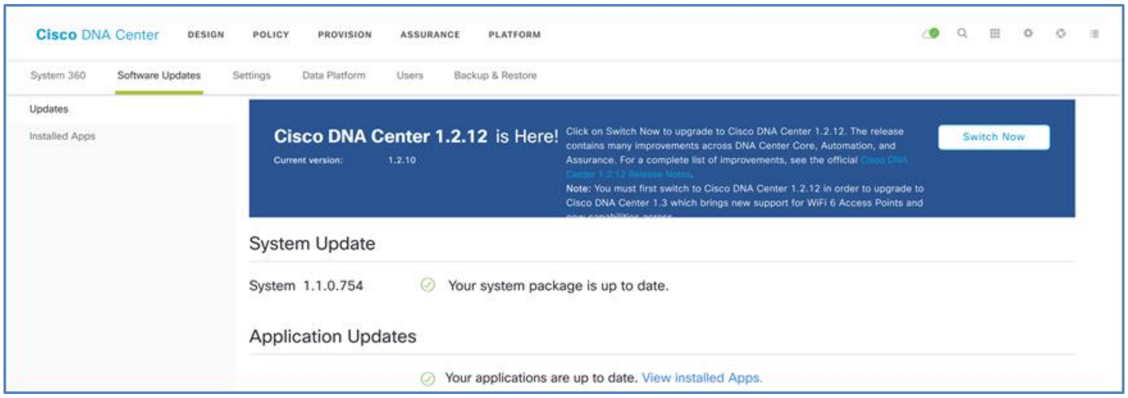
Assurance	Size	Version	Action	Install All
Assurance - Sensor	71.29 MB	1.2.10.254	Install	
Automation - Intelligent Capture	7.52 MB	2.1.28.60244	Install	
Automation - Sensor	581.86 MB	2.1.28.60244	Install	

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

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

While the packages are installing, you can work in parallel on the next process for installing the Identity Services Engine nodes.

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



Cisco DNA Center 1.2.12 is Here!

Current version: 1.2.10

Click on Switch Now to upgrade to Cisco DNA Center 1.2.12. The release contains many improvements across DNA Center Core, Automation, and Assurance. For a complete list of improvements, see the official Cisco DNA Center 1.2.12 Release Notes.

Note: You must first switch to Cisco DNA Center 1.2.12 in order to upgrade to Cisco DNA Center 1.3 which brings new support for WiFi 6 Access Points and

System Update

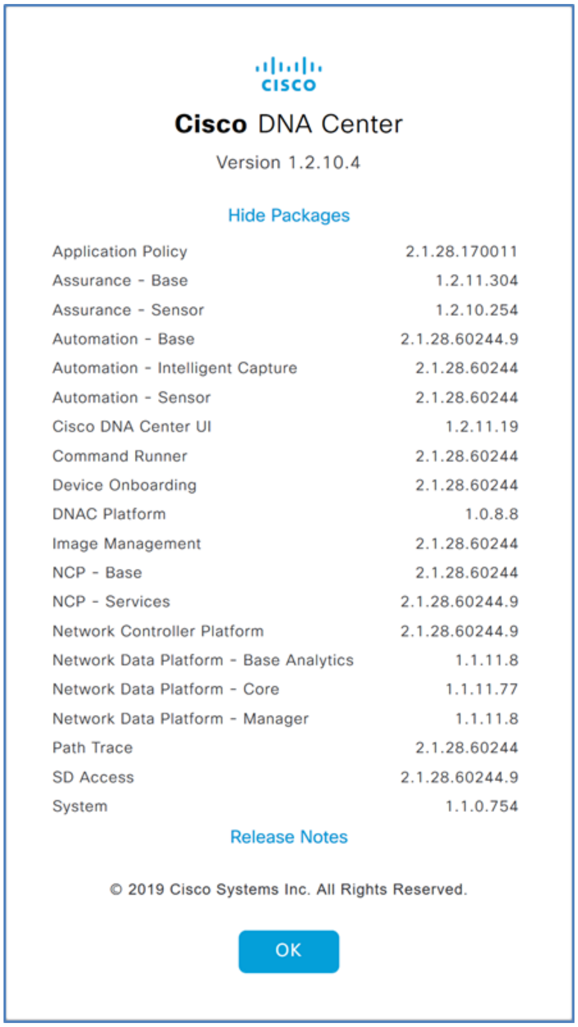
System 1.1.0.754 ✓ Your system package is up to date.

Application Updates

✓ Your applications are up to date. View installed Apps.

Continue to the next step after all packages are installed.

Step 6. In the top right of the main Cisco DNA Center dashboard, click the help (life preserver) icon, click **About**, and then click **Show Packages**. This view is useful for comparing to the release notes, which are available by clicking **Release Notes**.



Cisco DNA Center

Version 1.2.10.4

Hide Packages

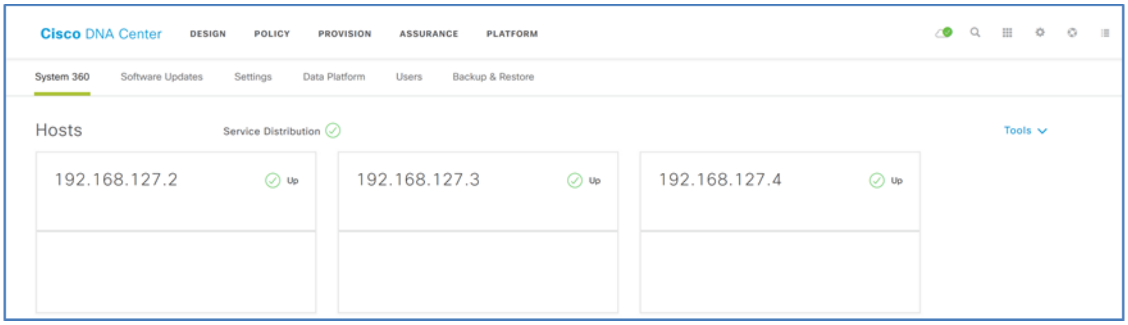
Application Policy	2.1.28.170011
Assurance - Base	1.2.11.304
Assurance - Sensor	1.2.10.254
Automation - Base	2.1.28.60244.9
Automation - Intelligent Capture	2.1.28.60244
Automation - Sensor	2.1.28.60244
Cisco DNA Center UI	1.2.11.19
Command Runner	2.1.28.60244
Device Onboarding	2.1.28.60244
DNAC Platform	1.0.8.8
Image Management	2.1.28.60244
NCP - Base	2.1.28.60244
NCP - Services	2.1.28.60244.9
Network Controller Platform	2.1.28.60244.9
Network Data Platform - Base Analytics	1.1.11.8
Network Data Platform - Core	1.1.11.77
Network Data Platform - Manager	1.1.11.8
Path Trace	2.1.28.60244
SD Access	2.1.28.60244.9
System	1.1.0.754

Release Notes

© 2019 Cisco Systems Inc. All Rights Reserved.

OK

Step 7. At the main Cisco DNA Center dashboard, click the Settings (gear) icon, and then click **System Settings**. Status is shown for hosts in the cluster.



Hosts

Service Distribution ✓

192.168.127.2 ✓ Up

192.168.127.3 ✓ Up

192.168.127.4 ✓ Up

If you need additional functionality in later Cisco DNA Center releases, such as support for new switches or features, you can continue the upgrade process as required.

With all application packages installed and hosts in the cluster showing a status of Up, the SD-Access functionality is available to configure, and integration with ISE can proceed.

Process 2: Installing SD-Access Wireless LAN controllers

For a Cisco SD-Access Wireless deployment, dedicate a WLC or pair of WLCs for SD-Access Wireless connectivity by integrating the WLCs 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.

For high availability stateful switchover (HA SSO) resiliency, use a pair of WLCs with all network connectivity in place before starting the configuration procedure. Redundant WLCs are connected to a set of devices configured to support the Layer 2 redundancy suitable for the HA SSO WLCs, such as a switch stack, Cisco Virtual Switching System, or Cisco StackWise® Virtual, which may exist in a data center or shared services network. For maximum resiliency, redundant WLCs should not be directly connected to the Layer 3 border nodes.

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 **-** (hyphen) 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 use the default name.

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

Step 3. Enter an administrator username and password. Use at least three of the following character classes in the password: lowercase letters, uppercase letters, digits, and special characters.

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

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

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

Step 5. Enable Link Aggregation (LAG).

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

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

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

Step 7. Configure the management interface VLAN identifier.

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

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

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

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

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

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

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

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

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

Step 12. If the option is presented, 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 IP address must be unique for each controller or HA pair in the network. The multicast IP 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 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…
```

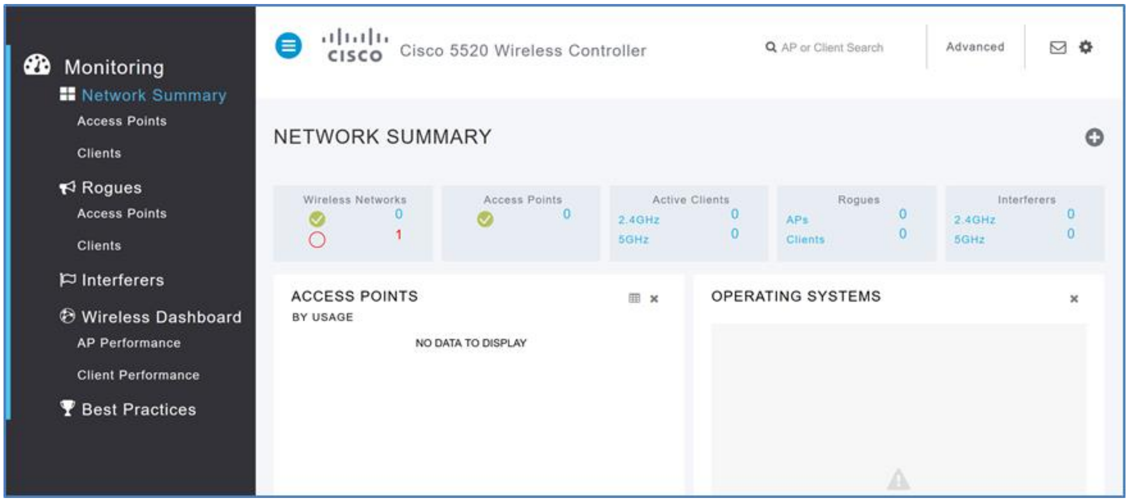
If you press Enter or respond with no, the system resets without saving the configuration, and you will have to complete this procedure again.

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).



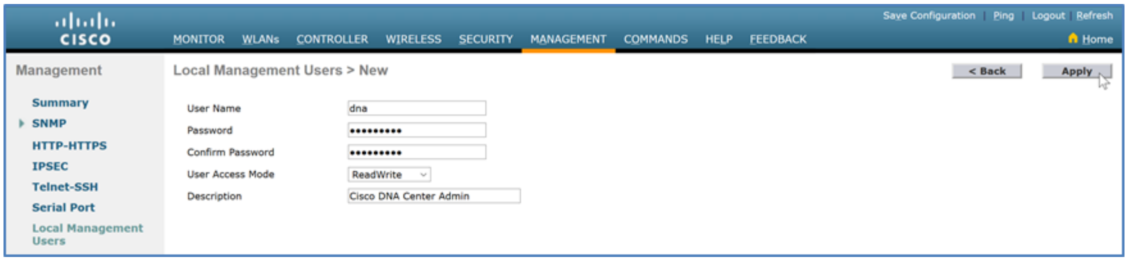
Step 26. From the home page, at the top right, click **Advanced**. Navigate to **COMMANDS > Set Time**. Verify that the date and time agree with the NTP server. If the time appears to be significantly different, manually correct it, and, if your network infrastructure devices use something other than the default time zone, also choose a time zone. The correct date and time are important for certificate validation and successful AP registration with the WLC. Repeat this step with each WLC.

Procedure 2. Configure the WLC discovery and management credentials

Add the credentials to the WLC used for discovery and management by Cisco DNA Center. During discovery, with the Device Controllability feature enabled, Cisco DNA Center uses the user credentials to configure additional management access requirements, such as SNMPv3.

Step 1. Use a web browser to connect to the Cisco WLC administration web page using the credentials created in Step 3 of Procedure 1 (example: https://10.4.174.26).

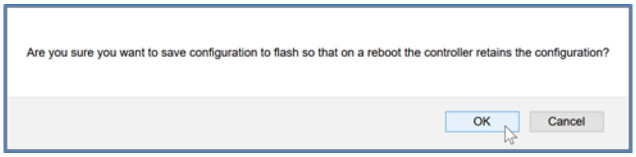
Step 2. Add a local login for Cisco DNA Center to manage the device. From the home page, at the top right, click **Advanced**. Navigate to **MANAGEMENT > Local Management Users**. At the top right, click **New…**, fill out the form, supplying **User Name** (example: dna), **Password**, **Confirm Password**, set **User Access Mode** to **ReadWrite**, supply a **Description**, and then click **Apply**.



Local Management Users > New

User Name	dna
Password	•••••••••
Confirm Password	•••••••••
User Access Mode	ReadWrite
Description	Cisco DNA Center Admin

Step 3. At the top right, click Save Configuration, and then, at the dialog box, click OK.



Are you sure you want to save configuration to flash so that on a reboot the controller retains the configuration?

Step 4. Repeat this procedure for the secondary WLC, using the appropriate parameters for it.

The WLCs are ready for integration into the Cisco DNA Center setup. Integration is part of the fabric deployment itself and consists of adding WLCs into inventory, optionally creating HA pairs, creating IP pools and SSIDs for fabric wireless, provisioning WLCs into the fabric, and assigning wireless endpoints to the fabric. These steps are outlined as part of the Software-Defined Access Medium and Large Site Fabric Provisioning Prescriptive Deployment Guide.

Process 3: Installing Identity Services Engine nodes

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

Table 3. 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

The identity services engine can be installed as a VM (virtual machine) or installed on dedicated Cisco Secure Network Server (SNS) appliances. The procedures below provide the steps to configure ISE once the appliance or virtual machine has been installed and wired. For additional details beyond the scope of the procedures below, please see Cisco Identity Services Engine Installation Guides.

Procedure 1. Install ISE server images

Before you begin, you must identify the following:

- IP addressing and network connectivity for all ISE nodes being deployed.
- A network-reachable Network Time Protocol (NTP) server, used during Identity Services Engine installation to help ensure reliable digital certificate operation for securing connections.
- Network-reachable Domain Name System (DNS) server used during installation and for ISE Distributed Deployments.
- Certificate server information, when self-signed digital certificates are not used.

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 Step 2 to Step 3 on the second ISE node, using the appropriate parameters for it.

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

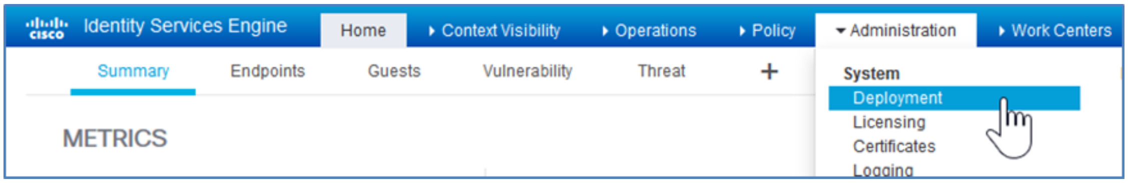
```
localhost login:
```

Procedure 2. Configure roles for first ISE node

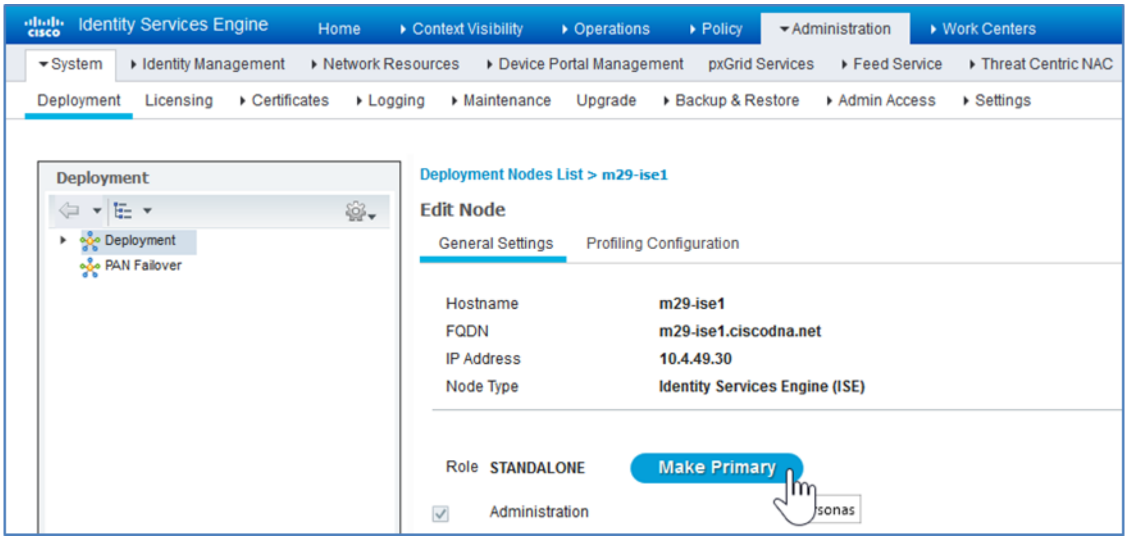
Step 1. On the first ISE node, log in using a web browser and the configured username and password, and then accept any informational messages.

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**.

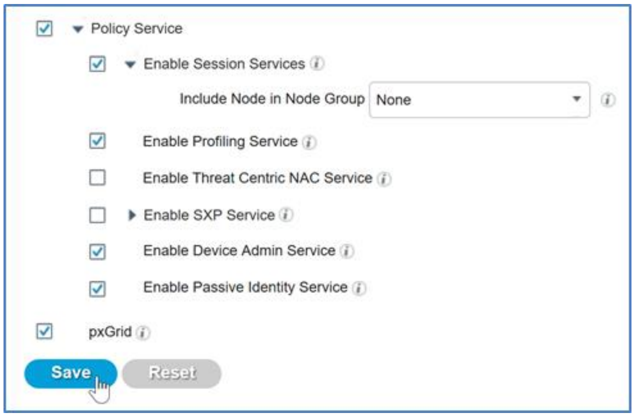


Hostname m29-ise1
FQDN m29-ise1.ciscodna.net
IP Address 10.4.49.30
Node Type Identity Services Engine (ISE)

Role STANDALONE

☑ Administration

Step 4. Under **Policy Service**, select **Enable Device Admin Service** and **Enable Passive Identity Service**, select **pxGrid**, and then click **Save**.



☑ Policy Service
☑ Enable Session Services
Include Node in Node Group None
☑ Enable Profiling Service
☐ Enable Threat Centric NAC Service
☐ Enable SXP Service
☑ Enable Device Admin Service
☑ Enable Passive Identity Service
☑ pxGrid

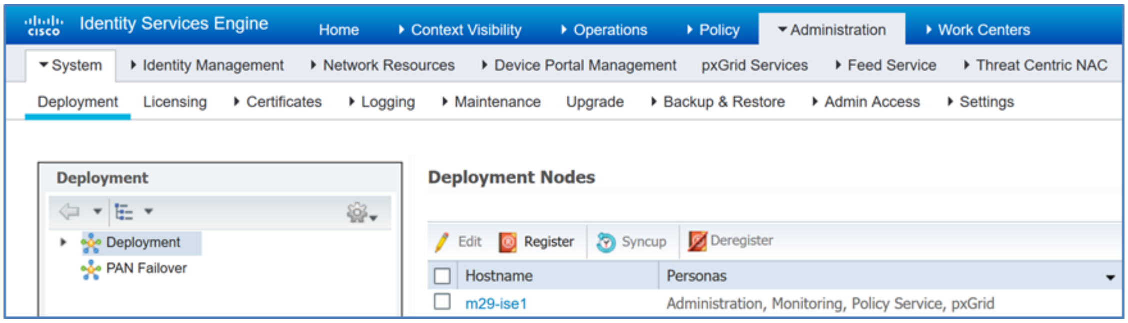
TACACS infrastructure device administration support, authentication using Cisco EasyConnect with domain controllers, and pxGrid services for Cisco DNA Center are now enabled, and the node configuration is saved.

Procedure 3. Register ISE node 2 and configure roles

Using the same ISE administration session started on the first node, integrate the additional ISE node.

> **Tech tip**
>
> ISE distributed deployments use mutual certificate identification to validate each node that is registered with the Primary. Communication between nodes is created using the FQDN (fully qualified domain names), not the IP address. Forward and reverse DNS entries must be available in the defined DNS server for the IP address and FQDN that are part of your distributed deployment or registration will fail.

Step 1. Using the existing session, refresh the view by navigating again to Administration > System > Deployment, and then under the Deployment Nodes section, click Register.



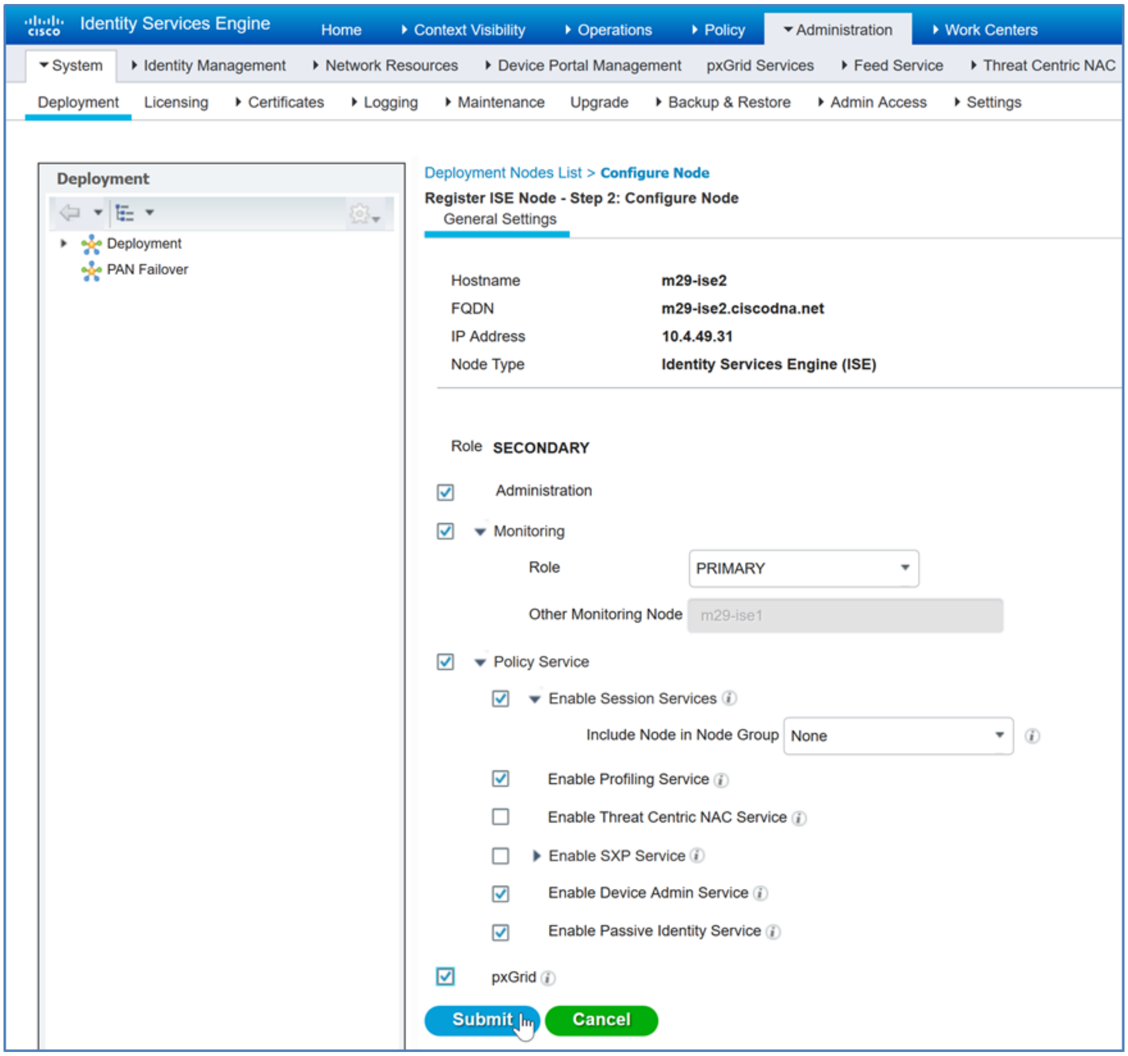
□	Hostname	Personas
□	m29-ise1	Administration, Monitoring, Policy Service, pxGrid

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

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**. Under **Policy Service**, select **Enable Device Admin Service** and **Enable Passive Identity Service**, select **pxGrid**, and then click **Submit**.



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

Include Node in Node Group None

☑ Enable Profiling Service

☐ Enable Threat Centric NAC Service

☐ Enable SXP Service

☑ Enable Device Admin Service

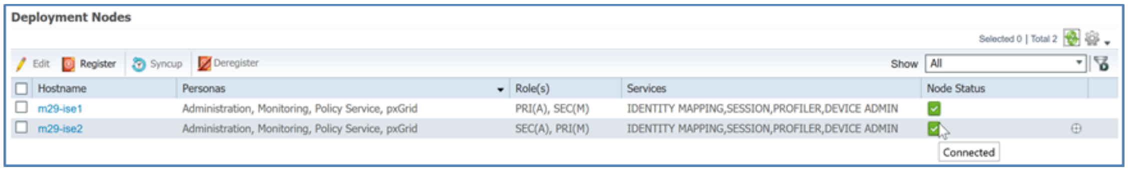
☑ Enable Passive Identity Service

☑ pxGrid

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.

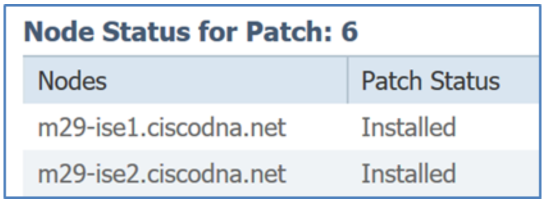
The synchronization and restart of the second node can take more than ten minutes to complete. You can use the refresh button on the screen to observe when the node returns from **In Progress** to a **Connected** state to proceed to the next step.



☐	Hostname	Personas	Role(s)	Services	Node Status
☐	m29-ise1	Administration, Monitoring, Policy Service, pxGrid	PRI(A), SEC(M)	IDENTITY MAPPING,SESSION,PROFILER,DEVICE ADMIN	✓
☐	m29-ise2	Administration, Monitoring, Policy Service, pxGrid	SEC(A), PRI(M)	IDENTITY MAPPING,SESSION,PROFILER,DEVICE ADMIN	✓

Step 6. Check Cisco.com for ISE release notes and the SD-Access Hardware and Software Compatibility Matrix and download any patch required for your installation. Then, 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.

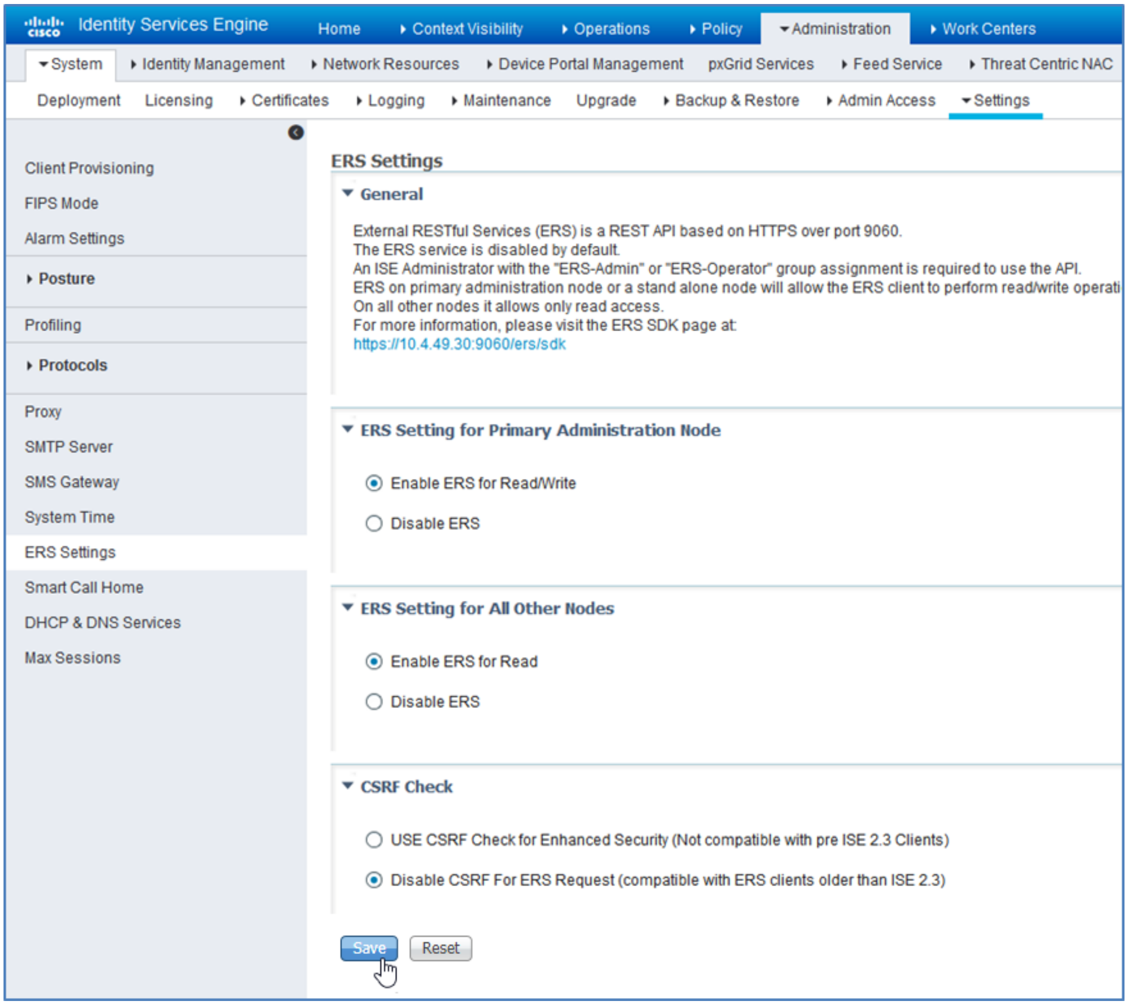
Step 7. After the ISE web interface is active again, check the progress of the patch installation by navigating to **Administration > System > Maintenance > Patch Management**, select the patch, and then select **Show Node Status**. Use the **Refresh** button to update status until all nodes are in **Installed**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



Node Status for Patch: 6

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**, and accept any dialog box that appears. Under **ERS Setting for All Other Nodes**, select **Enable ERS for Read**. Under **CRSF Check**, select **Disable CSRF for ERS Request**, and then click **Save**. Accept any additional dialog box that appears.



ERS Settings

General

External RESTful Services (ERS) is a REST API based on HTTPS over port 9060.
The ERS service is disabled by default.
An ISE Administrator with the "ERS-Admin" or "ERS-Operator" group assignment is required to use the API.
ERS on primary administration node or a stand alone node will allow the ERS client to perform read/write operati
On all other nodes it allows only read access.
For more information, please visit the ERS SDK page at:
https://10.4.49.30:9060/ers/sdk

ERS Setting for Primary Administration Node

● Enable ERS for Read/Write

○ Disable ERS

ERS Setting for All Other Nodes

● Enable ERS for Read

○ Disable ERS

CSRF Check

○ USE CSRF Check for Enhanced Security (Not compatible with pre ISE 2.3 Clients)

● Disable CSRF For ERS Request (compatible with ERS clients older than ISE 2.3)

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

Operate

Once Cisco DNA Center and Cisco Identity Services have been installed, this section demonstrates how to integrate these management controllers through a trust establishment created through mutual certificate authentication.

Process 1: Integrating Identity Services Engines with Cisco DNA Center

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

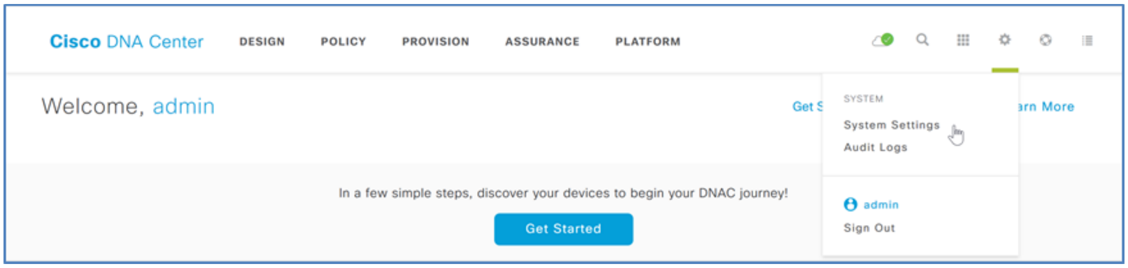
Tech tip

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

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

Procedure 1. Configure Cisco DNA Center authentication and policy servers

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

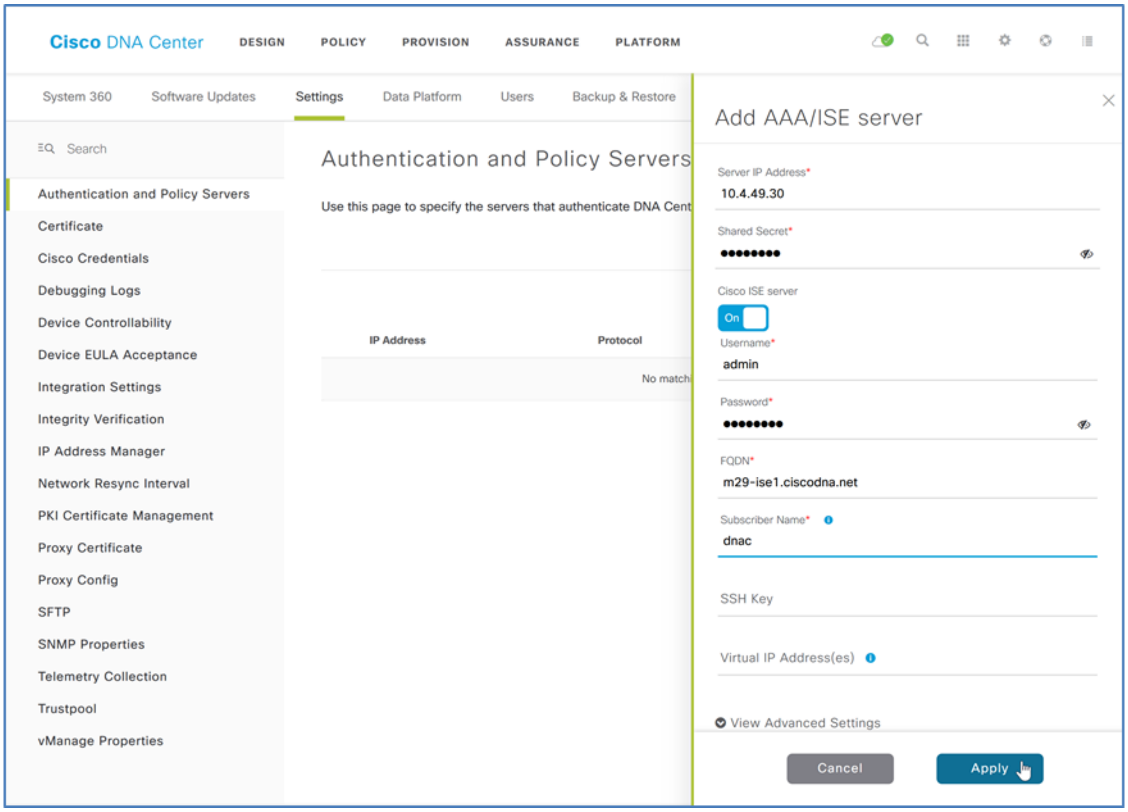


Step 2. Navigate to **Settings > Authentication and Policy Servers**, and then click the **+ Add** button.

Tech tip

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

Step 3. In the **Add AAA/ISE SERVER** slide-out display, enter the ISE node 1 (primary PAN) **Server IP Address** (example: 10.4.49.30) and **Shared Secret**, toggle the **Cisco ISE server** selector to **On**, enter the ISE **Username** (example: admin), enter the ISE **Password**. For the **FQDN** and enter the ISE fully qualified domain name, enter **Subscriber Name** (example: dnac) and leave the SSH Key blank. If you are using TACACS for infrastructure device administration, click **View Advanced Settings** and select **TACACS**. Click **Apply**.



Add AAA/ISE server

Server IP Address*: 10.4.49.30

Shared Secret*: ●●●●●●●●

Cisco ISE server: On

Username*: admin

Password*: ●●●●●●●●

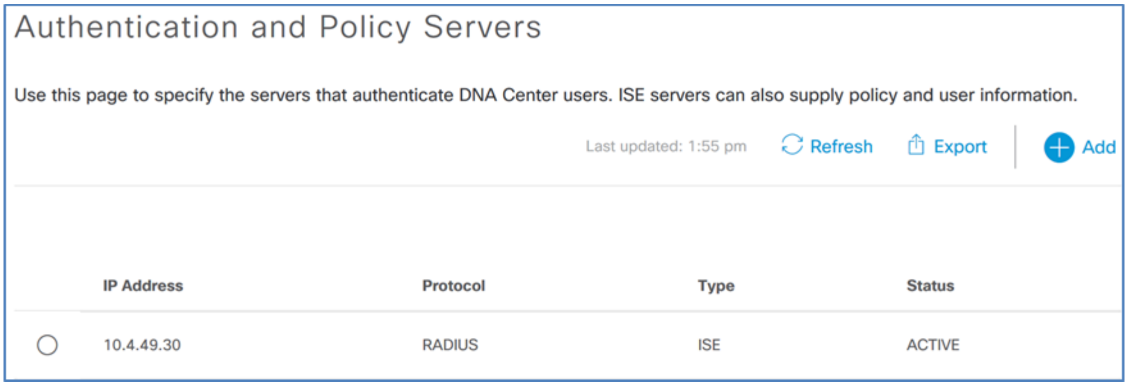
FQDN*: m29-ise1.ciscodna.net

Subscriber Name*: dnac

SSH Key

Virtual IP Address(es)

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



Authentication and Policy Servers

Use this page to specify the servers that authenticate DNA Center users. ISE servers can also supply policy and user information.

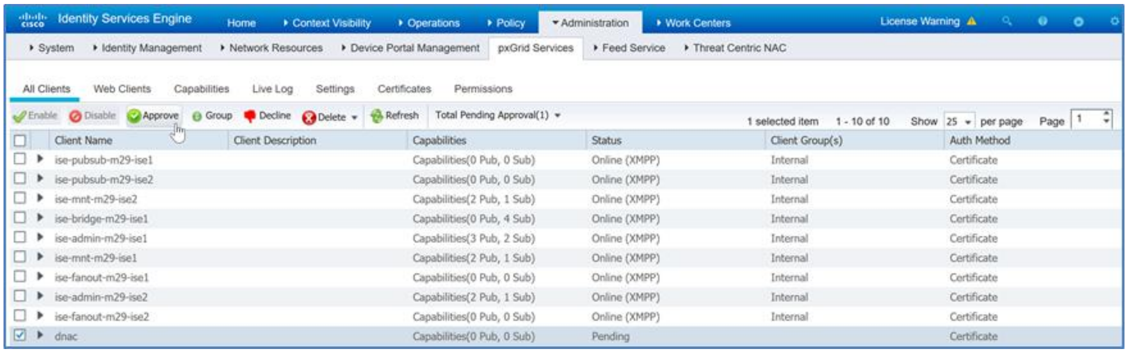
	IP Address	Protocol	Type	Status
○	10.4.49.30	RADIUS	ISE	ACTIVE

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

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

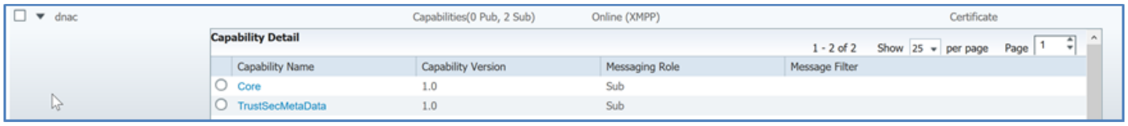
The client named ***dnac*** (**Subscriber Name** defined above) shows **Pending** in the **Status** column.

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



	Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Method
□	ise-pubsub-m29-ise1		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate
□	ise-pubsub-m29-ise2		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate
□	ise-mnt-m29-ise2		Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Internal	Certificate
□	ise-bridge-m29-ise1		Capabilities(0 Pub, 4 Sub)	Online (XMPP)	Internal	Certificate
□	ise-admin-m29-ise1		Capabilities(3 Pub, 2 Sub)	Online (XMPP)	Internal	Certificate
□	ise-mnt-m29-ise1		Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Internal	Certificate
□	ise-fanout-m29-ise1		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate
□	ise-admin-m29-ise2		Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Internal	Certificate
□	ise-fanout-m29-ise2		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate
☑	dnac		Capabilities(0 Pub, 0 Sub)	Pending		Certificate

A success message appears, 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**.



	Client Name	Capabilities	Status	Auth Method
□	dnac	Capabilities(0 Pub, 2 Sub)	Online (XMPP)	Certificate

Capability Detail

	Capability Name	Capability Version	Messaging Role	Message Filter
○	Core	1.0	Sub	
○	TrustSecMetaData	1.0	Sub	

If ISE is integrated with Cisco DNA Center after scalable groups are already created in ISE, in addition to the default groups available, any existing ISE groups also are visible by logging in to Cisco DNA Center and navigating to **Policy > Dashboard > Scalable Groups**.

Appendix A: Product List

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

Table 4. Cisco DNA Center

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

Table 5. Cisco DNA Center packages

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

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

Package	Version
Path Trace	2.1.28.60244
SD-Access	2.1.28.60244.9

Table 6. Identity management

Product	Part Number	Software version
Cisco ISE Server	R-ISE-VMM-K9=	2.4 Patch 6

Table 7. SD-Access Wireless Controller

Product	Part Number	Software Version
Wireless LAN controller	Cisco 8540, 5520, and 3504 Series Wireless Controllers	8.8.111.0 (8.8 MR1)

Feedback

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

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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