



## **Cisco DNA Center First-Generation Appliance Installation Guide, Release 2.3.5**

**First Published:** 2022-12-21

**Last Modified:** 2023-03-21

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022–2023 Cisco Systems, Inc. All rights reserved.



## CONTENTS

---

<b>CHAPTER 1</b>	<b>Review the Cisco DNA Center Appliance Features</b>	<b>1</b>
	Appliance Hardware Specifications	1
	Front and Rear Panels	2
	Physical Specifications	8
	Environmental Specifications	9
	Power Specifications	10
	10 Gigabit Ethernet Switches	11

---

<b>CHAPTER 2</b>	<b>Plan the Deployment</b>	<b>13</b>
	Planning Workflow	13
	Cisco DNA Center and Cisco Software-Defined Access	14
	Interface Cable Connections	14
	Required IP Addresses and Subnets	17
	Required Internet URLs and Fully Qualified Domain Names	20
	Provide Secure Access to the Internet	23
	Required Network Ports	23
	Required Ports and Protocols for Cisco Software-Defined Access	25
	Required Configuration Information	32
	Required First-Time Setup Information	33

---

<b>CHAPTER 3</b>	<b>Install the Appliance</b>	<b>37</b>
	Appliance Installation Workflow	37
	Unpack and Inspect the Appliance	37
	Review the Installation Warnings and Guidelines	38
	Review the Rack Requirements	39
	Connect and Power On the Appliance	39

Check the LEDs 40

---

**CHAPTER 4****Prepare the Appliance for Configuration 43**

Preparation for Appliance Configuration Overview 43

Enable Browser Access to Cisco Integrated Management Controller 43

Execute Preconfiguration Checks 48

Reimage the Appliance 55

Verify the Cisco DNA Center Image 57

Create a Bootable USB Flash Drive 58

Using Etcher 58

Using the Linux CLI 59

Using the Mac CLI 59

Install the Cisco DNA Center ISO Image 60

---

**CHAPTER 5****Configure the Appliance 61**

Appliance Configuration Overview 61

Configure the Primary Node 61

Configure a Secondary Node 75

Upgrade to the Latest Cisco DNA Center Release 88

---

**CHAPTER 6****Complete First-Time Setup 89**

First-Time Setup Workflow 89

Compatible Browsers 89

Complete the Quick Start Workflow 89

Integrate Cisco ISE with Cisco DNA Center 94

Group-Based Access Control: Policy Data Migration and Synchronization 97

Configure Authentication and Policy Servers 100

Configure SNMP Properties 103

---

**CHAPTER 7****Troubleshoot the Deployment 105**

Troubleshooting Tasks 105

Log Out 105

Reconfigure the Appliance Using the Configuration Wizard 106

Power Cycle the Appliance 107

Using the Cisco IMC GUI 107

Using SSH 108

---

**APPENDIX A**

**Review High Availability Cluster Deployment Scenarios 111**

New HA Deployment 111

Existing HA Deployment of the Primary Node with Standard Interface Configurations 112

Existing HA Deployment of the Primary Node with Nonstandard Interface Configurations 112

Activate HA 113

Additional HA Deployment Considerations 113

Telemetry 113

Wireless Controller 114





## CHAPTER 1

# Review the Cisco DNA Center Appliance Features

---

- [Appliance Hardware Specifications, on page 1](#)
- [Front and Rear Panels, on page 2](#)
- [Physical Specifications, on page 8](#)
- [Environmental Specifications, on page 9](#)
- [Power Specifications, on page 10](#)
- [10 Gigabit Ethernet Switches, on page 11](#)

## Appliance Hardware Specifications

Cisco supplies Cisco Digital Network Architecture (DNA) Center in the form of a rack-mountable, physical appliance. The first-generation Cisco DNA Center 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 Cisco DNA Center software image is preinstalled on the appliance, but must be configured for use.

The following table summarizes the appliance's hardware specifications.

Feature	Description
Chassis	One rack-unit (1RU) chassis
Processors	Two 22-core Intel Xeon E5-2699 v4 2.20 GHz processors
Memory	Eight 32-GB DDR4 2400 MHz registered DIMMs (RDIMMs)
Storage	<ul style="list-style-type: none"><li>• Six 1.9-TB, 2.5-inch Enterprise Value 6G SATA solid state drives (SSDs)</li><li>• Two 480-GB, 2.5-inch Enterprise Value 12G SATA SSDs</li></ul>
Disk Management (RAID)	<ul style="list-style-type: none"><li>• RAID 1 on slots 1 through 4</li><li>• RAID 10 on slots 5 through 8</li></ul>

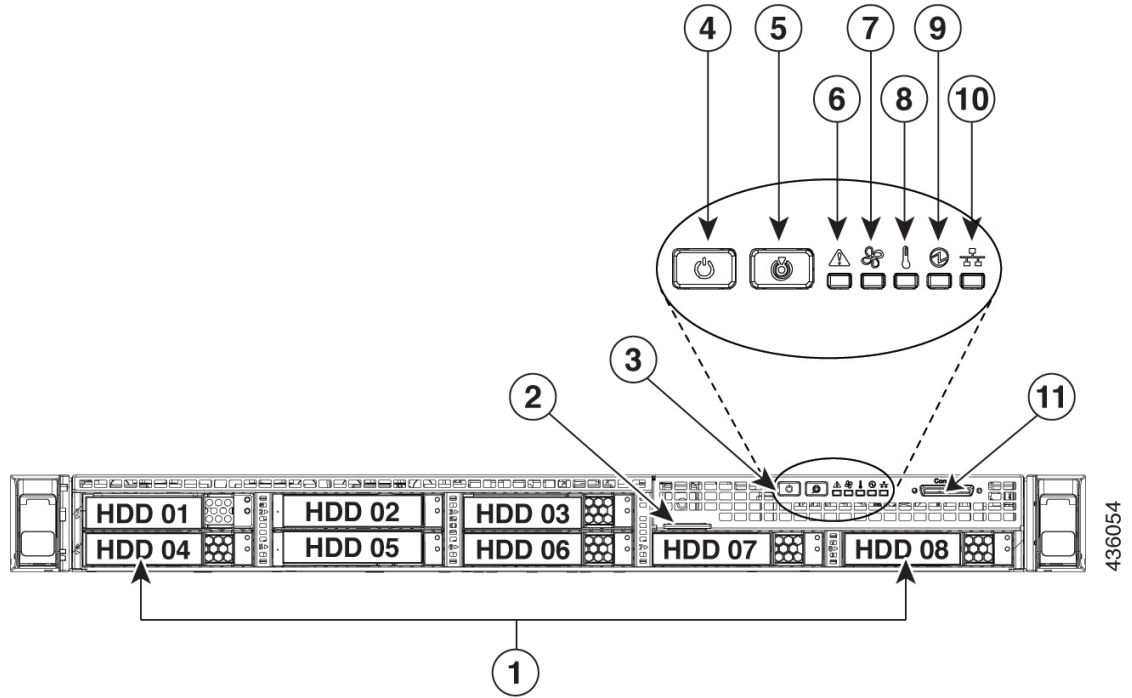
Feature	Description
Network and Management I/O	<p>Supported connectors:</p> <ul style="list-style-type: none"> <li>• Two 10-Gbps Ethernet ports on the Cisco UCS VIC 1227</li> <li>• One 1-Gbps Ethernet dedicated management port</li> <li>• Two 1-Gbps BASE-T Ethernet LAN ports</li> </ul> <p>The following connectors are available but not typically used in the day-to-day operation of Cisco DNA Center:</p> <ul style="list-style-type: none"> <li>• One RS-232 serial port (RJ-45 connector)</li> <li>• One 15-pin VGA2 connector</li> <li>• Two USB 3.0 connectors</li> <li>• One front-panel KVM connector that is used with the KVM cable, which provides two USB 2.0, one VGA, and one serial (DB-9) connector</li> </ul>
Power	<ul style="list-style-type: none"> <li>• Two 770-W AC power supplies</li> <li>• Redundant as 1+1</li> </ul>
Cooling	Six hot-swappable fan modules for front-to-rear cooling
Video	Video Graphics Array (VGA) video resolution up to 1920 x 1200, 16 bpp at 60 Hz, and up to 256 MB of video memory

## Front and Rear Panels

The following figures and tables describe the front and rear panels of the 44-core Cisco DNA Center appliance.



Figure 1: Appliance Front Panel

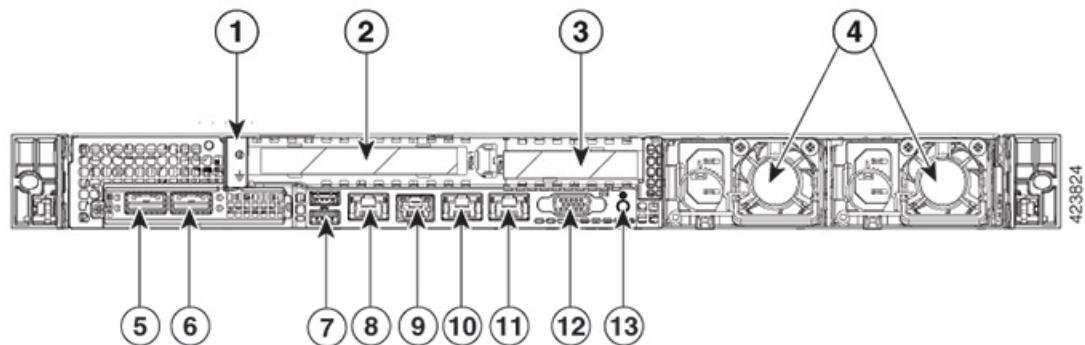


Component	Description
1	<p>A total of eight drives are available on the appliance:</p> <ul style="list-style-type: none"> <li>• Six 1.9 TB SATA SSD</li> <li>• Two 480 GB SAS SSD</li> </ul> <p>Each installed drive bay has a fault LED and an activity LED.</p> <p>When the drive fault LED is:</p> <ul style="list-style-type: none"> <li>• Off: The drive is operating properly.</li> <li>• Amber: The drive has failed.</li> <li>• Amber, blinking: The drive is rebuilding.</li> </ul> <p>When the drive activity LED is:</p> <ul style="list-style-type: none"> <li>• Off: There is no drive in the sled (no access, no fault).</li> <li>• Green: The drive is ready.</li> <li>• Green, blinking: The drive is reading or writing data.</li> </ul>
2	Pull-out asset tag
3	Operations sub-panel buttons and LEDs. LED states for these buttons and the conditions they indicate are described in the following entries.

Component	Description
4	<p>Power button/power status LED. When the LED is:</p> <ul style="list-style-type: none"> <li>• Off: There is no AC power to the appliance.</li> <li>• Amber: The appliance is in standby power mode. Power is supplied only to the Cisco Integrated Management Controller (CIMC) and some motherboard functions.</li> <li>• Green: The appliance is in main power mode. Power is supplied to all the server components.</li> </ul>
5	<p>Unit identification button and LED. When the LED is:</p> <ul style="list-style-type: none"> <li>• Blue: Unit identification is active.</li> <li>• Off: Unit identification is inactive.</li> </ul>
6	<p>System status LED. When the LED is:</p> <ul style="list-style-type: none"> <li>• Green: The appliance is running in a normal operating condition.</li> <li>• Green, blinking: The appliance is performing system initialization and memory checks.</li> <li>• Amber, steady: The appliance is in a degraded operational state, which may be due to one or more of the following causes: <ul style="list-style-type: none"> <li>• Power supply redundancy is lost.</li> <li>• CPUs are mismatched.</li> <li>• At least one CPU is faulty.</li> <li>• At least one DIMM is faulty.</li> <li>• At least one drive in a RAID configuration failed.</li> </ul> </li> <li>• Amber, blinking: The appliance is in a critical fault state, which may be due to one or more of the following: <ul style="list-style-type: none"> <li>• Boot failed.</li> <li>• Fatal CPU and/or bus error was detected.</li> <li>• Server is in an over-temperature condition.</li> </ul> </li> </ul>
7	<p>Fan status LED. When the LED is:</p> <ul style="list-style-type: none"> <li>• Green: All fan modules are operating properly.</li> <li>• Amber, steady: One fan module has failed.</li> <li>• Amber, blinking: Critical fault, two or more fan modules have failed.</li> </ul>

Component	Description
8	Temperature status LED. When the LED is: <ul style="list-style-type: none"> <li>• Green: The appliance is operating at normal temperature.</li> <li>• Amber, steady: One or more temperature sensors have exceeded a warning threshold.</li> <li>• Amber, blinking: One or more temperature sensors have exceeded a critical threshold.</li> </ul>
9	Power supply status LED. When the LED is: <ul style="list-style-type: none"> <li>• Green: All power supplies are operating normally.</li> <li>• Amber, steady: One or more power supplies are in a degraded operational state.</li> <li>• Amber, blinking: One or more power supplies are in a critical fault state.</li> </ul>
10	Network link activity LED. When the LED is: <ul style="list-style-type: none"> <li>• Green, blinking: One or more Ethernet LOM ports are link-active, with activity.</li> <li>• Green: One or more Ethernet LOM ports are link-active, but there is no activity.</li> <li>• Off: The Ethernet link is idle.</li> </ul>
11	KVM connector. Used with a KVM cable that provides two USB 2.0, one VGA, and one serial connector.

Figure 2: Appliance Rear Panel



Component	Description
1	Grounding-lug hole (for DC power supplies)
2	PCIe riser 1/slot 1
3	PCIe riser 2/slot 2

Component	Description
4	<p>Power supplies (up to two: redundant as 1+1). Each power supply has a power supply fault LED and an AC power LED.</p> <p>When the fault LED is:</p> <ul style="list-style-type: none"> <li>• Off: The power supply is operating normally.</li> <li>• Amber, blinking: An event warning threshold has been reached, but the power supply continues to operate.</li> <li>• Amber, solid: A critical fault threshold has been reached, causing the power supply to shut down (for example, a fan failure or an over-temperature condition).</li> </ul> <p>When the AC Power LED is:</p> <ul style="list-style-type: none"> <li>• Green, solid: AC power is OK, DC output is OK.</li> <li>• Green, blinking: AC power is OK, DC output is not enabled.</li> <li>• Off: There is no AC power to the power supply.</li> </ul> <p>For more details, see <a href="#">Power Specifications</a>.</p>
5	<p>10-Gbps Cluster Port (Port 2, enp10s0, Network Adapter 1): This is the second 10-Gbps port on the Cisco Virtual Interface Card (VIC) 1227 in the appliance mLOM slot. The rear panel labels it Port 2 and the Maglev Configuration wizard identifies it as enp10s0 and Network Adapter 1. Connect this port to a switch with connections to the other nodes in the Cisco DNA Center cluster.</p> <p>This port has a link status (ACT) LED and a link speed (LINK) LED.</p> <p>When the link status LED is:</p> <ul style="list-style-type: none"> <li>• Green, blinking: Traffic is present on the active link.</li> <li>• Green: Link is active, but there is no traffic present.</li> <li>• Off: No link is present.</li> </ul> <p>When the link speed LED is:</p> <ul style="list-style-type: none"> <li>• Green: Link speed is 10 Gbps.</li> <li>• Amber: Link speed is 1 Gbps.</li> <li>• Off: Link speed is 100 Mbps or less.</li> </ul> <p><b>Note</b> The enterprise and cluster ports must operate at 10 Gbps only.</p>

Component	Description
6	<p>10-Gbps Enterprise Port (Port 1, enp9s0, Network Adapter 4): This is the first 10-Gbps port on the Cisco Virtual Interface Card (VIC) 1227 in the appliance mLOM slot. The rear panel labels it Port 1 and the Maglev Configuration wizard identifies it as enp9s0 and Network Adapter 4. Connect this port to a switch with IP reachability to the networking equipment that Cisco DNA Center will manage.</p> <p>This port has a link status (ACT) LED and a link speed (LINK) LED.</p> <p>When the link status LED is:</p> <ul style="list-style-type: none"> <li>• Green, blinking: Traffic is present on the active link.</li> <li>• Green: Link is active, but there is no traffic present.</li> <li>• Off: No link is present.</li> </ul> <p>When the speed LED is:</p> <ul style="list-style-type: none"> <li>• Green: Link speed is 10 Gbps.</li> <li>• Amber: Link speed is 1 Gbps.</li> <li>• Off: Link speed is 100 Mbps or less.</li> </ul> <p><b>Note</b> The Cisco DNA Center appliance enterprise and cluster ports must operate at 10 Gbps only.</p>
7	Two USB 3.0 ports
8	<p>1-Gbps CIMC Port (M): This is the embedded port to the right of the two USB ports and to the left of the RJ45 serial port. The back panel labels it M and you assign an IP address to it when you enable browser access to the appliance's CIMC GUI (see <a href="#">Enable Browser Access to Cisco Integrated Management Controller</a>). This port is reserved for out-of-band (OOB) management of the Cisco DNA Center appliance chassis and software. Connect this port to a switch that provides access to your dedicated OOB enterprise management network.</p> <p>This port has a link status LED and a link speed LED. When the link status LED is:</p> <ul style="list-style-type: none"> <li>• Green, blinking: Traffic is present on the active link.</li> <li>• Green: Link is active, but there is no traffic present.</li> <li>• Off: No link is present.</li> </ul> <p>When the speed LED is:</p> <ul style="list-style-type: none"> <li>• Green: Link speed is 1 Gbps.</li> <li>• Amber: Link speed is 100 Mbps.</li> <li>• Off: Link speed is 10 Mbps or less.</li> </ul>
9	Serial port (RJ-45 connector)

Component	Description
10	<p>1-Gbps Cisco DNA Center GUI Port (1, enp1s0f0, Network Adapter 2): This is the first Intel i350 1Gb Ethernet controller port. It is embedded on the appliance motherboard. The rear panel labels it <b>1</b> and the Maglev Configuration wizard identifies it as enp1s0f0 and Network Adapter 2. Connect this port to a switch that provides access to your dedicated enterprise management network.</p> <p>This port has a link status LED and a link speed LED. When the status LED is:</p> <ul style="list-style-type: none"> <li>• Green, blinking: Traffic is present on the active link.</li> <li>• Green: Link is active, but there is no traffic present.</li> <li>• Off: No link is present.</li> </ul> <p>When the speed LED is:</p> <ul style="list-style-type: none"> <li>• Green: Link speed is 1 Gbps.</li> <li>• Amber: Link speed is 100 Mbps.</li> <li>• Off: Link speed is 10 Mbps or less.</li> </ul>
11	<p>1-Gbps Cloud Port (2, enp1s0f1, Network Adapter 3): This is the second embedded 1Gbps Ethernet controller port. The rear panel labels it <b>2</b> and the Maglev Configuration wizard identifies it as enp1s0f1 and Network Adapter 3. This port is optional. It is used for connecting to the Internet when it is not possible to do so via the 10-Gbps enterprise port (Port 1, enp9s0, Network Adapter 4).</p> <p>This port has a link status LED and a link speed LED. When the link status LED is:</p> <ul style="list-style-type: none"> <li>• Green, blinking: Traffic is present on the active link.</li> <li>• Green: Link is active, but there is no traffic.</li> <li>• Off: No link is present.</li> </ul> <p>When the speed LED is:</p> <ul style="list-style-type: none"> <li>• Green: Link speed is 1 Gbps.</li> <li>• Amber: Link speed is 100 Mbps.</li> <li>• Off: Link speed is 10 Mbps or less.</li> </ul>
12	VGA video port (DB-15). This panel area around this port is blue.
13	Blue LED locator button

## Physical Specifications

The following table lists the physical specifications for the appliance.

**Table 1: Physical Specifications**

Description	Specification
Height	1.7 in. (4.32 cm)
Width	16.89 in. (43.0 cm) Including handles: 18.98 in. (48.2 cm)
Depth (length)	29.8 in. (75.6 cm) Including handles: 30.98 in. (78.7 cm)
Front Clearance	3 in. (76 mm)
Side Clearance	1 in. (25 mm)
Rear Clearance	6 in. (152 mm)
Maximum weight (fully loaded chassis)	37.9 lb. (17.2 kg)

## Environmental Specifications

The following table lists the environmental specifications for the Cisco DNA Center appliance.

**Table 2: Environmental Specifications**

Description	Specification
Temperature, operating	41 to 95°F (5 to 35°C) Derate the maximum temperature by 1°C for every 1000 ft. (305 meters) of altitude above sea level.
Temperature, nonoperating (when the appliance is stored or transported)	-40 to 149°F (-40 to 65°C)
Humidity (RH), operating	10 to 90%, noncondensing at 82°F (28°C)
Humidity, nonoperating	5 to 93% at 82°F (28°C)
Altitude, operating	0 to 10,000 ft. (0 to 3,000 m)
Altitude, nonoperating (when the appliance is stored or transported)	0 to 40,000 ft. (0 to 12,192 m)
Sound power level, measure A-weighted per ISO7779 LwAd (Bels), operation at 73°F (23°C)	5.4

Description	Specification
Sound pressure level, measure A-weighted per ISO7779 LpAm (dBA), Operation at 73°F (23°C)	37

## Power Specifications

The specifications for the two 770 W AC power supplies (Cisco part number UCSC-PSU1-770W) provided with the Cisco DNA Center appliance are listed in the table below.

**Table 3: AC Power Supply Specifications**

Description	Specification
AC input voltage	Nominal range: 100–120 VAC, 200–240 VAC Range: 90–132 VAC, 180–264 VAC
AC input frequency	Nominal range: 50 to 60 Hz (Range: 47–63 Hz)
Maximum AC input current	9.5 A at 100 VAC 4.5 A at 208 VAC
Maximum input volt-amperes	950 VA at 100 VAC
Maximum output power per PSU	770 W at 100–120 VAC
Maximum inrush current	15 A at 35° C
Maximum hold-up time	12 ms at 770 W
Power supply output voltage	12 VDC
Power supply standby voltage	12 VDC
Efficiency rating	Climate Savers Platinum Efficiency (80Plus Platinum certified)
Form factor	RSP2
Input connector	IEC320 C14



**Note** You can get more specific power information for the exact configuration of your appliance by using the Cisco UCS Power Calculator: <http://ucspowercalc.cisco.com>



## 10 Gigabit Ethernet Switches

The following table lists the 10 Gigabit Ethernet Cisco switches that can currently be brought up from the first-generation Cisco DNA Center appliance. This table will be updated as more switches are tested.

Cisco Switch	Cisco Part Number	Comment
Cisco Nexus 5672UP	N5K-C5672UP	—
Cisco Catalyst 6880-X	C6880-X-LE	—
Cisco Nexus 7700 (6-Slot)	N77-C7706	Tested with the Cisco Nexus 7700 Switch Supervisor2 Enhanced Module (Cisco part number N77-SUP2E) installed.
<p>In order for the remaining switches in this table to function properly, ensure that the following settings are configured for both your switch and your Cisco DNA Center appliance:</p> <ul style="list-style-type: none"> <li>• <b>Default VLAN:</b> Specify the same port number on your appliance and switch.</li> <li>• <b>VLAN Mode:</b> Set <b>Trunk</b> mode.</li> </ul> <p>See Steps 3 and 4 in <a href="#">Execute Preconfiguration Checks, on page 48</a>.</p>		
Cisco Catalyst 3850-48XS-S	WS-C3850-48XS-S	—
Cisco Catalyst 4500X-32 SFP+	WS-C4500X-32SFP+	—
Cisco Catalyst C9500-40X-E	C9500-40X	—
Cisco Catalyst 3650-48PQ-E	WS-C3650-48PQ-E	—





## CHAPTER 2

# Plan the Deployment

---

- [Planning Workflow](#), on page 13
- [Cisco DNA Center and Cisco Software-Defined Access](#), on page 14
- [Interface Cable Connections](#), on page 14
- [Required IP Addresses and Subnets](#), on page 17
- [Required Internet URLs and Fully Qualified Domain Names](#), on page 20
- [Provide Secure Access to the Internet](#), on page 23
- [Required Network Ports](#), on page 23
- [Required Ports and Protocols for Cisco Software-Defined Access](#), on page 25
- [Required Configuration Information](#), on page 32
- [Required First-Time Setup Information](#), on page 33

## Planning Workflow

You must perform the following planning and information-gathering tasks before attempting to install, configure, and set up your Cisco DNA Center appliance. After you complete these tasks, you can continue by physically installing your appliance in the data center.

1. Review the recommended cabling and switching requirements for standalone and cluster installations. For more information, see [Interface Cable Connections](#).
2. Gather the IP addressing, subnetting, and other IP traffic information that you will apply during appliance configuration. For more information, see [Required IP Addresses and Subnets](#).
3. Prepare a solution for the required access to web-based resources. For more information, see [Required Internet URLs and Fully Qualified Domain Names](#) and [Provide Secure Access to the Internet](#).
4. Reconfigure your firewalls and security policies for Cisco DNA Center traffic. For more information, see [Required Network Ports](#). If you are using Cisco DNA Center to manage a Cisco Software-Defined Access (SD-Access) network, also see [Required Ports and Protocols for Cisco Software-Defined Access](#).
5. Gather the additional information used during appliance configuration and first-time setup. For more information, see [Required Configuration Information](#) and [Required First-Time Setup Information](#).

# Cisco DNA Center and Cisco Software-Defined Access

You can use Cisco DNA Center to manage any type of network, including networks that employ the Cisco SD-Access fabric architecture. Cisco SD-Access transforms conventional networks into intent-based networks, where business logic becomes a physical part of the network, making it easy to automate day-to-day tasks such as configuration, provisioning, and troubleshooting. The Cisco SD-Access solution reduces the time taken to adapt the network to business needs, improves issue resolutions, and reduces security-breach impacts.

A complete discussion of the Cisco SD-Access solution is outside the scope of this guide. Network architects and administrators planning to implement a Cisco SD-Access fabric architecture for use with Cisco DNA Center can find additional information and guidance from the following resources:

- For more information on how Cisco DNA Center leverages Cisco SD-Access to automate solutions that are not possible with normal networking approaches and techniques, see [Software Defined Access: Enabling Intent-Based Networking](#).
- For guidance in using Cisco SD-Access access segmentation to enhance network security, see the [Software-Defined Access Segmentation Design Guide](#).
- For guidance on deploying SDA with Cisco DNA Center, see the [Software-Defined Access Deployment Guide](#).
- For more information on the digital network architecture that is the foundation of Cisco DNA Center and the Cisco SD-Access solution, and the roles that other Cisco and third-party products and solutions play in this innovative architecture, see the [Cisco DNA Design Zone](#).

## Interface Cable Connections

Connect the ports on the appliance to switches providing the following types of network access. At a minimum, you must configure the Enterprise and Cluster port interfaces, as they are required for Cisco DNA Center functionality.



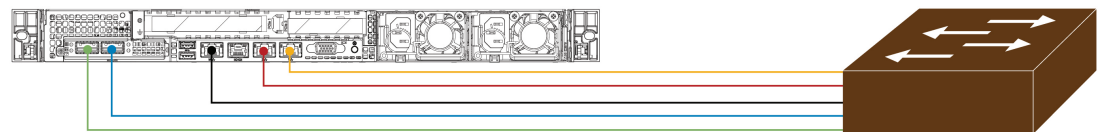
### Note

- During appliance configuration, the Maglev Configuration wizard does not let you proceed until you assign the **Cluster Link** option to an interface. For both single-node and three-node deployments in a production environment, designate port enp10s0 as the Cluster Link on the first-generation Cisco DNA Center appliance (Cisco part number DN1-HW-APL).
- Be aware that the interface marked as the Cluster Link cannot be changed after configuration completes. Later, if you must change the interface marked as the Cluster Link, you are required to reimage the appliance. (For a description of the tasks you need to complete in order to reimage your Cisco DNA Center appliance, see [Reimage the Appliance, on page 55](#).) With this in mind, we recommend that you set up the Cluster Port with an IP address, so as to allow for expansion to a three-node cluster in the future. Also, make sure that the cluster link interface is connected to a switch port and is in the UP state.
- If you plan to build multiple clusters, you must use a separate IP scheme for each cluster in order to prevent cross-cluster interaction (which might corrupt the clusters).

- **(Required) 10-Gbps Enterprise Port (Port 1, enp9s0, Network Adapter 4):** This is the right-hand port on the VIC 1227 card in the appliance mLOM slot. Its purpose is to enable Cisco DNA Center to communicate with and manage your network. Connect this port to a switch with connections to the enterprise network and configure one IP address with a subnet mask for the port.
- **(Required) 10-Gbps Cluster Port (Port 2, enp10s0, Network Adapter 1):** This is the left-hand port on the VIC 1227 card in the appliance mLOM slot. Its purpose is to enable communications among the primary and secondary nodes in a Cisco DNA Center cluster. Connect this port to a switch with connections to the other nodes in the cluster and configure one IP address with a subnet mask for the port.
- **(Optional) 1-Gbps Cisco DNA Center GUI Port (1, enp1s0f0, Network Adapter 2):** This port provides access to the Cisco DNA Center GUI. Its purpose is to enable users to use the software on the appliance. Connect this port to a switch with connections to your enterprise management network, and configure one IP address with a subnet mask for the port.
- **(Optional) 1-Gbps Cloud Port (2, enp1s0f1, Network Adapter 3):** This port is optional. Use it only if you cannot connect the appliance to the Internet (including to your Internet proxy server) using the 10-Gbps enterprise port (Port 1, enp9s0, Network Adapter 4). If you need to use the cloud port, connect it to a switch with connections to your Internet proxy server and configure an IP address with a subnet mask for the port.
- **(Optional, but strongly recommended) 1-Gbps CIMC Port (M):** This port provides browser access to the Cisco Integrated Management Controller (CIMC) out-of-band appliance management interface and its GUI. Its purpose is to allow you to manage the appliance and its hardware. Connect this port to a switch with connections to your enterprise management network and configure an IP address with a subnet mask for the port.

The following figure shows the recommended connections for a single-node Cisco DNA Center cluster:

**Figure 3: Recommended Cabling for Single-Node Cluster**



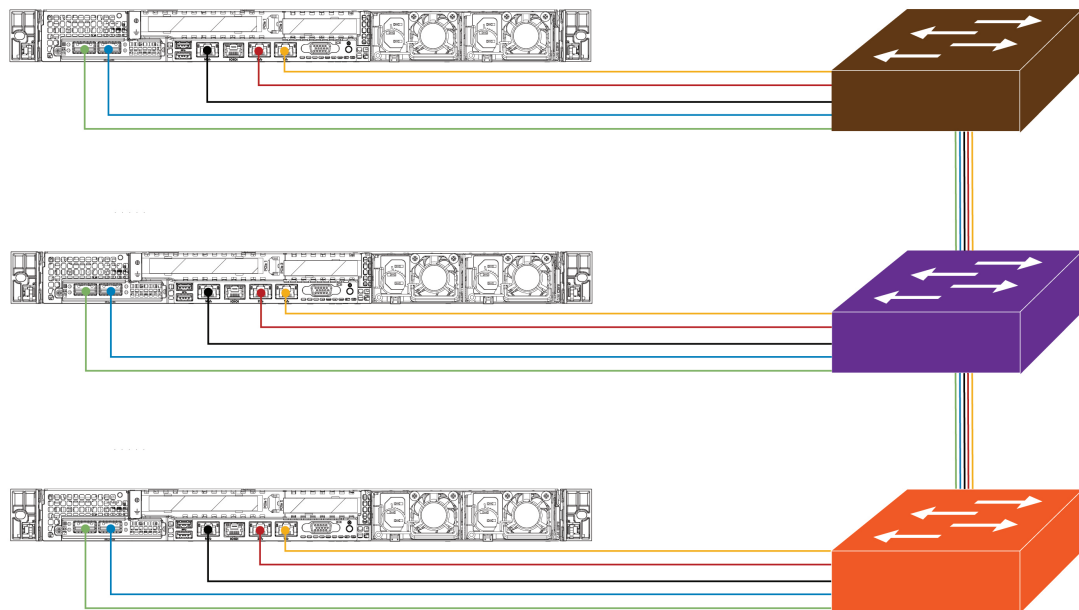
**Legend**

- |  |  |
|--|--|
| ● 10 Gbps Cluster Port<br>(Port 2, enp10s0, Network Adapter 1)   | ● 1 Gbps Cisco DNA Center GUI Port<br>(1, enp1s0f0, Network Adapter 2) |
| ● 10 Gbps Enterprise Port<br>(Port 1, enp9s0, Network Adapter 4) | ● 1 Gbps Cloud Port<br>(2, enp1s0f1, Network Adapter 3)                |
| ● 1 Gbps CIMC Port (M)   |  |

439671

The following figure shows the recommended connections for a three-node Cisco DNA Center cluster. All but one of the connections for each node in the three-node cluster are the same as those for the single-node cluster, and use the same ports. The exception is the Cluster Port (Port 2, enp10s0, Network Adapter 1), which is required so that each host in the three-node cluster can communicate with the other hosts.

Figure 4: Recommended Cabling for Three-Node Cluster



## Legend

- 10 Gbps Cluster Port (Port 2, enp10s0, Network Adapter 1)
- 10 Gbps Enterprise Port (Port 1, enp9s0, Network Adapter 4)
- 1 Gbps CIMC Port (M)
- 1 Gbps Cisco DNA Center GUI Port (1, enp1s0f0, Network Adapter 2)
- 1 Gbps Cloud Port (2, enp1s0f1, Network Adapter 3)

439812

For a short video presentation about the rear-panel ports and how they are used, see the first five minutes of [Unboxing Cisco DNA Center Appliance for Assurance and SD-Access](#) (under the section "Get Started").

For more details on each of the ports, see the rear panel diagram and accompanying descriptions for your appliance in [Front and Rear Panels](#).



**Note** Multinode cluster deployments require all the member nodes to be in the same network and at the same site. The appliance does not support distribution of nodes across multiple networks or sites.

When cabling the 10-Gbps enterprise and cluster ports, please note that both ports support only the following media types:

- SFP-10G-LR (Long range, SMF)
- SFP-H10GB-CU1M (Twinax cable, passive, 1 Meter)
- SFP-H10GB-CU3M (Twinax cable, passive, 3 Meters)
- SFP-H10GB-CU5M (Twinax cable, passive, 5 Meters)
- SFP-H10GB-ACU7M (Twinax cable, active, 7 Meters)

# Required IP Addresses and Subnets

Before beginning the installation, you must ensure that your network has sufficient IP addresses available to assign to each of the appliance ports that you plan on using. Depending on whether you are installing the appliance as a single-node cluster or as a primary or secondary node in a three-node cluster, you will need the following appliance port (NIC) addresses:

- **Enterprise Port Address (Required):** One IP address with a subnet mask.
- **Cluster Port Address (Required):** One IP address with a subnet mask.
- **Management Port Address (Optional):** One IP address with a subnet mask.
- **Cloud Port Address (Optional):** One IP address with a subnet mask. This is an optional port, used only when you cannot connect to the cloud using the Enterprise port. You do not need an IP address for the Cloud port unless you must use it for this purpose.
- **CIMC Port Address (Optional, but strongly recommended):** One IP address with a subnet mask.



---

**Note** All of the IP addresses called for in these requirements must be valid IPv4 addresses with valid IPv4 netmasks. Ensure that the addresses and their corresponding subnets do not overlap. Service communication issues can result if they do.

---

You will also need the following additional IP addresses and dedicated IP subnets, which are prompted for and applied during configuration of the appliance:

1. **Cluster Virtual IP Addresses:** One virtual IP (VIP) address per configured network interface per cluster. This requirement applies to three-node clusters and single-node clusters that are likely to be converted into a three-node cluster in the future. You must supply a VIP for each network interface you configure. Each VIP should be from the same subnet as the IP address of the corresponding configured interface. There are four interfaces on each appliance: Enterprise, Cluster, Management, and Cloud. At a minimum, you must configure the Enterprise and Cluster port interfaces, as they are required for Cisco DNA Center functionality. An interface is considered configured if you supply an IP address for that interface, along with a subnet mask and one or more associated gateways or static routes. If you skip an interface entirely during configuration, that interface is considered as not configured.

Note the following:

- If you have a single-node setup and do not plan to convert it into a three-node cluster in the future, you are not required to specify a virtual IP address. However, if you decide to do so, you must specify a virtual IP address for every configured network interface (just as you would for a three-node cluster).
- If the intracluster link for a single-node cluster goes down, the VIP addresses associated with the Management and Enterprise interfaces also go down. When this happens, Cisco DNA Center is unusable until the intracluster link is restored (because the Software Image Management [SWIM] and Cisco Identity Services Engine [ISE] integration is not operational and Cisco DNA Assurance data is not displayed because information cannot be gathered from Network Data Platform [NDP] collectors).
- Do *not* use a link-local or nonroutable IP address for the Enterprise or Management interface.

2. **Default Gateway IP Address:** The IP address for your network's preferred default gateway. If no other routes match the traffic, traffic will be routed through this IP address. Typically, you should assign the default gateway to the interface in your network configuration that accesses the internet. For information on security considerations to keep in mind when deploying Cisco DNA Center, see the [Cisco Digital Network Architecture Center Security Best Practices Guide](#).
3. **DNS Server IP Addresses:** The IP address for one or more of your network's preferred DNS servers. During configuration, you can specify multiple DNS server IP addresses by entering them as a space-separated list.
4. **(Optional) Static Route Addresses:** The IP addresses, subnet masks, and gateways for one or more static routes. During configuration, you can specify multiple static-route IP addresses, netmasks, and gateways by entering them as a space-separated list.

You can set one or more static routes for any interface on the appliance. You should supply static routes when you want to route traffic in a specific direction other than the default gateway. Each of the interfaces with static routes will be set as the *device* the traffic will be routed through in the IP route command table. For this reason, it is important to match the static route directions with the interface through which the traffic will be sent.

Static routes are not recommended in network device routing tables such as those used by switches and routers. Dynamic routing protocols are better for this. However, you should add them where needed to allow the appliance access to particular parts of the network that can be reached no other way.

5. **NTP Server IP Addresses:** The DNS-resolvable hostname, or IP address, for at least one Network Time Protocol (NTP) server.

During configuration, you can specify multiple NTP server IP addresses/masks or hostnames by entering them as a space-separated list. For a production deployment, we recommend that you configure a minimum of three NTP servers.

You will specify these servers during pre-flight hardware synchronization and again during configuration of the software on each appliance in the cluster. Time synchronization is critical to the accuracy of data and coordination of processing across a multi-host cluster. Before deploying the appliance in production, make sure that the time on the appliance system clock is current and that the Network Time Protocol (NTP) servers you specified are keeping accurate time. If you are planning to integrate the appliance with Cisco Identity Services Engine (ISE), you should also ensure that ISE is synchronizing with the same NTP servers as the appliance.

6. **Container Subnet:** Identifies one dedicated IP subnet for the appliance to use in managing and getting IP addresses for communications among its internal application services, such as Assurance, inventory collection, and so on. By default, Cisco DNA Center configures a link-local subnet (**169.254.32.0/20**) for this parameter, and we recommend that you use this subnet. If you choose to enter another subnet, ensure that it does not conflict with or overlap any other subnet used by Cisco DNA Center's internal network or any external network. Also ensure that the minimum size of the subnet is 21 bits. The subnet you specify must conform with the IETF RFC 1918 and RFC 6598 specifications for private networks, which support the following address ranges:

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16
- 100.64.0.0/10



For details, see RFC 1918, [Address Allocation for Private Internets](#), and RFC 6598, [IANA-Reserved IPv4 Prefix for Shared Address Space](#).

**Important**

- Ensure that you specify a valid CIDR subnet. Otherwise, incorrect bits will be present in the 172.17.1.0/20 and 172.17.61.0/20 subnets.
- After configuration of your Cisco DNA Center appliance is completed, you cannot assign a different subnet without first reimaging the appliance (see the "Reimage the Appliance" topic in the "Configure the Appliance" chapter for more information).

7. **Cluster Subnet:** Identifies one dedicated IP subnet for the appliance to use in managing and getting IPs for communications among its infrastructure services, such as database access, the message bus, and so on. By default, Cisco DNA Center configures a link-local subnet (**169.254.48.0/20**) for this parameter, and we recommend that you use this subnet. If you choose to enter another subnet, ensure that it does not conflict with or overlap any other subnet used by Cisco DNA Center's internal network or any external network. Also ensure that the minimum size of the subnet is 21 bits. The subnet you specify must conform with the IETF RFC 1918 and RFC 6598 specifications for private networks, which support the following address ranges:

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16
- 100.64.0.0/10

For details, see RFC 1918, [Address Allocation for Private Internets](#), and RFC 6598, [IANA-Reserved IPv4 Prefix for Shared Address Space](#).

If you were to specify 10.10.10.0/21 as your Container subnet, you could also specify a Cluster subnet of 10.0.8.0/21 since these two subnets do not overlap. Also note that the configuration wizard detects overlaps (if any) between these subnets and prompts you to correct the overlap.

**Important**

- Ensure that you specify a valid CIDR subnet. Otherwise, incorrect bits will be present in the 172.17.1.0/20 and 172.17.61.0/20 subnets.
- After configuration of your Cisco DNA Center appliance is completed, you cannot assign a different subnet without first reimaging the appliance (see the "Reimage the Appliance" topic in the "Configure the Appliance" chapter for more information).

The recommended total IP address space for the two Container and Cluster subnets contains 4,096 addresses, broken down into two /21 subnets of 2,048 addresses each. The two /21 subnets must not overlap. Cisco DNA Center's internal services require a dedicated set of IP addresses to operate (a requirement of the Cisco DNA Center microservice architecture. To accommodate this requirement, you must allocate two dedicated subnets per Cisco DNA Center system.

One reason the appliance requires this amount of address space is to maintain system performance. Because it uses internal routing and tunneling technologies for east-west (inter-node) communications, using overlapping address spaces would force the appliance to run Virtual Routing and Forwarding FIBs internally. This would

lead to multiple encaps/decaps for packets going from one service to another, causing high internal latency at a very low level, with cascading impacts at higher layers.

Another reason is the Cisco DNA Center [Kubernetes-based service containerization](#) architecture. Each appliance uses the IP addresses in this space per Kubernetes K8 node. Multiple nodes can make up a single service. Currently, Cisco DNA Center supports more than 100 services, each requiring several IP addresses, and new features and corresponding services are being added all the time. The address space requirement is purposely kept large at the start to ensure that Cisco can add new services and features without either running out of IPs or requiring customers to reallocate contiguous address spaces simply to upgrade their systems.

The services supported over these subnets are also enabled at Layer 3. The Cluster space, in particular, carries data between application and infrastructure services, and is heavily used.

The RFC 1918 and RFC 6598 requirement is because of the requirement by Cisco DNA Center to download packages and updates from the cloud. If the selected IP address ranges do not conform with RFC 1918 and RFC 6598, this can quickly lead to problems with public IP address overlaps.

## Required Internet URLs and Fully Qualified Domain Names

The appliance requires secure access to the following table of URLs and Fully Qualified Domain Names (FQDNs).

The table describes the features that make use of each URL and FQDN. You must configure either your network firewall or a proxy server so that IP traffic can travel to and from the appliance and these resources. If you cannot provide this access for any listed URL and FQDN, the associated features will be impaired or inoperable.

For more on requirements for proxy access to the internet, see [Provide Secure Access to the Internet](#).

**Table 4: Required URLs and FQDN Access**

In order to...	...Cisco DNA Center must access these URLs and FQDNs
Download updates to the system and application package software; submit user feedback to the product team.	Recommended: *.ciscoconnectdna.com:443 <sup>1</sup> Customers who want to avoid wildcards can specify these URLs instead: <ul style="list-style-type: none"> <li>• https://www.ciscoconnectdna.com</li> <li>• https://cdn.ciscoconnectdna.com</li> <li>• https://registry.ciscoconnectdna.com</li> <li>• https://registry-cdn.ciscoconnectdna.com</li> </ul>
Cisco DNA Center update package.	<ul style="list-style-type: none"> <li>• <a href="https://*.ciscoconnectdna.com/">https://*.ciscoconnectdna.com/</a></li> <li>• *.cloudfront.net</li> <li>• *.tesseractcloud.com</li> </ul>

In order to...	...Cisco DNA Center must access these URLs and FQDNs
Smart Account and SWIM software downloads.	<ul style="list-style-type: none"> <li>• <a href="https://apx.cisco.com">https://apx.cisco.com</a></li> <li>• <a href="https://cloudsso.cisco.com/as/token.oauth2">https://cloudsso.cisco.com/as/token.oauth2</a></li> <li>• <a href="https://*.cisco.com/*">https://*.cisco.com/*</a></li> <li>• <a href="https://download-ssc.cisco.com/">https://download-ssc.cisco.com/</a></li> </ul>
Authenticate with the cloud domain.	<a href="https://dnaservices.cisco.com">https://dnaservices.cisco.com</a>
Integrate with ThousandEyes.	<ul style="list-style-type: none"> <li>• *.awsglobalaccelerator.com</li> <li>• api.thousandeyes.com</li> </ul>
Manage Cisco Enterprise Network Function Virtualization Infrastructure Software (NFVIS) devices.	*.amazonaws.com
Collect customer behavior telemetry.	<a href="https://data.pendo.io">https://data.pendo.io</a>
Allow API calls to enable access to Cisco CX Cloud Success Tracks. Otherwise, the enhancements made to extended configuration-based scanning for the Security Advisories, Bug Identifier, and EOX features that Machine Reasoning Engine (MRE) supports will not operate as expected.	<a href="https://api-cx.cisco.com">https://api-cx.cisco.com</a>
Integrate with Webex.	<ul style="list-style-type: none"> <li>• <a href="http://analytics.webexapis.com">http://analytics.webexapis.com</a></li> <li>• <a href="https://webexapis.com">https://webexapis.com</a></li> </ul>
User feedback.	<a href="https://dnacenter.uservoice.com">https://dnacenter.uservoice.com</a>
Integrate with Cisco Meraki.	<p>Recommended: *.meraki.com:443</p> <p>Customers who want to avoid wildcards can specify these URLs instead:</p> <ul style="list-style-type: none"> <li>• dashboard.meraki.com:443</li> <li>• api.meraki.com:443</li> <li>• n63.meraki.com:443</li> </ul>
Check SSL/TLS certificate revocation status using OCSP/CRL.	<ul style="list-style-type: none"> <li>• <a href="http://validation.identrust.com">http://validation.identrust.com</a></li> <li>• <a href="http://commercial.ocsp.identrust.com">http://commercial.ocsp.identrust.com</a></li> </ul> <p><b>Note</b> These URLs should be reachable both directly and through the proxy server that's configured for Cisco DNA Center.</p>
Allow Cisco authorized specialists to collect troubleshooting data when Cisco DNA Center Remote Support functionality is enabled.	wss://prod.radkit-cloud.cisco.com:443

In order to...	...Cisco DNA Center must access these URLs and FQDNs
Integrate with cisco.com and Cisco Smart Licensing.	<p>*.cisco.com:443</p> <p>Customers who want to avoid wildcards can specify these URLs instead:</p> <ul style="list-style-type: none"> <li>• software.cisco.com</li> <li>• cloudsso.cisco.com</li> <li>• cloudsso1.cisco.com</li> <li>• cloudsso2.cisco.com</li> <li>• apiconsole.cisco.com</li> <li>• api.cisco.com</li> <li>• apx.cisco.com</li> <li>• sso.cisco.com</li> <li>• apmx-prod1-vip.cisco.com</li> <li>• apmx-prod2-vip.cisco.com</li> <li>• tools.cisco.com</li> <li>• tools1.cisco.com</li> <li>• tools2.cisco.com</li> <li>• smartreceiver.cisco.com</li> </ul>
Connect to the Network-Based Application Recognition (NBAR) cloud.	prod.sdavc-cloud-api.com:443
Render accurate information in site and location maps.	<ul style="list-style-type: none"> <li>• www.mapbox.com</li> <li>• *.tiles.mapbox.com/* :443. For a proxy, the destination is *.tiles.mapbox.com/*</li> </ul>
For Cisco AI Network Analytics data collection, configure your network or HTTP proxy to allow outbound HTTPS (TCP 443) access to the cloud hosts.	<ul style="list-style-type: none"> <li>• <a href="https://api.use1.prd.kairos.ciscolabs.com">https://api.use1.prd.kairos.ciscolabs.com</a> (US East Region)</li> <li>• <a href="https://api.eu1.prd.kairos.ciscolabs.com">https://api.eu1.prd.kairos.ciscolabs.com</a> (EU Central Region)</li> </ul>
Access a menu of interactive help flows that let you complete specific tasks from the GUI.	<a href="https://ec.walkme.com">https://ec.walkme.com</a>
Access the licensing service.	<a href="https://swapi.cisco.com">https://swapi.cisco.com</a>
Integrate with Cisco Spaces.	<ul style="list-style-type: none"> <li>• <a href="https://dnaspaces.io">https://dnaspaces.io</a></li> <li>• <a href="https://dnaspaces.eu">https://dnaspaces.eu</a></li> <li>• <a href="https://ciscospaces.sg">https://ciscospaces.sg</a></li> </ul>

<sup>1</sup> Cisco owns and maintains ciscoconnectdna.com and its subdomains. The Cisco Connect DNA infrastructure meets Cisco Security and Trust guidelines and undergoes continuous security testing. This infrastructure is robust, with built-in load balancing and automation capabilities, and is monitored and maintained by a cloud operations team to ensure 24x7x365 availability.

## Provide Secure Access to the Internet

By default, the appliance is configured to access the internet in order to download software updates, licenses, and device software, as well as provide up-to-date map information, user feedback, and so on. Providing internet connections for these purposes is a mandatory requirement.

Using an HTTPS proxy server is a reliable way to access remote URLs securely. We recommend that you use an HTTPS proxy server to provide the appliance with the access it needs to the URLs listed in [Required Internet URLs and Fully Qualified Domain Names](#). During appliance installation, you are prompted to enter the URL and port number of the proxy server you want to use for this purpose, along with the proxy's login credentials (if the proxy requires them).

As of this release, the appliance supports communication with proxy servers over HTTP only. You can place the HTTPS proxy server anywhere within your network. The proxy server communicates with the internet using HTTPS, while the appliance communicates with the proxy server via HTTP. Therefore, we recommend that you specify the proxy's HTTP port when configuring the proxy during appliance configuration.

If you need to change the proxy setting after configuration, you can do so using the GUI.

## Required Network Ports

The following tables list the well-known network service ports that the appliance uses. You must ensure that these ports are open for traffic flows to and from the appliance, whether you open them using firewall settings or a proxy gateway.

Additional ports, protocols, and types of traffic must be accommodated if you are deploying the appliance in a network that employs SDA infrastructure. For details, see [Required Ports and Protocols for Cisco Software-Defined Access](#).



**Note** For information on security considerations when deploying Cisco DNA Center, see the [Cisco DNA Center Security Best Practices Guide](#).

**Table 5: Ports: Incoming Traffic**

Port Number	Permitted Traffic	Protocol (TCP or UDP)
22	SSH	TCP
67	BOOTP	UDP
80	HTTP	TCP
111	NFS (used for Assurance backups)	TCP and UDP
123	NTP	UDP

Port Number	Permitted Traffic	Protocol (TCP or UDP)
162	SNMP	UDP
443	HTTPS	TCP
514	Syslog	UDP
2049	NFS (used for Assurance backups)	TCP and UDP
2068	HTTPS	TCP <b>Note</b> This port acts as the remote KVM console redirect port. If Cisco IMC is used during appliance configuration, the port must be open until configuration of the appliance is complete.
2222	SSH	TCP
9991	Multicast Domain Name System (mDNS)	TCP
20048	NFS (used for Assurance backups)	TCP and UDP
21730	Application Visibility Service (used for CBAR device communication)	UDP
32767	NFS (used for Assurance backups)	TCP and UDP

Table 6: Ports: Outgoing Traffic

Port Number	Permitted Traffic	Protocol (TCP or UDP)
22	SSH (to network devices)	TCP
23	Telnet (to network devices)	TCP
53	DNS	UDP
80	Port 80 can be used for an outgoing proxy configuration. Other common ports (such as 8080) can also be used when a proxy is configured using the Configuration wizard (if a proxy is already in use for your network). To access Cisco-supported certificates and trust pools, configure your network to allow outgoing IP traffic from the appliance to the Cisco addresses listed at: <a href="https://www.cisco.com/security/pki/">https://www.cisco.com/security/pki/</a>	TCP
123	NTP	UDP
161	SNMP agent	UDP

Port Number	Permitted Traffic	Protocol (TCP or UDP)
443	HTTPS	TCP
5222, 8910	Cisco ISE XMP for PxGrid	TCP
9060	Cisco ISE ERS API traffic	TCP



---

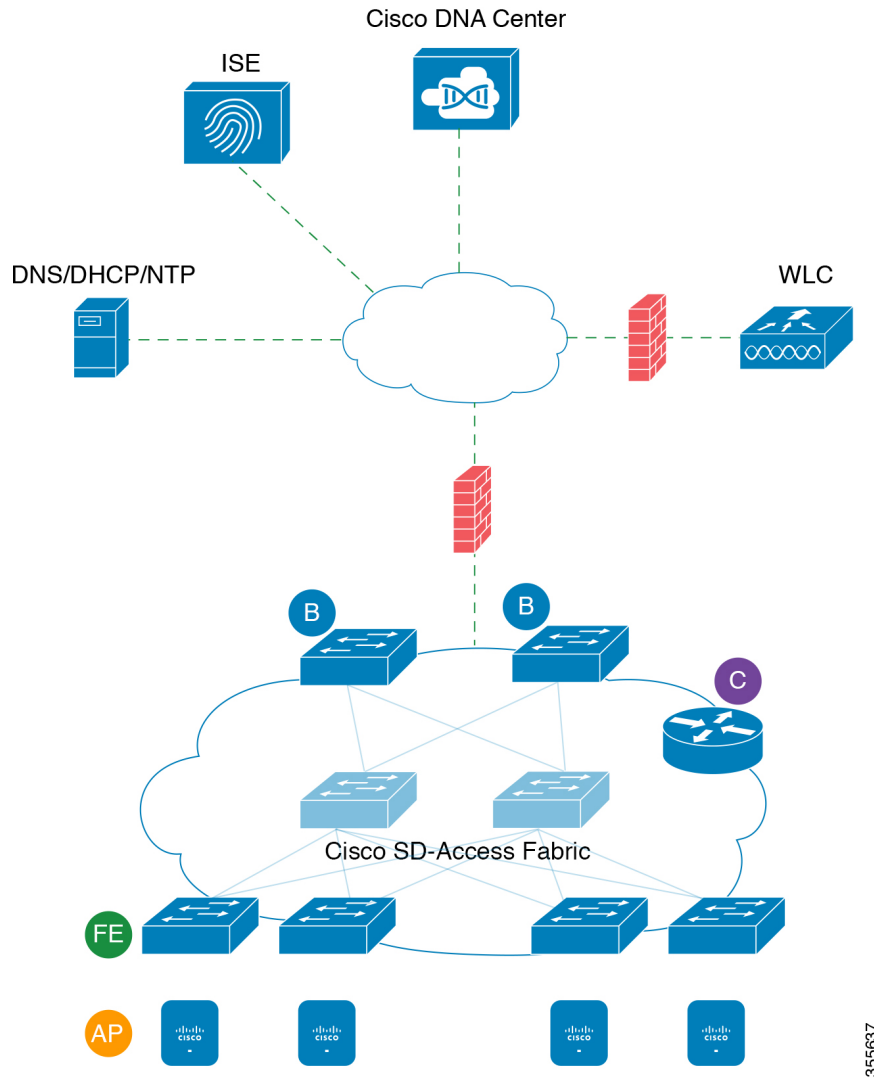
**Note** Additionally, you can configure your network to allow outgoing IP traffic from the appliance to the Cisco addresses at: <https://www.cisco.com/security/pki/>. The appliance uses the IP addresses listed at the above URL to access Cisco-supported certificates and trust pools.

---

## Required Ports and Protocols for Cisco Software-Defined Access

This topic details the ports, protocols, and types of traffic native to a typical Cisco SD-Access fabric deployment that is similar to the one shown in the following figure.

Figure 5: Cisco SD-Access Fabric Infrastructure



If you have implemented Cisco SD-Access in your network, use the information in the following tables to plan firewall and security policies that secure your Cisco SD-Access infrastructure properly while providing Cisco DNA Center with the access it requires to automate your network management.

Table 7: Cisco DNA Center Traffic

Source Port <sup>2</sup>	Source	Destination Port	Destination	Description
Any	Cisco DNA Center	UDP 53	DNS Server	From Cisco DNA Center to DNS server
Any	Cisco DNA Center	TCP 22	Fabric underlay	From Cisco DNA Center to fabric switches' loopbacks for SSH



Any	Cisco DNA Center	TCP 23	Fabric underlay	From Cisco DNA Center to fabric switches' loopbacks for TELNET
Any	Cisco DNA Center	UDP 161	Fabric underlay	From Cisco DNA Center to fabric switches' loopbacks for SNMP device discovery
ICMP	Cisco DNA Center	ICMP	Fabric underlay	From Cisco DNA Center to fabric switches' loopbacks for SNMP device discovery
Any	Cisco DNA Center	TCP 443	Fabric underlay	App hosting for switches and NFVIS
Any	Cisco DNA Center	UDP 6007	Switches and routers	From Cisco DNA Center to switches and routers for NetFlow
Any	Cisco DNA Center	TCP 830	Fabric underlay	From Cisco DNA Center to fabric switches for Netconf (Cisco SD-Access embedded wireless)
UDP 123	Cisco DNA Center	UDP 123	Fabric underlay	From Cisco DNA Center to fabric switches for the initial period during LAN automation
Any	Cisco DNA Center	UDP 123	NTP Server	From Cisco DNA Center to NTP server
Any	Cisco DNA Center	TCP 22, UDP 161	Cisco Wireless Controller	From Cisco DNA Center to Cisco Wireless Controller
ICMP	Cisco DNA Center	ICMP	Cisco Wireless Controller	From Cisco DNA Center to Cisco Wireless Controller
Any	AP	TCP 32626	Cisco DNA Center	Used for receiving traffic statistics and packet capture data used by the Cisco DNA Assurance Intelligent Capture (gRPC) feature.

<sup>2</sup> Cluster, PKI, SFTP server, and proxy port traffic are not included in this table.

**Table 8: Internet Connectivity Traffic**

Source Port	Source	Destination Port	Destination	Description
Any	Cisco DNA Center	TCP 443	registry.ciscoconnectdna.com	Download Cisco DNA Center package updates
Any	Cisco DNA Center	TCP 443	www.ciscoconnectdna.com	Download Cisco DNA Center package updates
Any	Cisco DNA Center	TCP 443	registry-cdn.ciscoconnectdna.com	Download Cisco DNA Center package updates
Any	Cisco DNA Center	TCP 443	cdn.ciscoconnectdna.com	Download Cisco DNA Center package updates
Any	Cisco DNA Center	TCP 443	software.cisco.com	Download device software

Any	Cisco DNA Center	TCP 443	cloudsso.cisco.com	Validate Cisco.com and Smart Account credentials
Any	Cisco DNA Center	TCP 443	cloudsso1.cisco.com	Validate Cisco.com and Smart Account credentials
Any	Cisco DNA Center	TCP 443	cloudsso2.cisco.com	Validate Cisco.com and Smart Account credentials
Any	Cisco DNA Center	TCP 443	apiconsole.cisco.com	CSSM Smart Licensing API
Any	Cisco DNA Center	TCP 443	sso.cisco.com	Cisco.com credentials and Smart Licensing
Any	Cisco DNA Center	TCP 443	api.cisco.com	Cisco.com credentials and Smart Licensing
Any	Cisco DNA Center	TCP 443	apx.cisco.com	Cisco.com credentials and Smart Licensing
Any	Cisco DNA Center	TCP 443	dashboard.meraki.com	Meraki integration
Any	Cisco DNA Center	TCP 443	api.meraki.com	Meraki integration
Any	Cisco DNA Center	TCP 443	n63.meraki.com	Meraki integration
Any	Cisco DNA Center	TCP 443	dnacenter.uservoice.com	User feedback submission
Any	Cisco DNA Center Admin Client	TCP 443	*.tiles.mapbox.com	Render maps in the browser (for access through proxy; the destination is *.tiles.mapbox.com/*)
Any	Cisco DNA Center	TCP 443	www.mapbox.com	Maps and Cisco Wireless Controller country code identification

Table 9: Cisco Software-Defined Access Fabric Underlay Traffic

Source Port <sup>3</sup>	Source	Destination Port	Destination	Description
UDP 68	Fabric underlay	UDP 67	DHCP server	From fabric switches and routers to the DHCP server for DHCP Relay packets initiated by the fabric edge nodes.
Any	Fabric underlay	TCP 80	Cisco DNA Center	From fabric switch and router loopback IPs to Cisco DNA Center for PnP
Any	Fabric underlay	TCP 443	Cisco DNA Center	From fabric switch and router loopback IPs to Cisco DNA Center for image upgrade
Any	Fabric underlay	UDP 162	Cisco DNA Center	From fabric switch and router loopback IPs to Cisco DNA Center for SNMP Traps
Any	Fabric underlay	UDP 514	Cisco DNA Center	From fabric switches and routers to Cisco DNA Assurance
Any	Fabric underlay	UDP 6007	Cisco DNA Center	From fabric switches and routers to Cisco DNA Center for NetFlow

Any	Fabric underlay	UDP 123	Cisco DNA Center	From fabric switches to Cisco DNA Center; used when doing LAN automation
ICMP	Fabric underlay	ICMP	Cisco DNA Center	From fabric switch and router loopbacks to Cisco DNA Center for SNMP: device discovery
UDP 161	Fabric underlay	Any	Cisco DNA Center	From fabric switch and router loopbacks to Cisco DNA Center for SNMP: Device Discovery
Any	Fabric underlay	UDP 53	DNS Server	From fabric switches and routers to DNS server for name resolution
TCP and UDP 4342	Fabric underlay	TCP and UDP 4342	Fabric Routers and Switches	LISP-encapsulated control messages
TCP and UDP 4342	Fabric underlay	Any	Fabric Routers and Switches	LISP control-plane communications
Any	Fabric underlay	UDP 4789	Fabric Routers and Switches	Fabric-encapsulated data packets (VXLAN-GPO)
Any	Fabric underlay	UDP 1645/1646/1812/1813	ISE	From fabric switch and router loopback IPs to ISE for RADIUS
ICMP	Fabric underlay	ICMP	ISE	From fabric switches and routers to ISE for troubleshooting
UDP 1700/3799	Fabric underlay	Any	ISE	From fabric switches to ISE for care-of address (CoA)
Any	Fabric underlay	UDP 123	NTP Server	From fabric switch and router loopback IPs to the NTP server
Any	control-plane	UDP and TCP 4342/4343	Cisco Wireless Controller	From control-plane loopback IP to Cisco Wireless Controller for Fabric-enabled wireless

<sup>3</sup> Border routing protocol, SPAN, profiling, and telemetry traffic are not included in this table.

**Table 10: Cisco Wireless Controller Traffic**

Source Port	Source	Destination Port	Destination	Description
UDP 5246/5247/5248	Cisco Wireless Controller	Any	AP IP Address Pool	From Cisco Wireless Controller to an AP subnet for CAPWAP
ICMP	Cisco Wireless Controller	ICMP	AP IP Address Pool	From Cisco Wireless Controller to APs allowing ping for troubleshooting
Any	Cisco Wireless Controller	<ul style="list-style-type: none"> <li>• TCP 443 (Cisco AireOS wireless controllers)</li> <li>• TCP 25103 (Cisco 9800 wireless controllers)</li> </ul>	Cisco DNA Center	From Cisco Wireless Controller to Cisco DNA Center for Assurance

Any	Cisco Wireless Controller	UDP 69/5246/5247 TCP 22	AP IP Address Pool	From Cisco Wireless Controller to an AP subnet for CAPWAP
Any	Cisco Wireless Controller	UDP and TCP 4342/4343	Control plane	From Cisco Wireless Controller to control-plane loopback IP address
Any	Cisco Wireless Controller	TCP 22	Cisco DNA Center	From Cisco Wireless Controller to Cisco DNA Center for device discovery
UDP 161	Cisco Wireless Controller	Any	Cisco DNA Center	From Cisco Wireless Controller to Cisco DNA Center for SNMP
Any	Cisco Wireless Controller	UDP 162	Cisco DNA Center	From Cisco Wireless Controller to Cisco DNA Center for SNMP traps
Any	Cisco Wireless Controller	TCP 16113	Cisco Mobility Services Engine (MSE) and Cisco Spectrum Expert	From Cisco Wireless Controller to Cisco MSE and Spectrum Expert for NMSP
Any	Cisco Wireless Controller	UDP 6007	Cisco DNA Center	From wireless controllers to Cisco DNA Center for NetFlow network telemetry
ICMP	Cisco Wireless Controller	ICMP	Cisco DNA Center	From Cisco Wireless Controller to allow ping for troubleshooting
Any	Cisco Wireless Controller and various syslog servers	UDP 514	Cisco Wireless Controller	Syslog (optional)
Any	Cisco Wireless Controller	UDP 53	DNS Server	From Cisco Wireless Controller to DNS server
Any	Cisco Wireless Controller	TCP 443	ISE	From Cisco Wireless Controller to ISE for Guest SSID web authorization
Any	Cisco Wireless Controller	UDP 1645,1812	ISE	From Cisco Wireless Controller to ISE for RADIUS authentication
Any	Cisco Wireless Controller	UDP 1646, 1813	ISE	From Cisco Wireless Controller to ISE for RADIUS accounting
Any	Cisco Wireless Controller	UDP 1700, 3799	ISE	From Cisco Wireless Controller to ISE for RADIUS CoA
ICMP	Cisco Wireless Controller	ICMP	ISE	From Cisco Wireless Controller to ISE ICMP for troubleshooting
Any	Cisco Wireless Controller	UDP 123	NTP server	From Cisco Wireless Controller to NTP server

Table 11: Fabric-Enabled Wireless AP IP Address Pool Traffic

Source Port	Source	Destination Port	Destination	Description
UDP 68	AP IP Address Pool	UDP 67	DHCP server	From an AP IP Address pool to DHCP server.

ICMP	AP IP Address Pool	ICMP	DHCP server	From an AP IP Address pool to ICMP for troubleshooting.
Any	AP IP Address Pool	514	Various	Syslog—Destination configurable. Default is 255.255.255.255.
Any	AP IP Address Pool	UDP 69/5246/5247/5248	Cisco Wireless Controller	From an AP IP Address pool to Cisco Wireless Controller for CAPWAP.
ICMP	AP IP Address Pool	ICMP	Cisco Wireless Controller	From an AP IP Address pool to Cisco Wireless Controller, allowing ping for troubleshooting.

Table 12: Cisco ISE Traffic

Source Port <sup>4</sup>	Source	Destination Port	Destination	Description
Any	ISE	TCP 64999	Border	From ISE to border node for SGT Exchange Protocol (SXP)
Any	ISE	UDP 514	Cisco DNA Center	From ISE to syslog server (Cisco DNA Center)
UDP 1645/1646/1812/1813	ISE	Any	Fabric underlay	From ISE to fabric switches and routers for RADIUS and authorization
Any	ISE	UDP 1700/3799	Fabric underlay, Cisco Wireless Controller	From ISE to fabric switch and router loopback IP addresses for RADIUS Change of Authorization (CoA).  UDP port 3799 must also be open from ISE to the wireless controller for CoA.
ICMP	ISE	ICMP	Fabric underlay	From ISE to fabric switches for troubleshooting
Any	ISE	UDP 123	NTP Server	From ISE to NTP server
UDP 1812/1645/1813/1646	ISE	Any	Cisco Wireless Controller	From ISE to Cisco Wireless Controller for RADIUS
ICMP	ISE	ICMP	Cisco Wireless Controller	From ISE to Cisco Wireless Controller for troubleshooting

<sup>4</sup> Note: High availability and profiling traffic are not included in this table.

Table 13: DHCP Server Traffic

Source Port	Source	Destination Port	Destination	Description
UDP 67	DHCP server	UDP 68	AP IP Address Pool	From DHCP server to fabric APs
ICMP	DHCP server	ICMP	AP IP Address Pool	ICMP for troubleshooting: Fabric to DHCP
UDP 67	DHCP server	UDP 68	Fabric underlay	From DHCP to fabric switches and routers

ICMP	DHCP server	ICMP	Fabric underlay	ICMP for troubleshooting: Fabric to DHCP
UDP 67	DHCP server	UDP 68	User IP Address Pool	From DHCP server to fabric switches and routers
ICMP	DHCP server	ICMP	User IP Address Pool	ICMP for troubleshooting: User to DHCP

Table 14: NTP Server Traffic

Source Port	Source	Destination Port	Destination	Description
UDP 123	NTP Server	Any	ISE	From NTP server to ISE
UDP 123	NTP Server	Any	Cisco DNA Center	From NTP server to Cisco DNA Center
UDP 123	NTP Server	Any	Fabric underlay	From NTP server to fabric switch and router loopback
UDP 123	NTP Server	Any	Cisco Wireless Controller	From NTP server to Cisco Wireless Controller

Table 15: DNS Traffic

Source Port	Source	Destination Port	Destination	Description
UDP 53	DNS Server	Any	Fabric underlay	From DNS server to fabric switches
UDP 53	DNS Server	Any	Cisco Wireless Controller	From DNS server to Cisco Wireless Controller

## Required Configuration Information

During appliance configuration, you will be prompted for the following information, in addition to the [Required IP Addresses and Subnets](#):

- **Linux User Name:** This is **maglev**. This user name is the same on all the appliances in a cluster, including the primary node and secondary nodes, and cannot be changed.
- **Linux Password:** Identifies the password for the Linux user name **maglev**. This password ensures secure access to each appliance using the Linux command line. If required, you can assign a different Linux password for each **maglev** Linux user name on each appliance in a cluster.

You must create the Linux password because there is no default. The password must meet the following requirements:

- Minimum length of eight characters.

- Cannot contain a tab or a line break.
- Contains characters from at least three of the following categories:
  - Uppercase letters (A–Z)
  - Lowercase letters (a–z)
  - Numbers (0–9)
  - Special characters (for example, ! or #)

The Linux password is encrypted and hashed in the Cisco DNA Center database. If you are deploying a multinode cluster, you will also be prompted to enter the primary node's Linux password on each of the secondary nodes.

- **Password Generation Seed (Optional):** Instead of creating a Linux password, you can enter a seed phrase and click **Generate Password**. The **Maglev Configuration** wizard generates a random and secure password using this seed phrase. You can further edit the generated password by using the **Auto Generated Password** field.
- **Administrator Passphrase:** Identifies the password used for web access to Cisco DNA Center in a cluster. This is the password for the superuser account **admin**, which you use to log in to Cisco DNA Center for the first time (see [#unique\\_23](#)). You are prompted to change this password when you log in for the first time.

You must create this password because there is no default. The Administrator Passphrase must meet the same requirements as the Linux password, described earlier.

- **CIMC User Password:** Identifies the password used for access to the CIMC GUI. The factory default is *password*, but you are prompted to change it when you first set up CIMC for access using a web browser (see [Enable Browser Access to Cisco Integrated Management Controller](#)).

The CIMC user password must meet the same requirements as the Linux password described earlier. It can be changed back to *password* only by a reset to factory defaults.

- **Primary Node IP Address:** Required only when you are installing secondary nodes in a cluster. This is the IP address of the cluster port on the primary node (see [Interface Cable Connections](#)).

## Required First-Time Setup Information

After you have configured your appliances, log in to Cisco DNA Center and complete the essential setup tasks. During this first-time setup, you should have the following information:

- **New Admin Superuser Password:** You will be prompted to enter a new password for the Cisco DNA Center admin super user. Resetting the super user password enhances operational security. This is especially important if, for example, the enterprise staff who installed and configured the Cisco DNA Center appliance is not a Cisco DNA Center user or administrator.
- **Cisco.com Credentials:** The Cisco.com user ID and password that your organization uses to register software downloads and receive system communications through email.
- **Cisco Smart Account Credentials:** The Cisco.com Smart Account user ID and password your organization uses for managing your device and software licenses.

- **IP Address Manager URL and Credentials:** The host name, URL, admin user name, and admin password of the third-party IP address manager (IPAM) server you plan to use with Cisco DNA Center. This release supports InfoBlox and Bluecat.
- **Proxy URL, Port, and Credentials:** The URL (host name or IP address), port number, user name, and user password of the proxy server you plan to use with Cisco DNA Center in order to get updates to the Cisco DNA Center software, manage device licenses, and retrieve other downloadable content.
- **Cisco DNA Center Users:** User names, passwords, and privilege settings for the new Cisco DNA Center users you will be creating. We recommend that you always use one of these new user accounts for all your normal Cisco DNA Center operations. Avoid using the admin super user account for activities, except reconfiguring Cisco DNA Center and operations where super user privileges are explicitly required.

For details about how to launch and respond to the first-time setup wizard that prompts you for this information, see [Complete the Quick Start Workflow, on page 89](#).

You will also need the following information to complete the remaining setup tasks, which can be done after your first login:

- **ISE Server IP and Credentials:** You will need the Cisco ISE server IP address and credentials, administrative user name, and password. These are needed to log in to and configure your organization's ISE server to share data with Cisco DNA Center, as explained in [Integrate Cisco ISE with Cisco DNA Center](#).

Installation of or upgrade to Cisco DNA Center checks to see if Cisco ISE is configured as an authentication and policy (AAA) server. If the correct version of Cisco ISE is already configured, you can start migrating group policy data from Cisco ISE to Cisco DNA Center.

If Cisco ISE is not configured, or if the required version of Cisco ISE is not present, Cisco DNA Center installs, but Group Based Policy is disabled. You must install or upgrade Cisco ISE and connect it to Cisco DNA Center. You can then start the data migration.

Cisco DNA Center data present in the previous version is preserved when you upgrade. The data migration operation merges data from Cisco DNA Center and Cisco ISE. If the migration encounters a conflict, preference is given to data from Cisco ISE.

If Cisco DNA Center becomes unavailable, and it is imperative to manage policies before Cisco DNA Center becomes available once more, there is an option in Cisco ISE to override the Read-Only setting. This allows you to make policy changes directly in Cisco ISE. After Cisco DNA Center is available again, you must disable the Read-Only override on Cisco ISE, and re-synchronize the policy data on Cisco DNA Center Group Based Access Control Settings page. Only use this option when absolutely necessary, since changes made directly in Cisco ISE are not propagated to Cisco DNA Center.

- **Authorization and Policy Server Information:** If you are using Cisco ISE as your authentication and policy server, you will need the same information listed in the previous bullet, plus the ISE CLI user name, CLI password, server FQDN, a subscriber name (such as *cdnac*), the ISE SSH key (optional), the protocol choice (RADIUS or TACACS), the authentication port, the accounting port, and retry and timeout settings.

If you are using an authorization and policy server that is not Cisco ISE, you will need the server's IP address, protocol choice (RADIUS or TACACS), authentication port, accounting port, and retry and timeout settings.

This information is required to integrate Cisco DNA Center with your chosen authentication and policy server, as explained in [Configure Authentication and Policy Servers, on page 100](#).



- **SNMP Retry and Timeout Values:** This is required to set up device polling and monitoring, as explained in [Configure SNMP Properties](#).





## CHAPTER 3

# Install the Appliance

---

- [Appliance Installation Workflow, on page 37](#)
- [Unpack and Inspect the Appliance, on page 37](#)
- [Review the Installation Warnings and Guidelines, on page 38](#)
- [Review the Rack Requirements, on page 39](#)
- [Connect and Power On the Appliance, on page 39](#)
- [Check the LEDs, on page 40](#)

## Appliance Installation Workflow

Complete the tasks described in this chapter to physically install your Cisco DNA Center appliance. Complete these tasks for each appliance you want to install, and be sure to install all of the appliances before configuring the primary node.

## Unpack and Inspect the Appliance



---

**Caution** When handling internal appliance components, wear an ESD strap and handle modules by the carrier edges only.

---

- 
- Step 1** Remove the appliance from its cardboard container and save all the packaging material (in case the appliance requires shipping in the future).
- Step 2** Compare the shipment with the equipment list provided by your customer service representative. Verify that you have all the items.
- Step 3** Check for damage and report discrepancies or damage, if any, to your customer service representative immediately. Have the following information ready:
- Invoice number of the shipper (see the packing slip)
  - Model and serial number of the damaged unit
  - Description of damage

- Effect of damage on the installation

---

## Review the Installation Warnings and Guidelines



---

**Warning** To prevent the system from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of: 95°F (35°C). Statement 1047

---



---

**Warning** The plug-socket combination must be accessible at all times, because it serves as the main disconnecting device. Statement 1019

---



---

**Warning** This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than: 250 V, 15 A. Statement 1005

---



---

**Warning** Installation of the equipment must comply with local and national electrical codes. Statement 1074

---



---

**Caution** To ensure proper airflow it is necessary to rack the appliances using rail kits. Physically placing the units on top of one another or “stacking” without the use of the rail kits blocks the air vents on top of the appliances, which could result in overheating, higher fan speeds, and higher power consumption. We recommend that you mount your appliances on rail kits when you are installing them into the rack because these rails provide the minimal spacing required between the appliances. No additional spacing between the appliances is required when you mount the units using rail kits.

---



---

**Caution** Avoid uninterruptible power supply (UPS) types that use ferroresonant technology. These UPS types can become unstable with systems such as the Cisco UCS, which can have substantial current-draw fluctuations due to fluctuating data traffic patterns.

---

When you are installing an appliance, follow these guidelines:

- Plan your site configuration and prepare the site before installing the appliance. See the [Cisco UCS Site Preparation Guide](#) for help with recommended site planning and preparation tasks.
- Ensure that there is adequate space around the appliance to allow for servicing the appliance and for adequate airflow. The airflow in this appliance is from front to back.
- Ensure that the site air-conditioning meets the thermal requirements listed in the [Environmental Specifications](#).

- Ensure that the cabinet or rack meets the requirements listed in [Review the Rack Requirements, on page 39](#)
- Ensure that the site power meets the requirements listed in [Power Specifications, on page 10](#). If available, you can use a UPS to protect against power failures.

## Review the Rack Requirements

For proper operation, the rack in which you install the appliance must meet the following requirements:

- A standard 19-in. (48.3-cm) wide, four-post EIA rack, with mounting posts that conform to English universal hole spacing, per section 1 of ANSI/EIA-310-D-1992.
- The rack post holes can be square 0.38-in. (9.6 mm), round 0.28-in. (7.1 mm), #12-24 UNC, or #10-32 UNC when you use the supplied slide rails.
- The minimum vertical rack space per server must be one RU, equal to 1.75 in. (44.45 mm).

## Connect and Power On the Appliance

This section describes how to power on the appliance and check that it is functional.

---

**Step 1** Attach the supplied power cord to each power supply in the appliance and then attach the power cords to a grounded AC power outlet. See [Power Specifications, on page 10](#) for details.

Wait for approximately two minutes to let the appliance boot into standby power mode during the first boot up.

You can verify the power status by looking at the Power Status LED:

- Off—There is no AC power present in the appliance.
- Amber—The appliance is in standby power mode. Power is supplied only to the CIMC and some motherboard functions.
- Green—The appliance is in main power mode. Power is supplied to all appliance components.

For more information on these and other appliance LEDs, see [Front and Rear Panels](#).

**Step 2** Connect a USB keyboard and VGA monitor to the server, using the supplied KVM cable connected to the KVM connector on the front panel. Alternatively, you can use the VGA and USB ports on the rear panel. You can only connect to one VGA interface at a time.

---

### What to do next

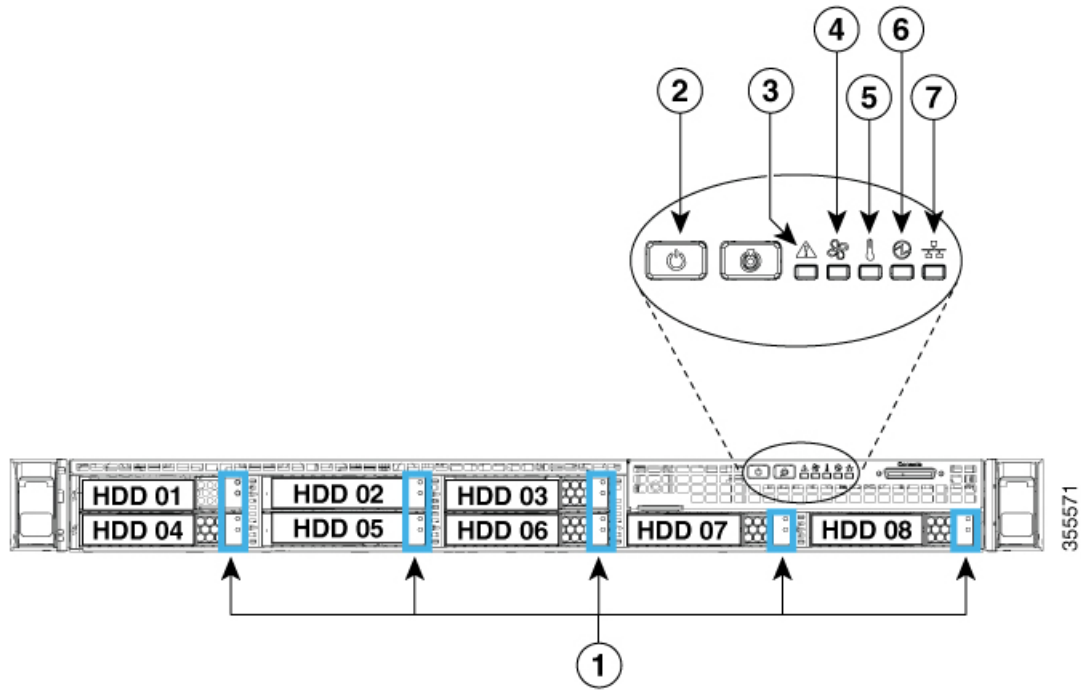
Continue by following the procedure described in [Check the LEDs](#).

# Check the LEDs

After you have powered up the Cisco DNA Center appliance, check the state of the front-panel and rear-panel LEDs and buttons to ensure it is functioning.

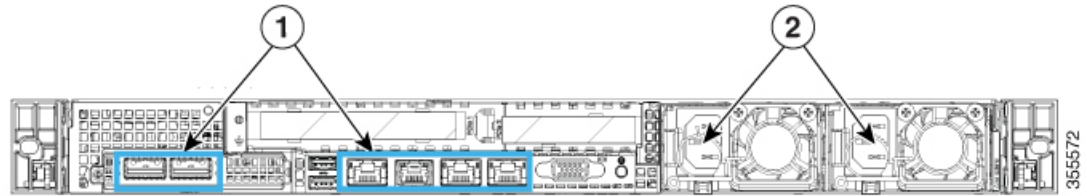
The following illustrations show the LEDs for a functional appliance after physical installation and first power-up and before configuration.

**Figure 6: Front Panel LEDs**



LED	Desired Status Indicator
1	Drive Fault LEDs: Off. Drive Activity LEDs: Green
2	Power Status: Green
3	System Status: Green
4	Fan Status: Green
5	Temperature Status: Green
6	Power Supply Status: Green
7	Network Link Activity: Off

Figure 7: Rear Panel LEDs



LED	Desired Status Indicator
1	<p>After initial power-up, all the ports should have their Link Status and Link Speed LEDs showing as off, and their Power Status LED should be green.</p> <p>After network settings are configured and tested using the Maglev Configuration Wizard (see <a href="#">Configure the Primary Node</a> and <a href="#">Configure a Secondary Node</a>), the Link Status, Link Speed and Power Status LEDs for all <b>cabled</b> ports should be green. All <b>uncabled</b> port LEDs should be unchanged.</p>
2	<p>Power Supply Fault LEDs: Off.</p> <p>AC Power LEDs: Green</p>

If you see LEDs with colors other than those shown above, you may have a problem condition. See [Front and Rear Panels](#) for details on the likely causes of the status. Be sure to correct any problem conditions before proceeding to configure the appliance.







## CHAPTER 4

# Prepare the Appliance for Configuration

---

- [Preparation for Appliance Configuration Overview](#), on page 43
- [Enable Browser Access to Cisco Integrated Management Controller](#), on page 43
- [Execute Preconfiguration Checks](#), on page 48
- [Reimage the Appliance](#), on page 55

## Preparation for Appliance Configuration Overview

Before you can successfully configure your Cisco DNA Center appliance, first complete the following tasks:

1. Enable browser access to the appliance's Cisco IMC (see [Enable Browser Access to Cisco Integrated Management Controller](#)).
2. Use Cisco IMC to check and adjust important hardware and switch settings (see [Execute Preconfiguration Checks](#)).
3. Cisco DNA Center software is preinstalled on your appliance, but you may need to reinstall the software in certain situations (such as before you change the current cluster link configuration). If this is the case, you must also complete the tasks described in [Reimage the Appliance](#).



---

**Note** If you do not need to reimage your appliance, proceed to [Appliance Configuration Overview](#).

---

## Enable Browser Access to Cisco Integrated Management Controller

After installing the appliance, as described in [Appliance Installation Workflow](#), use the Cisco IMC configuration utility to assign an IP address and gateway to the appliance's CIMC port. This gives you access to the Cisco IMC GUI, which you should use to configure the appliance.

After you complete the Cisco IMC setup, log in to Cisco IMC and run the tasks listed in [Execute Preconfiguration Checks](#) to ensure correct configuration.



**Tip** To help ensure the security of your deployment, Cisco IMC prompts you to change the Cisco IMC user's default password when you boot the appliance for the first time. To change the Cisco IMC user password later, use the Cisco IMC GUI, as follows:

1. From the top-left corner of the GUI, click the **Toggle Navigation** icon () and then choose **Admin > User Management**.

The **Local User Management** tab should already be selected.

2. Check the check box for user **1**, and then click **Modify User**.

The **Modify User Details** dialog box opens.

3. Check the **Change Password** check box.

4. Enter and confirm the new password, and then click **Save**.

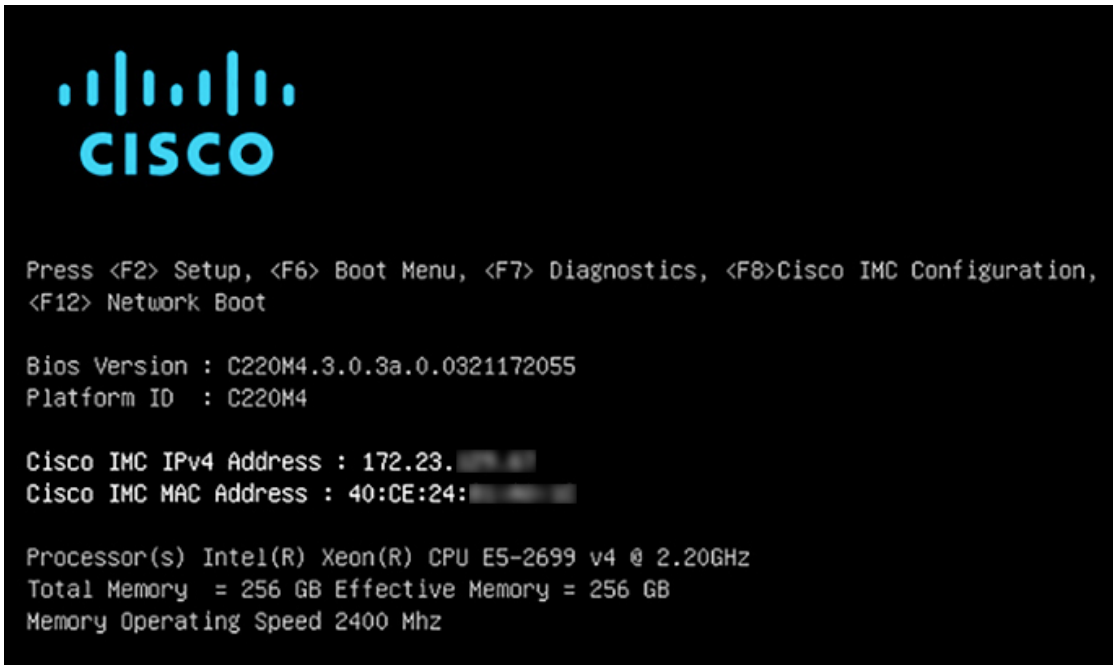
**Step 1** Access the appliance console by attaching either of the following:

- A KVM cable to the KVM connector on the appliance's front panel (component 12 on the front panel illustrated in [Front and Rear Panels](#))
- A keyboard and monitor to the USB and VGA ports on the appliance's rear panel (components 7 and 12, respectively, on the rear panel illustrated in [Front and Rear Panels](#)).

**Step 2** Make sure that the appliance's power cord is plugged in and the power is on.

**Step 3** Press the **Power** button on the front panel to boot the appliance.

The Cisco IMC configuration utility boot screen should be displayed, as shown below.



```

Cisco
Press <F2> Setup, <F6> Boot Menu, <F7> Diagnostics, <F8>Cisco IMC Configuration,
<F12> Network Boot

Bios Version : C220M4.3.0.3a.0.0321172055
Platform ID : C220M4

Cisco IMC IPv4 Address : 172.23.
Cisco IMC MAC Address : 40:CE:24:

Processor(s) Intel(R) Xeon(R) CPU E5-2699 v4 @ 2.20GHz
Total Memory = 256 GB Effective Memory = 256 GB
Memory Operating Speed 2400 Mhz

```

- Step 4** As soon as the boot screen is displayed, press **F8** to perform Cisco IMC configuration.  
The CIMC configuration utility displays the **CIMC User Details** screen, as shown below.

```

CIMC User Details          (Press Enter to Save / Continue)
-----
Enter current CIMC password [XXXXXXXXXX]
Enter new CIMC password    [          ]
Re-Enter new CIMC password [          ]
  
```

- Step 5** Enter the default CIMC user password (the default on a new appliance is *password*) in the **Enter current CIMC Password** field.
- Step 6** Enter and confirm the new CIMC user password in the **Enter new CIMC password** and **Re-Enter new CIMC password** fields.
- When you press **Enter** after entering the new password in the **Re-Enter new CIMC password** field, the Cisco IMC configuration utility displays the **NIC Properties** screen, as shown below.

```

Cisco IMC Configuration Utility Version 2.0 Cisco Systems, Inc.
*****
NIC Properties
NIC mode                NIC redundancy
Dedicated:             [X]          None:                   [X]
Shared LOM:            [ ]          Active-standby:         [ ]
Cisco Card:            [ ]          Active-active:          [ ]
  Riser1:               [ ]          VLAN (Advanced)
  Riser2:               [ ]          VLAN enabled:           [ ]
  MLOm:                 [ ]          VLAN ID:                 1
Shared LOM Ext:        [ ]          Priority:                 0
IP (Basic)
IPV4:                  [X]          IPV6:                   [ ]
DHCP enabled           [ ]
CIMC IP:               172.23.
Prefix/Subnet:         255.255.0.0
Gateway:               172.23.
Pref DNS Server:       171.70.
*****
<Up/Down>Selection  <F10>Save  <Space>Enable/Disable  <F5>Refresh  <ESC>Exit
<F1>Additional settings
  
```

- Step 7** Perform the following actions:
- **NIC mode:** Select **Dedicated**.
  - **IP (Basic):** Select **IPV4**.
  - **CIMC IP:** Enter the IP address of the CIMC port.

- **Prefix/Subnet:** Enter the subnet mask for the CIMC port IP address.
- **Gateway:** Enter the IP address of your preferred default gateway.
- **Pref DNS Server:** Enter the IP address of your preferred DNS server.
- **NIC Redundancy:** Select **None**.

**Step 8** Press **F1** to specify **Additional settings**.

The Cisco IMC configuration utility displays the **Common Properties** screen, as shown below.

```

Cisco IMC Configuration Utility Version 2.0 Cisco Systems, Inc.
*****
Common Properties
  Hostname:      C220-FCH212
  Dynamic DNS:   [ ]
  DDNS Domain:
FactoryDefaults
  Factory Default: [ ]
Default User(Basic)
  Default password:
  Reenter password:
Port Properties
  Auto Negotiation: [X]
                               Admin Mode      Operation Mode
  Speed[1000/100/10Mbps]:    Auto          1000
  Duplex mode[half/full]:    Auto          full
Port Profiles
  Reset:          [ ]
  Name:
*****
<Up/Down>Selection  <F10>Save  <Space>Enable/Disable  <F5>Refresh  <ESC>Exit
<F2>PreviousPageettings

```

**Step 9** Perform the following actions:

- **Hostname:** Enter a hostname for CIMC on this appliance.
- **Dynamic DNS:** Uncheck the check box to disable this feature.
- **Factory Defaults:** Uncheck the check box to disable this feature.
- **Default User (Basic):** Leave these fields blank.
- **Port Properties:** Enter new settings or accept the defaults shown in these fields.
- **Port Profiles:** Uncheck the check box to disable this feature.

**Step 10** Press **F10** to save the settings.

**Step 11** Press **Escape** to exit and reboot the appliance.

**Step 12** After the settings are saved and the appliance finishes rebooting, open a compatible browser on a client machine with access to the subnet on which the appliance is installed, and enter the following URL:

`https://CIMC_ip_address`, where `CIMC_ip_address` is the Cisco IMC port IP address that you entered in Step 7.

Your browser displays a main Cisco IMC GUI login window similar to the one shown below.

**Step 13**

Log in using the Cisco IMC user ID and password you set in Step 5.

If the login is successful, your browser displays a **Cisco Integrated Management Controller Chassis Summary** window similar to the one shown below.

The screenshot displays the Cisco IMC GUI for a Cisco C220-M4SX server. The interface is divided into several sections:

- Server Properties:** Lists details such as Product Name (UCS C220 M4SX), Serial Number (FCH212), PID (UCSC-C220-M4SX), UUID (1DB0E03F-59AF-4B5B-BAB7-), BIOS Version (C220M4.3.1.3c.0.0307181404), Description, and Asset Tag (Unknown).
- Cisco Integrated Management Controller (Cisco IMC) Information:** Shows Hostname (C220-FCH212), IP Address (172.25), MAC Address (70:79:F0), Firmware Version (3.1(3a)), Current Time (UTC) (Tue Aug 14 15:20:18 2018), Local Time (Tue Aug 14 15:20:18 UTC +0000), and Timezone (UTC).
- Chassis Status:** A list of health indicators: Power State (On), Overall Server Status (Good), Temperature (Good), Overall DIMM Status (Good), Power Supplies (Good), Fans (Good), Locator LED (Off), and Overall Storage Status (Good).
- Server Utilization:** A bar chart showing utilization percentages for Overall Utilization (%), CPU Utilization (%), Memory Utilization (%), and IO Utilization (%). The chart shows very low utilization across all categories.

At the bottom right of the GUI, there are buttons for "Save Changes" and "Reset Values".

**Step 14**

Confirm that this version of Cisco IMC is supported by the Cisco DNA Center release you're going to install:

- Note the version listed in the **Firmware Version** field.
- See the [release notes](#) for the Cisco DNA Center release you are installing. The “Supported Firmware” section indicates the Cisco IMC version that your Cisco DNA Center release supports.
- Do one of the following:
  - If the right Cisco IMC version is installed, you can stop here.
  - If you need to update your Cisco IMC version, see the [Cisco Host Upgrade Utility User Guide](#) for instructions.

## Execute Preconfiguration Checks

After installing the appliance (as described in [Appliance Installation Workflow](#)) and setting up access to the Cisco IMC GUI (as described in [Enable Browser Access to Cisco Integrated Management Controller](#)), use Cisco IMC to perform the following preconfiguration tasks, which help ensure correct configuration and deployment:

- Synchronize the appliance hardware with the Network Time Protocol (NTP) servers you use to manage your network. These must be the same NTP servers whose hostnames or IPs you gathered for use when planning your implementation, as explained in [Required IP Addresses and Subnets](#). This is a critical task that ensures that your Cisco DNA Center data is synchronized properly across the network.
- Check that the appliance's 10-Gbps ports are enabled and properly configured for high throughput.
- Reconfigure the switches connected to the 10-Gbps appliance ports to support higher throughput settings.

- Reconfigure the switches connected to the 10-Gbps appliance ports to support oversized 802.1p frames.

**Step 1**

Log in to the appliance's Cisco IMC using the Cisco IMC IP address, user ID, and password you set in [Enable Browser Access to Cisco Integrated Management Controller](#).

If the login is successful, your browser displays the **Cisco Integrated Management Controller Chassis Summary** window, as shown below.

The screenshot shows the Cisco IMC Chassis Summary page for a UCS C220 M4SX server. The page is titled "Cisco Integrated Management Controller (Cisco IMC) Information" and "Chassis / Summary".

**Server Properties:**

- Product Name: UCS C220 M4SX
- Serial Number: FCH212
- PID: UCSC-C220-M4SX
- UUID: 1DB0E03F-59AF-4B5B-BAB7-
- BIOS Version: C220M4.3.1.3c.0.0307181404
- Description: [Empty field]
- Asset Tag: Unknown

**Cisco IMC Information:**

- Hostname: C220-FCH212
- IP Address: 172. .25
- MAC Address: 70:79: . F0
- Firmware Version: 3.1(3a)
- Current Time (UTC): Tue Aug 14 . 15 2018
- Local Time: Tue Aug 14 . 15 2018 UTC +0000
- Timezone: UTC

**Chassis Status:**

- Power State: ● On
- Overall Server Status: ✔ Good
- Temperature: ✔ Good
- Overall DIMM Status: ✔ Good
- Power Supplies: ✔ Good
- Fans: ✔ Good
- Locator LED: ● Off
- Overall Storage Status: ✔ Good

**Server Utilization:**

A bar chart showing utilization percentages for the server. The Y-axis represents percentage from 0 to 100. The X-axis is labeled "Server". The legend indicates:


- Overall Utilization (%) (Blue bar)
- CPU Utilization (%) (Purple bar)
- Memory Utilization (%) (Green bar)
- IO Utilization (%) (Yellow bar)

The chart shows very low utilization for all categories, with Overall Utilization being the highest at approximately 10%.

Buttons at the bottom right: Save Changes, Reset Values.

**Step 2**

Synchronize the appliance's hardware with the Network Time Protocol (NTP) servers you use to manage your network, as follows:

- From the top-left corner of the Cisco IMC GUI, click the **Toggle Navigation** icon (.
- From the Cisco IMC menu, select **Admin > Networking**, and then choose the **NTP Setting** tab.
- Make sure that the **NTP Enabled** check box is checked and enter up to four NTP server host names or addresses in the numbered **Server** fields, as shown in the example below.

Cisco Integrated Management Controller

admin@1 -C220-FCH212

Networking / NTP Setting

Network Network Security NTP Setting

**NTP Properties**

NTP Enabled:

Server 1:

Server 2:

Server 3:

Server 4:


Status: NTP service disabled

Save Changes Reset Values

- d) Click **Save Changes**. Cisco IMC validates your entries and then begins to synchronize the time on the appliance's hardware with the time on the NTP servers.

**Note** Cisco IMC does not support NTP authentication.

**Step 3** Next, check that the appliance NICs are configured to support high throughput, as follows:

- If needed, click the  icon to display the Cisco IMC menu.
- From the Cisco IMC menu, select **Chassis > Inventory > Cisco VIC Adapters**. Verify that the Product ID "UCSC-MLOM-CSC-02" is listed for the MLOM slot, as shown below:

Cisco Integrated Management Controller

Inventory / Cisco VIC Adapters

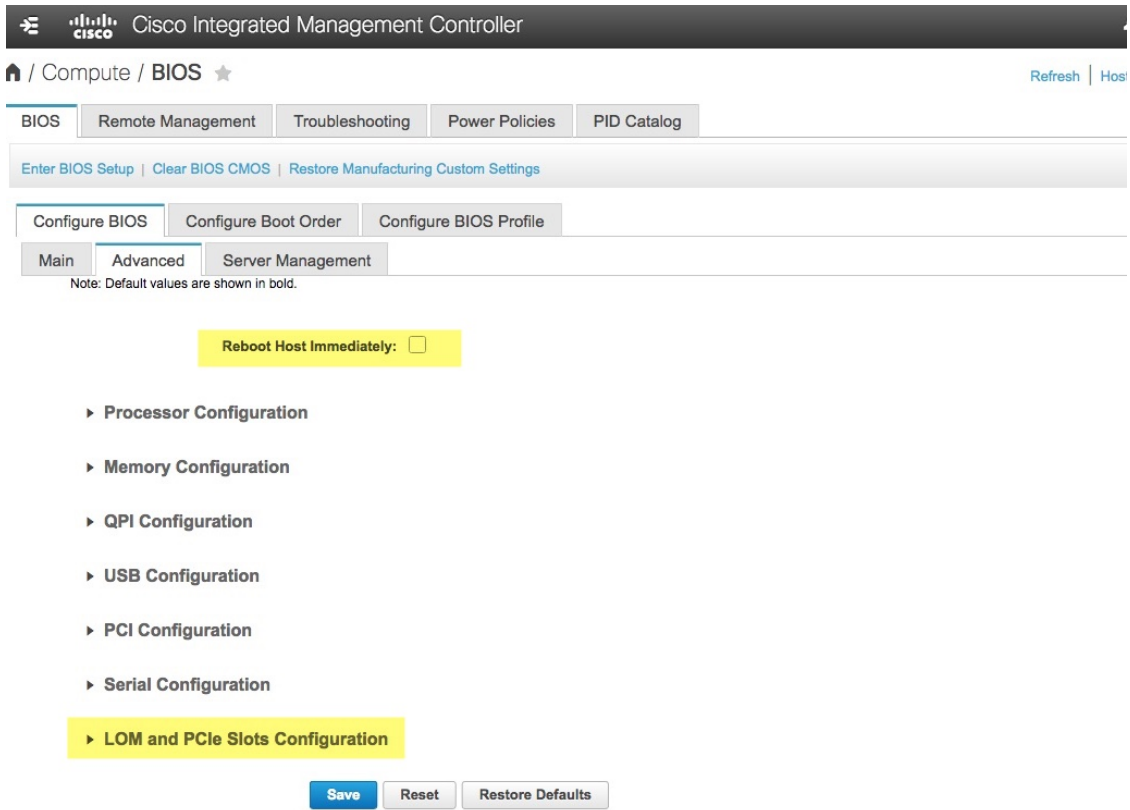
CPU Memory PCI Adapters Power Supplies Cisco VIC Adapters Network Adapters

**Cisco VIC Adapters**

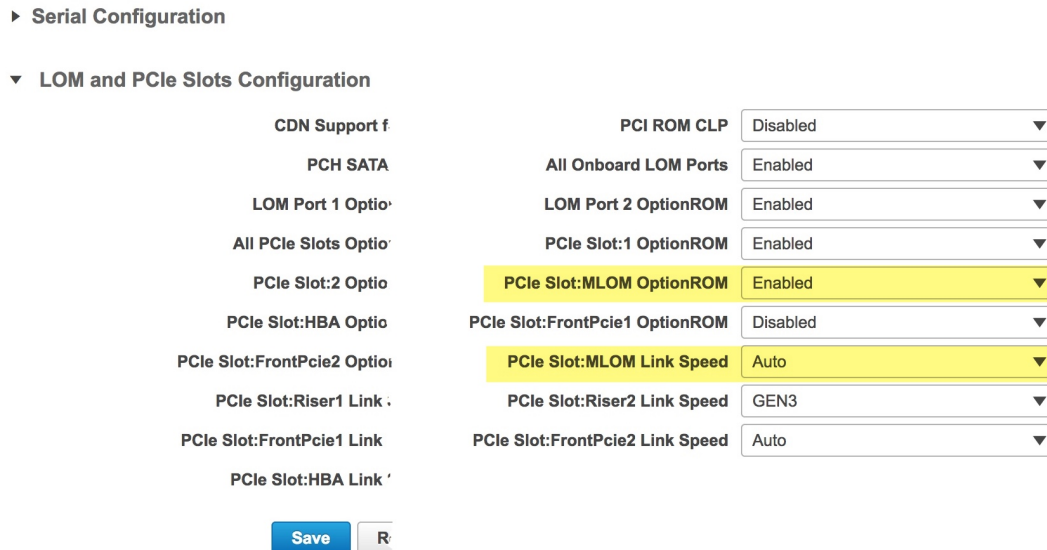
Slot Number	Serial Number	Product ID	Chassis
MLOM	2146J012	UCSC-MLOM-CSC-02	no

- Select  > **Compute > BIOS > Configure BIOS > Advanced**. Verify that the **Reboot Host Immediately** checkbox is unchecked and note the location of the **LOM and PCIe Slots Configuration** dropdown.





d) Select **LOM and PCIe Slots Configuration**. Then, using the dropdown selectors, set **PCIe Slot: MLOM OptionROM** to **Enabled** and **PCIe Slot: MLOM Link Speed** to **Auto**.



e) Click **Save**. You will be prompted to reboot the host. Click **OK** to continue instead of rebooting.  
 f) Select **Networking > Adapter Card MLOM > General**. Take note of the MAC addresses for **Port-0** and **Port-1** (shown in the **External Ethernet Interfaces** section at the bottom of the page). In the **Adapter Card Properties**

section, use the dropdown selectors next to **Port-0** and **Port-1** to set the speed of both these ports to **Auto**, as shown below. Then click **Save Changes**.

The screenshot displays the Cisco IMC configuration page for Adapter Card MLOM. The page is divided into several sections:

- Adapter Card Properties:**
  - PCI-Slot: MLOM
  - Vendor: Cisco Systems Inc
  - Product Name: UCS VIC 1227
  - Product ID: UCSC-MLOM-CSC-02
  - Serial Number: 146J9L2
  - Version ID: V01
  - Hardware Revision: 3
  - Cisco IMC Management Enabled: no
  - Configuration Pending: no
  - ISCSI Boot Capable: True
  - CDN Capable: True
  - usNIC Capable: True
  - Description: [Text Field]
  - Enable FIP Mode:
  - Enable LLDP:
  - Enable VNTAG Mode:
  - Port-0: Auto (dropdown)
  - Port-1: Auto (dropdown)
- Firmware:**
  - Running Version: 4.1(3a)
  - Backup Version: 4.1(3a)
  - Startup Version: 4.1(3a)
  - Bootloader Version: 4.1(3a)
  - Status: Fwupdate never issued
- External Ethernet Interfaces:**
  - Port-0:**
    - MAC Address: E:31:63:2
    - Link State: Link Down
    - Encap: CE
    - Admin Speed: 10Gbps
    - Operating Speed: -
  - Port-1:**
    - MAC Address: E:31:63:2
    - Link State: Link Down
    - Encap: CE
    - Admin Speed: 10Gbps
    - Operating Speed: -

g) Click the **vNICs** tab and select **eth0** from the **vNICs** dropdown. Use the selectors and fields to set these values for **eth0**:

- **VLAN Mode: Trunk**
- **MTU: 1500**
- **Default VLAN: 99** (Please note that "99" is only an example. You should enter the default VLAN value you want your appliances and their connected uplink switch to use.)

**Tip** 1500 is the minimum maximum transmission unit (MTU) size. You can improve throughput on the 10Gbps ports by entering any higher value, up to a maximum of 9000.

- h) Click **Save Changes**. You will be prompted to reboot the host again. Click **Cancel** to continue instead of rebooting.
- i) Select **eth1** from the **vNICs** dropdown and set the values that you want your appliances and their connected uplink switch to use.
- j) When you are finished, click **Save Changes**. You will be prompted to reboot the host. This time, click **OK** to reboot the appliance.
- k) When the appliance is finished rebooting, log in to the Cisco IMC GUI again. Select **Networking > Adapter Card MLOM > General > vNICs**. Verify the accuracy of the vNIC MAC addresses and the MTU, VLAN and VLAN Mode parameters you set earlier.
- l) When you are finished: Click the **Host Power** menu at top right and select **Power Cycle**. Then click **OK**.



**Step 4** Reconfigure your switches to match the high-throughput settings on the appliance, as follows:

- a) Using a Secure Shell (SSH) client, log in to the switch to be configured and enter EXEC mode at the switch prompt.
- b) Configure the switch port.

On a Cisco Catalyst switch, enter the following commands. For example:

```
MySwitch#Config terminal
MySwitch(config)#interface tengigabitethernet 1/1/3
MySwitch(config-if)#switchport
MySwitch(config-if)#switchport mode trunk
MySwitch(config-if)#switchport trunk allowed vlan 99
MySwitch(config-if)#switchport voice vlan dot1p
MySwitch(config-if)#speed auto
MySwitch(config-if)#duplex full
MySwitch(config-if)#mtu 1500
MySwitch(config-if)#no shut
MySwitch(config-if)#end
MySwitch(config)#do copy running-config startup-config
```

On a Cisco Nexus switch, enter the following commands to disable Link Layer Discovery Protocol (LLDP) and priority flow control (PFC). For example:

```
N7K2# configure terminal
N7K2(config)# interface eth 3/4
N7K2(config-if)# no priority-flow-control mode auto
N7K2(config-if)# no lldp transmit
N7K2(config-if)# no lldp receive
```

Note that these commands are examples only. When configuring your appliance's NICs, use the same VLAN ID and MTU values you entered in Step 3 of this procedure. The values displayed for the link speed, duplex, and MTU parameters are the defaults for your switch. Enter new values for these parameters only if you have changed the defaults. You may, as with the appliance NICs, also set the MTU up to a maximum of 9000 for better throughput.

- c) Run the `show interface tengigabitethernet portID` command and verify that the port is connected, running, and has the correct MTU, duplex, and link-type settings in the command output. For example:

```
MySwitch#show interface tengigabitethernet 1/1/3
TenGigabitEthernet1/1/3 is up, line protocol is up (connected)
Hardware is Ten Gigabit Ethernet, address is XXXe.310.8000 (bia XXX.310.8000)
  MTU 1500 bytes, BW 10000000 Kbit/sec, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive not set
  Full-duplex, 10GB/s, link type is auto, media type is SFP-10Gbase-SR
```

- d) Run the `show run interface tengigabitethernet portID` command to configure the switch ports where the cables from the VIC 1227 ports are connected. For example:

```
MySwitch#show run interface tengigabitethernet 1/1/3
Building configuration...
Current configuration : 129 bytes
!
interface TenGigabitEthernet1/1/3
  switchport trunk allowed vlan 99
  switchport mode trunk
end

MySwitch#
```

- e) Run the `show run interface tengigabitethernet portID` command and verify from the command output that the port has the correct `voice vlan dot1p` setting. For example:

```
MySwitch#show run interface tengigabitEthernet 1/1/3
Building configuration...
Current configuration : 129 bytes
!
interface TenGigabitEthernet1/1/3
  switchport trunk allowed vlan 99
```

```

switchport mode trunk
switchport voice vlan dot1p
end

```

```
MySwitch#
```

- f) Run the `show mac address-table interface tengigabitethernet portID` command and verify the MAC address from the command output. For example:

```
MySwitch#show mac address-table interface tengigabitethernet 1/1/3
          Mac Address Table
-----
```

Vlan	Mac Address	Type	Ports
99	xxx.e.3161.1000	DYNAMIC	Tel1/1/3

Total Mac Addresses for this criterion: 1

```
MySwitch#
```

### What to do next

When this task is complete, do one of the following:

- If you need to reinstall Cisco DNA Center software before you configure your appliance, see [Reimage the Appliance](#).
- If you are ready to configure your appliance, proceed to [Appliance Configuration Overview](#).

## Reimage the Appliance

Situations may arise that require you to reimage your Cisco DNA Center appliance, such as recovering from a backup or changing your cluster link configuration. To do so, complete the following procedure.

- Step 1** Download the Cisco DNA Center ISO image and verify that it is a genuine Cisco image.  
See [Verify the Cisco DNA Center Image, on page 57](#).
- Step 2** Create a bootable USB drive that contains the Cisco DNA Center ISO image.  
See [Create a Bootable USB Flash Drive, on page 58](#).
- Step 3** Reinitialize the three virtual drives that are managed by your appliance's RAID controller:
- a) Log in to Cisco IMC and start a KVM session.
  - b) Power on or power cycle the appliance by choosing one of the following menu options:
    - **Power > Power On System**
    - **Power > Power Cycle System (cold boot)**

As your appliance reboots, a screen that lists every drive on the appliance (both physical and virtual) will appear.

```

ID  LUN  VENDOR      PRODUCT                REVISION      CAPACITY
--  ---  -
15  0     ATA         INTEL SSDSC2BB48      CS01          457862MB
   0     AVAGO      Virtual Drive         RAID1         456809MB
   1     AVAGO      Virtual Drive         RAID1         1830101MB
   2     AVAGO      Virtual Drive         RAID10        3660202MB

0 JBOD(s) found on the host adapter
0 JBOD(s) handled by BIOS

3 Virtual Drive(s) found on the host adapter.
3 Virtual Drive(s) handled by BIOS

Press <Ctrl><R> to Run MegaRAID Configuration Utility

```

- c) As soon as you see this screen, press **Ctrl + R** to run the MegaRAID Configuration Utility.

If you wait too long, this screen will disappear. To get back to this screen, choose **Power > Reset System (warm boot)** from the KVM menu to reboot your appliance.

- d) Select a drive's entry (ID: 0, 446.102 GB, for example) and then press **F2**.

```

Cisco 12G SAS Modular Raid BIOS Configuration Utility 5.15-0611
UD Mgmt PD Mgmt Ctrl Mgmt Properties
Virtual Drive Management
[-] Cisco 12G SAS Modular Raid(Bus 0x0d, Dev 0x00)
  [-] Drive Group: 0, RAID 1
    [-] Virtual Drives
      ID: 0, 446.102 GB
    [+ ] Drives
      [+ ] Available size: 0.000 KB
      Hot spare drives
  [-] Drive Group: 1, RAID 1
    [-] Virtual Drives
      ID: 1, 1.745 TB
    [+ ] Drives
      [+ ] Available size: 0.000 KB
      Hot spare drives
  [-] Spanned Drive Group: 0, RAID 10
    [-] Virtual Drives
      ID: 2, 3.490 TB
    [+ ] Drives
      [+ ] Available size: 0.000 KB
      Hot spare drives

Virtual Drive 0:
State: Optimal
RAID Level: 1
Hidden: No

Drive Group 0:
Virtual Drives: 1
Drives: 2
Free Cap.: 0.000 KB
Free Areas: 0

F1-Help F2-Operations F5-Refresh Ctrl-N-Next Page Ctrl-P-Prev Page F12-Ctrl

```

This opens the drive's **Advanced Properties** screen.

- e) In the resulting menu, choose **Initialization > Full Initialization** for the first virtual drive.  
 f) Repeat Steps 3b through 3e for the other virtual drives on your appliance, but choose **Fast Initialize**. (Only the first virtual drive requires full initialization. The second and third virtual drives don't require full initialization.)

#### Step 4 Reinstall Cisco DNA Center onto your appliance.

See [Install the Cisco DNA Center ISO Image, on page 60](#).

## Verify the Cisco DNA Center Image

Before deploying Cisco DNA Center, we strongly recommend that you verify that the image you downloaded is a genuine Cisco image.

### Before you begin

Obtain the location of the Cisco DNA Center image (through email or by contacting the Cisco support team).

- 
- Step 1** Download the Cisco DNA Center image (.iso, .bin, .zip) from the location specified by Cisco.
  - Step 2** Download the Cisco public key (cisco\_image\_verification\_key.pub) for signature verification from the location specified by Cisco.
  - Step 3** Download the secure hash algorithm (SHA512) checksum file for the image from the location specified by Cisco.
  - Step 4** Obtain the image's signature file (.sig) from Cisco support through email or by download from the secure Cisco website (if available).
  - Step 5** (Optional) Perform an SHA verification to determine whether the image is corrupted due to a partial download.

Depending on your operating system, enter one of the following commands:

- On a Linux system: **sha512sum image-filename**
- On a Mac system: **shasum -a 512 image-filename**

Microsoft Windows does not include a built-in checksum utility, but you can use the certutil tool:

```
certutil -hashfile <filename> sha256 | md5
```

For example:

```
certutil -hashfile D:\Customers\FINALIZE.BIN sha256
```

On Windows, you can also use the [Windows PowerShell](#) to generate the digest. For example:

```
PS C:\Users\Administrator> Get-FileHash -Path D:\Customers\FINALIZE.BIN
Algorithm Hash Path
SHA256 B84B6FFD898A370A605476AC7EC94429B445312A5EEDB96166370E99F2838CB5 D:\Customers\FINALIZE.BIN
```

Compare the command output to the SHA512 checksum file that you downloaded. If the command output does not match, download the image again and run the appropriate command a second time. If the output still does not match, contact Cisco support.

- Step 6** Verify that the image is genuine and from Cisco by verifying its signature:

```
openssl dgst -sha512 -verify cisco_image_verification_key.pub -signature signature-filename image-filename
```

**Note** This command works in both Mac and Linux environments. For Windows, you must download and install OpenSSL (available [here](#)) if you have not already done so.

If the image is genuine, running this command displays a `Verified OK` message. If this message fails to appear, do not install the image and contact Cisco support.

- Step 7** After confirming that you have downloaded a Cisco image, create a bootable USB drive that contains the Cisco DNA Center image. See [Create a Bootable USB Flash Drive](#).

## Create a Bootable USB Flash Drive

Complete one of the following procedures to create a bootable USB flash drive from which you can install the Cisco DNA Center ISO image.

Before you begin:

- Download and verify your copy of the Cisco DNA Center ISO image. See [Verify the Cisco DNA Center Image](#).
- Confirm that the USB flash drive you are using:
  - Is USB 3.0 or later.
  - Has a capacity of at least 64 GB.
  - Is unencrypted.




---

**Note** Do not use the Rufus utility to burn the Cisco DNA Center ISO image. Use only Etcher, the Linux CLI, or the Mac CLI.

---

## Using Etcher

**Step 1** Download and install Etcher (Version 1.3.1 or later), an open-source freeware utility that allows you to create a bootable USB drive on your laptop or desktop.

Linux, macOS, and Windows versions of Etcher are currently available. You can download a copy at <https://www.balena.io/etcher/>.

**Note** Use only the Windows version of Etcher on machines running Windows 10, as there are known compatibility issues with older versions of Windows.

**Step 2** From the machine on which you installed Etcher, connect a USB drive and then start Etcher.


**Step 3** In the top-right corner of the window, click  and verify that the following Etcher settings are set:

- Auto-unmount on success
- Validate write on success

**Step 4** Click **Back** to return to the main Etcher window.

**Step 5** Click **Select Image**.

**Step 6** Navigate to the Cisco DNA Center ISO image you downloaded previously, select it, and then click **Open**.

The name of the USB drive you connected should be listed under the drive icon (). If it is not:

- a. Click **Select drive**.
- b. Click the radio button for the correct USB drive, and then click **Continue**.

**Step 7** Click **Flash!** to copy the ISO image to the USB drive.



Etcher configures the USB drive as a bootable drive with the Cisco DNA Center ISO image installed.

## Using the Linux CLI

**Step 1** Verify that your USB flash drive is recognized by your machine:

- a) Insert a flash drive into your machine's USB port.
- b) Open a Linux shell and run the following command: **lsblk**

The command lists the disk partitions that are currently configured on your machine, as illustrated in the following example:

```
$ lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
sda 8:0 0 446.1G 0 disk
├─sda1 8:1 0 1M 0 part
├─sda2 8:2 0 28.6G 0 part /
├─sda3 8:3 0 28.6G 0 part /install2
├─sda4 8:4 0 9.5G 0 part /var
├─sda5 8:5 0 30.5G 0 part [SWAP]
├─sda6 8:6 0 348.8G 0 part /data
sdb 8:16 0 1.8T 0 disk
├─sdb1 8:17 0 426.1G 0 part /data/maglev/srv/fusion
├─sdb2 8:18 0 1.3T 0 part /data/maglev/srv/maglev-system
sdc 8:32 0 3.5T 0 disk
├─sdc1 8:33 0 3.5T 0 part /data/maglev/srv/ndp
sdd 8:48 1 28.7G 0 disk
├─sdd1 8:49 1 12G 0 part
```

- c) Confirm that an `sdd` partition (which indicates the presence of a USB flash drive) is listed.

**Step 2** Burn the Cisco DNA Center ISO image you downloaded previously onto your USB flash drive: **time sudo dd if=/data/tmp/ISO-image-filename of=/dev/flash-drive-partition bs=4M && sync status=progress**

For example, to create a bootable USB drive using an ISO image named `CDNAC-SW-1.330.iso`, you would run the following command: **time sudo dd if=/data/tmp/CDNAC-SW-1.330.iso of=/dev/sdd bs=4M && sync status=progress**

## Using the Mac CLI

**Step 1** Determine the disk partition associated with your USB flash drive:

- a) Open a Terminal window and run the following command: **diskutil list**

The command lists the disk partitions that are currently configured on your machine.

- b) Insert a flash drive into your machine's USB port and run the **diskutil list** command a second time.

The partition that was not listed the first time you ran this command corresponds to your flash drive. For example, let's assume that your flash drive's partition is `/dev/disk2`.

**Step 2** Unmount the flash drive's partition: **diskutil unmountDisk flash-drive-partition**

Continuing our example, you would enter **diskutil unmountDisk /dev/disk2**

**Step 3** Using the Cisco DNA Center ISO image you downloaded previously, create a disk image: **hdiutil convert -format UDRW -o Cisco-DNA-Center-version ISO-image-filename**

Continuing our example, let's assume that you are working with a Cisco DNA Center ISO image named `CDNAC-SW-1.330.iso`. You would run the following command, which creates a macOS disk image named `CDNAC-1.330.dmg`:  
**hdiutil convert -format UDRW -o CDNAC-1.330 CDNAC-SW-1.330.iso**

**Important** Ensure that the ISO image does not reside on a Box partition.

**Step 4** Create a bootable USB drive: **sudo dd if=macOS-disk-image-filename of=flash-drive-partition bs=1m status=progress**  
 Continuing our example, you would run the following command: **sudo dd if=CDNAC-1.330.dmg of=/dev/disk2 bs=1m status=progress**

The ISO image is about 18 GB in size, so this can take around an hour to complete.

## Install the Cisco DNA Center ISO Image

Complete the following procedure to install the Cisco DNA Center ISO image onto your appliance.

### Before you begin

Create the bootable USB drive from which you will install the Cisco DNA Center ISO image. See [Create a Bootable USB Flash Drive](#).

**Step 1** Connect the bootable USB drive with the Cisco DNA Center ISO image to the appliance.

**Step 2** Log in to Cisco IMC and start a KVM session.

**Step 3** Power on or power cycle the appliance:

- Choose **Power > Power On System** if the appliance is not currently running.
- Choose **Power > Power Cycle System (cold boot)** if the appliance is already running.

**Step 4** In the resulting pop-up window, click **Yes** to acknowledge that you are about to execute a server control action.

**Step 5** When the Cisco logo appears, either press the **F6** key or choose **Macros > User Defined Macros > F6** from the KVM menu.

The boot device selection menu appears.

**Step 6** Select your USB drive and then press **Enter**.

**Step 7** In the **GNU GRUB** bootloader window, choose **Cisco DNA Center Installer** and then press **Enter**.

**Note** The bootloader automatically boots the Cisco DNA Center Installer instead if you do not make a selection within 30 seconds.

The installer reboots and opens the wizard's welcome screen. Depending on whether you are going to configure a primary or secondary cluster node, proceed to Step 4 in either [Configure the Primary Node](#) or [Configure a Secondary Node](#).



## CHAPTER 5

# Configure the Appliance

- [Appliance Configuration Overview, on page 61](#)
- [Configure the Primary Node, on page 61](#)
- [Configure a Secondary Node, on page 75](#)
- [Upgrade to the Latest Cisco DNA Center Release, on page 88](#)

## Appliance Configuration Overview

You can deploy the appliance in your network in one of the following two modes:

- **Standalone:** As a single node offering all the functions. This option is usually preferred for initial or test deployments and in smaller network environments.
- **Cluster:** As a node that belongs to a three-node cluster. In this mode, all the services and data are shared among the hosts. This is the preferred option for large deployments.

If you choose the Standalone mode for your initial deployment, you can add more appliances later to form a cluster. When configuring the standalone host, ensure that it is set up as the first, or primary, node in the cluster.

If you choose the Cluster mode for your initial deployment, be sure to finish configuring the primary node before configuring the secondary nodes.

To proceed, complete the following tasks:

1. Launch the Maglev Configuration wizard from Cisco IMC and configure the primary node in your cluster. See [Configure the Primary Node](#).
2. If you have installed three appliances and want to add the second and third nodes to your cluster, see [Configure a Secondary Node](#).

## Configure the Primary Node

Perform the steps in this procedure to configure the first installed appliance as the primary node. You must always configure the first appliance as the primary node, whether it will operate standalone or as part of a cluster.

If you are configuring the installed appliance as a secondary node for an existing cluster that already has a primary node, follow the steps described in [Configure a Secondary Node](#) instead.



---

**Note** Ensure that all of the IP addresses you enter while completing this procedure are valid IPv4 addresses with valid IPv4 netmasks. Also make sure that the addresses and their corresponding subnets do not overlap. Service communication issues can result if they do.

---



---

**Important** Before you configure the appliances in a three-node cluster, ensure that you have logged out of those appliances. Otherwise, the Quick Start workflow (which you complete to discover your network's devices and enable telemetry) will not start after you have configured your cluster's appliances and log in to Cisco DNA Center for the first time.

---

### Before you begin

Ensure that you:

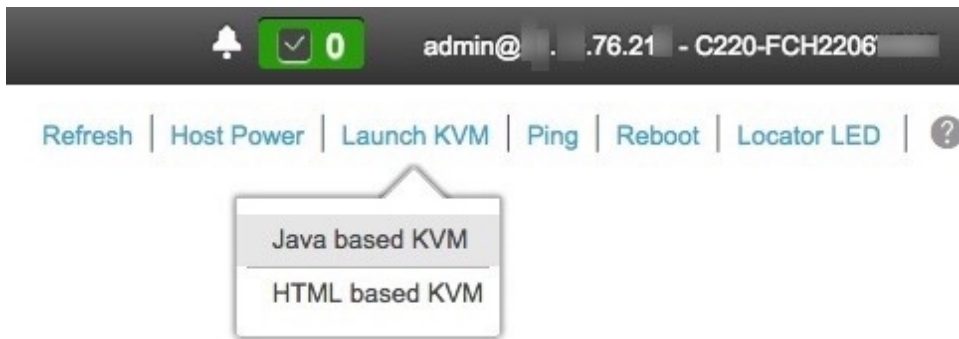
- Collected all of the information specified in [Required IP Addresses and Subnets](#) and [Required Configuration Information](#).
- Installed the first appliance, as described in [Appliance Installation Workflow](#).
- Configured Cisco IMC browser access on the primary node, as described in [Enable Browser Access to Cisco Integrated Management Controller](#).
- Checked that the primary node appliance's ports, and the switches they use, are properly configured, as described in [Execute Preconfiguration Checks](#).
- Confirmed that you are using a compatible browser. For a list of compatible browsers, see the [Release Notes](#) document for the version of Cisco DNA Center you are installing.
- Enabled ICMP on the firewall between Cisco DNA Center and both the default gateway and the DNS server you specify in the following procedure. The Maglev Configuration wizard uses ping to verify the gateway and DNS server you specify. This ping might get blocked if a firewall is in place and ICMP is not enabled on that firewall. When this happens, you will not be able to complete the wizard.

---

### Step 1

Point your browser to the Cisco IMC IP address you set during the Cisco IMC GUI configuration you performed, and log in to the Cisco IMC GUI as the Cisco IMC user (see [Enable Browser Access to Cisco Integrated Management Controller](#)).

After successful login, the appliance displays the **Cisco Integrated Management Controller Chassis Summary** window, with a hyperlinked menu at the top of the window, as shown below.



**Step 2** From the hyperlinked menu, choose **Launch KVM** and then select either **Java based KVM** or **HTML based KVM**. If you select **Java-based KVM**, you will need to launch the Java startup file from your browser or file manager in order to view the KVM console in its own window. If you select **HMTL-based KVM**, it launches the KVM console in a separate window or tab automatically.

Irrespective of the KVM type you choose, use the KVM console to monitor the progress of the configuration and respond to the Maglev Configuration wizard prompts.

**Step 3** With the KVM displayed, reboot the appliance by making one of the following selections:

- In the main Cisco IMC GUI browser window: Choose **Host Power > Power Cycle**, and switch to the KVM console to continue.
- In the KVM console: Choose **Power > Power Cycle System (cold boot)**.

If you are asked to confirm your choice to reboot the appliance, click **OK**.

After displaying reboot messages, the KVM console displays the Maglev Configuration wizard welcome screen.



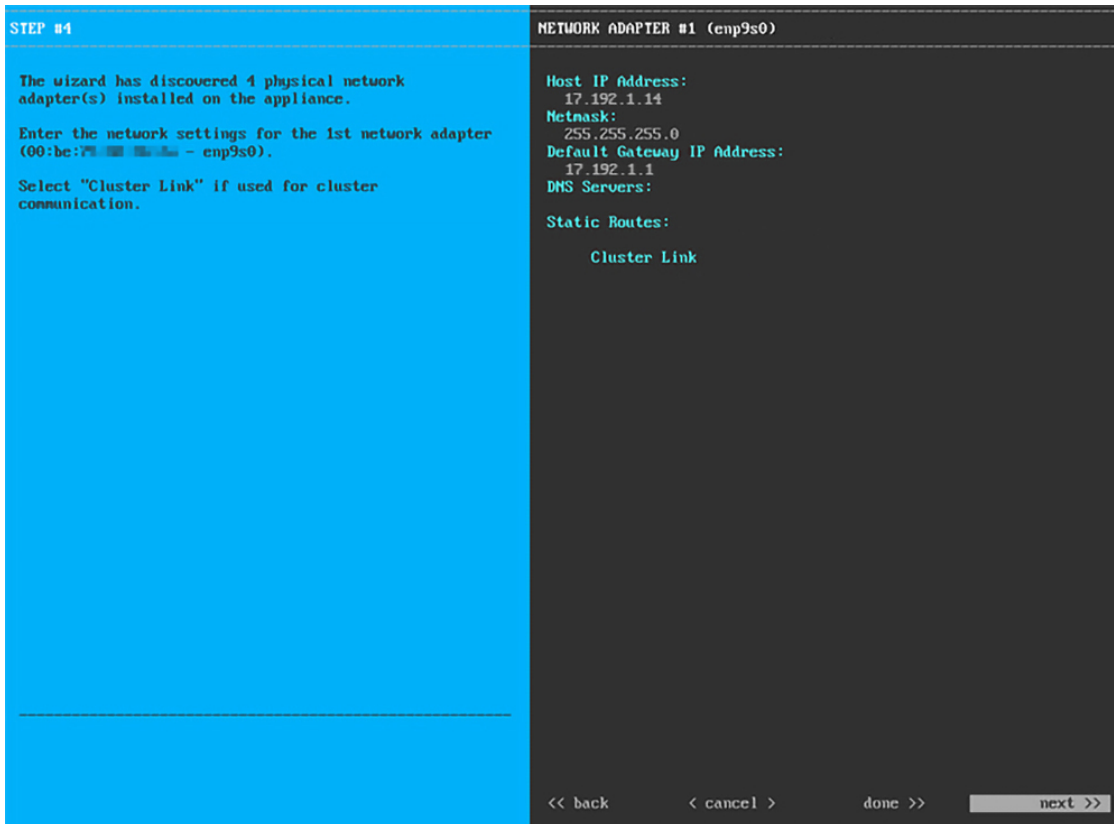
**Step 4** Click **Start a Cisco DNA Center Cluster** to begin configuring the primary node.

The wizard discovers all of the ports on the appliance and presents them to you one by one, in separate screens, in the following order:

- a. 10-Gbps Enterprise port (Port 1, enp9s0, Network Adapter #1)
- b. 10-Gbps Cluster port (Port 2, enp10s0, Network Adapter #2)
- c. 1-Gbps Cisco DNA Center GUI port (1, enp1s0f0, Network Adapter #3)
- d. 1-Gbps Cloud port (2, enp1s0f1, Network Adapter #4)

**Note** If the wizard fails to display either or both of the Enterprise and Cluster ports during the course of configuration, these ports may be non-functional or disabled. These two ports are required for Cisco DNA Center functionality. If you discover that they are non-functional, choose **cancel** to exit the configuration immediately. Be sure you have completed all of the steps provided in [Execute Preconfiguration Checks](#) before resuming configuration or contacting the Cisco Technical Assistance Center (TAC).

**Step 5** The wizard discovers the 10-Gbps Enterprise port (Port 1, enp9s0) first, and presents it as **NETWORK ADAPTER #1**. As explained in [Interface Cable Connections](#), this port is required to link the appliance to the enterprise network. Apply the host IP address, netmask, and other values that are appropriate for this purpose, (see [Required IP Addresses and Subnets](#) and [Required Configuration Information](#) for the values to enter).



Enter the configuration values for **NETWORK ADAPTER #1**, as shown in the table below.

**Table 16: Primary Node Entries for Network Adapter #1: 10-Gbps Enterprise Port (enp9s0)**

<b>Host IP address</b>	Enter the IP address for the 10-Gbps Enterprise port. This is required.
<b>Netmask</b>	Enter the netmask for the port's IP address. This is required.
<b>Default Gateway IP address</b>	Enter a default gateway IP address to use for the port. <b>Important</b> Ensure that you enter a default gateway IP address for at least one of your appliance's interfaces. Otherwise, you will not be able to complete the configuration wizard.
<b>DNS Servers</b>	Enter the IP address of the preferred DNS server. If you are entering multiple DNS servers, separate the IP addresses in the list with spaces. <b>Important</b> For each appliance in your cluster, configure a maximum of three DNS servers. Problems can occur if you configure more than three DNS servers for an appliance.
<b>Static Routes</b>	Enter one or more static routes in the following format, separated by spaces: <code>&lt;network&gt;/&lt;netmask&gt;/&lt;gateway&gt;</code> . This is usually required on the Cisco DNA Center GUI port only.
<b>Cluster Link</b>	Leave this field blank. It is required on the Cluster port only.

After you provide the necessary information, click **next>>** to proceed. Correct validation errors, if any, as you did in previous screens. The wizard validates and applies your network adapter configurations.

### Step 6

After successful validation of the Enterprise port values you entered, the wizard presents the 10-Gbps Cluster port (Port 2, enp10s0) as **NETWORK ADAPTER #2**. As explained in [Interface Cable Connections](#), this port is used to link the appliance to the cluster, so apply the host IP address, netmask, and other values that are appropriate for this purpose (see [Required IP Addresses and Subnets](#) and [Required Configuration Information](#) for the values to enter).

Enter the configuration values for **NETWORK ADAPTER #2**, as shown in the table below.

**Table 17: Primary Node Entries for Network Adapter #2: 10-Gbps Cluster Port (enp10s0)**

<b>Host IP address</b>	Enter the IP address for the Cluster port. This is required. Note that you cannot change the address of the Cluster port later.
<b>Netmask</b>	Enter the netmask for the port's IP address. This is required.
<b>Default Gateway IP address</b>	Enter a default gateway IP address to use for the port.  <b>Important</b> Ensure that you enter a default gateway IP address for at least one of your appliance's interfaces. Otherwise, you will not be able to complete the configuration wizard.

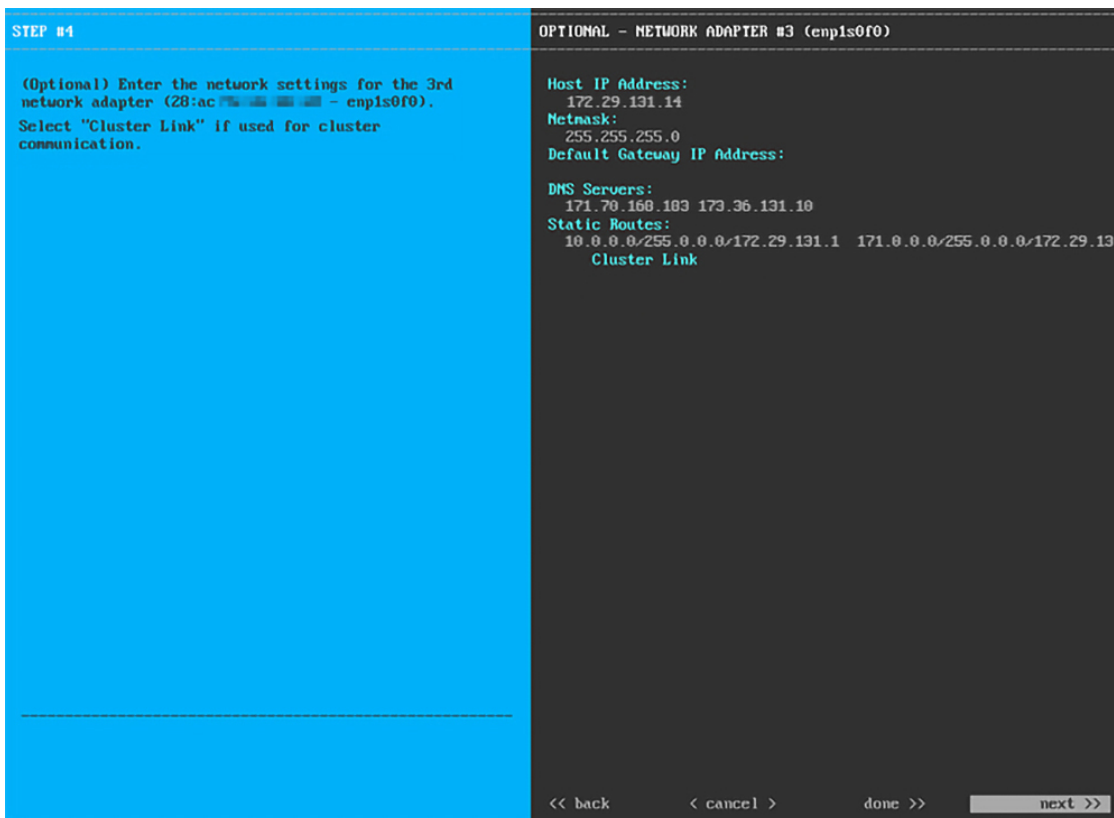


<b>DNS Servers</b>	Enter the IP address of the preferred DNS server. If you are entering multiple DNS servers, separate the IP addresses in the list with spaces.  <b>Important</b> For each appliance in your cluster, configure a maximum of three DNS servers. Problems can occur if you configure more than three DNS servers for an appliance.
<b>Static Routes</b>	Enter one or more static routes in the following format, separated by spaces: <i>&lt;network&gt;/&lt;netmask&gt;/&lt;gateway&gt;</i> . This is usually required on the GUI port only.
<b>Cluster Link</b>	Check the check box to indicate that this port will be the link to a cluster. This is required on the Cluster port only.

After you finish entering the configuration values, click **next>>** to proceed. The wizard validates the values you entered and issues an error message if any are incorrect. If you receive an error message, check that the value you entered is correct, then reenter it. If needed, click **<<back** to reenter it.

**Step 7**

After successful validation of the Cluster port values you entered, the wizard presents the 1-Gbps Cisco DNA Center GUI port (1, enp1s0f0) as **NETWORK ADAPTER #3**. As explained in [Interface Cable Connections](#), this port is used to access the Cisco DNA Center GUI from your management network. Apply the host IP address, netmask, and other values that are appropriate for this purpose (see [Required IP Addresses and Subnets](#) and [Required Configuration Information](#) for the values to enter).



Enter the configuration values for **NETWORK ADAPTER #3**, as shown in the table below.

Table 18: Primary Node Entries for Network Adapter #3: 1-Gbps GUI Port (enp1s0f0)

<b>Host IP address</b>	Enter the IP address for the 1-Gbps GUI Port. This is required only if you are using the GUI Port to access the Cisco DNA Center GUI from your management network; otherwise, you can leave it blank.
<b>Netmask</b>	Enter the netmask for the port's IP address. This is required if you enter an IP address.
<b>Default Gateway IP address</b>	Enter a default gateway IP address to use for the port. <b>Important</b> Ensure that you enter a default gateway IP address for at least one of your appliance's interfaces. Otherwise, you will not be able to complete the configuration wizard.
<b>DNS Servers</b>	Enter the IP address of the preferred DNS server. If you are entering multiple DNS servers, separate the IP addresses in the list with spaces. <b>Important</b> <ul style="list-style-type: none"> <li>• For NTP, ensure port 123 (UDP) is open between Cisco DNA Center and your NTP server.</li> <li>• For each appliance in your cluster, configure a maximum of three DNS servers. Problems can occur if you configure more than three DNS servers for an appliance.</li> </ul>
<b>Static Routes</b>	Enter one or more static routes in the following format, separated by spaces: <network>/<netmask>/<gateway>.
<b>Cluster Link</b>	Leave this field blank. It is required on the Cluster port only.

After you provide the necessary information, click **next>>** to proceed. Correct any validation errors as you did in previous screens.

**Step 8**

After successful validation of the Cisco DNA Center GUI port values you entered, the wizard presents the 1-Gbps Cloud port (2, enp1s0f1) as **NETWORK ADAPTER #4**. As explained in [Interface Cable Connections](#), this is an optional port used to link the appliance to the Internet when you cannot do so through the 10-Gbps Enterprise port (Port 1, enp9s0). Apply the host IP address, netmask, and other values that are appropriate for this purpose (see [Required IP Addresses and Subnets](#) and [Required Configuration Information](#) for the values to enter).



Enter the configuration values for **NETWORK ADAPTER #4**, as shown in the table below.

**Table 19: Primary Node Entries for Network Adapter #4: 1-Gbps Cloud Port (enp1s0f1)**

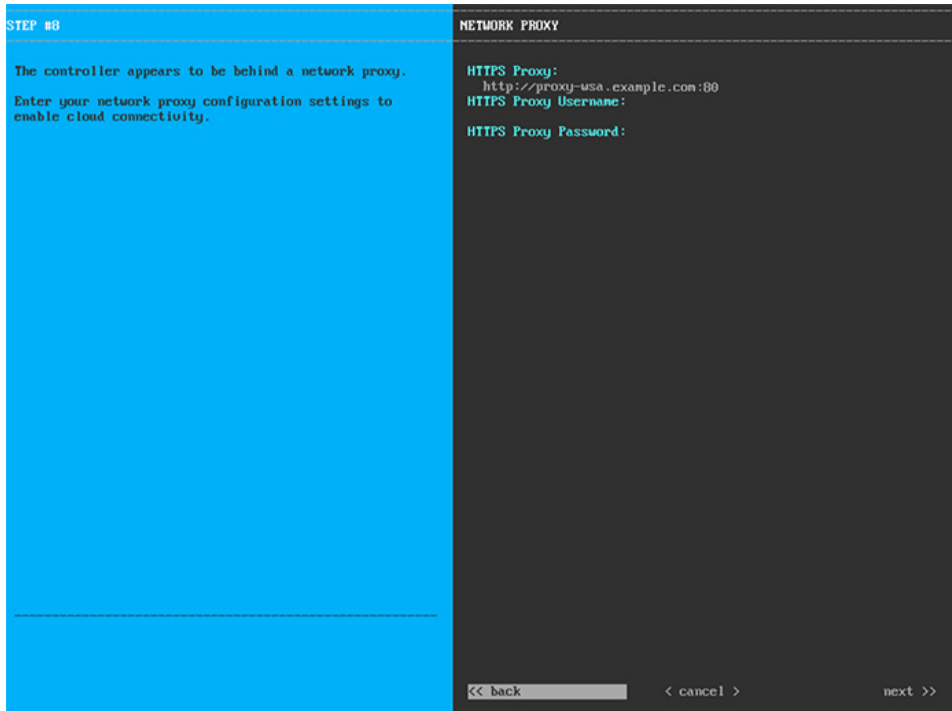
<b>Host IP address</b>	Enter the IP address for the Cloud port. This is required only if you are using the Cloud port for internet connection; otherwise, you can leave it blank.
<b>Netmask</b>	Enter the netmask for the port's IP address. This is required if you enter an IP address.
<b>Default Gateway IP address</b>	Enter a default gateway IP address to use for the Cloud port.  <b>Important</b> Ensure that you enter a default gateway IP address for at least one of your appliance's interfaces. Otherwise, you will not be able to complete the configuration wizard.
<b>DNS Servers</b>	Enter the IP address of the preferred DNS server. If you are entering multiple DNS servers, separate the IP addresses in the list with spaces.  <b>Important</b> For each appliance in your cluster, configure a maximum of three DNS servers. Problems can occur if you configure more than three DNS servers for an appliance.
<b>Static Routes</b>	Enter one or more static routes in the following format, separated by spaces: <code>&lt;network&gt;/&lt;netmask&gt;/&lt;gateway&gt;</code> . This is usually required on the Cisco DNA Center GUI port only.

<b>Cluster Link</b>	Leave this field blank. It is required on the Cluster port only.
---------------------	--

After you provide the necessary information, click **next>>** to proceed. Correct any validation errors as you did in previous screens.

**Step 9**

After the network adapter configuration is complete, the wizard prompts you to enter configuration values for the **NETWORK PROXY** you are using, as shown below.



Enter the configuration values for the **NETWORK PROXY**, as shown in the table below.

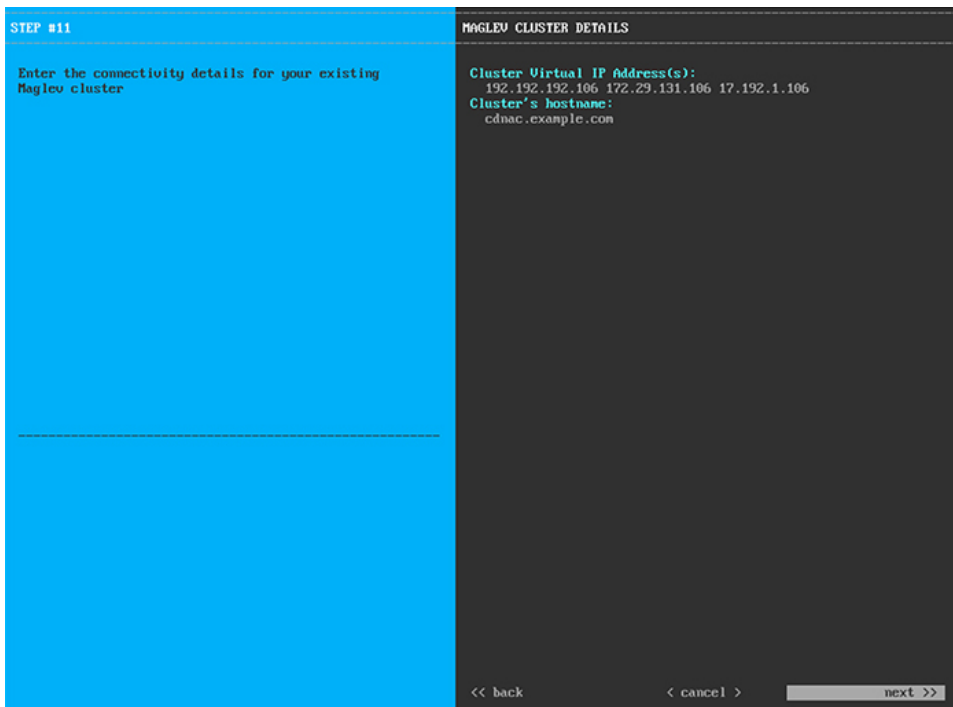
**Table 20: Primary Node Entries for Network Proxy**

<b>HTTPS Proxy</b>	Enter the URL or host name of an HTTPS network proxy used to access the Internet.  <b>Note</b> Connection from Cisco DNA Center to the HTTPS proxy is supported only via HTTP in this release.
<b>HTTPS Proxy Username</b>	Enter the user name used to access the network proxy. If no proxy login is required, leave this field blank.
<b>HTTPS Proxy Password</b>	Enter the password used to access the network proxy. If no proxy login is required, leave this field blank.

After you provide the necessary information, click **next>>** to proceed. Correct validation errors, if any, as you did in previous screens.

**Step 10**

After network proxy configuration completes, the wizard prompts you to enter virtual IP addresses for the primary node, in **MAGLEV CLUSTER DETAILS**, as shown below.



Enter a space-separated list of the virtual IP addresses used for traffic between the cluster and your network. This is required for both three-node clusters and single-node clusters that will be converted into a three-node cluster in the future. If you have a single-node cluster setup and plan to stick with it, skip this step and proceed to Step 11.

**Important** You must enter one virtual IP address for each configured network interface. You will not be able to complete the wizard unless you do so. These addresses are tied to the cluster link's status, which must be in the **UP** state.

You also have the option to specify the fully qualified domain name (FQDN) for your cluster. Cisco DNA Center uses this domain name to do the following:

- It uses this hostname to access your cluster's web interface and the Representational State Transfer (REST) APIs used by devices in the enterprise network that Cisco DNA Center manages.
- In the Subject Alternative Name (SAN) field of Cisco DNA Center certificates, it uses the FQDN to define the Plug and Play server that should be used for device provisioning.

After you provide the necessary information, click **next>>** to proceed. Correct validation errors, if any, as you did in previous screens.

**Step 11** After you have entered the virtual IP addresses, the wizard prompts you to enter **USER ACCOUNT SETTINGS** values, as shown below.

**STEP #13**

Specify a new password for the 'maglev' Linux user, and specify a passphrase of the 'admin' UI user.

\* Indicates a mandatory field

Password generation is optional, but recommended.

User is advised to append personal password with generated password for recommended security

Caution: Store generated password for future log ins

---

**USER ACCOUNT SETTINGS**

Linux Password: \*

Re-enter Linux Password: \*

Password Generation Seed:

< Generate Password >

Auto Generated Password:

< Use Generated Password >

Administrator Passphrase: \*

Re-enter Administrator Passphrase: \*

<< back      < cancel >      next >>

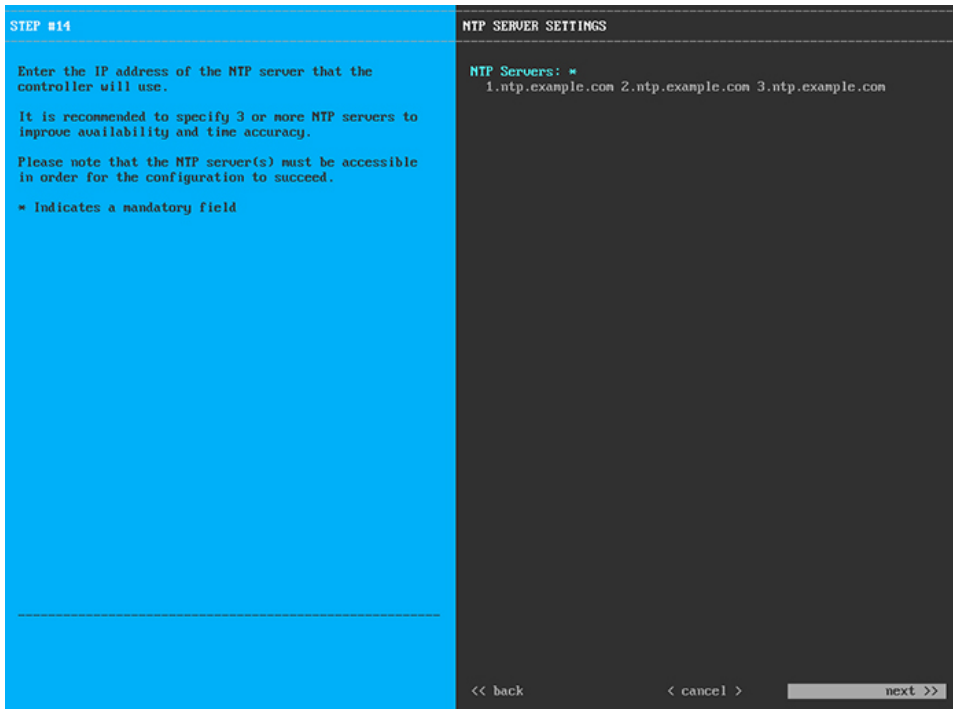
Enter the values for **USER ACCOUNT SETTINGS**, as shown in the table below.

**Table 21: Primary Node Entries for User Account Settings**

<b>Linux Password</b>	Enter a Linux password for the maglev user.
<b>Re-enter Linux Password</b>	Confirm the Linux password by entering it a second time.
<b>Password Generation Seed</b>	If you do not want to create the Linux password yourself, enter a seed phrase in this field and then press < <b>Generate Password</b> > to generate the password.
<b>Auto Generated Password</b>	(Optional) The seed phrase appears as part of a random and secure password. If desired, you can either use this password "as is", or you can further edit this auto-generated password.  Press < <b>Use Generated Password</b> > to save the password.
<b>Administrator Passphrase</b>	Enter a password for the default admin superuser, used to log in to Cisco DNA Center for the first time.
<b>Re-enter Administrator Passphrase</b>	Confirm the administrator passphrase by entering it a second time.

After you provide the necessary information, click **next>>** to proceed. Correct validation errors, if any, as you did in previous screens.

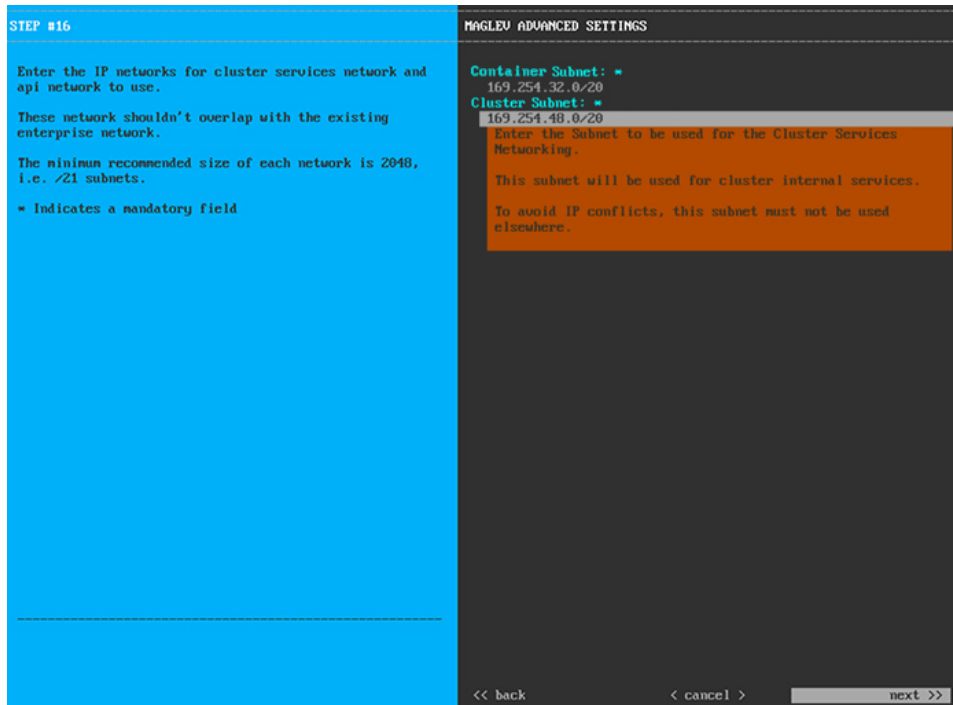
**Step 12** After you have entered the user account details, the wizard prompts you to enter **NTP SERVER SETTINGS** values, as shown below.



Enter one or more NTP server addresses or hostnames, separated by spaces. At least one NTP address or hostname is required. For a production deployment, we recommend that you configure a minimum of three NTP servers.

After you provide the necessary information, click **next>>** to proceed. Correct validation errors, if any, as you did in previous screens. The wizard validates and applies your NTP server configuration.

**Step 13** After you have specified the appropriate NTP servers, the wizard prompts you to enter **MAGLEV ADVANCED SETTINGS** values, as shown below.



Enter the configuration values for **MAGLEV ADVANCED SETTINGS**, as shown in the table below.

**Table 22: Primary Node Entries for Maglev Advanced Settings**

<b>Container Subnet</b>	A dedicated, non-routed IP subnet that Cisco DNA Center uses to manage internal services. By default, this is already set to <b>169.254.32.0/20</b> , and we recommend that you use this subnet. If you choose to enter another subnet, ensure that it does not conflict with or overlap any other subnet used by the Cisco DNA Center internal network or an external network. For more information, see the Container Subnet description in <a href="#">Required IP Addresses and Subnets, on page 17</a> .
<b>Cluster Subnet</b>	A dedicated, non-routed IP subnet that Cisco DNA Center uses to manage internal cluster services. By default, this is already set to <b>169.254.48.0/20</b> , and we recommend that you use this subnet. If you choose to enter another subnet, ensure that it does not conflict with or overlap any other subnet used by the Cisco DNA Center internal network or an external network. For more information, see the Cluster Subnet description in <a href="#">Required IP Addresses and Subnets, on page 17</a> .

When you are finished, click **next>>** to proceed. Correct validation errors, if any, as you did in previous screens.

**Step 14** After you have entered the Maglev advanced settings, a final message appears, stating that the wizard is ready to apply the configuration (as shown below).



```
The wizard is now ready to apply the configuration on the controller.
Use the [back] button below to verify/modify controller settings.
Use the [cancel] button to discard your changes and exit the wizard.
Use the [proceed] button to save your changes and proceed with applying them on the controller.

<< back                < cancel >                proceed >>
```

Click **proceed>>** to complete the configuration wizard.

The host will reboot automatically and display messages on the KVM console as it applies your settings and brings up services. This process can take several hours. You can monitor its progress via the KVM console.

At the end of the configuration process, the appliance power cycles again, then displays a **CONFIGURATION SUCCEEDED!** message.

---

### What to do next

- If you are deploying this appliance in standalone mode only, perform the first-time setup: [First-Time Setup Workflow](#).
- If you are deploying this appliance as the primary node in a cluster, configure the second and third installed appliances in the cluster: [Configure a Secondary Node](#).

## Configure a Secondary Node

Perform the steps in this procedure to configure the second and third appliances in the cluster.



---

### Important

In order to build a three-node cluster, the same version of the **System** package must be installed on your three Cisco DNA Center appliances. Otherwise, unexpected behavior and possible downtime can occur.

---



**Note** Ensure that all of the IP addresses you enter while completing this procedure are valid IPv4 addresses with valid IPv4 netmasks. Also make sure that the addresses and their corresponding subnets do not overlap. Service communication issues can result if they do.



**Important** Before you configure the appliances in a three-node cluster, ensure that you have logged out of those appliances. Otherwise, the Quick Start workflow (which you complete to discover your network's devices and enable telemetry) will not start after you have configured your cluster's appliances and log in to Cisco DNA Center for the first time.

When joining each new secondary node to the cluster, you must specify the first host in the cluster as the primary node. Note the following when joining secondary nodes to a cluster:

- Be sure to join only a single node to the cluster at a time. Do not attempt to add multiple nodes at the same time, because this results in unpredictable behavior.
- Before adding a new node to the cluster, be sure that all installed packages are deployed on the primary node. You can check this by using Secure Shell to log in to the primary node's Cisco DNA Center Management port as the Linux User (maglev) and then running the command `maglev package status`. All installed packages should appear in the command output as `DEPLOYED`. In the following example, a few packages were not installed, such as the `application-policy` and `sd-access` packages. They are the only packages whose status is `NOT_DEPLOYED`. Your package status should look similar to this before configuring a secondary node.

```
maglev-1 [main - https://kong-frontend.maglev-system.svc.cluster.local:443]
NAME                               DISPLAY_NAME                               DEPLOYED   AVAILABLE   STATUS           PROGRESS
-----
access-control-application          Access Control Application                  -           2.1.369.60050 NOT_DEPLOYED
ai-network-analytics                AI Network Analytics                       -           2.6.10.494   NOT_DEPLOYED
app-hosting                         Application Hosting                         -           1.6.6.2201241723 NOT_DEPLOYED
application-policy                  Application Policy                           -           2.1.369.170033 NOT_DEPLOYED
application-registry                Application Registry                         -           2.1.369.170033 NOT_DEPLOYED
application-visibility-service      Application Visibility Service              -           2.1.369.170033 NOT_DEPLOYED
assurance                           Assurance - Base                            2.2.2.485   -             DEPLOYED
automation-core                    NCP - Services                            2.1.368.60015 2.1.369.60050 DEPLOYED
base-provision-core                 Automation - Base                           2.1.368.60015 2.1.369.60050 DEPLOYED
cloud-connectivity-contextual-content Cloud Connectivity - Contextual Content    1.3.1.364    -             DEPLOYED
cloud-connectivity-data-hub         Cloud Connectivity - Data Hub              1.6.0.380   -             DEPLOYED
cloud-connectivity-tethering        Cloud Connectivity - Tethering              2.12.1.2    -             DEPLOYED
cloud-provision-core                Cloud Device Provisioning Application      -           2.1.369.60050 NOT_DEPLOYED
command-runner                      Command Runner                             2.1.368.60015 2.1.369.60050 DEPLOYED
device-onboarding                  Device Onboarding                          2.1.368.60015 2.1.369.60050 DEPLOYED
disaster-recovery                  Disaster Recovery                           -           2.1.367.360196 NOT_DEPLOYED
dna-core-apps                       Network Experience Platform - Core         2.1.368.60015 2.1.369.60050 DEPLOYED
dnac-platform                       Cisco DNA Center Platform                  1.5.1.180   1.5.1.182   DEPLOYED
dnac-search                         Cisco DNA Center Global Search             1.5.0.466   -             DEPLOYED
endpoint-analytics                  AI Endpoint Analytics                      -           1.4.375     NOT_DEPLOYED
group-based-policy-analytics        Group-Based Policy Analytics               -           2.2.1.401   NOT_DEPLOYED
icap-automation                    Automation - Intelligent Capture           -           2.1.369.60050 NOT_DEPLOYED
image-management                    Image Management                           2.1.368.60015 2.1.369.60050 DEPLOYED
machine-reasoning                  Machine Reasoning                           2.1.368.210017 2.1.369.210024 DEPLOYED
ncp-system                          NCP - Base                                2.1.368.60015 2.1.369.60050 DEPLOYED
ndp-base-analytics                  Network Data Platform - Base Analytics     1.6.1028    1.6.1031    DEPLOYED
ndp-platform                        Network Data Platform - Core               1.6.596     -             DEPLOYED
ndp-ui                              Network Data Platform - Manager            1.6.543     -             DEPLOYED
network-visibility                  Network Controller Platform                 2.1.368.60015 2.1.369.60050 DEPLOYED
path-trace                          Path Trace                                 2.1.368.60015 2.1.369.60050 DEPLOYED
platform-ui                         Cisco DNA Center UI                        1.6.2.446   1.6.2.448   DEPLOYED
rbac-extensions                     RBAC Extensions                           2.1.368.1910001 2.1.369.1910003 DEPLOYED
rogue-management                    Rogue and aWIPS                             -           2.2.0.51    NOT_DEPLOYED
sd-access                           SD Access                                  2.1.369.60050 2.1.369.60050 NOT_DEPLOYED
sensor-assurance                    Assurance - Sensor                          -           2.2.2.484   NOT_DEPLOYED
sensor-automation                  Automation - Sensor                         2.1.369.60050 2.1.369.60050 NOT_DEPLOYED
ssa                                 Stealthwatch Security Analytics            2.1.368.1091226 2.1.369.1091317 DEPLOYED
system                              System                                      1.6.594     -             DEPLOYED
system-commons                      System Commons                             2.1.368.60015 2.1.369.60050 DEPLOYED
umbrella                            Cisco Umbrella                             -           2.1.368.592066 NOT_DEPLOYED
wide-area-bonjour                   Wide Area Bonjour                          -           2.4.368.75006 NOT_DEPLOYED
```

[wed Nov 30 15:45:08 UTC] maglev@192.0.2.1 (maglev-master-192.0.2.1) ~

- Expect some service downtime during the cluster attachment process for each secondary node. Services will need to be redistributed across the nodes and the cluster will be down for periods of time during that process.

## Before you begin

Ensure that you:

- Configured the first appliance in the cluster, following the steps in [Configure the Primary Node](#).
- Collected all of the information specified in [Required IP Addresses and Subnets](#) and [Required Configuration Information](#).
- Installed the second and third appliances, as described in [Appliance Installation Workflow](#).
- Have done the following:
  1. Ran the **maglev package status** command on the first appliance.  
You can also access this information from the Cisco DNA Center GUI by clicking the **Help** icon (🔗) and choosing **About > Packages**.
  2. Contacted the Cisco TAC, gave them the output of this command, and asked them to point you to the ISO that you should install on your second and third appliances.
- Configured Cisco IMC browser access on both secondary appliances, as described in [Enable Browser Access to Cisco Integrated Management Controller](#).
- Checked that both the secondary node appliances' ports, and the switches they use, are properly configured, as described in [Execute Preconfiguration Checks](#).
- Confirmed that you are using a compatible browser. For a list of compatible browsers, see the [Release Notes](#) document for the version of Cisco DNA Center you are installing.
- Enabled ICMP on the firewall between Cisco DNA Center and both the default gateway and the DNS server you specify in the following procedure. The Maglev Configuration wizard uses ping to verify the gateway and DNS server you specify. This ping might get blocked if a firewall is in place and ICMP is not enabled on that firewall. When this happens, you will not be able to complete the wizard.

## Step 1

Point your browser to the Cisco IMC IP address you set during the Cisco IMC GUI configuration you performed, and log in to the Cisco IMC GUI as the Cisco IMC user (see [Enable Browser Access to Cisco Integrated Management Controller](#)).

After successful login, the appliance displays the **Cisco Integrated Management Controller Chassis Summary** window, with a hyperlinked menu at the top of the window, as shown below.



**Step 2** From the hyperlinked menu, choose **Launch KVM** and then select either **Java based KVM** or **HTML based KVM**. If you select **Java-based KVM**, you will need to launch the Java startup file from your browser or file manager in order to view the KVM console in its own window. If you select **HMTL-based KVM**, it launches the KVM console in a separate window or tab automatically.

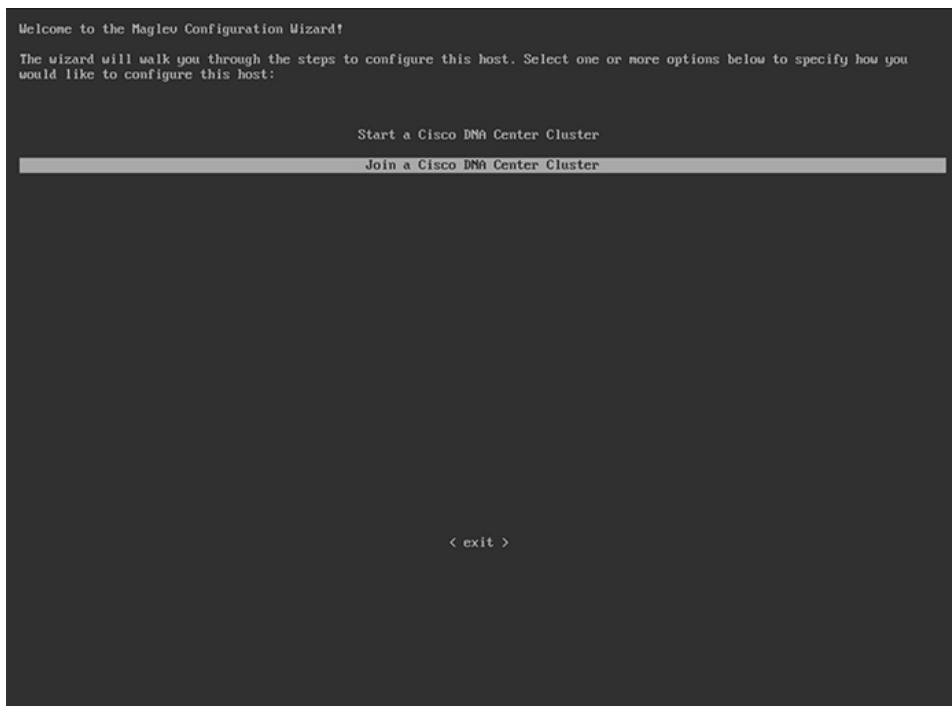
Irrespective of the KVM type you choose, use the KVM console to monitor the progress of the configuration and respond to the Maglev Configuration wizard prompts.

**Step 3** With the KVM displayed, reboot the appliance by choosing one of the following options:

- In the main Cisco IMC GUI browser window: Choose **Host Power > Power Cycle**, and switch to the KVM console to continue.
- In the KVM console: Choose **Power > Power Cycle System (cold boot)**.

If you are asked to confirm your choice to reboot the appliance, click **OK**.

After displaying reboot messages, the KVM console displays the Maglev Configuration wizard welcome screen.



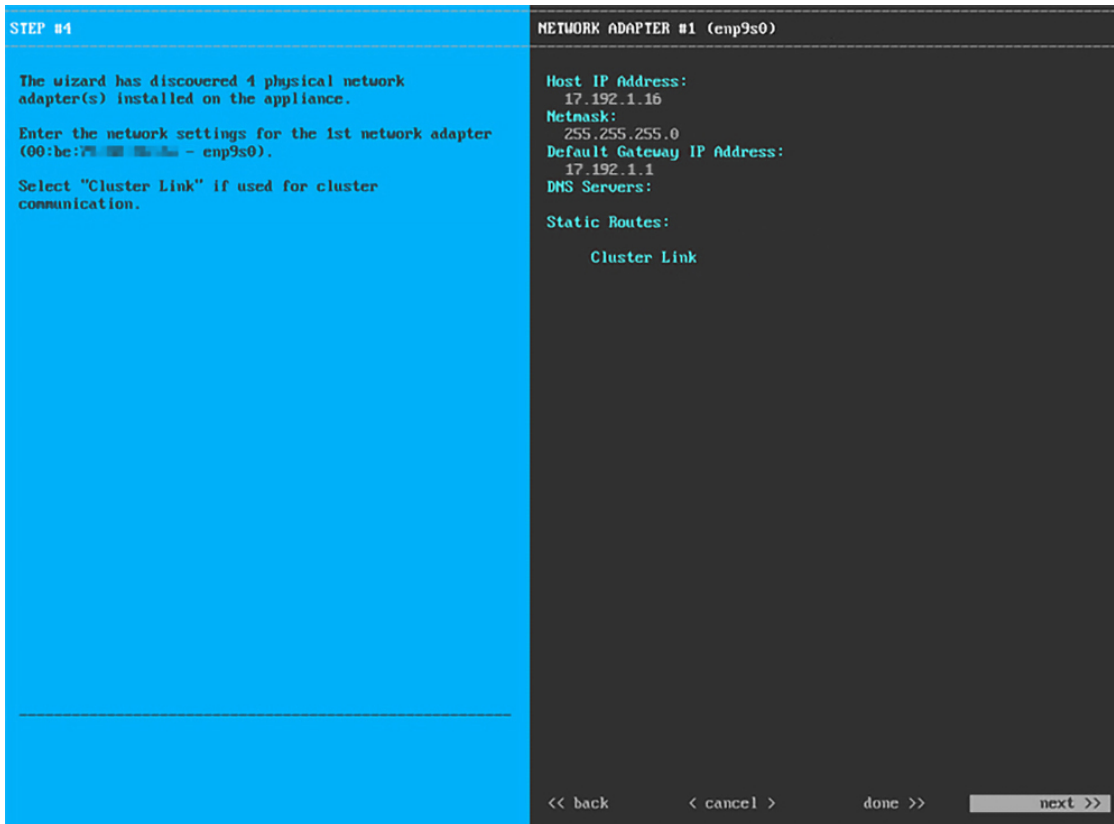
**Step 4** Click **Join a Cisco DNA Center Cluster** to begin configuring the secondary node.

The wizard discovers all of the ports on the appliance and presents them to you one by one, in separate screens, in the following order:

- a. 10-Gbps Enterprise port (Port 1, enp9s0, Network Adapter #1)
- b. 10-Gbps Cluster port (Port 2, enp10s0, Network Adapter #2)
- c. 1-Gbps Cisco DNA Center GUI port (1, enp1s0f0, Network Adapter #3)
- d. 1-Gbps Cloud port (2, enp1s0f1, Network Adapter #4)

**Note** If the wizard fails to display one or both of the 10-Gbps ports during the course of configuration, it might indicate that these ports are nonfunctional or disabled. These 10-Gbps ports are required for Cisco DNA Center functionality. If you discover that they are nonfunctional, choose **cancel** to exit the configuration wizard immediately. Be sure that you have completed all of the steps provided in [Execute Preconfiguration Checks](#) before resuming the configuration or by contacting the Cisco Technical Assistance Center (for more information, see the "Get Assistance from the Cisco TAC" topic in the [Release Notes](#) document).

**Step 5** The wizard discovers the 10-Gbps Enterprise port (Port 1, enp9s0) first, and presents it as **NETWORK ADAPTER #1**. As explained in [Interface Cable Connections](#), this port is required to link the appliance to the enterprise network. Apply the host IP address, netmask, and other values that are appropriate for this purpose (see [Required IP Addresses and Subnets](#) and [Required Configuration Information](#) for the values to enter).



Enter the configuration values for **NETWORK ADAPTER #1**, as shown in the table below.

**Table 23: Secondary Node Entries for Network Adapter #1: 10-Gbps Enterprise Port (enp9s0)**

<b>Host IP address</b>	Enter the IP address for the 10-Gbps Enterprise port. This is required.
<b>Netmask</b>	Enter the netmask for the port's IP address. This is required.
<b>Default Gateway IP address</b>	Enter a default gateway IP address to use for the port. <b>Important</b> Ensure that you enter a default gateway IP address for at least one of your appliance's interfaces. Otherwise, you will not be able to complete the configuration wizard.

<b>DNS Servers</b>	Enter the IP address of the preferred DNS server. If you are entering multiple DNS servers, separate the IP addresses in the list with spaces.  <b>Important</b> For each appliance in your cluster, configure a maximum of three DNS servers. Problems can occur if you configure more than three DNS servers for an appliance.
<b>Static Routes</b>	Enter one or more static routes in the following format, separated by spaces: <code>&lt;network&gt;/&lt;netmask&gt;/&lt;gateway&gt;</code> . This is usually required on the GUI port only.
<b>Cluster Link</b>	Leave this field blank. It is required on the Cluster port only.

After you provide the necessary information, click **next>>** to proceed. Correct validation errors, if any, as you did in previous screens.

### Step 6

After successful validation of the Enterprise port values you entered, the wizard presents the 10-Gbps Cluster port (Port 2, enp10s0) as **NETWORK ADAPTER #2**. As explained in [Interface Cable Connections](#), this port is used to link the appliance to the cluster, so apply the host IP address, netmask, and other values that are appropriate for this purpose (see [Required IP Addresses and Subnets](#) and [Required Configuration Information](#) for the values to enter).

Enter configuration values for **NETWORK ADAPTER #2** as shown in the table below.

**Table 24: Secondary Node Entries for Network Adapter #2: 10-Gbps Cluster Port (enp10s0)**

<b>Host IP address</b>	Enter the IP address for the Cluster port. This is required. Note that you cannot change the address of the Cluster port later.
------------------------	---

<b>Netmask</b>	Enter the netmask for the port's IP address. This is required.
<b>Default Gateway IP address</b>	Enter a default gateway IP address to use for the port.  <b>Important</b> Ensure that you enter a default gateway IP address for at least one of your appliance's interfaces. Otherwise, you will not be able to complete the configuration wizard.
<b>DNS Servers</b>	Enter the IP address of the preferred DNS server. If you are entering multiple DNS servers, separate the IP addresses in the list with spaces.  <b>Important</b> For each appliance in your cluster, configure a maximum of three DNS servers. Problems can occur if you configure more than three DNS servers for an appliance.
<b>Static Routes</b>	Enter one or more static routes in the following format, separated by spaces: <code>&lt;network&gt;/&lt;netmask&gt;/&lt;gateway&gt;</code> . This is usually required on the Cisco DNA Center GUI port only.
<b>Cluster Link</b>	Check the check box to indicate that this port will be the link to a cluster. This is required on the Cluster port only.

After you finish entering the configuration values, click **next>>** to proceed. The wizard validates the values you entered and issues an error message if any are incorrect. If you receive an error message, check that the value you entered is correct, then reenter it. If needed, click **<<back** to reenter it.

### Step 7

After successful validation of the Cluster port values you entered, the wizard presents the 1-Gbps Cisco DNA Center GUI port (1, enp1s0f0) as **NETWORK ADAPTER #3**. As explained in [Interface Cable Connections](#), this port is used to access the Cisco DNA Center GUI from your management network. Apply the host IP address, netmask, and other values that are appropriate for this purpose (see [Required IP Addresses and Subnets](#) and [Required Configuration Information](#) for the values to enter).



Enter the configuration values for **NETWORK ADAPTER #3**, as shown in the table below.

**Table 25: Secondary Node Entries for Network Adapter #3: 1-Gbps GUI Port (enp1s0f0)**

<b>Host IP address</b>	Enter the IP address for the 1-Gbps GUI Port. This is required only if you are using the GUI Port to access the Cisco DNA Center GUI from your management network; otherwise, you can leave it blank.
<b>Netmask</b>	Enter the netmask for the port's IP address. This is required if you enter an IP address.
<b>Default Gateway IP address</b>	Enter a default gateway IP address to use for the port. <b>Important</b> Ensure that you enter a default gateway IP address for at least one of your appliance's interfaces. Otherwise, you will not be able to complete the configuration wizard.
<b>DNS Servers</b>	Enter the IP address of the preferred DNS server. If you are entering multiple DNS servers, separate the IP addresses in the list with spaces. <b>Important</b> <ul style="list-style-type: none"> <li>For NTP, ensure port 123 (UDP) is open between Cisco DNA Center and your NTP server.</li> <li>For each appliance in your cluster, configure a maximum of three DNS servers. Problems can occur if you configure more than three DNS servers for an appliance.</li> </ul>



<b>Static Routes</b>	Enter one or more static routes in the following format, separated by spaces: <network>/<netmask>/<gateway>.
<b>Cluster Link</b>	Leave this field blank. It is required on the Cluster port only.

After you provide the necessary information, click **next>>** to proceed. Correct validation errors, if any, as you did in previous screens.

### Step 8

After successful validation of the Cisco DNA Center GUI port values you entered, the wizard presents the 1-Gbps Cloud port (2, enp1s0f1) as **NETWORK ADAPTER #4**. As explained in [Interface Cable Connections](#), this is an optional port used to link the appliance to the Internet when you cannot do so through the 10-Gbps Enterprise port (Port 1, enp9s0). Apply the host IP address, netmask, and other values that are appropriate for this purpose (see [Required IP Addresses and Subnets](#) and [Required Configuration Information](#) for the values to enter).

Enter the configuration values for **NETWORK ADAPTER #4**, as shown in the table below.

**Table 26: Secondary Node Entries for Network Adapter #4: 1-Gbps Cloud Port (enp1s0f1)**

<b>Host IP address</b>	Enter the IP address for the Cloud port. This is required only if you are using the Cloud port for internet connection; otherwise, you can leave it blank.
<b>Netmask</b>	Enter the netmask for the port's IP address. This is required if you enter an IP address.

<b>Default Gateway IP address</b>	Enter a default gateway IP address to use for the Cloud port.  <b>Important</b> Ensure that you enter a default gateway IP address for at least one of your appliance's interfaces. Otherwise, you will not be able to complete the configuration wizard.
<b>DNS Servers</b>	Enter the IP address of the preferred DNS server. If you are entering multiple DNS servers, separate the IP addresses in the list with spaces.  <b>Important</b> For each appliance in your cluster, configure a maximum of three DNS servers. Problems can occur if you configure more than three DNS servers for an appliance.
<b>Static Routes</b>	Enter one or more static routes in the following format, separated by spaces: <code>&lt;network&gt;/&lt;netmask&gt;/&lt;gateway&gt;</code> . This is usually required on the GUI port only.
<b>Cluster Link</b>	Leave this field blank. It is required on the Cluster port only.

After you provide the necessary information, click **next>>** to proceed. Correct validation errors, if any, as you did in previous screens.

### Step 9

After the network adapter configuration is complete, the wizard prompts you to enter configuration values for the **NETWORK PROXY** that you are using, as shown below.

Enter the configuration values for the **NETWORK PROXY**, as shown in the table below.

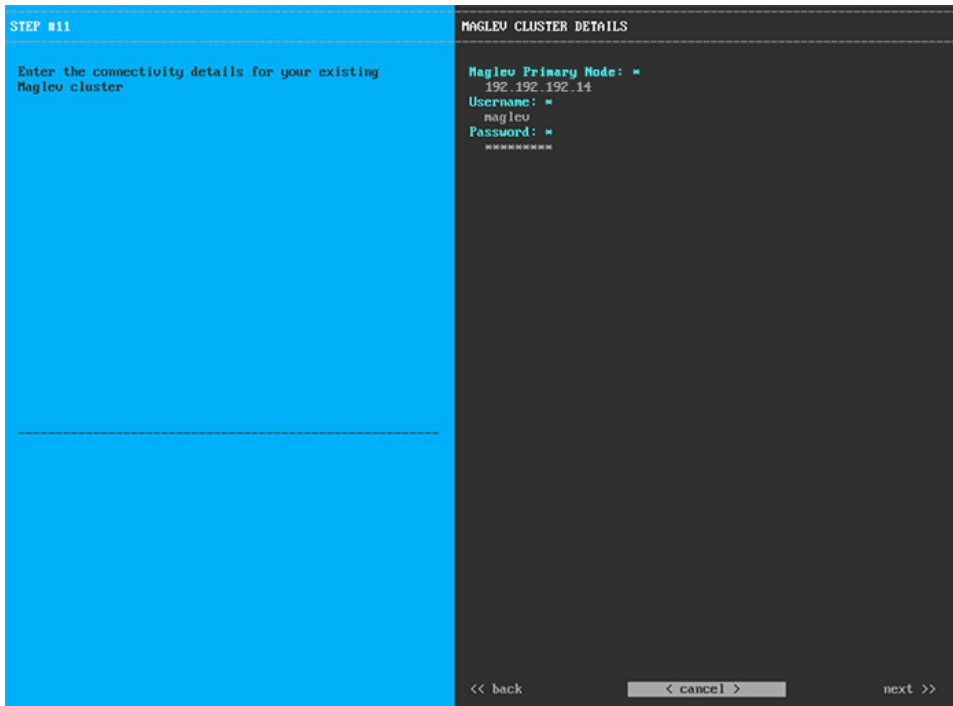
Table 27: Secondary Node Entries for Network Proxy

<b>HTTPS Proxy</b>	Enter the URL or host name of an HTTPS network proxy used to access the Internet.  <b>Note</b> Connection from Cisco DNA Center to the HTTPS proxy is supported only through HTTP in this release.
<b>HTTPS Proxy Username</b>	Enter the user name used to access the network proxy. If no proxy login is required, leave this field blank.
<b>HTTPS Proxy Password</b>	Enter the password used to access the network proxy. If no proxy login is required, leave this field blank.

After you provide the necessary information, click **next>>** to proceed. Correct validation errors, if any, as you did in previous screens.

**Step 10**

After network proxy configuration completes, the wizard prompts you to identify the Cluster port on the primary node, and primary node login details, in **MAGLEV CLUSTER DETAILS**, as shown below.



Enter the values for **MAGLEV CLUSTER DETAILS**, as shown in the table below.

Table 28: Secondary Node Entries for Maglev Cluster Details

<b>Maglev Primary Node</b>	Enter the IP address of the Cluster port on the primary node in the cluster. If you have followed the recommendations for port assignment, this will be the IP address of Port 2, enp10s0, Network Adapter #1 on the primary node.
<b>Username</b>	Enter <b>maglev</b> .
<b>Password</b>	Enter the Linux password you configured on the primary node.

After you provide the necessary information, click **next>>** to proceed. Correct validation errors, if any, as you did in previous screens.

**Step 11**

After you have entered the Maglev cluster details, the wizard prompts you to enter **USER ACCOUNT SETTINGS** values for this secondary node, as shown below.

**STEP #13**

Specify a new password for the 'maglev' Linux user, and specify a passphrase of the 'admin' UI user.

\* Indicates a mandatory field

Password generation is optional, but recommended.

User is advised to append personal password with generated password for recommended security

Caution: Store generated password for future log ins

---

**USER ACCOUNT SETTINGS**

Linux Password: \*

Re-enter Linux Password: \*

Password Generation Seed:

< Generate Password >

Auto Generated Password:

< Use Generated Password >

Administrator Passphrase: \*

Re-enter Administrator Passphrase: \*

<< back      < cancel >      next >>

Enter the values for **USER ACCOUNT SETTINGS**, as shown in the table below.

**Table 29: Secondary Node Entries for User Account Settings**

<b>Linux Password</b>	Enter a Linux password for the maglev user.
<b>Re-enter Linux Password</b>	Confirm the Linux password by entering it a second time.
<b>Password Generation Seed</b>	If you do not want to create the Linux password yourself, enter a seed phrase in this field and then press < <b>Generate Password</b> > to generate the password.
<b>Auto Generated Password</b>	(Optional) The seed phrase appears as part of a random and secure password. If required, you can either use this password as is, or you can further edit this auto-generated password.  Click < <b>Use Generated Password</b> > to save the password.
<b>Administrator Passphrase</b>	Enter a password for the default admin superuser, used to log in to Cisco DNA Center for the first time.
<b>Re-enter Administrator Passphrase</b>	Confirm the administrator passphrase by entering it a second time.

After you provide the necessary information, click **next>>** to proceed. Correct validation errors, if any, as you did in previous screens.

**Step 12** After you have entered the user account details, the wizard prompts you to enter **NTP SERVER SETTINGS** values, as shown below.

```
STEP #14
Enter the IP address of the NTP server that the
controller will use.

It is recommended to specify 3 or more NTP servers to
improve availability and time accuracy.

Please note that the NTP server(s) must be accessible
in order for the configuration to succeed.

* Indicates a mandatory field

NTP SERVER SETTINGS
NTP Servers: *
1.ntp.example.com 2.ntp.example.com 3.ntp.example.com

<< back          < cancel >          next >>
```

Enter one or more NTP server addresses or hostnames, separated by spaces. At least one NTP address or hostname is required. They should be the same NTP servers you specified for the primary node.

After you provide the necessary information, click **next>>** to proceed. Correct validation errors, if any, as you did in previous screens.

**Step 13** When you are finished entering the NTP server settings, a final message appears, stating that the wizard is ready to apply the configuration (as shown below).

```
The wizard is now ready to apply the configuration on the controller.
Use the [back] button below to verify/modify controller settings.
Use the [cancel] button to discard your changes and exit the wizard.
Use the [proceed] button to save your changes and proceed with applying them on the controller.

<< back                < cancel >                proceed >>
```

Click **proceed>>** to complete the configuration wizard.

The host will reboot automatically and display messages on the KVM console as it applies your settings and brings up services. This process can take several hours. You can monitor its progress via the KVM console.

At the end of the configuration process, the appliance power cycles again, then displays a **CONFIGURATION SUCCEEDED!** message.

---

### What to do next

- If you have an additional appliance to deploy as the third and final node in the cluster, repeat this procedure.
- If you have finished adding hosts to the cluster, perform the first-time setup: [First-Time Setup Workflow](#).

## Upgrade to the Latest Cisco DNA Center Release

For information about upgrading your current release of Cisco DNA Center, see the [Cisco DNA Center Upgrade Guide](#).



## CHAPTER 6

# Complete First-Time Setup

---

- [First-Time Setup Workflow](#), on page 89
- [Compatible Browsers](#), on page 89
- [Complete the Quick Start Workflow](#), on page 89
- [Integrate Cisco ISE with Cisco DNA Center](#), on page 94
- [Configure Authentication and Policy Servers](#), on page 100
- [Configure SNMP Properties](#), on page 103

## First-Time Setup Workflow

After you finish configuring all of the Cisco DNA Center appliances you have installed, perform the tasks described in this chapter to prepare Cisco DNA Center for production use. Note the following points:

- For the parameter information you need to complete this work, see [Required First-Time Setup Information](#).
- If you plan to deploy high availability (HA) in your production environment, you will need to redistribute services among your cluster nodes to optimize HA operation (see [Activate HA](#), on page 113). Complete this step after you have configured the SNMP settings for your appliances.

## Compatible Browsers

The Cisco DNA Center GUI is compatible with the following HTTPS-enabled browsers:

- Google Chrome: Version 93 or later.
- Mozilla Firefox: Version 92 or later.

We recommend that the client systems you use to log in to Cisco DNA Center be equipped with 64-bit operating systems and browsers.

## Complete the Quick Start Workflow

After you have installed and configured the Cisco DNA Center appliance, you can log in to its GUI. Use a compatible, HTTPS-enabled browser when accessing Cisco DNA Center.

When you log in for the first time as the admin superuser (with the username `admin` and the `SUPER-ADMIN-ROLE` assigned), the Quick Start workflow automatically starts. Complete this workflow to discover the devices that Cisco DNA Center will manage and enable the collection of telemetry from those devices.

### Before you begin

To log in to Cisco DNA Center and complete the Quick Start workflow, you will need:

- The `admin` superuser username and password that you specified while completing the procedure described in [Configure the Primary Node, on page 61](#).
- The information described in [Required First-Time Setup Information, on page 33](#).

**Step 1** After the Cisco DNA Center appliance reboot is completed, launch your browser.

**Step 2** Enter the host IP address to access the Cisco DNA Center GUI, using **HTTPS://** and the IP address of the Cisco DNA Center GUI that was displayed at the end of the configuration process.

After entering the IP address, one of the following messages appears (depending on the browser you are using):

- Google Chrome: `Your connection is not private`
- Mozilla Firefox: `Warning: Potential Security Risk Ahead`

**Step 3** Ignore the message and click **Advanced**.

One of the following messages appears:

- Google Chrome:

```
This server could not prove that it is GUI-IP-address; its security certificate is not trusted
by your computer's
operating system. This may be caused by a misconfiguration or an attacker intercepting your
connection.
```

- Mozilla Firefox:

```
Someone could be trying to impersonate the site and you should not continue.
```

```
Websites prove their identity via certificates. Firefox does not trust GUI-IP-address because
its certificate issuer is unknown,
the certificate is self-signed, or the server is not sending the correct intermediate certificates.
```

These messages appear because the controller uses a self-signed certificate. For information on how Cisco DNA Center uses certificates, see the "Certificate and Private Key Support" section in the [Cisco DNA Center Administrator Guide](#).

**Step 4** Ignore the message and do one of the following:

- Google Chrome: Click the **Proceed to GUI-IP-address (unsafe)** link.
- Mozilla Firefox: Click **Accept the Risk and Continue**.

The Cisco DNA Center login screen appears.

**Step 5** Enter the admin's username (`admin`) and password that you set when you configured your Cisco DNA Center appliance, then click **Log In**.

In the next screen, you are prompted to specify a new admin password (as a security measure).



**Step 6** Do one of the following:

- If you don't want to change the admin password at this time, click **Skip**.
- To set a new admin password:
  - a. Enter the same password that you specified in Step 5.
  - b. Enter and confirm a new admin password.
  - c. Click **Next**.

**Step 7** Enter your cisco.com username and password (which are used to register software downloads and receive system communications) and then click **Next**.

**Note** If you don't want to enter these credentials at this time, click **Skip** instead.

The **Terms & Conditions** screen opens, providing links to the software End User License Agreement (EULA) and any supplemental terms that are currently available.

**Step 8** After reviewing these documents, click **Next** to accept the EULA.

The **Quick Start Overview** slider opens. Click > to view a description of the tasks that the Quick Start workflow will help you complete in order to start using Cisco DNA Center.

**Step 9** Complete the Quick Start workflow:

- a) Click **Let's Do it**.
- b) In the **Discover Devices: Provide IP Ranges** screen, enter the following information and then click **Next**:
  - The name for the device discovery job.
  - The IP address ranges of the devices you want to discover. Click + to enter additional ranges.
  - Specify whether you want to designate your appliance's loopback address as its preferred management IP address. For more information, see the "Preferred Management IP Address" topic in the [Cisco DNA Center User Guide](#).
- c) In the **Discover Devices: Provide Credentials** screen, enter the information described in the following table for the type of credentials you want to configure and then click **Next**:

Field	Description
<b>CLI (SSH) Credentials</b>	
Username	Username used to log in to the CLI of the devices in your network.
Password	Password used to log in to the CLI of the devices in your network.
Name/Description	Name or description of the CLI credentials.
Enable Password	Password used to enable a higher privilege level in the CLI. Configure this password only if your network devices require it.
<b>SNMP Credentials: SNMPv2c Read tab</b>	
Name/Description	Name or description of the SNMPv2c read community string.

Field	Description
Community String	Read-only community string password used only to view SNMP information on the device.
<b>SNMP Credentials: SNMPv2c Write tab</b>	
Name/Description	Name or description of the SNMPv2c write community string.
Community String	Write community string used to make changes to the SNMP information on the device.
<b>SNMP Credentials: SNMPv3</b>	
Name/Description	Name or description of the SNMPv3 credentials.
Username	Username associated with the SNMPv3 credentials.
Mode	Security level that SNMP messages require: <ul style="list-style-type: none"> <li>• <b>No Authentication, No Privacy</b> (noAuthNoPriv): Does not provide authentication or encryption.</li> <li>• <b>Authentication, No Privacy</b> (authNoPriv): Provides authentication, but does not provide encryption.</li> <li>• <b>Authentication and Privacy</b> (authPriv): Provides both authentication and encryption.</li> </ul>
Authentication Password	Password required to gain access to information from devices that use SNMPv3. The password must be at least eight characters in length. Note the following points: <ul style="list-style-type: none"> <li>• Some wireless controllers require that passwords be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center.</li> <li>• Passwords are encrypted for security reasons and are not displayed in the configuration.</li> </ul>
Authentication Type	Hash-based Message Authentication Code (HMAC) type used when either <b>Authentication and Privacy</b> or <b>Authentication, No Privacy</b> is set as the authentication mode: <ul style="list-style-type: none"> <li>• <b>SHA</b>: HMAC-SHA authentication.</li> <li>• <b>MD5</b>: HMAC-MD5 authentication.</li> </ul>

Field	Description
Privacy Type	<p>Privacy type used when <b>Authentication and Privacy</b> is set as the authentication mode. Choose one of the following privacy types:</p> <ul style="list-style-type: none"> <li>• <b>AES128</b>: 128-bit CBC mode AES for encryption.</li> <li>• <b>AES192</b>: 192-bit CBC mode AES for encryption.</li> <li>• <b>AES256</b>: 256-bit CBC mode AES for encryption.</li> </ul> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• Discovery and Inventory features support only AES192 and AES256 privacy types.</li> <li>• Cisco DNA Assurance does not support any of these privacy types.</li> </ul>
Privacy Password	<p>SNMPv3 privacy password that is used to generate the secret key for encrypting messages are exchanged with devices supported with AES128, AES192, and AES256 encryption standards. Passwords (or passphrases) must be at least eight characters long.</p> <p>Note the following points:</p> <ul style="list-style-type: none"> <li>• Some wireless controllers require that passwords be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center.</li> <li>• Passwords are encrypted for security reasons and are not displayed in the configuration.</li> </ul>
<b>NETCONF</b>	
Port	The NETCONF port that Cisco DNA Center should use in order to discover wireless controllers that run Cisco IOS-XE.

- d) In the **Create Site** screen, group the devices you are going to discover into one site in order to facilitate telemetry and then click **Next**.

You can enter the site's information manually or click the location you want to use in the provided map.

- e) In the **Enable Telemetry** screen, check the network components that you want Cisco DNA Center to collect telemetry for and then click **Next**.

**Note** If both the **Enable Telemetry** and **Disable Telemetry** options are grayed out, this indicates that either devices are not capable of supporting telemetry or devices are running an OS version that does not support telemetry enablement.

- f) In the **Summary** screen, review the settings that you have entered and then do one of the following:
- If you want to make changes, click the appropriate **Edit** link to open the relevant screen.
  - If you're happy with the settings, click **Start Discovery and Telemetry**. Cisco DNA Center validates your settings to ensure that they will not result in any issues. After validation is complete, the screen updates.

Cisco DNA Center begins the process of discovering your network's devices and enabling telemetry for the network components you selected. The process will take a minimum of 30 minutes (more for larger networks).

A message appears at the top of the homepage to indicate when the Quick Start workflow has completed.

g) Do one of the following:

- Click **View Discovery** to open the **Discovery** page and confirm that the devices in your network have been discovered.
- Click the **Go to Network Settings** link to open the **Device Credentials** page. From here, you can verify that the credentials you entered previously have been configured for your site.
- Click the **View Activity Page** link to open the **Tasks** page and view any tasks (such as a weekly scan of the network for security advisories) that Cisco DNA Center has already scheduled to run.
- Click the **Workflow Home** link to access guided workflows that will help you set up and maintain your network.

---

## Integrate Cisco ISE with Cisco DNA Center

Cisco DNA Center provides a mechanism to create a trusted communications link with Cisco ISE and to share data with Cisco ISE in a secure manner. After Cisco ISE is registered with Cisco DNA Center, any device that Cisco DNA Center discovers, along with relevant configuration and other data, is pushed to Cisco ISE. You can use Cisco DNA Center to discover devices and then apply both Cisco DNA Center and Cisco ISE functions to them because these devices will be displayed in both the applications. Cisco DNA Center and Cisco ISE devices are all uniquely identified by their device names.

As soon as the devices are provisioned and assigned to a particular site in the Cisco DNA Center site hierarchy, Cisco DNA Center devices are pushed to Cisco ISE. Any updates to a Cisco DNA Center device (such as changes to IP address, SNMP or CLI credentials, Cisco ISE shared secret, and so on) will be sent to the corresponding device instance on ISE automatically. Note that Cisco DNA Center devices are pushed to Cisco ISE only when these devices are associated with a particular site where Cisco ISE is configured as its AAA server.

### Before you begin

Before attempting to integrate Cisco ISE with Cisco DNA Center, ensure that you have met the following prerequisites:

- You have deployed one or more Cisco ISE hosts on your network. For information on supported Cisco ISE versions, see the [Cisco DNA Center Compatibility Matrix](#). For information on installing Cisco ISE, see the [Cisco Identity Services Engine Install and Upgrade guides](#).
- If you have a standalone Cisco ISE deployment, you must integrate Cisco DNA Center with the Cisco ISE node and enable the pxGrid service and External RESTful Services (ERS) on that node.



---

**Note** Although pxGrid 2.0 allows up to four pxGrid nodes in the Cisco ISE deployment, Cisco DNA Center releases earlier than 2.2.1.x do not support more than two pxGrid nodes.

---

- If you have a distributed Cisco ISE deployment:
  - You must integrate Cisco DNA Center with the primary policy administration node (PAN), and enable ERS on the PAN.



---

**Note** We recommend that you use ERS through the PAN. However, for backup, you can enable ERS on the PSNs.

---

- You must enable the pxGrid service on one of the Cisco ISE nodes within the distributed deployment. Although you can choose to do so, you do not have to enable pxGrid on the PAN. You can enable pxGrid on any Cisco ISE node in your distributed deployment.
- The PSNs that you configure in Cisco ISE to handle TrustSec or SD Access content and PACs must also be defined in **Work Centers > Trustsec > Trustsec Servers > Trustsec AAA Servers**. For more information, see the [Cisco Identity Services Engine Administrator Guide](#).
- Only a user with Super Admin role permissions can integrate Cisco ISE with Cisco DNA Center.
- Cisco DNA Center does not support ERS API access if the **Use CSRF Check for Enhanced Security** option is enabled in Cisco ISE.
- You must enable communication between Cisco DNA Center and Cisco ISE on the following ports: 443, 5222, 8910, and 9060.
- The Cisco ISE host on which pxGrid is enabled must be reachable from Cisco DNA Center on the IP address of the Cisco ISE eth0 interface.
- The Cisco ISE node can reach the fabric underlay network via the appliance's NIC.
- Cisco DNA Center will check the certificate revocation status if Online Certificate Status Protocol (OCSP) or certificate revocation list (CRL) validation is defined for the certificates used by the Cisco ISE services.
- The Cisco ISE admin node certificate must contain the Cisco ISE IP address or FQDN in either the certificate subject name or the Subject Alternative Name (SAN).
- Your ability to use an FQDN-only system certificate depends on whether LAN automation is enabled in your Cisco DNA Center deployment. For more information, see the **alt\_names** section bullet in Step 3 of the [Cisco DNA Center Security Best Practices Guide's](#) "Generate a Certificate Request Using Open SSL" topic.



---

**Note** For Cisco ISE 2.4 Patch 13, 2.6 Patch 7, and 2.7 Patch 3, if you are using the Cisco ISE default self-signed certificate as the pxGrid certificate, Cisco ISE might reject that certificate after applying those patches. This is because the older versions of that certificate have the Netscape Cert Type extension specified as the SSL server, which now fails (because a client certificate is required).

This issue does not occur in Cisco ISE 3.0 and later. For more information, see the [Cisco ISE Release Notes](#).

---

For more information about configuring Cisco ISE for Cisco DNA Center, see the "Integration with Cisco DNA Center" topic in the *Cisco Identity Services Engine Administrator Guide*.

**Step 1** Enable the pxGrid service and ERS on Cisco ISE:

- a) Log in to the primary policy administration node.
- b) In the Cisco ISE GUI, click the menu icon (☰) and choose **Administration > System > Deployment**.

The **Deployment Nodes** window appears.

- c) Click the hostname of the Cisco ISE node on which you want to enable the pxGrid service. In a distributed deployment, this can be any Cisco ISE node in the deployment.

The **Edit Node** window appears.

- d) In the **General Settings** tab, check the **pxGrid** check box, and click **Save**.
- e) In the Cisco ISE GUI, click the menu icon (☰) and choose **Administration > System > Settings**.
- f) From the left navigation pane, click **ERS Settings** to open the **ERS Settings** window.
- g) Click the **Enable ERS for Read/Write** radio button, and then click **OK** in the notification prompt.
- h) Click **Save**.

**Step 2** Add the Cisco ISE node to Cisco DNA Center as a AAA server:

- a) Log in to the Cisco DNA Center GUI.
- b) Click the menu icon (☰) and choose **System > System 360**.
- c) In the Identity Services Engine (ISE) pane, click the **Configure** link.
- d) From the **Authentication and Policy Servers** window, click **Add** and choose **ISE** from the drop-down list.
- e) Enter the following details in the **Add ISE server** slide-in pane:

- In the **Server IP Address** field, enter the IP address of the Cisco ISE server.
- Enter the **Shared Secret** used to secure communications between your network devices and Cisco ISE.
- In the **Username** and **Password** fields, enter the corresponding Cisco ISE admin credentials.
- Enter the **FQDN** for the Cisco ISE node.
- (Optional) Enter the **virtual IP address** of the load balancer behind which the Cisco ISE PSNs are located. If you have multiple policy service node farms behind different load balancers, you can enter a maximum of six virtual IP addresses.
- **Connect to pxGrid**: Check this check box under **Advanced Settings** to enable pxGrid connection.

If you want to use the Cisco DNA Center system certificate as the pxGrid client certificate (sent to ISE to authenticate the Cisco DNA Center system as a pxGrid client), check the **Use Cisco DNA Center Certificate for pxGrid** check box. You can use this option if all the certificates that are used in your operating environments must be generated by the same Certificate Authority (CA). If this option is disabled, Cisco DNA Center will send a request to Cisco ISE to generate a pxGrid client certificate for the system to use.

When you enable this option, ensure that:

- The Cisco DNA Center certificate is generated by the same CA as is in use by Cisco ISE (otherwise the pxGrid authentication will fail).
- The Certificate Extended Key Use (EKU) field includes "Client Authentication".
- In the **Advanced Settings** area:

- You can choose the protocol that must be used by checking the check box for **RADIUS** or **TACACS**
- Enter the required values in the following fields: **Authentication Port**, **Accounting Port**, **Retries**, and **(Timeout seconds)**.

**Note** This option is available only if third-party certificates are used by Cisco DNA Center. If Cisco DNA Center uses the default self-signed system certificate, then this option is disabled.

f) Click **Add**.

When the integration with Cisco ISE is initiated, you will see a notification that the certificate from Cisco ISE is not yet trusted. You can view the certificate to see the details.


Click **Accept** to trust the certificate and continue with the integration process, or choose **Decline** if you do not wish to trust the certificate and terminate the integration process.

After the integration completes successfully, a confirmation message is displayed.

If there is any issue in the integration process, an error message is displayed. An option to edit or retry is displayed where applicable.

- If the error message says that the Cisco ISE Admin credentials are invalid, click **Edit** and re-enter the correct information.
- If errors are found with certificates in the integration process, you must delete the Cisco ISE server entry and restart the integration from the beginning after the certificate issue has been resolved.

**Step 3** Verify that Cisco DNA Center is connected to Cisco ISE, and that the Cisco ISE SGT groups and devices are pushed to Cisco DNA Center:

- a) Log in to the Cisco DNA Center GUI.
- b) Click the menu icon () and choose **System > System 360**.
- c) In the Identity Services Engine (ISE) pane, verify that the status of all listed ISE servers is displayed as **Available** or **Configured**.
- d) In the Identity Services Engine (ISE) pane, click the **Update** link.
- e) From the **Authentication and Policy Servers** window, verify that the status of the Cisco ISE AAA server is still **Active**.

**Step 4** Verify that Cisco ISE is connected to Cisco DNA Center and that the connection has subscribers:

- a) Log in to the Cisco ISE nodes that are shown as pxGrid servers in the **Identity Services Engine (ISE)** pane.
- b) Choose **Administration > pxGrid Services** and click the **Web Clients** tab.

You should see the pxGrid clients in the list with the IP address of the Cisco DNA Center server.

---

## Group-Based Access Control: Policy Data Migration and Synchronization

### When You Start Using Cisco DNA Center

In earlier releases of Cisco DNA Center, the Group-Based Access Control policy function stored some policy Access Contracts and Policies locally in Cisco DNA Center. Cisco DNA Center also propagated that data to Cisco ISE. Cisco ISE provides the runtime policy services to the network, which includes group-based access

control policy downloads to the network devices. Usually, the policy information in Cisco DNA Center matches the policy information in Cisco ISE. But it is possible that the data is not in sync; the data may not be consistent. Because of this, after installing or upgrading to Cisco DNA Center, the following steps are necessary before you can use the Group-Based Access Control capabilities.

- Integrate Cisco ISE with Cisco DNA Center, if it is not already integrated.
- Upgrade Cisco ISE, if the version is not the minimum required. See the Cisco DNA Center Release Notes for the required versions of Cisco ISE.
- Perform Policy Migration and Synchronization.

### What Is “Migration and Synchronization”?

Cisco DNA Center reads all the Group-Based Access Control policy data in the integrated Cisco ISE and compares that data with the policy data in Cisco DNA Center. If you upgraded from an earlier version, existing policy data is retained. You must synchronize the policies before you can manage Group-Based Access Control Policy in Cisco DNA Center.

### How Does Migration and Synchronization Work?

Usually, the policy data in Cisco ISE and in Cisco DNA Center is consistent, so no special handling or conversion of data is necessary. Sometimes, when there are minor discrepancies or inconsistencies, only some of the data is converted during the migration. If there is a conflict, the data in Cisco ISE is given precedence, so as not to introduce changes in policy behavior in the network. The following list describes the actions taken during migration:

- Security Groups: The Security Group Tag (SGT), which is a numeric value, uniquely identifies a Security Group. Cisco ISE Security Groups are compared to Security Groups in Cisco DNA Center.
  - When the Name and SGT value are the same, nothing is changed. The information in Cisco DNA Center is consistent with Cisco ISE and does not need to be changed.
  - When a Cisco ISE Security Group SGT value does not exist in Cisco DNA Center, a new Security Group is created in Cisco DNA Center. The new Security Group is given the default association of “Default\_VN.”
  - When a Cisco ISE Security Group SGT value exists in Cisco DNA Center, but the names do not match, the name from Cisco ISE Security Group replaces the name of that Security Group in Cisco DNA Center.
  - When the Cisco ISE Security Group Name is the same, but the SGT value is different, the Security Group from Cisco ISE is migrated. It retains the name and tag value, and the Cisco DNA Center Security Group is renamed. A suffix of “\_DNA” is added.

### Contracts

All the SGACLs in Cisco ISE that are referenced by policies are compared to Contracts in Cisco DNA Center.

- When the SGACL and Contract have the same name and content, there is no need for further action. The information in Cisco DNA Center is consistent with Cisco ISE and does not need to be changed.
- When the SGACL and Contract have the same name, but the content is different, the SGACL content from Cisco ISE is migrated. The previous Contract content in Cisco DNA Center is discarded.



When the SGACL name does not exist in Cisco DNA Center, a new Contract with that name is created, and the SGACL content from Cisco ISE is migrated.



---

**Note** When creating new Access Contracts based on Cisco ISE SGACL content, Cisco DNA Center parses the text command lines, and, where possible, renders these SGACL commands as a modeled Access Contract. Each ACE line renders as an “Advanced” application line. If a Cisco ISE SGACL contains text that cannot be parsed successfully, the text content of the SGACL is not converted into modeled format. It is stored as raw command line text. These SGACL text contracts may be edited, but no parsing or syntax checking of the text content is performed during migration.

---

### Policies

A Policy is uniquely identified by a source group-destination group pair. All Cisco ISE TrustSec Egress Policy Matrix policies are compared to the policies in Cisco DNA Center.

- When a policy for a source group-destination group references the same SGACL/Contract name in Cisco ISE, no changes are made.
- When a policy for a source group-destination group references a different SGACL/Contract name in Cisco ISE, the Cisco ISE Contract name is referenced in the policy. This overwrites the previous Contract reference in Cisco DNA Center.
- The Cisco ISE default policy is checked and migrated to Cisco DNA Center.



---

**Note** Cisco DNA Center supports a single contract in access policies. Cisco ISE has an option to use multiple SGACLs in access policies, but this option is not enabled by default in Cisco ISE, and in general is not widely used. Existing SDA customers who have been using the previous release of Cisco DNA Center to manage Group-Based Access Control policy did not use this option.

---

If you enabled the option to allow multiple SGACLs on Cisco ISE and used this when creating policies, those policies cannot be migrated to Cisco DNA Center in this release. The specific policy features that make use of the “multiple SGACL” option and cannot be migrated are:

- Multiple SGACLs in a policy.
- Policy Level catch-all rules set to “Permit” or “Deny.” Only the value of “None” is currently supported for migration to Cisco DNA Center.
- Default Policy set to use a customer-created SGACL, but only the standard values of “Permit IP,” “Permit\_IP\_Log,” “Deny IP,” and “Deny\_IP\_Log” are currently supported for migration to Cisco DNA Center.

If any of the preceding SGACLs are detected during the policy migration and synchronization operation, a notification is generated, and you must choose between the following options to continue:

- **Manage Group-Based Access Control policy in Cisco DNA Center:** If this option is selected, all management of Group-Based Access Control Policy is done in Cisco DNA Center. The user interface screens in Cisco ISE for management of Cisco ISE Security Groups, SGACLs, and Egress Policies are available in Read-Only mode. If there were any issues migrating policies (due to use of multiple SGACLs in Cisco ISE), those policies have no contract selected in Cisco DNA Center. The policy uses the default

policy, and you can select a new contract for those policies after completing the migration. If there was an problem migrating the default policy, the default policy is set to "Permit."

- **Manage Group-Based Access Control Policy in Cisco ISE:** If this option is selected, Cisco DNA Center Group-Based Access Control policy management is inactive. No changes are made to Cisco ISE and there is no effect on policy enforcement in the network. Group-Based Access Control policy is managed in Cisco ISE at the TrustSec workcenter.
- **Manage Group-Based Access Control policy in both Cisco DNA Center and Cisco ISE:** This option is not recommended for general use, because policy changes made in Cisco ISE are not synchronized with Cisco DNA Center. The two systems cannot be kept in sync. This option is intended as a short-term or interim option, and should only be considered when you enabled the "Allow Multiple SGACLs" option in Cisco ISE. Use this option if you need more time and flexibility updating Cisco ISE.

## Configure Authentication and Policy Servers

Cisco DNA Center uses AAA servers for user authentication and Cisco ISE for both user authentication and access control. Use this procedure to configure AAA servers, including Cisco ISE.

### Before you begin

- If you are using Cisco ISE to perform both policy and AAA functions, make sure that Cisco DNA Center and Cisco ISE are integrated.
- If FIPS mode is enabled for Cisco DNA Center, ensure that you enable KeyWrap when integrating Cisco DNA Center and Cisco ISE. See Step 2e in [Integrate Cisco ISE with Cisco DNA Center, on page 94](#).




---

**Note** You cannot enable KeyWrap if Cisco DNA Center and Cisco ISE have already been integrated. To enable this feature, you need to delete Cisco ISE and then reintegrate it with Cisco DNA Center.

---

- If you are using another product (not Cisco ISE) to perform AAA functions, make sure to do the following:
  - Register Cisco DNA Center with the AAA server, including defining the shared secret on both the AAA server and Cisco DNA Center.
  - Define an attribute name for Cisco DNA Center on the AAA server.
  - For a Cisco DNA Center multihost cluster configuration, define all individual host IP addresses and the virtual IP address for the multihost cluster on the AAA server.
- Before you configure Cisco ISE, confirm that:
  - You have deployed Cisco ISE on your network. For information on supported Cisco ISE versions, see the [Cisco DNA Center Compatibility Matrix](#). For information on installing Cisco ISE, see the [Cisco Identity Services Engine Install and Upgrade guides](#).
  - If you have a standalone ISE deployment, you must integrate Cisco DNA Center with the Cisco ISE node and enable the pxGrid service and External RESTful Services (ERS) on that node.



---

**Note** Although pxGrid 2.0 allows up to four pxGrid nodes in the Cisco ISE deployment, Cisco DNA Center releases earlier than 2.2.1.x do not support more than two pxGrid nodes.

---

- If you have a distributed Cisco ISE deployment:
  - You must integrate Cisco DNA Center with the primary policy administration node (PAN), and enable ERS on the PAN.



---

**Note** We recommend that you use ERS through the PAN. However, for backup, you can enable ERS on the PSNs.

---

- You must enable the pxGrid service on one of the Cisco ISE nodes within the distributed deployment. Although you can choose to do so, you do not have to enable pxGrid on the PAN. You can enable pxGrid on any Cisco ISE node in your distributed deployment.
- The PSNs that you configure in Cisco ISE to handle TrustSec or SD Access content and PACs must also be defined in **Work Centers > Trustsec > Trustsec Servers > Trustsec AAA Servers**. For more information, see the [Cisco Identity Services Engine Administrator Guide](#).
- You must enable communication between Cisco DNA Center and Cisco ISE on the following ports: 443, 5222, 8910, and 9060.
- The Cisco ISE host on which pxGrid is enabled must be reachable from Cisco DNA Center on the IP address of the Cisco ISE eth0 interface.
- The Cisco ISE node can reach the fabric underlay network via the appliance's NIC.
- The Cisco ISE admin node certificate must contain the Cisco ISE IP address or FQDN in either the certificate subject name or the Subject Alternative Name (SAN).
- The Cisco DNA Center system certificate must list both the Cisco DNA Center appliance IP address and FQDN in the SAN field.



---

**Note** For Cisco ISE 2.4 Patch 13, 2.6 Patch 7, and 2.7 Patch 3, if you are using the Cisco ISE default self-signed certificate as the pxGrid certificate, Cisco ISE might reject that certificate after applying those patches. This is because the older versions of that certificate have the Netscape Cert Type extension specified as the SSL server, which now fails (because a client certificate is required).

This issue does not occur in Cisco ISE 3.0 and later. For more information, see the [Cisco ISE Release Notes](#).

---

---

**Step 1** Click the menu icon (☰) and choose **System > Settings > External Services > Authentication and Policy Servers**.

**Step 2** From the **Add** drop-down list, choose **AAA** or **ISE**.

**Step 3** To configure the primary AAA server, enter the following information:

- **Server IP Address:** IP address of the AAA server.
- **Shared Secret:** Key for device authentications. The shared secret can contain up to 100 characters.

**Step 4** To configure a Cisco ISE server, enter the following details:

- **Server IP Address:** IP address of the ISE server.
- **Shared Secret:** Key for device authentications.
- **Username:** Username that is used to log in to the Cisco ISE CLI.
- **Note** This user must be a Super Admin.
- **Password:** Password for the Cisco ISE CLI username.
- **FQDN:** Fully qualified domain name (FQDN) of the Cisco ISE server.

- Note**
- We recommend that you copy the FQDN that is defined in Cisco ISE (**Administration > Deployment > Deployment Nodes > List**) and paste it directly into this field.
  - The FQDN that you enter must match the FQDN, Common Name (CN), or Subject Alternative Name (SAN) defined in the Cisco ISE certificate.

The FQDN consists of two parts, a hostname and the domain name, in the following format:

*hostname.domainname.com*

For example, the FQDN for a Cisco ISE server can be ise.cisco.com.

- **Virtual IP Address(es):** Virtual IP address of the load balancer behind which the Cisco ISE policy service nodes (PSNs) are located. If you have multiple PSN farms behind different load balancers, you can enter a maximum of six virtual IP addresses.

**Step 5** Click **Advanced Settings** and configure the settings:

- **Connect to pxGrid:** Check this check box to enable a pxGrid connection.

If you want to use the Cisco DNA Center system certificate as the pxGrid client certificate (sent to Cisco ISE to authenticate the Cisco DNA Center system as a pxGrid client), check the **Use Cisco DNA Center Certificate for pxGrid** check box. You can use this option if all the certificates that are used in your operating environments must be generated by the same CA. If this option is disabled, Cisco DNA Center will send a request to Cisco ISE to generate a pxGrid client certificate for the system to use.

When you enable this option, ensure that:

- The Cisco DNA Center certificate is generated by the same Certificate Authority (CA) as is in use by Cisco ISE (otherwise, the pxGrid authentication fails).
  - The Certificate Extended Key Use (EKU) field includes "Client Authentication."
- **Protocol:** **TACACS** and **RADIUS** (the default). You can select both protocols.

**Attention** If you do not enable TACACS for a Cisco ISE server here, you cannot configure the Cisco ISE server as a TACACS server under **Design > Network Settings > Network** when configuring a AAA server for network device authentication.

- **Authentication Port:** Port used to relay authentication messages to the AAA server. The default UDP port is 1812.
- **Accounting Port:** Port used to relay important events to the AAA server. The default UDP port is 1813.
- **Port:** The default TACACS port is 49.
- **Retries:** Number of times that Cisco DNA Center attempts to connect with the AAA server before abandoning the attempt to connect. The default number of attempts is 3.
- **Timeout:** The time period for which the device waits for the AAA server to respond before abandoning the attempt to connect. The default timeout is 4 seconds.

**Note** After the required information is provided, Cisco ISE is integrated with Cisco DNA Center in two phases. It takes several minutes for the integration to complete. The phase-wise integration status is shown in the **Authentication and Policy Servers** window and **System 360** window:

Cisco ISE server registration phase:

- **Authentication and Policy Servers** window: "In Progress"
- **System 360** window: "Primary Available"

pxGrid subscriptions registration phase:

- **Authentication and Policy Servers** window: "Active"
- **System 360** window: "Primary Available" and "pxGrid Available"

If the status of the configured Cisco ISE server is shown as "FAILED" due to a password change, click **Retry**, and update the password to resynchronize the Cisco ISE connectivity.

**Step 6** Click **Add**.

**Step 7** To add a secondary server, repeat the preceding steps.

---

## Configure SNMP Properties

You can configure the retry and timeout values for SNMP.

### Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see the [Cisco DNA Center Administrator Guide](#).

---

**Step 1** Click the menu icon (☰) and choose **System > Settings > Device Settings > SNMP**.

**Step 2** Configure the following fields:

- **Retries:** Number of attempts allowed to connect to the device. Valid values are from 1 to 3. The default is 3.

- **Timeout (in Seconds):** Number of seconds Cisco DNA Center waits when trying to establish a connection with a device before timing out. Valid values are from 1 to 300 seconds, in intervals of 5 seconds. The default is 5 seconds.

**Step 3** Click **Save**.

**Note** To return to the default settings, click **Reset and Save**.

---



## CHAPTER 7

# Troubleshoot the Deployment

---

- [Troubleshooting Tasks, on page 105](#)
- [Log Out, on page 105](#)
- [Reconfigure the Appliance Using the Configuration Wizard, on page 106](#)
- [Power Cycle the Appliance, on page 107](#)

## Troubleshooting Tasks

When troubleshooting issues with the appliance's configuration, you will normally perform the following tasks:

1. If you are currently using the Cisco DNA Center GUI: [Log Out](#).
2. To reconfigure the appliance's hardware, log in to and use the Cisco IMC GUI, as explained in Steps 12 and 13 of [Enable Browser Access to Cisco Integrated Management Controller](#).
3. To change the appliance configuration, launch and use the Maglev Configuration wizard, as explained in [Reconfigure the Appliance Using the Configuration Wizard](#).
4. Power cycle the appliance so that your changes are active: [Power Cycle the Appliance, on page 107](#).

For more information about the appliance's network adapters, see the [Managing Adapters](#) section of the *Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide, Release 3.1*. As noted elsewhere, never attempt to manage the appliance hardware through the Linux CLI. Use only the Cisco IMC GUI or the Maglev Configuration wizard to change appliance settings.

## Log Out

Follow the steps below to log out of the Cisco DNA Center GUI.

For security reasons, we recommend that you log out after you complete a work session. If you do not log out yourself, you will be logged out automatically after 30 minutes of inactivity.

---

**Step 1** Click the menu icon (☰).

**Step 2** Click **Sign out**.

This ends your session and logs you out.

## Reconfigure the Appliance Using the Configuration Wizard

To reconfigure an appliance, you must use the Configuration wizard to update the appliance settings. You cannot use the Linux CLI to do this. The normal Linux administration procedures that you might use to update configuration settings on a standard Linux server will not work and should not be attempted.

After the appliance is configured, you cannot use the Configuration wizard to change all of the appliance settings. Changes are restricted to the following settings only:

- Host IP address of the appliance
- DNS server IP addresses
- Default gateway IP address
- NTP server IP addresses
- Cluster Virtual IP address
- Cluster hostname (FQDN)
- Static routes
- Proxy server IP address
- Maglev user password
- Admin user password

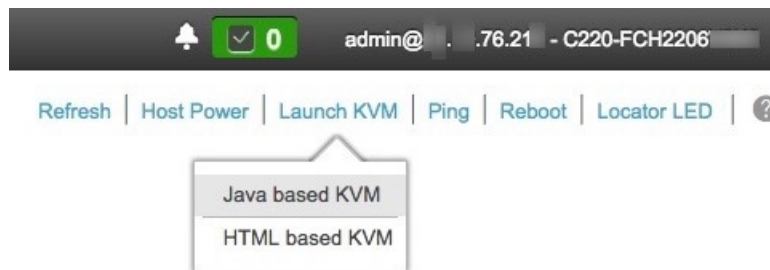
### Before you begin

You will need the Linux user name (*maglev*) and password that are currently configured on the target appliance.

### Step 1

Point your browser to the Cisco IMC IP address you set during the Cisco IMC GUI configuration you performed, and log in to the Cisco IMC GUI as the Cisco IMC user (see [Enable Browser Access to Cisco Integrated Management Controller](#)).

After successful login, the appliance displays the **Cisco Integrated Management Controller Chassis Summary** window, with a hyperlinked menu at the top of the window, as shown below.





**Step 2** From the hyperlinked menu, choose **Launch KVM** and then select either **Java based KVM** or **HTML based KVM**. If you select **Java-based KVM**, you will need to launch the Java startup file from your browser or file manager in order to view the KVM console in its own window. If you select **HMTL-based KVM**, it launches the KVM console in a separate window or tab automatically.

Irrespective of the KVM type you choose, use the KVM console to monitor the progress of the configuration and respond to the Maglev Configuration wizard prompts.

**Step 3** When prompted, enter the Linux password.

**Step 4** Enter the following command to access the Configuration wizard.

```
sudo maglev-config update
```

If you are prompted for the Linux password, enter it again.

**Step 5** The Configuration wizard presents an abbreviated version of the same series of screens shown in, for example, [Configure a Secondary Node](#). Make changes to the settings presented, if required. After you finish making changes on each screen, choose **[Next]**, as needed, to proceed through the Configuration wizard.

**Step 6** At the end of the configuration process, a message appears, stating that the Configuration wizard is now ready to apply your changes. The following options are available:

- **[back]**: Review and verify your changes.
- **[cancel]**: Discard your changes and exit the Configuration wizard.
- **[proceed]**: Save your changes and begin applying them.

Choose **proceed>>** to complete the installation. The Configuration wizard applies the changes you made.

At the end of the configuration process, a `CONFIGURATION SUCCEEDED!` message appears.

---

## Power Cycle the Appliance

Complete one of the following procedures on your Cisco DNA Center appliance to either halt it or perform a warm restart. You can halt the appliance before you make hardware repairs, or you can initiate a warm restart after you have corrected software issues.

### Using the Cisco IMC GUI

If you want to use the KVM console that is accessible from the Cisco IMC GUI in order to halt your appliance or perform a warm restart, complete the tasks described in this procedure.

#### Before you begin

Note that any hardware changes you make using the Cisco IMC GUI will be applied after the appliance reboots.



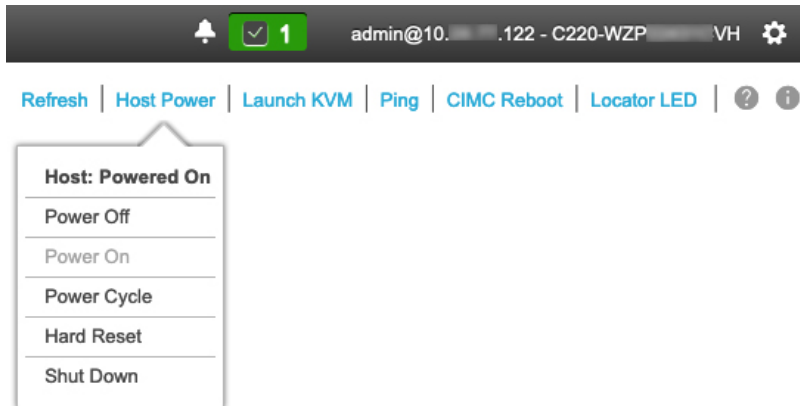
---

**Caution** Power cycling your appliance from the Cisco IMC GUI can result in the corruption or loss of data. Only do so if your appliance is completely unresponsive to SSH, the Cisco IMC console, or the physical console.

---

**Step 1** Point your browser to the Cisco IMC IP address you set during the Cisco IMC GUI configuration you performed, and log in to the Cisco IMC GUI as the Cisco IMC user (see [Enable Browser Access to Cisco Integrated Management Controller, on page 43](#)).

After successful login, the appliance displays the **Cisco Integrated Management Controller Chassis Summary** window, with a hyperlinked menu at the top of the window, as shown below.



**Step 2** With the KVM displayed, reboot the appliance by choosing **Host Power > Power Cycle**.  
If you are asked to confirm your choice to reboot the appliance, click **OK**.

## Using SSH

If you want to use SSH in order to halt your appliance or perform a warm restart, complete the following tasks:

### Before you begin

You will need the following:

- Secure Shell (SSH) client software.
- The IP address that you configured for the 10-Gbps Enterprise port on the appliance that needs reconfiguration. Log in to the appliance at this address, on port 2222.  
To identify the Enterprise port, see the rear-panel figure in [Front and Rear Panels, on page 2](#).
- The Linux user name (*maglev*) and the password that is currently configured on the target appliance.

**Step 1** Using a Secure Shell (SSH) client, log in to the IP address of the Enterprise port of the appliance that needs to be reconfigured, on port 2222:

```
ssh maglev@Enterprise-port's-IP-address -p 2222
```

**Step 2** When prompted, enter the Linux password.

**Step 3** Enter the command that is appropriate for the task you want to perform:

- To halt the appliance, enter: **sudo shutdown -h now**
  - To initiate a warm restart, enter: **sudo shutdown -r now**
- If you are prompted for the Linux password, enter it again.

**Step 4** Review the command output that is displayed as the host shuts down.

**Step 5** If you halted your appliance, power up the Maglev root process by turning the appliance back on, using the front-panel power button.

---





## APPENDIX **A**

# Review High Availability Cluster Deployment Scenarios

---

Cisco DNA Center's implementation of high availability (HA) is described in the [Cisco DNA Center High Availability Guide](#). We recommend that you first review this information and then determine whether you want to deploy HA in your production environment. If you choose to do so, complete the following tasks:

1. Complete the deployment procedure that is appropriate for your network:
  - [New HA Deployment](#)
  - [Existing HA Deployment of the Primary Node with Standard Interface Configurations](#)
  - [Existing HA Deployment of the Primary Node with Nonstandard Interface Configurations](#)
2. [Activate HA](#) on your Cisco DNA Center cluster.
3. See [Additional HA Deployment Considerations](#) and make any additional configurations that are necessary.
  - [New HA Deployment, on page 111](#)
  - [Existing HA Deployment of the Primary Node with Standard Interface Configurations, on page 112](#)
  - [Existing HA Deployment of the Primary Node with Nonstandard Interface Configurations, on page 112](#)
  - [Activate HA, on page 113](#)
  - [Additional HA Deployment Considerations, on page 113](#)

## New HA Deployment

To install a brand new HA cluster, complete the following steps:

- 
- Step 1** Configure the first installed appliance as the primary node.  
See [Configure the Primary Node](#).
- Step 2** Configure the second and third appliances in the cluster.  
See [Configure a Secondary Node](#).
-

## Existing HA Deployment of the Primary Node with Standard Interface Configurations

To deploy an existing HA cluster, where the primary node uses the required interface cable configurations, complete the following steps.

- 
- Step 1** Upgrade the primary node to the latest Cisco DNA Center version.  
For information about upgrading your current release of Cisco DNA Center, see the [Cisco DNA Center Upgrade Guide](#).
- Step 2** Confirm that you are using the required interface cable configurations on the primary node.  
See [Interface Cable Connections](#).
- Step 3** Update the virtual IP address (if the virtual IP address is not yet added).  
See [Reconfigure the Appliance Using the Configuration Wizard](#).
- Step 4** Configure the second and third appliances in the cluster.  
See [Configure a Secondary Node](#).
- Step 5** Enter the following command to check the GlusterFS size:  
`sudo du -h /data/maglev/srv/maglev-system/glusterfs/mnt/bricks/default_brick/ | tail -1 | awk '{print $1}'`  
If the GlusterFS file system size is larger than 150 GB, complete the steps described in [Existing HA Deployment of the Primary Node with Nonstandard Interface Configurations](#).
- 

## Existing HA Deployment of the Primary Node with Nonstandard Interface Configurations

To deploy an existing HA cluster where the primary node uses nonstandard interface configurations, complete the following steps.

- 
- Step 1** Upgrade the primary node to the latest Cisco DNA Center version.  
For information about upgrading your current release of Cisco DNA Center, see the [Cisco DNA Center Upgrade Guide](#).
- Step 2** Create a backup of the remote repository.  
See the "Backup and Restore" chapter in the [Cisco DNA Center Administrator Guide](#).
- Step 3** Reimage the primary node with the required interface cable configuration.  
See [Interface Cable Connections](#) and [Install the Cisco DNA Center ISO Image](#). Make sure that the VIP has been configured correctly on the primary node.

- Step 4** On the primary node, install the same set of packages that you selected during the backup.
- Step 5** Using the backup file that you created in Step 2, restore the remote repository's data.
- Step 6** Configure the second and third appliances in the cluster.
- See [Configure a Secondary Node](#).
- 

## Activate HA

Cisco DNA Center's implementation of HA is described in the [Cisco DNA Center High Availability Guide](#). We recommend that you first review this information and then determine whether you want to deploy HA in your production environment. If you choose to do so, complete the following steps:

1. Click the menu icon (☰) and choose **System > Settings > System Configuration > High Availability**.
2. Click **Activate High Availability**.

After you click **Activate High Availability**, Cisco DNA Center enters into maintenance mode. In this mode, Cisco DNA Center is unavailable until the redistribution of services is completed. You should take this into account when scheduling an HA deployment.



---

**Note** Cisco DNA Center goes into maintenance mode every time you restore the database, perform a system upgrade (not a package upgrade), and activate HA (as described above).

---

## Additional HA Deployment Considerations

For an existing HA deployment, the following additional configurations must be made.



---

**Note** For information about known HA bugs and workarounds, see “Open Bugs—HA” in the [Release Notes for Cisco Digital Network Architecture Center](#).

---

## Telemetry

If you enabled telemetry for a device (without enabling the VIP), complete the following steps:

---

- Step 1** Use the `sudo maglev-config update` command to update the cluster VIP.
- Step 2** Disable telemetry on the device:
- a. From the Cisco DNA Center home page, choose **Network Telemetry** from the **Tools** area.  
The **Network Telemetry** window appears.
  - b. Click the **Site View** tab.

- c. Check the check box of the device on which you want to disable telemetry, and then choose **Actions > Disable Telemetry**.

**Step 3** Reenable telemetry using the profile associated with the device previously.

---

## Wireless Controller

You must update the wireless controllers in your network with the new VIP of Cisco DNA Center.