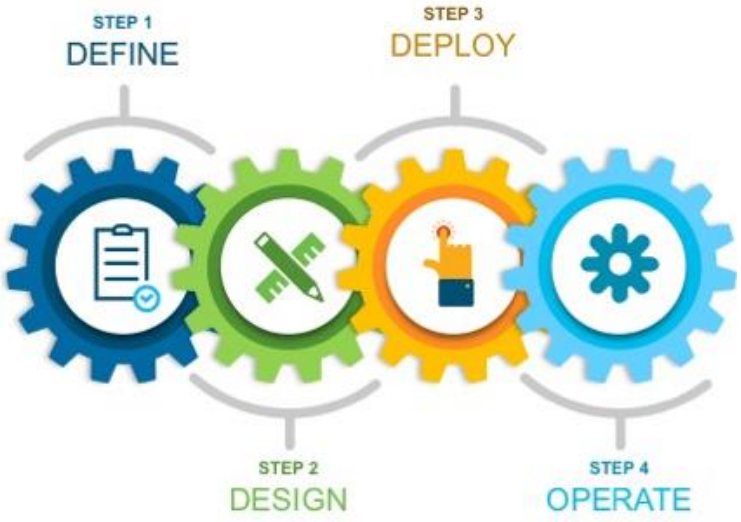
Cisco DNA Center & Identity Services Engine Management Infrastructure

Solution Adoption Prescriptive Reference Deployment Guide

April, 2020

Contents

About this Guide



This guide contains four major sections:

The **DEFINE** section defines both Software-Defined Access and traditional network architectures, highlights their relationship to Cisco DNA Center, and provides information on companion solution guides.

The **DESIGN** section shows deployment topologies 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 and Cisco Identity Services Engine (ISE).

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

Define

This section introduces the Software-Defined Access and traditional network solutions, and highlights their relationship to Cisco DNA Center. It also provides links to additional resources and companion guides.

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.

About traditional network designs & Cisco DNA Center

Traditional network architectures use a hierarchical design model to break the design up into modular groups or layers. Breaking the design up into layers allows each layer to implement specific functions, which simplifies the network design and therefore the deployment and management of the network. Modularity in network design allows you to create design elements that can be replicated throughout the network. Replication provides an easy way to scale the network as well as a consistent deployment method.

Traditional networks can be managed by Cisco Prime Infrastructure. They can also be managed now with Cisco DNA Center. Cisco DNA Center can be used automate, monitor and gather telemetry for traditional networks as well as SDA.

This guide is used to deploy the management infrastructure, including Cisco DNA Center and Cisco Identity Services Engine (ISE). The deployment described in this guide is used in advance of deploying a Cisco SD-Access fabric or traditional campus LAN design.

Companion Resources

You can 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, Campus LAN and Wireless LAN Design 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

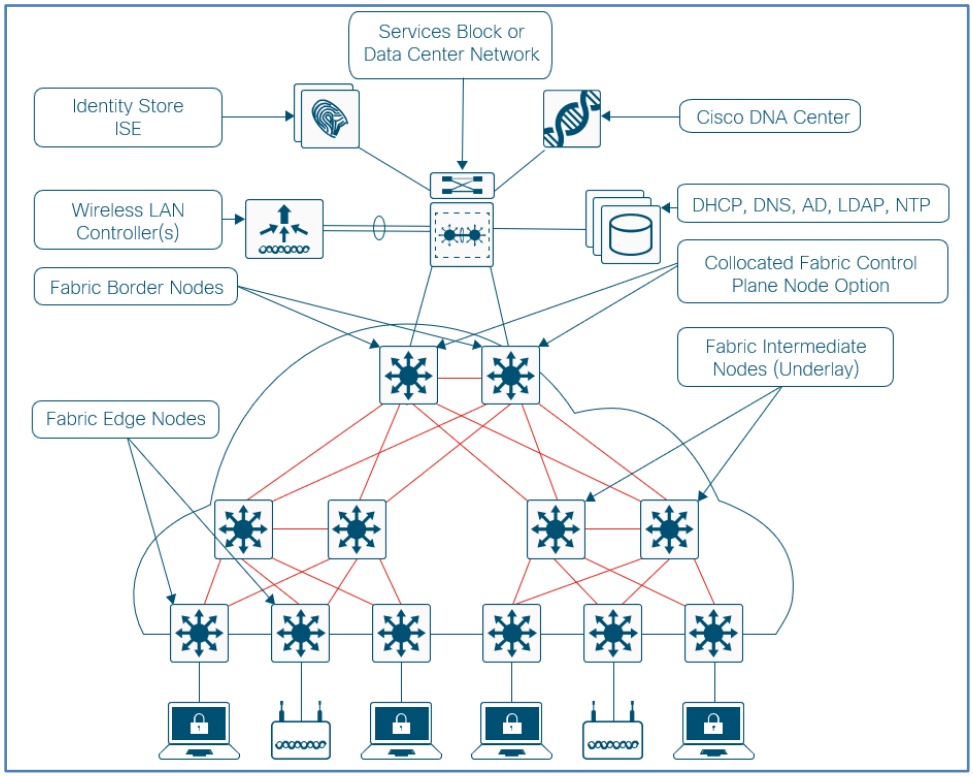
For scale metrics and latency information, please see the SD-Access Resources and Latency Design Guidance on Cisco Communities.

Design

This guide covers the deployment of Cisco DNA Center and Cisco Identity Services Engine (ISE) within a services block or data center network connected to either a Cisco SD-Access fabric or traditional 3-tiered campus topology as shown in the figures below. The design and deployment of the campus network is not covered within this document. Additional network planning items for Cisco DNA Center and for the management infrastructure are also discussed.

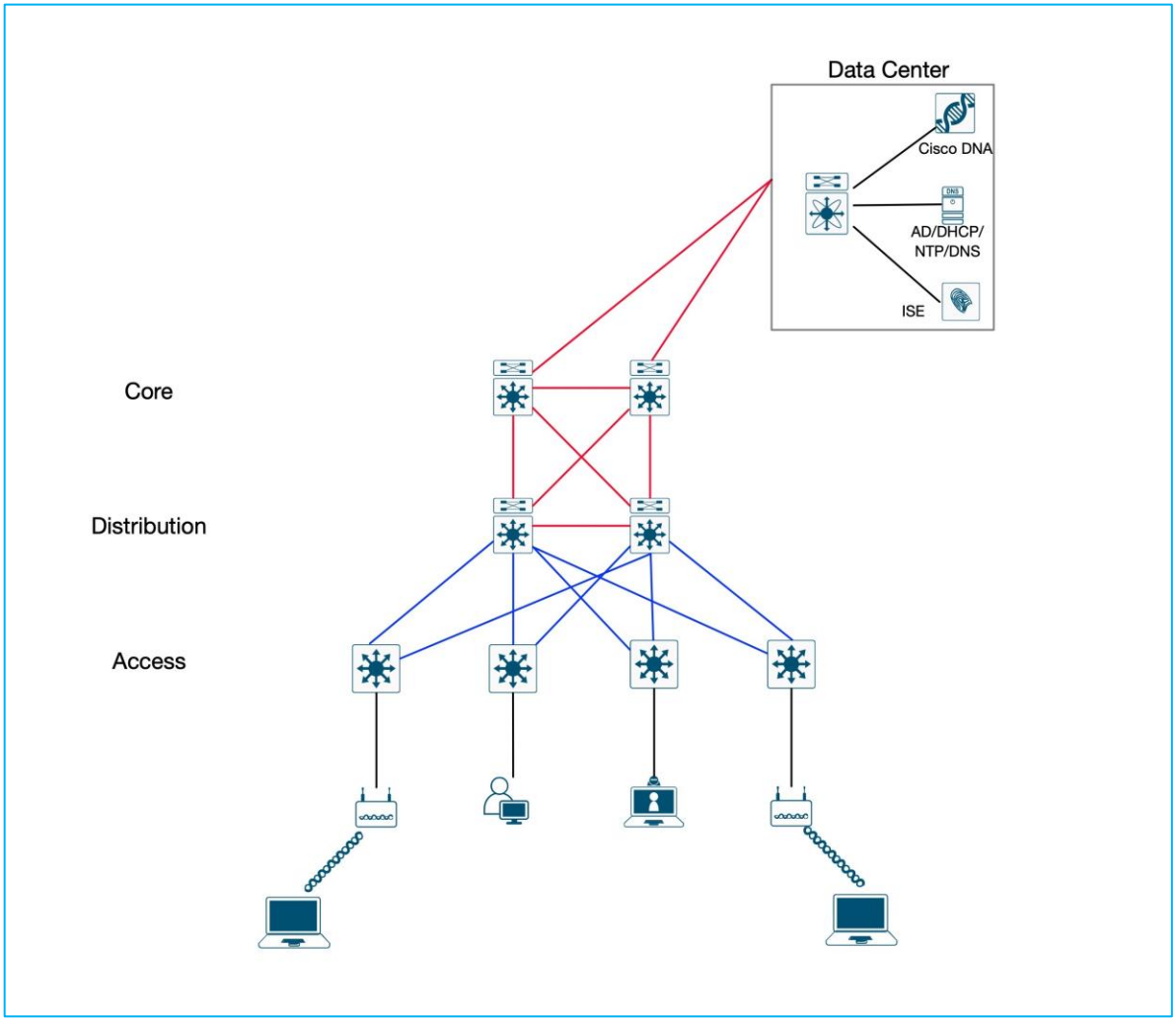
Topology Overview

Figure 1. Cisco SD-Access Design Topology



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

Figure 2. Traditional 3-Tiered Campus Design Topology



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 for time synchronization, 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 and Cisco Identity Services engine, and configure basic IP connectivity for this infrastructure. The basic 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

Cisco supplies Cisco Digital Network Architecture (DNA) Center in the form of a rack-mountable, physical appliance. There are currently two generations of the Cisco DNA Center appliance.

The first generation appliance (Cisco part number DN1-HW-APL) consists of a Cisco Unified Computing System (UCS) C220 M4 small form factor (SFF) chassis, with the addition of a Virtual Interface Card (VIC) 1227 in the mLOM slot. The following network connections are supported on the first generation appliance:

- Two 10-Gbps Ethernet ports on the Cisco UCS VIC 1227
- One 1-Gbps Ethernet dedicated management port
- Two 1-Gbps BASE-T Ethernet LAN ports

The second generation appliances consists of either a Cisco Unified Computing System (UCS) C220 M5 small form-factor (SFF) chassis or Cisco UCS C480 M5 chassis, both with the addition of one Intel X710-DA2 network interface card (NIC) and one Intel X710-DA4 NIC (currently unused). The following are the available Cisco part numbers for the second generation appliance:

- DN2-HW-APL – 1 RU, 44 core appliance
- DN2-HW-APL-L – 1 RU, 56 core appliance
- DN2-HW-APL-XL – 4 RU, 112 core appliance

The following network connections are supported on the second generation appliances:

- Two 10-Gbps Ethernet ports on the Intel X710-DA2 NIC

- One 1-Gbps RJ-45 management port (Marvell 88E6176)
- Two 10GBase-T LOM ports (Intel X550 controller embedded on the motherboard)

This guide discusses deployment with the second generation Cisco DNA Center appliance (DN2-HW-APL or DN2-HW-APL-L).

The deployment starts with a single-node cluster that uses a virtual IP (VIP) address configured on a single Cisco DNA Center appliance, easing the 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 supported.

Use the following table to assist with IP address assignment and connections. 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 second-generation M5-based appliances are numbered from right to left. The second generation M5-based appliances requires a basic interface access VLAN configuration for the Ethernet switch connection, as described in the associated installation guides.

Figure 3. Figure 3 Rear view of the second-generation Cisco DNA Center appliance – DN2-HW-APL (44 and 56 cores) (M5-based)

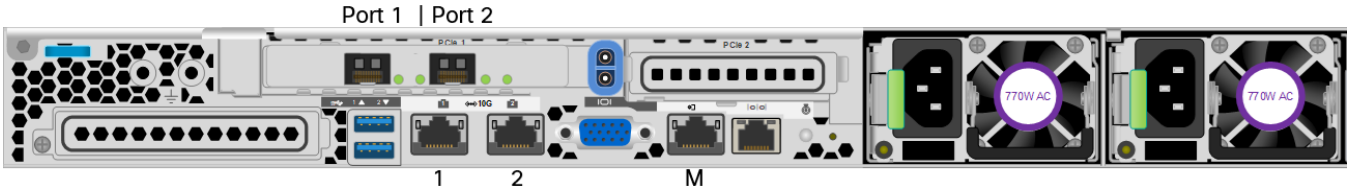


Table 1. Cisco DNA Center second generation appliance LAN Ethernet interface assignments

	PORT 1 PCIe SFP+ 10 Gbps	PORT 2 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	–
Use	Enterprise: Enterprise network infrastructure	Cluster: Intra-cluster communications	Management: Dedicated management network for web access	Cloud: Optional cloud network port for separate Internet connectivity	CIMC: Cisco Integrated Management Controller out-of-band server appliance management
Example cluster VIP address	10.4.48.151 255.255.255.0	10.4.49.151 255.255.255.0	–	–	–
Example interface address (node 1)	10.4.48.150 255.255.255.0	10.4.49.150 255.255.255.248	Unused in this example	Unused in this example	100.119.103.235 255.255.255.0
Example interface address (node 2)	10.4.48.160 255.255.255.0	10.4.49.160 255.255.255.0	Unused in this example	Unused in this example	100.119.103.236 255.255.255.0
Example interface address (node 3)	10.4.48.170 255.255.255.0	10.4.49.170 255.255.255.0	Unused in this example	Unused in this example	100.119.103.237 255.255.255.0

Tech tip

Connecting Cisco DNA Center to your network using a single network interface (enterprise network infrastructure, 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

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.

The described deployment uses the required minimum three ports on the Cisco DNA Center Appliance- the Cisco IMC port and both SFP+ ports. For your deployment, connect any other ports as needed, such as the dedicated web management port or the cloud network port for separate Internet connectivity. These ports are not used for this deployment guide.

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 PCIe card (named enp94s0f0 in the wizard).

- Using the 10 Gbps port SFP+ labeled PORT 2 on the PCIe card (named enp94s0f1 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 (CIMC) port (labeled with a gear symbol or letter M on the integrated copper Ethernet ports).

The following example steps are described in detail 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.

Step 2. Boot the Cisco DNA Center hardware appliance.

A welcome message appears, as shown below.

```
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; 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:
  10.4.48.150
Netmask:
  255.255.255.0
Default Gateway IP Address:
  10.4.48.1
DNS Servers:
  10.4.48.10
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:
  10.4.49.150
Netmask:
  255.255.255.0
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 Virtual IP (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 and NTP server entries using ICMP. Do not restrict ICMP echo communication between the appliance and any configured DNS and NTP servers.

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. If the wizard detects a network proxy server, you will be 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 7. 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 any order, and each VIP must be separated with a space.

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

```
Cluster Virtual IP address(s):
    10.4.48.151 10.4.49.151
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 8. 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: *
  10.4.48.17
```

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

```
Validating NTP Server: 10.4.48.17 ...
```

Step 10. 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: *
  192.168.0.0/21
Cluster Services Subnet: *
  192.168.8.0/21
```

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

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

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

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 12. 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 13. 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
```

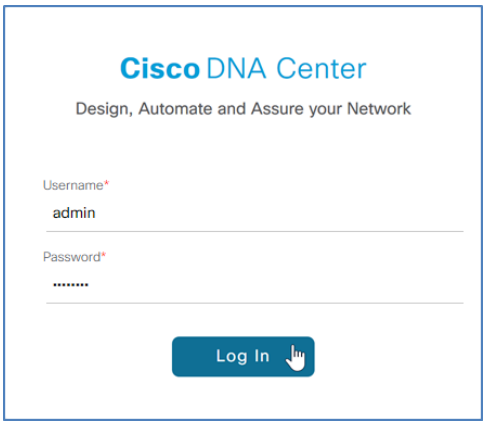
This guide demonstrates how to upgrade Cisco DNA Center to the next version. Therefore, these packages will remain NOT_DEPLOYED at this point in the installation, as they will be upgraded and installed in later steps.

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://10.4.48.151).

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**.

Figure 4. Cisco DNA Center login



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.

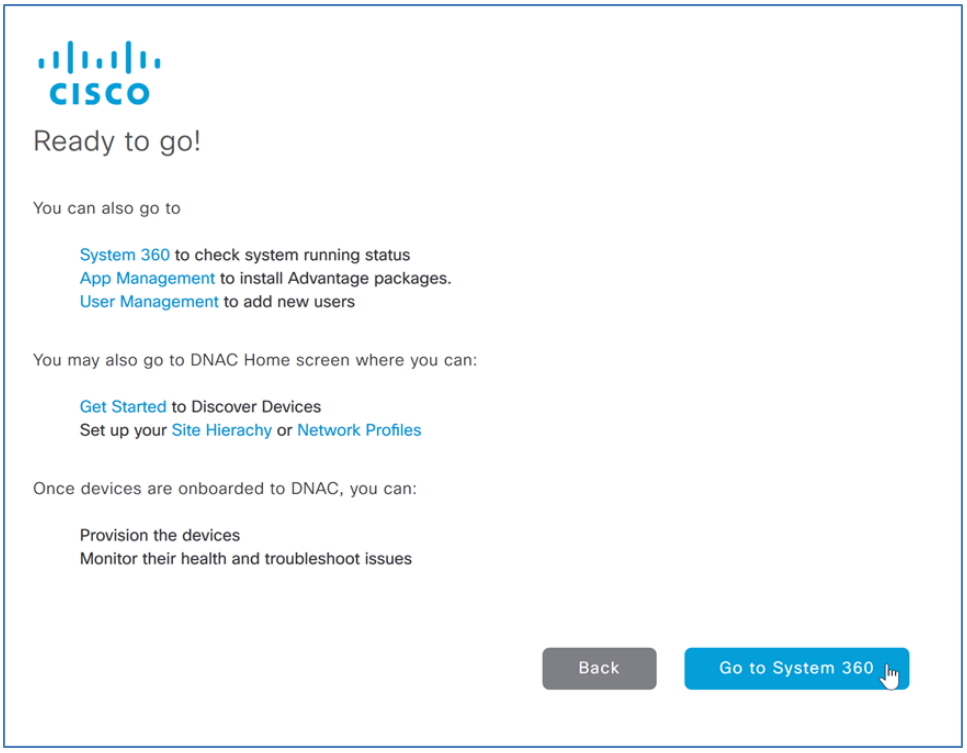
Step 5. In the previous step, if you did not enter an ID with Smart Account access with privileges for managing Cisco software licenses for your organization, a **Smart Account** prompt displays. Enter a Cisco.com ID associated with a Smart Account or click **Skip**.

Step 6. If you have an IP address management (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**.

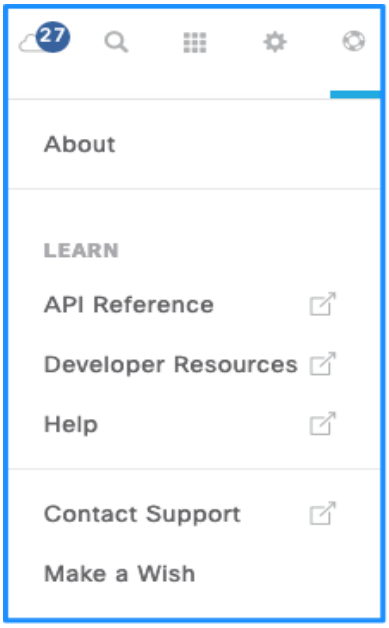
Step 8. At the **Terms and Conditions** display, click **Next**, and then at the **Ready to go!** display, click **Go to System 360**.

Figure 5. Ready to go! screen



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

Figure 6. Cisco DNA Center Help → About



Step 10. Check the Cisco DNA Center version.

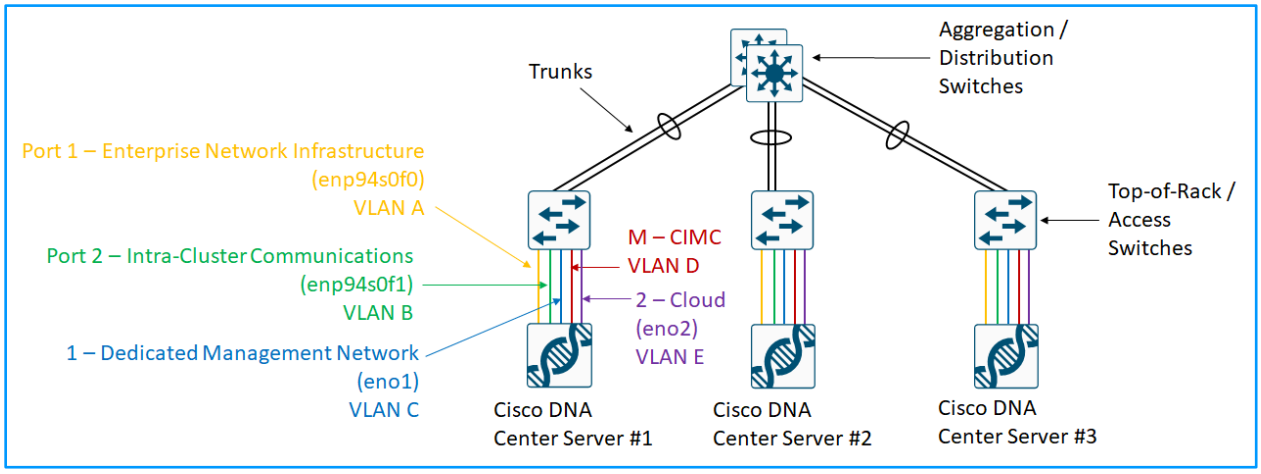
Figure 7. Displaying the Cisco DNA Center version

If you are using a first generation M4-based appliance (DN1-HW-APL), 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 Cisco 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 Cisco cloud catalog server. Newer second generation 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

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. An example is shown in the figure below.

Figure 8. Example Network Resiliency in a 3-Node Cluster



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.

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 switch port in your network, by:

- Using the 10 Gbps SFP+ port labeled PORT 1 on the PCIe card (named enp94s0f1 in the wizard).
- Using the 10 Gbps port SFP+ labeled PORT 2 on the PCIe card (named enp94s0f0 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 (CIMC) 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:
  10.4.48.160
Netmask:
  255.255.255.0
Default Gateway IP Address:
  10.4.48.1
DNS Servers:
  10.4.48.10
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:
  10.4.49.160
Netmask:
  255.255.255.0
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: *
    10.4.49.150
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: *
  10.4.48.17
```

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

The installation validates connectivity to the NTP servers.

```
Validating NTP Server: 10.4.48.17 ...
```

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    ROLES     AGE       VERSION
10.4.49.150     Ready     master    1d        v1.11.5
10.4.49.160     Ready     master    22h       v1.11.5
```

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:
  10.4.48.170
Netmask:
  255.255.255.0
Default Gateway IP Address:
  10.4.48.1
DNS Servers:
  10.4.48.10
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:
  10.4.49.170
Netmask:
  255.255.255.0
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: *
    10.4.49.150
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: *
  10.4.48.17
```

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

The installation validates connectivity to the NTP servers.

```
Validating NTP Server: 10.4.48.17 ...
```

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    ROLES     AGE       VERSION
10.4.49.150     Ready     master    1d        v1.11.5
10.4.49.160     Ready     master    22h       v1.11.5
10.4.49.170     Ready     master    2h        v1.11.5
```

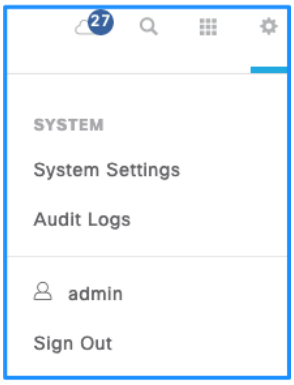
Step 27. Verify that which of the Cisco DNA Center is node 0, 1 and 2

```
$ magctl node display
NAME          STATUS    ROLES     AGES      VERSION
10.4.49.150   Ready     master    5d        v1.11.5
allAppstacks=enabled,appstack.assurance-backend=enabled,appstack.dnac-
search=enabled,appstack.dnacaap=enabled,appstack.fusion=enabled,appstack.maglev-
system=enabled,appstack.ndp=enabled,beta.kubernetes.io/arch=amd64,beta.kubernetes.io/os
=linux,compute=allowed,data=allowed,dna_role=DNA,kubernetes.io/hostname=10.4.49.150,mac
hine_profile=t2_large,node-role.kubernetes.io/master=,nodename=node-
0,roles=master,web=allowed
10.4.49.160   Ready     master    4d        v1.11.5
allAppstacks=enabled,appstack.assurance-backend=enabled,appstack.dnac-
search=enabled,appstack.dnacaap=enabled,appstack.fusion=enabled,appstack.maglev-
system=enabled,appstack.ndp=enabled,beta.kubernetes.io/arch=amd64,beta.kubernetes.io/os
=linux,compute=allowed,data=allowed,dna_role=DNA,kubernetes.io/hostname=10.4.49.160,mac
hine_profile=t2_large,node-role.kubernetes.io/master=,nodename=node-
1,roles=master,web=allowed
10.4.49.170   Ready     master    4d        v1.11.5
allAppstacks=enabled,appstack.assurance-backend=enabled,appstack.dnac-
search=enabled,appstack.dnacaap=enabled,appstack.fusion=enabled,appstack.maglev-
system=enabled,appstack.ndp=enabled,beta.kubernetes.io/arch=amd64,beta.kubernetes.io/os
=linux,compute=allowed,data=allowed,dna_role=DNA,kubernetes.io/hostname=10.4.49.170,mac
hine_profile=medium,node-role.kubernetes.io/master=,nodename=node-
2,roles=master,web=allowed
```

Step 28. Log in to the Cisco DNA Center web interface by directing a web browser to the cluster VIP address (example: https://10.4.48.151/).

Step 29. At the main Cisco DNA Center dashboard, click the settings (gear) icon, and then click **System Settings**.

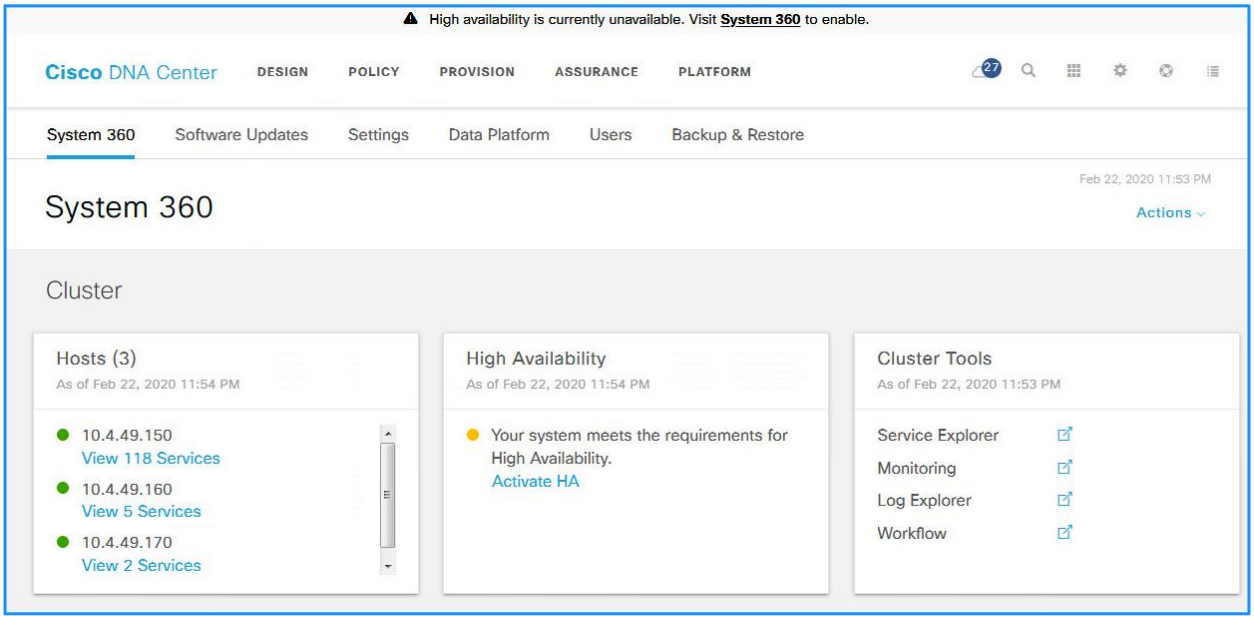
Figure 9. Cisco DNA Center Help → System Settings



Tech tip
In a 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.

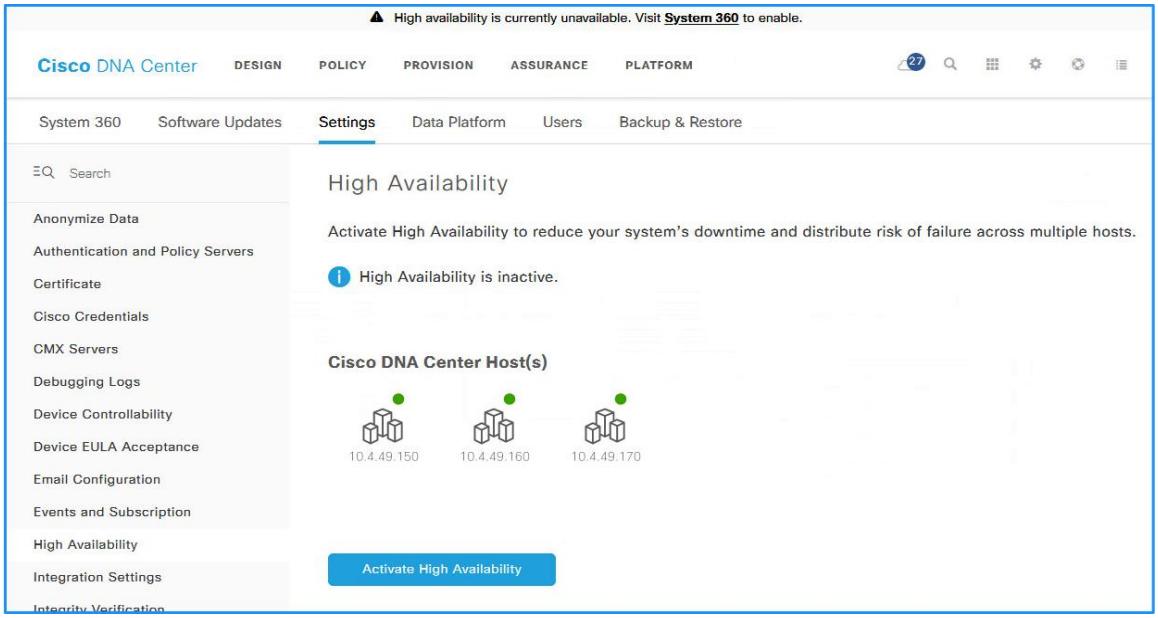
Step 30. In the **High Availability** box, click on **Activate HA** and then at the warning message click **Continue**.

Figure 10. System 360 – High Availability



Step 31. After clicking on **Activate HA**, it will go to the **Settings** screen, there you click on **Activate High Availability**.

Figure 11. **Activate High Availability**

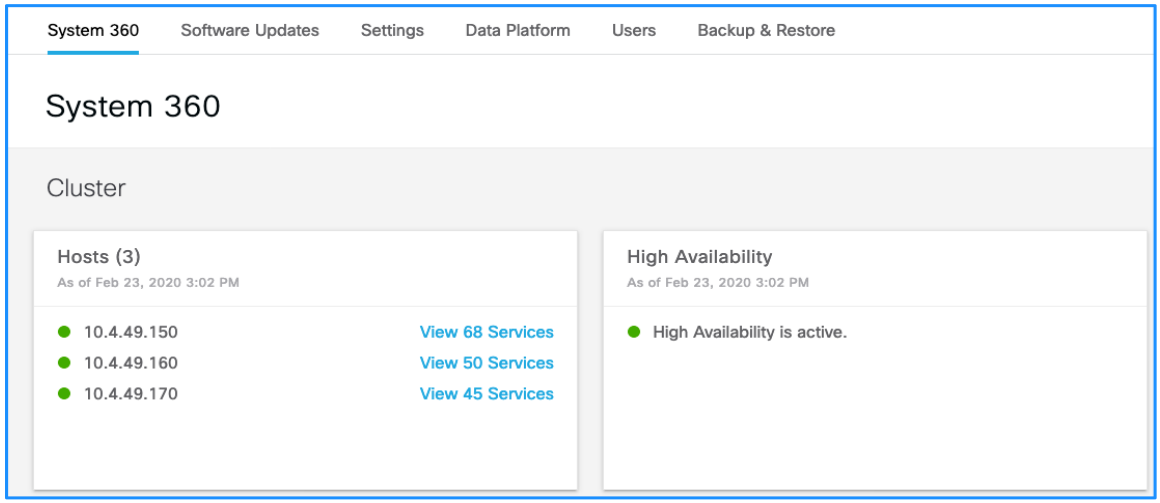


After click on the **Activate High Availability**, you will see the following screen.

Figure 12. **High Availability Activation – Maintenance Mode**

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

Figure 13. High Availability Activated



Procedure 4. Update the Cisco DNA Center software

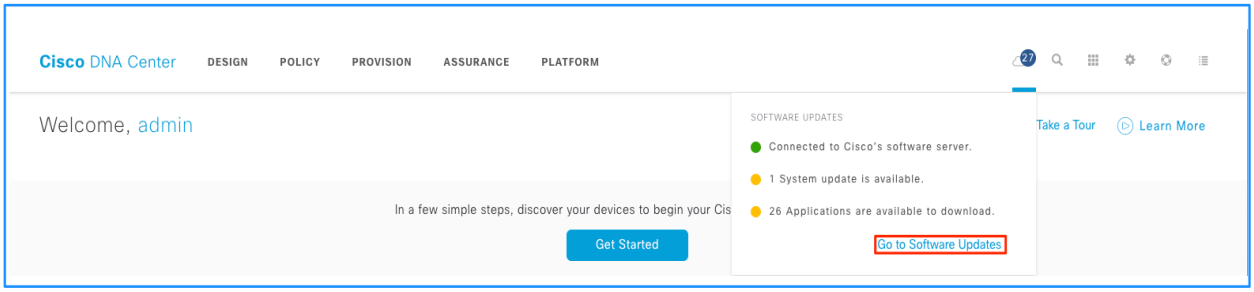
Updating Cisco DNA Center software is a two-step process – first update the system package (system version), then update the application packages (application versions).

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 1.3.1.x, 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.

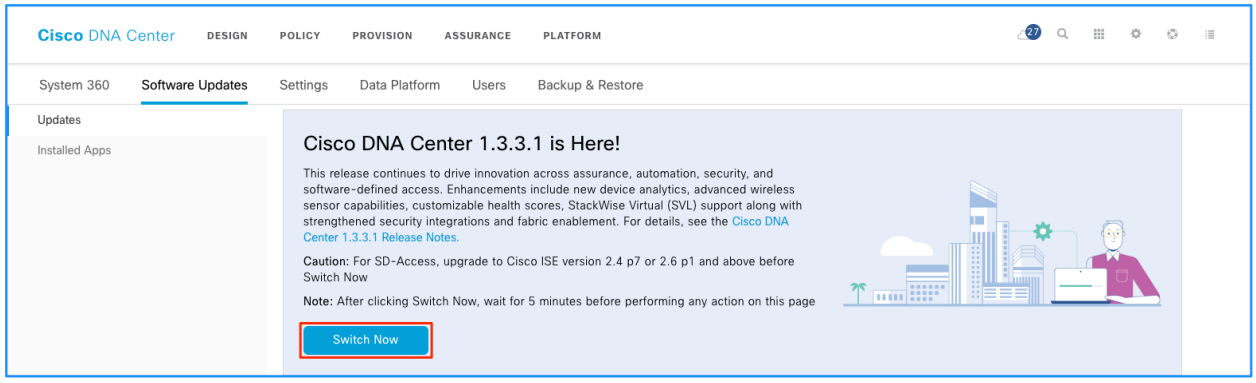
Step 1. At the main Cisco DNA Center dashboard, at the top right of the window, click the **Software Updates** (cloud) button, and then click **Go to Software Updates**.

Figure 14. Navigating to Software Updates



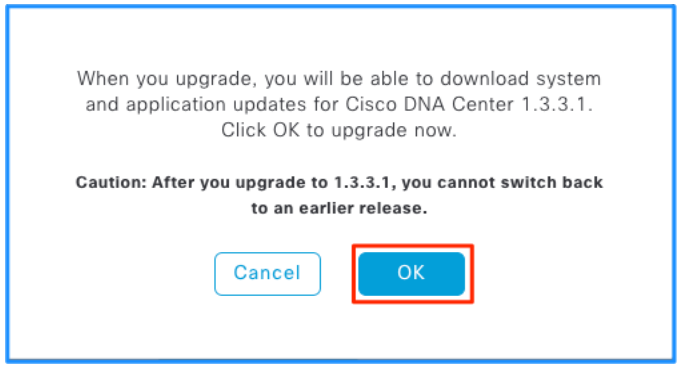
The **Settings > Software Updates > Updates** screen appears. This screen is used to install updates and packages that add functionality to the controller, including Cisco SD-Access. For significant system-wide updates, an announcement is displayed at the top of the updates window.

Figure 15. Example of significant system-wide update



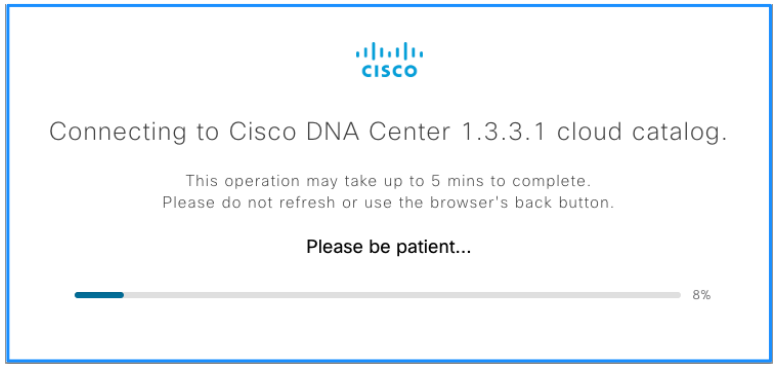
Step 2. Click the **Switch Now** button, and then acknowledge that the migration is irreversible by clicking **OK**.

Figure 16. Confirming the software update



Cisco DNA Center connects to the cloud catalog server.

Figure 17. Contacting the Cisco cloud catalog server



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.

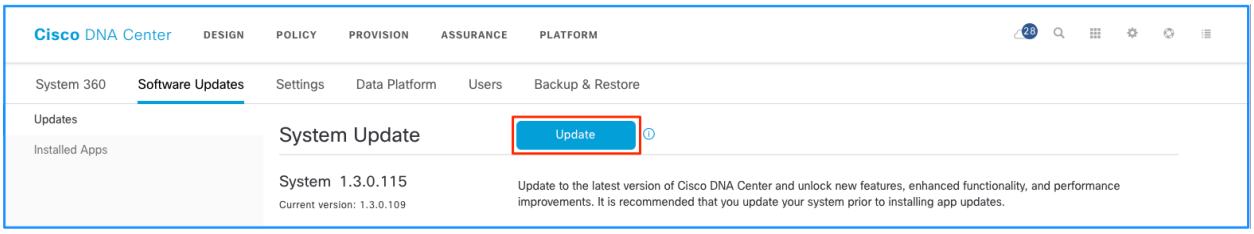
Step 3. Immediately to the right of the available system update, click the **Update** button, click **Continue**, and then click **Continue**.

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.

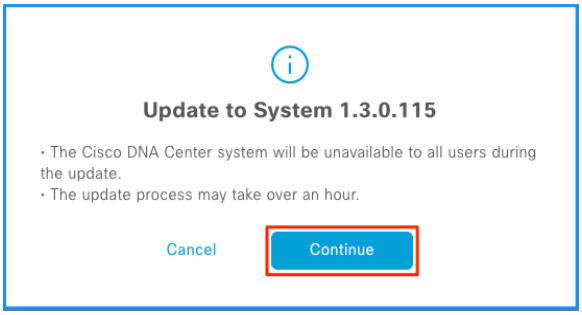
Do not switch to a new version of Cisco DNA Center until you have completely updated the system. Before switching, check the listing of permitted update paths in the Cisco Digital Network Architecture Center Upgrade Guide.

Figure 18. Updating the System package



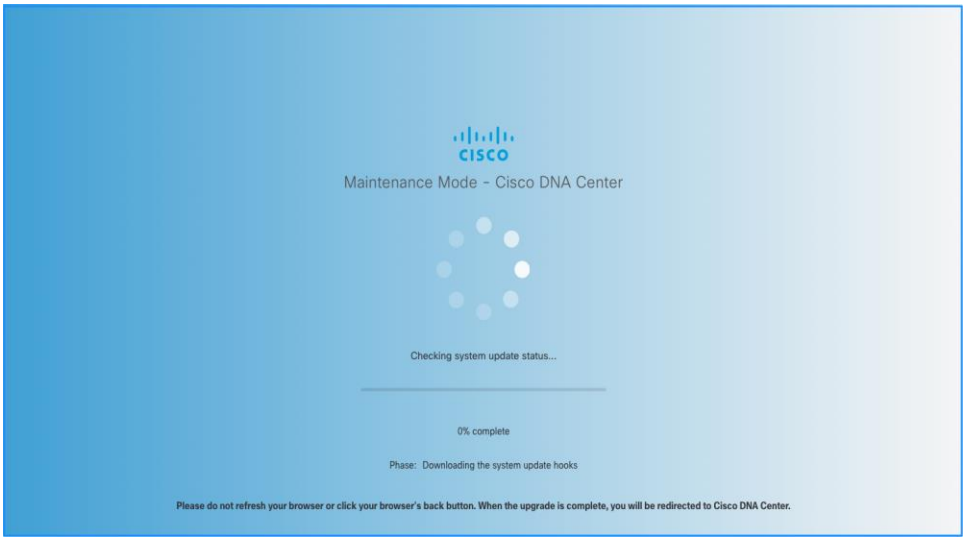
Another screen will pop up to say that the system will unavailable for the next hour

Figure 19. Notification of system update



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.

Figure 20. System update in progress



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

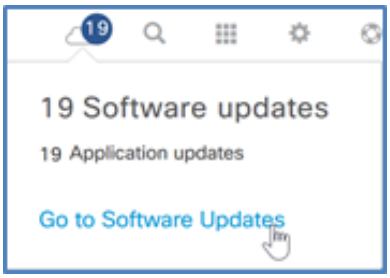
Procedure 5. Upgrade the Cisco DNA Center application packages

When Cisco DNA Center is running the latest system update, you upgrade the application packages to the versions associated with the updated system version. Updating application packages is a three-step process – download the application packages (and dependencies), update the application packages, and install the application packages.

Step 4. Log in to the Cisco DNA Center web interface and navigate to the main dashboard.

Step 5. In the top right of the Cisco DNA Center dashboard, click the **Software Updates** (cloud) button, and then click **Go to Software Updates**.

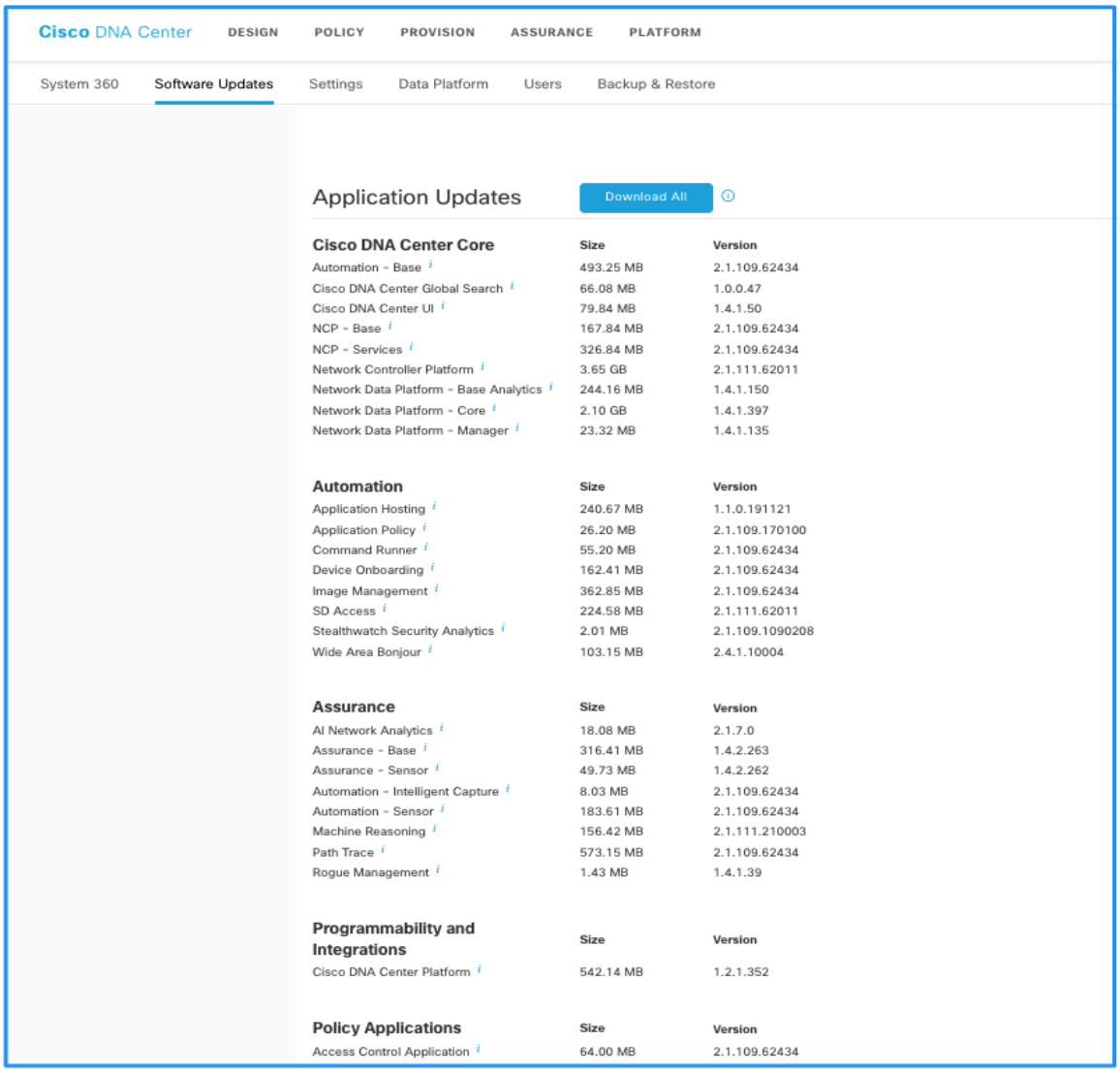
Figure 21. Navigating to Software Updates



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

Step 6. At the top right of the screen, on the same row as **Application Updates**, click the upper **Download All** button.

Figure 22. **Application updates ready for download**



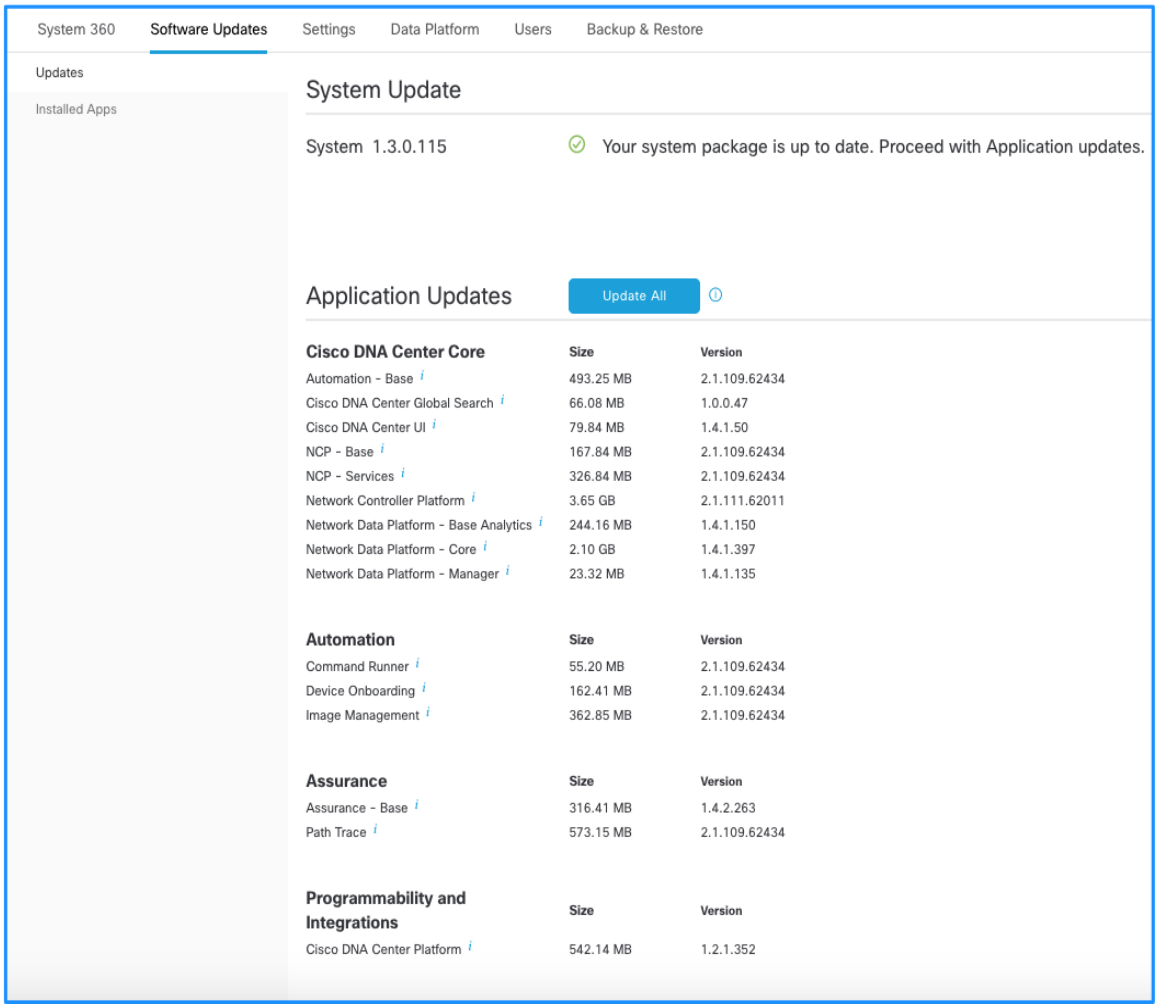
Step 7. At the pop-up window, click **Continue** to confirm the update operation, and then, at the second **System Readiness Check** pop-up window, click **Continue**.

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.

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.

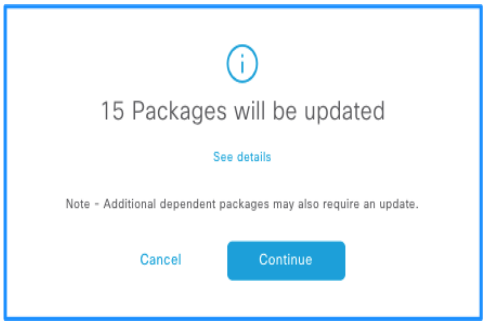
Step 8. After the downloads complete, there will be an **Update All** button. Click **Update All.**

Figure 23. **Application updates ready for update**



Step 9. Click **Continue** in the notification screen.

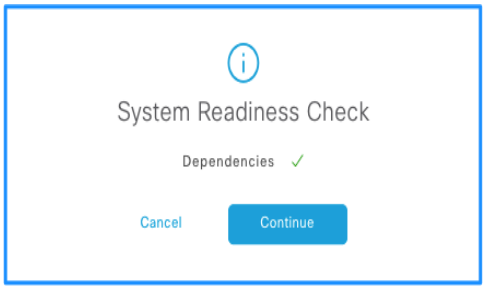
Figure 24. **Notification of application updates**



There will be a **System Readiness Check** screen with a dependency check mark, indicating all dependencies have been met.

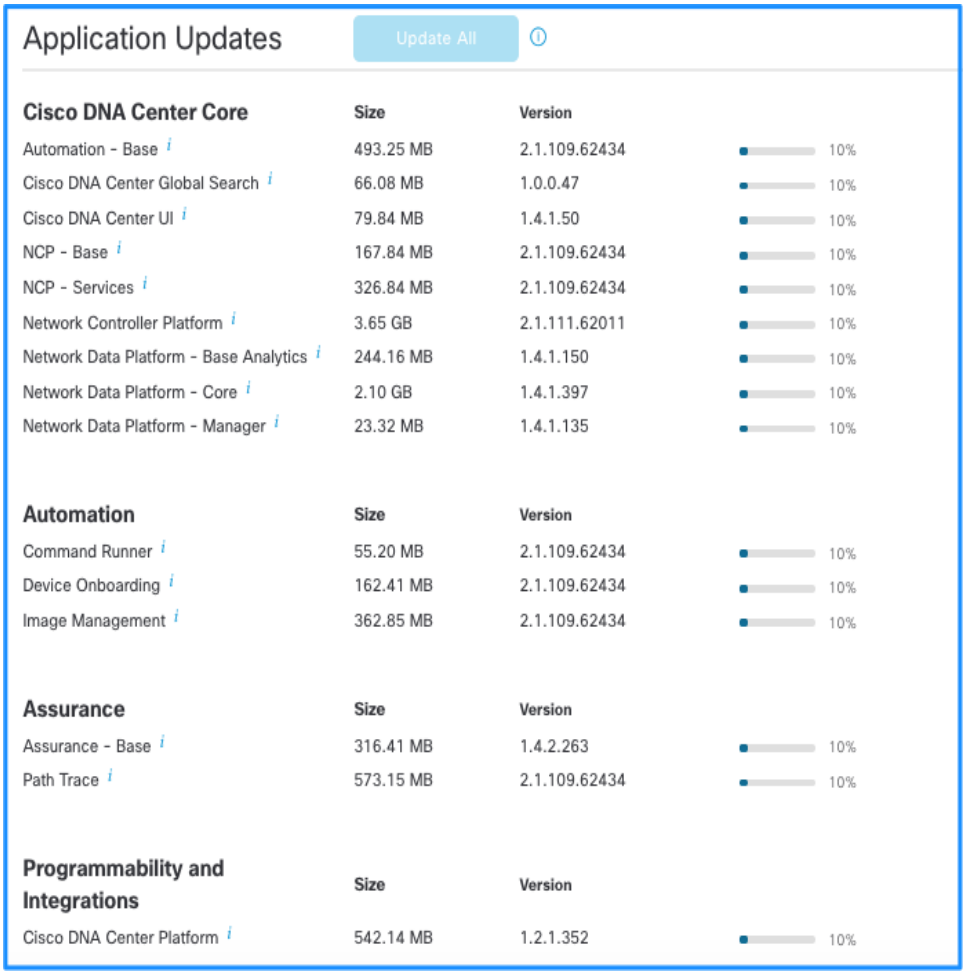
Step 10. Click on **Continue** to proceed with the update.

Figure 25. **System Readiness Check screen**



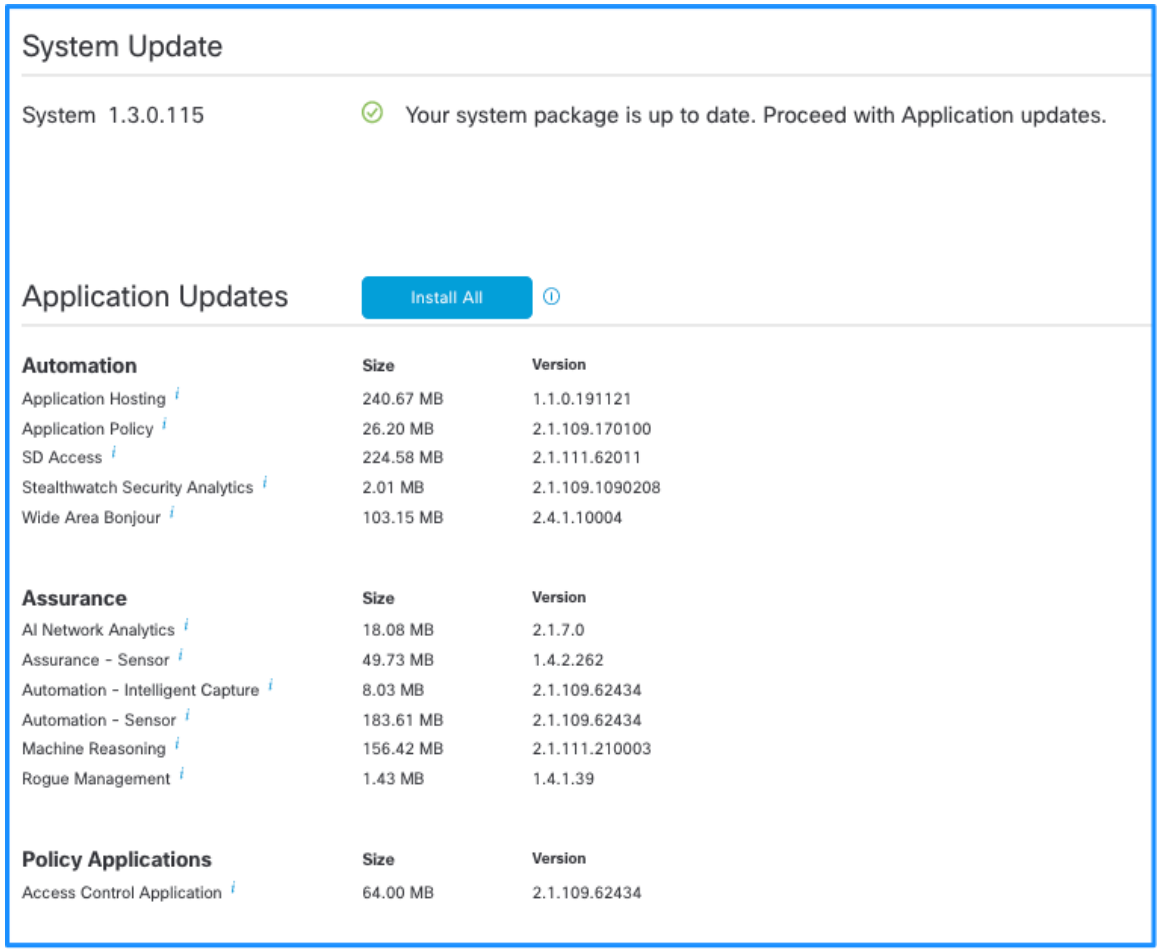
The following screen will pop up indicating the packages are being updated.

Figure 26. **Application packages being updated**



Step 11. 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.

Figure 27. Application package installation



Step 12. 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.

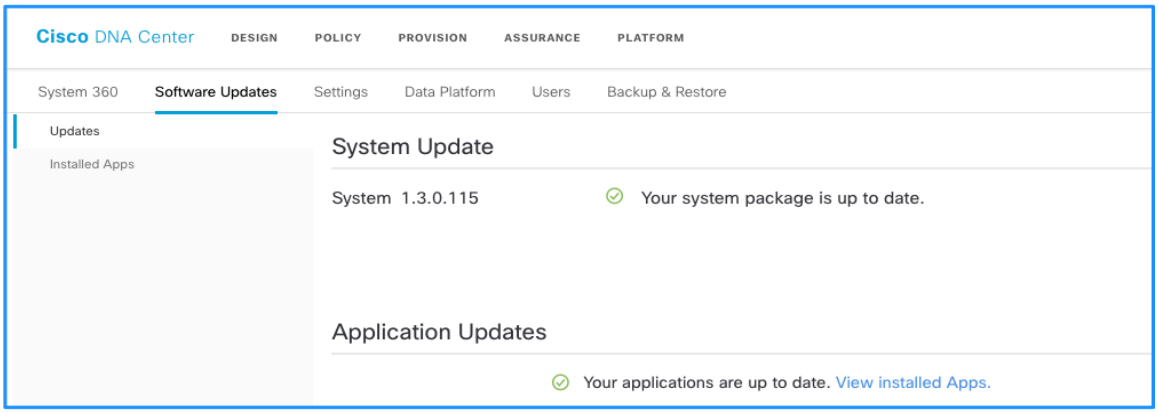
The remaining package installations begin. The browser refreshes automatically, showing the updated status for each package. The installation process can take over an hour to complete.

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.

Figure 28. **System and application packages up to date**



Continue to the next step after all packages are installed.

Step 13. In the top right of the main Cisco DNA Center dashboard, click the help (life preserver) icon and then click **About**.

This view is useful for accessing the release notes for the version you are running, which are available by clicking **Release Notes**.

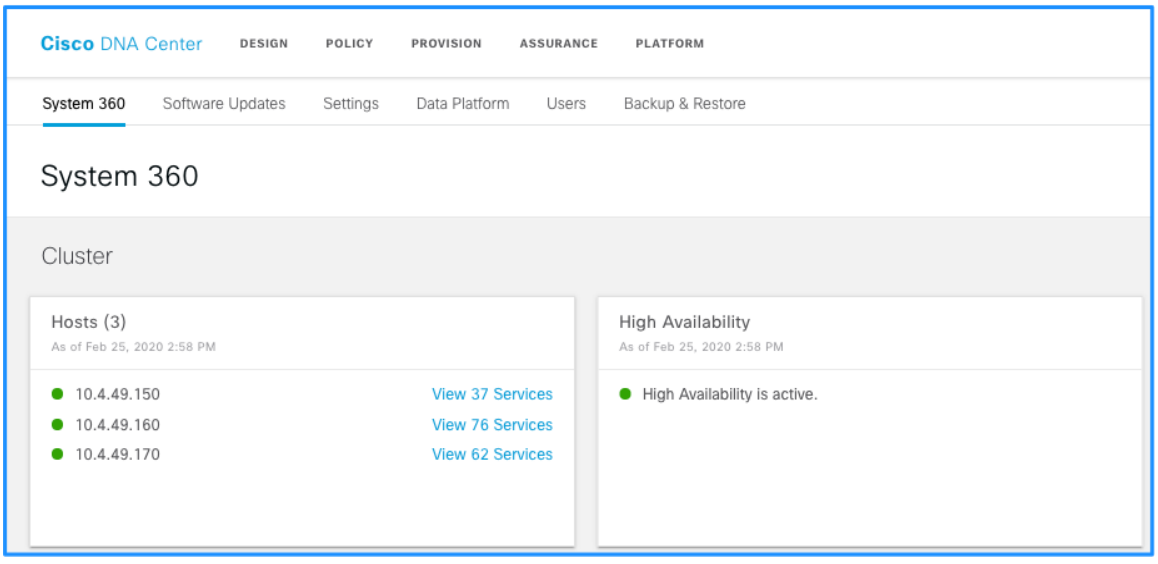
Figure 29. **Displaying the Cisco DNA Center version**

In this view you can also view the packages installed and serial number of the server. In this case, there are three serial number since this deployment is a cluster of three Cisco DNA Center servers.

Figure 30. **Displaying installed packages**

Step 14. At the main Cisco DNA Center dashboard, click the Settings (gear) icon, and then click **System Settings**. The status for each of the hosts in the cluster is shown.

Figure 31. **Displaying the status of the hosts in a Cisco DNA Center cluster**



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

With all application packages installed and all hosts in the cluster showing a status of running, integration with Cisco ISE can proceed.

Process 2: Installing Cisco Identity Services Engine nodes

The SD-Access solution described in this guide uses two Cisco ISE nodes in a high-availability standalone configuration, integrated with Cisco DNA Center. The first Cisco ISE node has the primary policy administration node (PAN) persona configuration and the secondary monitoring and troubleshooting (MnT) persona configuration. The second Cisco 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 Cisco ISE nodes.

Table 2. Cisco ISE node configurations

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

Tech tip

The Cisco 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 Cisco 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 Cisco ISE server images

Before you begin, you must identify the following:

- IP addressing and network connectivity for all Cisco ISE nodes being deployed.
- A network-reachable Network Time Protocol (NTP) server, used during Cisco 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 Cisco ISE distributed deployments.
- Certificate server information, when self-signed digital certificates are not used.

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

Step 2. On the console of the first Cisco 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[]: dna-ise1
Enter IP address []: 10.4.48.20
Enter IP netmask[]: 255.255.255.0
Enter IP default gateway[]: 10.4.48.1
Enter default DNS domain[]: cisco.local
Enter Primary nameserver[]: 10.4.48.10
Add secondary nameserver? Y/N [N]: N
Enter NTP server[time.nist.gov]: 10.4.48.17
Add another NTP server? Y/N [N]: N

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, use the following parameters for the second node

```
Hostname – dna-ise2
IP address – 10.4.48.21
```

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

```
localhost login:
```

Procedure 2. Configure roles for first Cisco ISE node

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

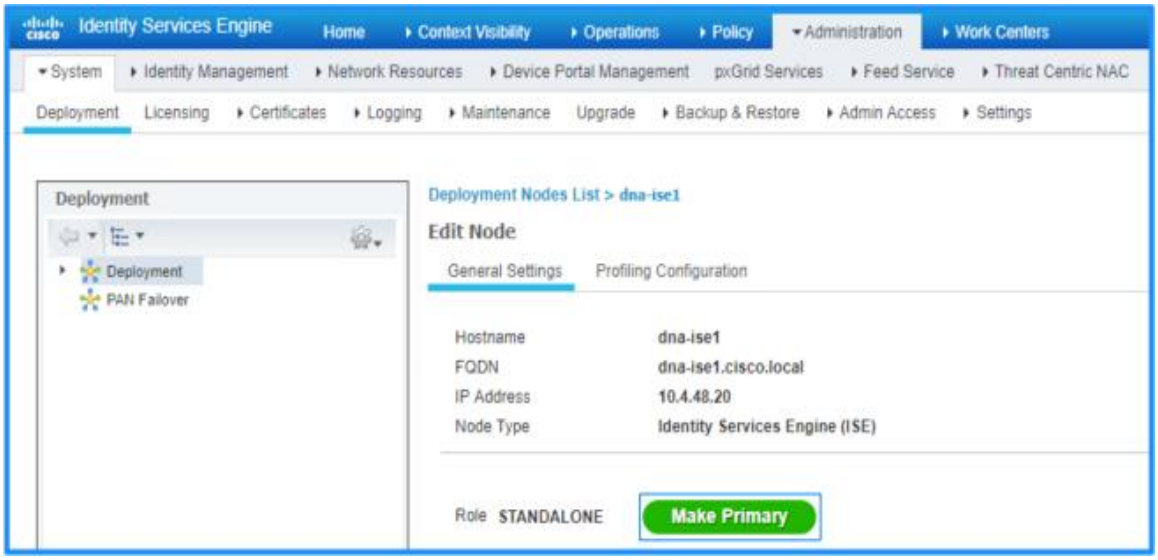
https://dna-ise1.cisco.local

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

Figure 32. **Cisco ISE – Administration > System > Deployment**

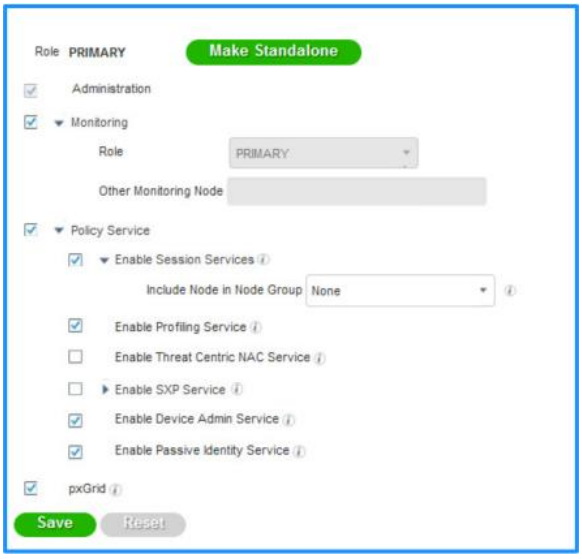
Step 3. Click on the first Cisco ISE node under hostname on the right pane window, and then, under **Role**, click **Make Primary**.

Figure 33. **Assign the first Cisco ISE node to the Primary role**



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

Figure 34. **Enable Policy Service and pxGrid for primary Cisco ISE node**



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.

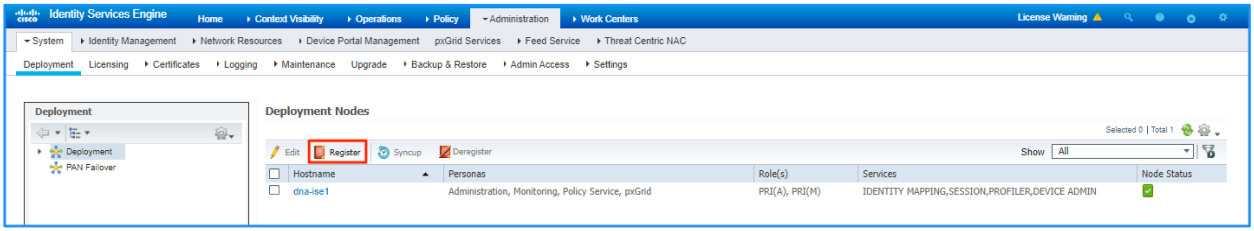
Procedure 3. Register the second Cisco ISE node and configure roles

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

Tech tip
Cisco 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**.

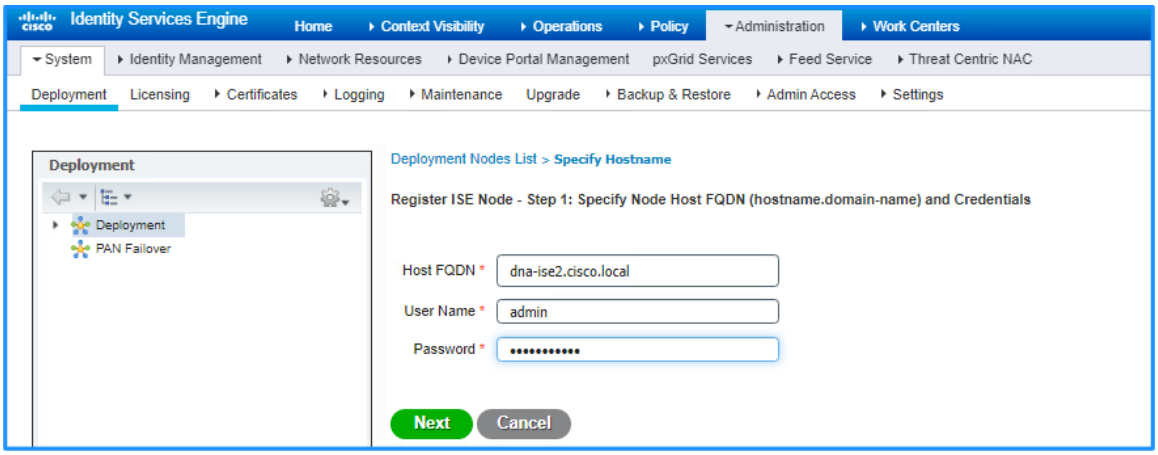
Figure 35. Register the second Cisco ISE node



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

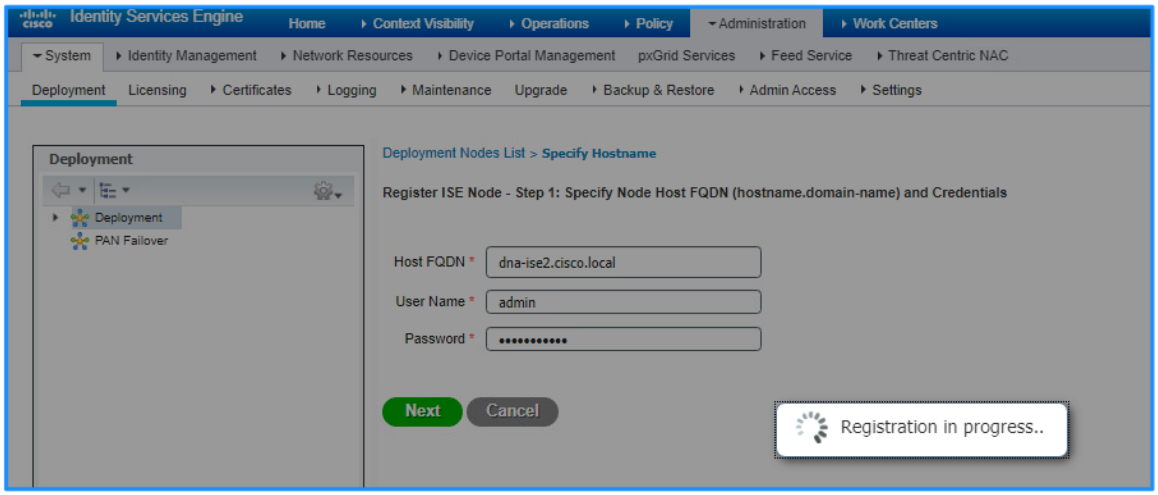
Step 2. Enter the Cisco ISE fully-qualified domain name **Host FQDN** (***dna-ise2.cisco.local***), **User Name** (***admin***), and **Password** (***[admin password]***), and then click **Next**.

Figure 36. FQDN and credentials for the second Cisco ISE node



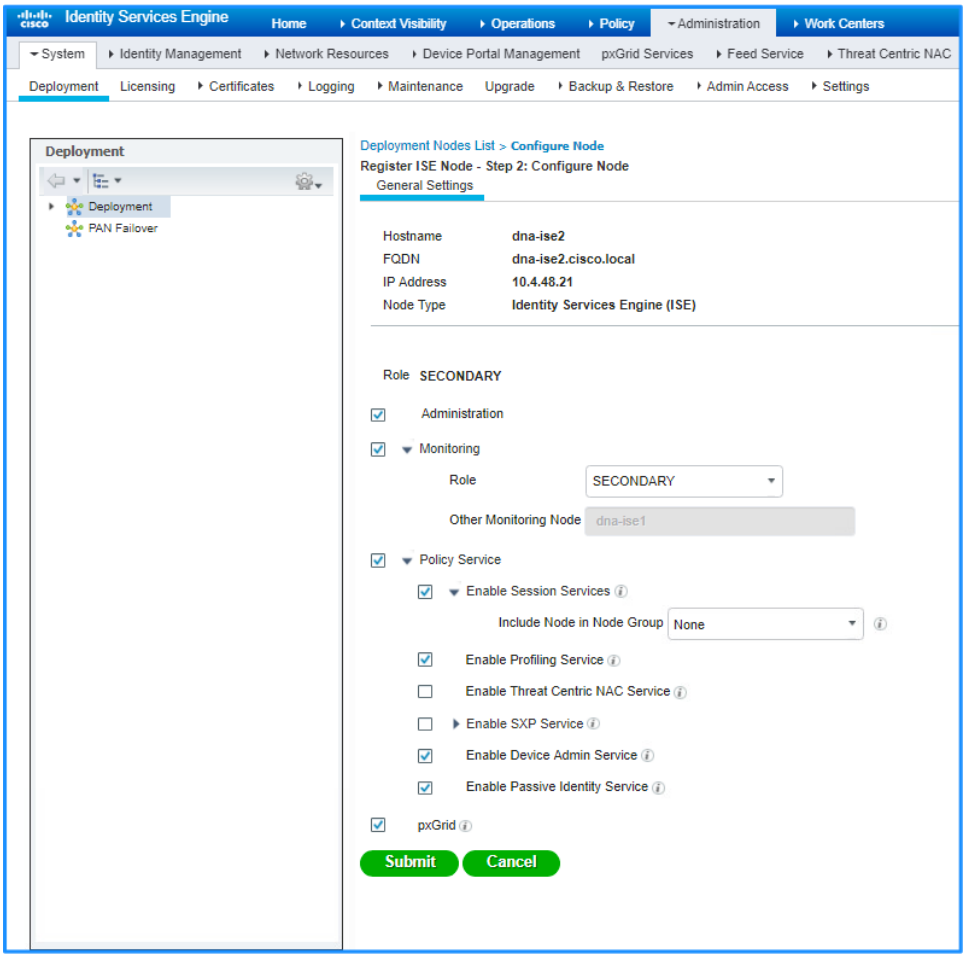
Step 3. If you are using self-signed certificates, click **Import Certificate and Proceed**. If you are not using self-signed certificates, follow the instructions for importing certificates and canceling this registration, and then return to the previous step. It will take a couple of minutes to process the registration.

Figure 37. Cisco ISE second node registration in progress



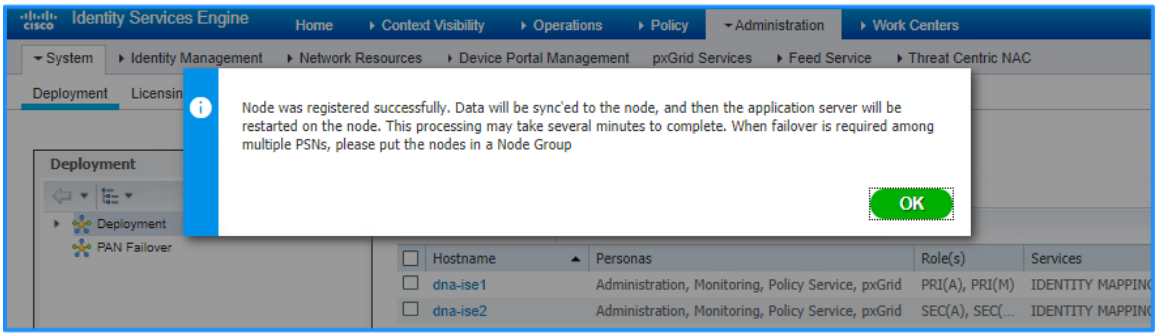
Step 4. On the **Register ISE Node – Step 2: Configure Node** screen, under **Monitoring**, leave the role as **SECONDARY**. Under **Policy Service**, select **Enable Device Admin Service** and **Enable Passive Identity Service**, select **pxGrid**, and then click **Submit**.

Figure 38. Enable Policy Service and pxGrid for secondary Cisco ISE node



The node configuration is saved and registered successfully

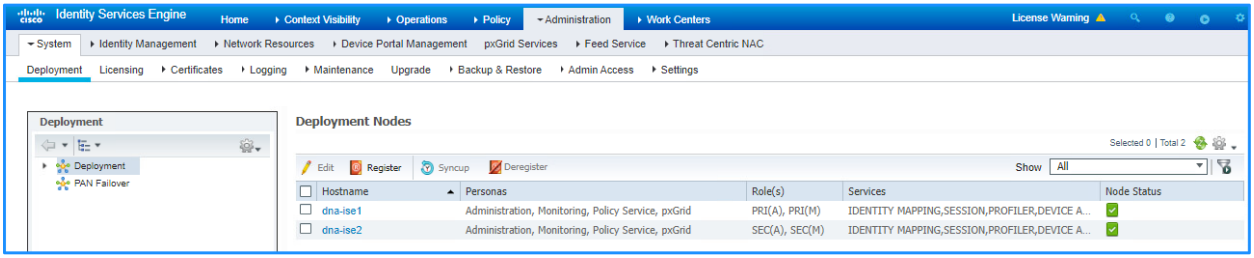
Figure 39. **Successful registration of the secondary Cisco ISE node**



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.

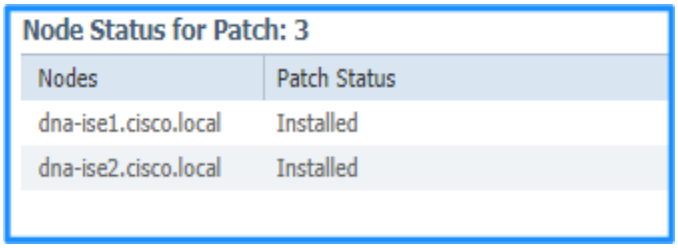
Figure 40. **Primary and secondary Cisco ISE nodes synchronized**



Step 6. Check Cisco.com for Cisco 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 Cisco 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.

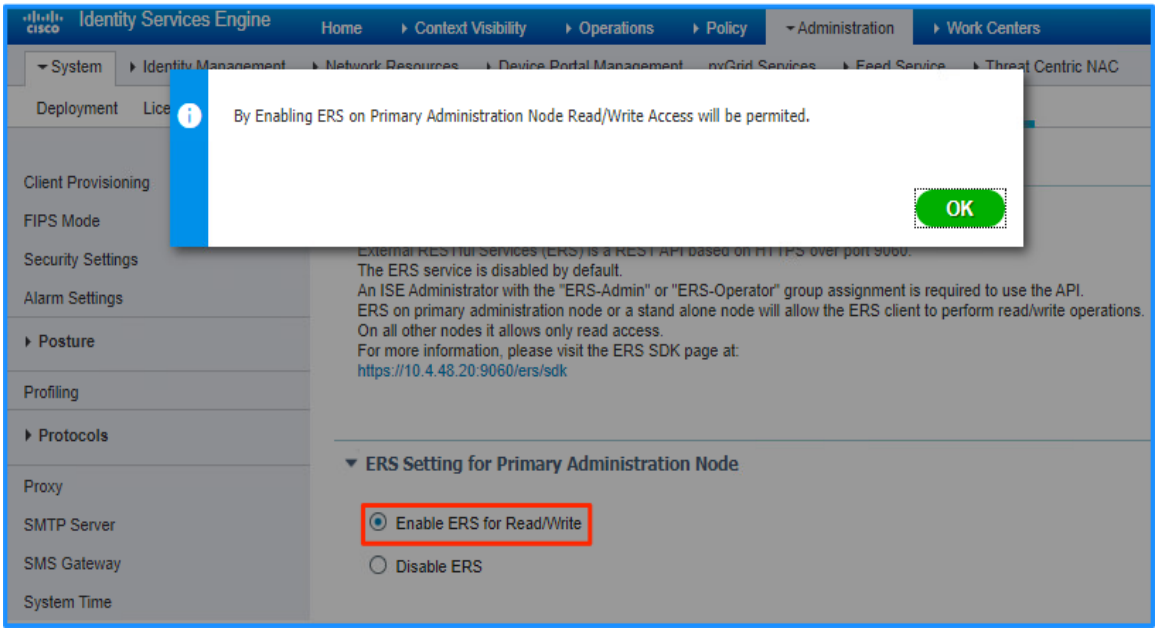
Step 7. After the Cisco ISE web interface is active again, check the progress of the patch installation by navigating to **Administration > System > Maintenance > Patch Management**, select the patch, and then select **Show Node Status**. Use the **Refresh** button to update status until all nodes are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

Figure 41. **Cisco ISE patches installed**



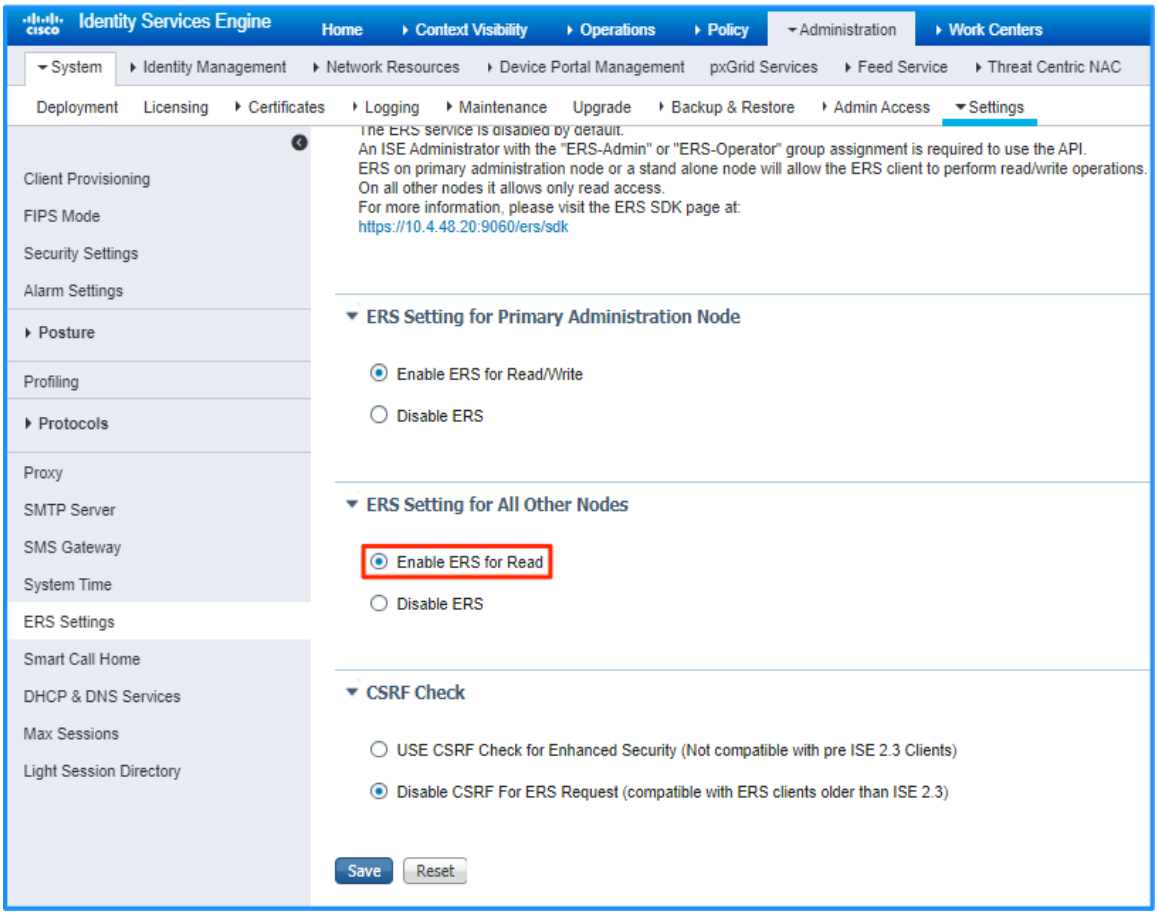
Step 8. Navigate to **Administration > System > Settings**. On the left pane, navigate to **ERS Settings**. Under **ERS Setting for Primary Administration Node**, select **Enable ERS for Read/Write**, and accept any dialog box that appears.

Figure 42. **Enabling External RESTful Services (ERS) for the primary Cisco ISE node**



Step 9. 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.

Figure 43. **Enabling ERS for the secondary Cisco ISE node**



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

Operate

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

Process 1: Integrating Cisco Identity Services Engine (ISE) with Cisco DNA Center

Integrate Cisco ISE with Cisco DNA Center by defining Cisco ISE as an authentication and policy server to Cisco DNA Center and permitting pxGrid connectivity from Cisco DNA Center into Cisco 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 Cisco ISE.

Tech tip

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

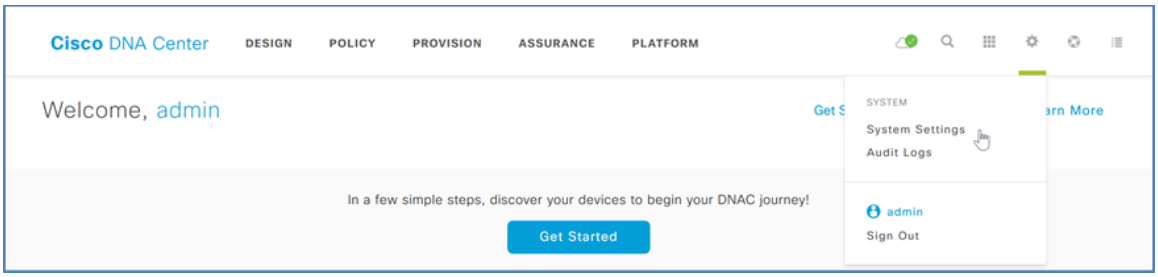
The versions of Cisco ISE and Cisco DNA Center validated in HA standalone mode for this guide are listed in Appendix A: Product List. You may find alternative recommended images in the latest Cisco SD-Access Hardware and Software Compatibility Matrix.

Procedure 4. Configure Cisco DNA Center authentication and policy servers

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

Example - https://<Cisco_Cisco_DNA_Center_IPaddr_or FQDN>

Figure 44. Navigating to Cisco DNA Center – System Settings

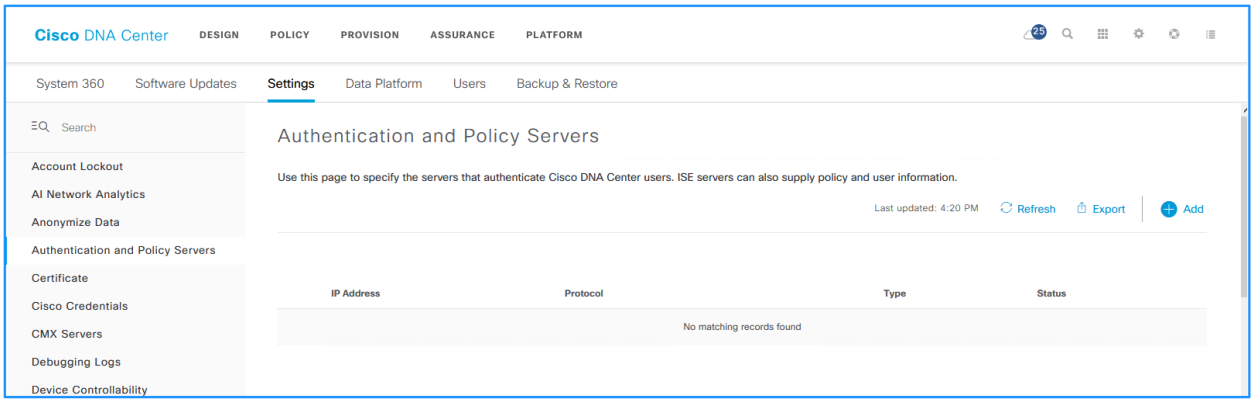


Step 2. Navigate to **Settings > Authentication and Policy Servers**, and then click the **+ Add** button.

Tech tip

The next step for integrating a Cisco ISE installation is the same whether you use a high-availability standalone Cisco ISE deployment, as shown in this example, or a distributed Cisco 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 Cisco ISE using SSH and must be the default super admin account that was created during the Cisco ISE installation. The Cisco ISE CLI and GUI passwords must be the same.

Figure 45. **Cisco DNA Center Authentication and Policy Servers**



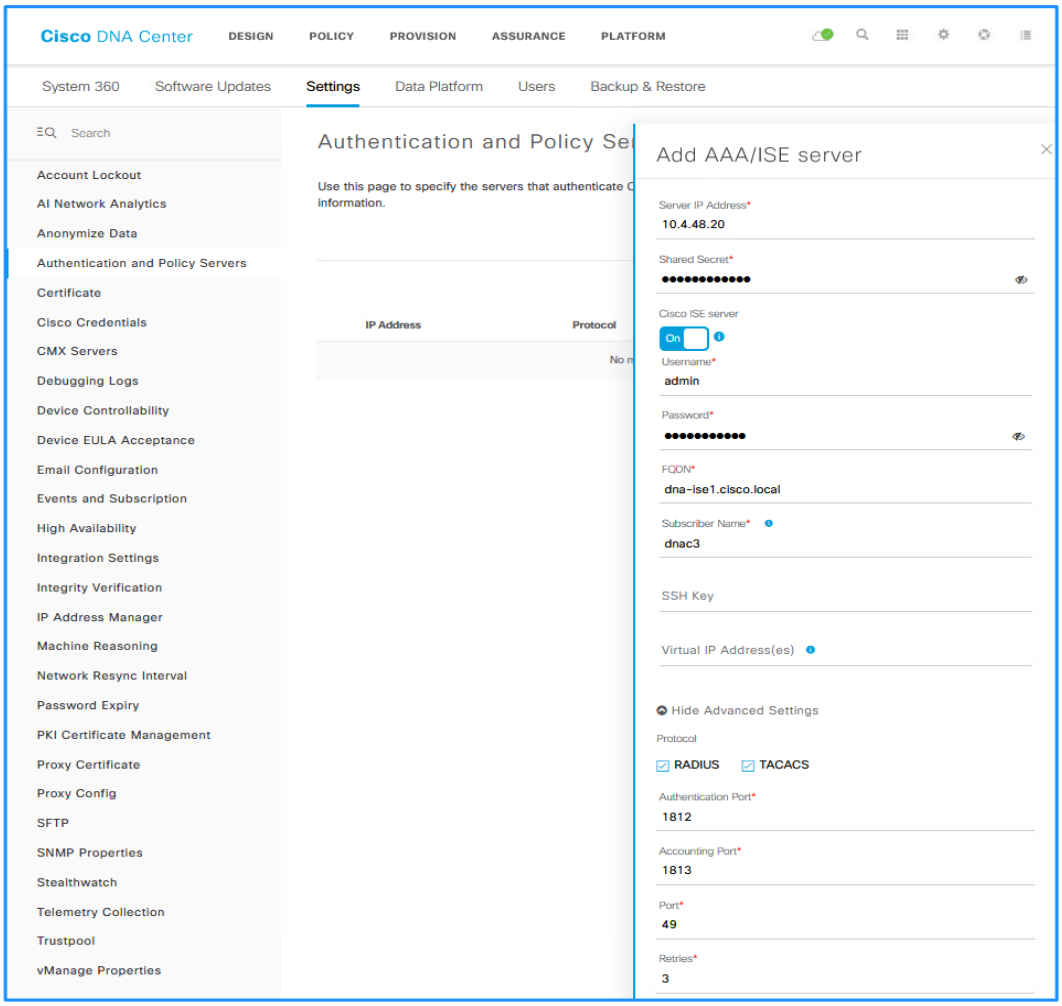
Step 3. In the **Add AAA/ISE SERVER** slide-out display, enter the Cisco ISE node 1 (primary PAN) **Server IP Address** (example: 10.4.48.20) and **Shared Secret**, toggle the **Cisco ISE server** selector to **On**, enter the Cisco ISE **Username** (example: admin), enter the Cisco ISE **Password**. For the **FQDN** and enter the Cisco 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**.

Table 3. Fields when adding a AAA / Cisco ISE server

Field	Settings	Description
Server IP Address	Text Field	The IP address of the AAA / Cisco ISE server
Shared Secret	Text Field	This is the shared secret used by network devices for communicating with the AAA / Cisco ISE server. This is also referred to the PAC key within IOS-XE device configuration
Cisco ISE Server	Toggle Switch	Enabled when the AAA server is a Cisco ISE server. Note that although there can be multiple AAA servers, there can only be one Cisco ISE server (high-availability standalone Cisco ISE deployment or distributed Cisco ISE deployment) defined to Cisco DNA Center.
Username	Text Field	This is the username of the default super admin account that you created during Cisco ISE installation.
Password	Text Field	This is the password of the default super admin account you created during Cisco ISE installation.
FQDN	Text Field	This is a fully-qualified domain name of the Cisco ISE server.
Subscriber Name	Text Field	This is the client name which the Cisco DNA Center server will be known by to the pxGrid service within Cisco ISE
SSH Key	Check Box	Optional SSH key for authentication between Cisco DNA Center and Cisco ISE
Virtual IP Address	Text Field	One or more Policy Services Nodes (PSN) may be behind a single load balancer. In those cases, you can add the load balancer IP(s) in the Virtual IP field.
Advanced Settings	Multiple Choice Radio	Determines the authentication protocol(s) used. The choices are as follows:

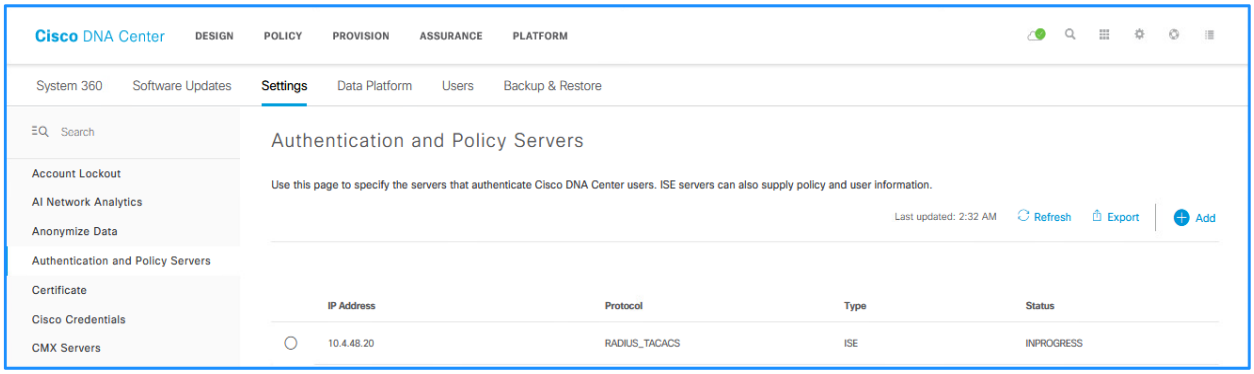
Field	Settings	Description
>Protocol	Button	RADIUS – This is the default setting, using the RADIUS protocol TACACS – Uses the TACACS protocol
Advanced Settings >Authentication Port	Text Field	When RADIUS is selected, the default port is 1812.
Advanced Settings >Accounting Port	Text Field	When RADIUS is selected, the default port is 1813.
Advanced Settings >Port	Text Field	This field appears only when TACACS is selected. The default port is 49
Retries	Number	The number of authentications retries before failure. The default is 3
Timeout (seconds)	Number	The number of seconds before an attempt timeout. The default is 4 seconds.

Figure 46. Adding a Cisco ISE server



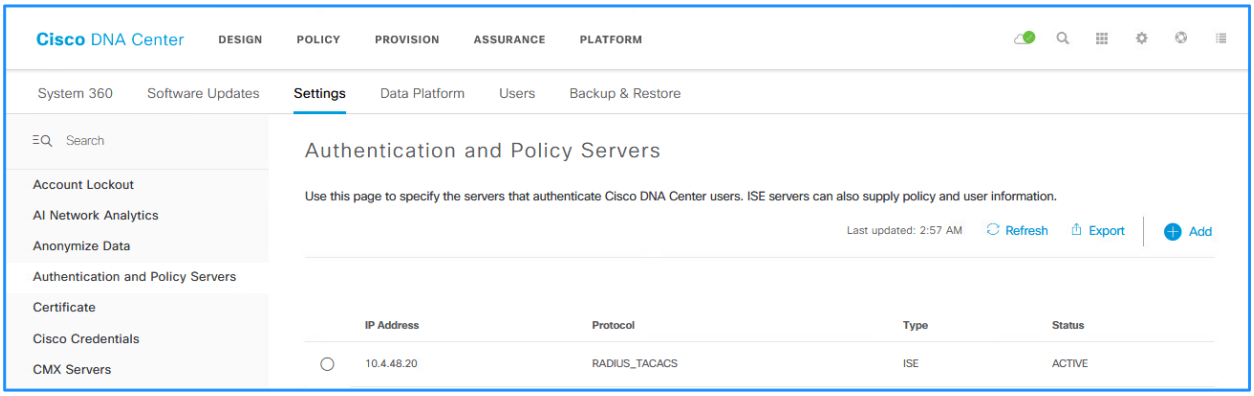
During communication establishment, status from Cisco DNA Center displays **Creating AAA server...**

Figure 47. Cisco ISE server creation in progress



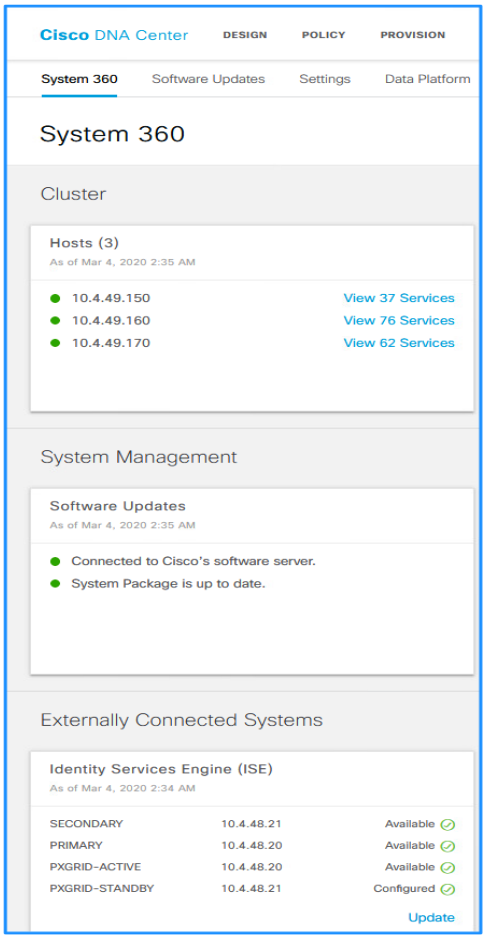
Use the **Refresh** button until communication establishes with Cisco ISE and the server displays **ACTIVE** status. If communication is not established, an error message displays information reported from Cisco ISE regarding the problem to be addressed before continuing. You also can see the communication 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.

Figure 48. Cisco ISE server status



You also can see the communication status by navigating from the **Settings** (gear) icon to **System Settings > System 360**. Under **External Connected System**, the Cisco ISE server shows as **Available**.

Figure 49. Displaying the Cisco ISE server status within System 360



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

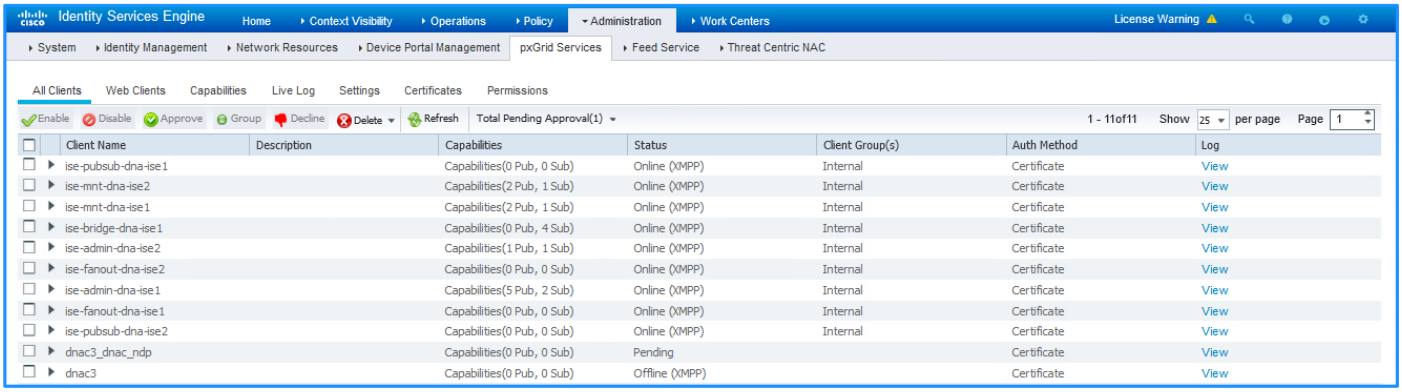
Step 4. Log in to Cisco ISE using the IP address or FQDN and navigate to **Administration > pxGrid Services**.

Example – https://<Identity_Service_Engine_IPaddr_or FQDN>

The Cisco ISE client (named ***dnac3*** in this example [**Subscriber Name** defined above]) shows **Pending** in the **Status** column.

Step 5. Check the box next to the client (***dnac3*** in this example) above the list, click **Approve**, and then click **Yes** to confirm.

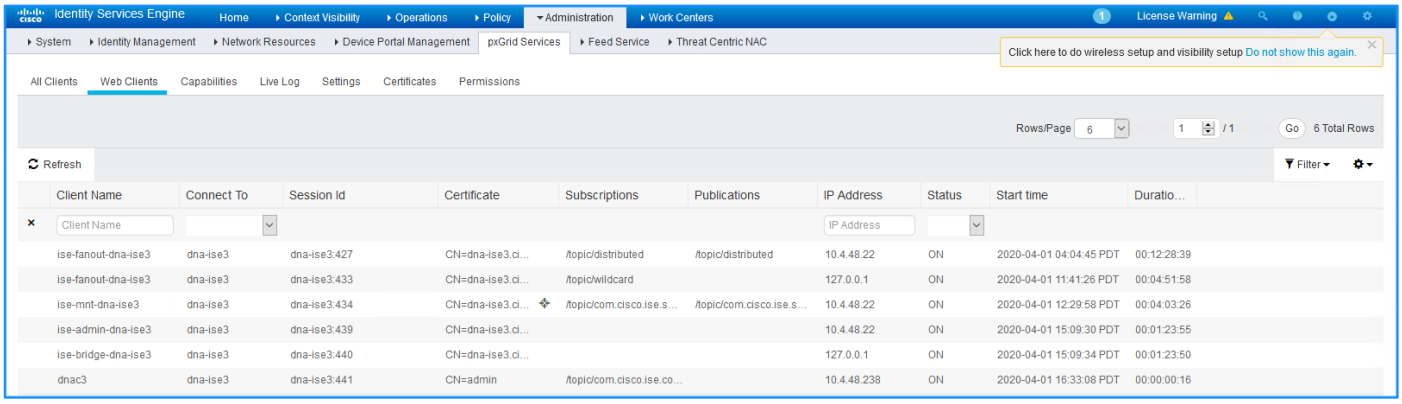
Figure 50. List of pxGrid clients in Cisco ISE



A success message appears, and the **Pending** status changes to **Online** for the client.

You can additionally verify that the integration is active by going to **Web clients** on the right of the **All Clients** and that the **Status** of the **Client Name** of your subscriber is **ON**.

Figure 51. Verifying the status of the pxGrid client



If Cisco ISE is integrated with Cisco DNA Center after scalable groups are already created in Cisco ISE, in addition to the default groups available, any existing Cisco 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 Cisco Software-Defined Access Solution Design Guide, the Cisco 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)	1.3.3.1

Table 5. Identity management

Product	Part Number	Software version
Cisco ISE Server	R-ISE-VMM-K9=	2.6 Patch 5

Appendix B: Hardware and Software Version Summary

Table 6. Hardware and software version summary

Product	Part number	Software version
Cisco DNA Center Appliance	DN2-HW-APL-L (M5-based chassis)	1.3.3.1 (System 1.3.0.115)
Cisco Identity Services Engine	R-ISE-VMM-K9=	2.6 Patch 5

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**.