



## **Cisco DNA Center Second-Generation Appliance Installation Guide, Release 2.3.4**

**First Published:** 2022-09-21

**Last Modified:** 2023-03-20

### **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

---

### CHAPTER 1

#### **Review the Cisco DNA Center Appliance Features 1**

- Appliance Hardware Specifications 1
- Front and Rear Panels 5
- Physical Specifications 18
- Environmental Specifications 19
- Power Specifications 20

---

### CHAPTER 2

#### **Plan the Deployment 23**

- Planning Workflow 23
- Cisco DNA Center and Cisco Software-Defined Access 24
- Interface Cable Connections 24
- Required IP Addresses and Subnets 29
- Required Internet URLs and Fully Qualified Domain Names 32
- Provide Secure Access to the Internet 35
- Required Network Ports 36
- Required Ports and Protocols for Cisco Software-Defined Access 37
- Required Configuration Information 44
- Required First-Time Setup Information 45

---

### CHAPTER 3

#### **Install the Appliance 49**

- Appliance Installation Workflow 49
- Unpack and Inspect the Appliance 49
- Review the Installation Warnings and Guidelines 50
- Review the Rack Requirements 52
- Connect and Power On the Appliance 52
- Check the LEDs 53

---

<b>CHAPTER 4</b>	<b>Prepare the Appliance for Configuration</b>	<b>57</b>
	Preparation for Appliance Configuration Overview	57
	Enable Browser Access to Cisco Integrated Management Controller	58
	Execute Preconfiguration Checks	63
	NIC Bonding Overview	67
	Appliance Support	68
	Enable NIC on an Upgraded Appliance	68
	Reimage the Appliance	74
	Verify the Cisco DNA Center ISO Image	74
	Create a Bootable USB Flash Drive	75
	Using Etcher	76
	Using the Linux CLI	76
	Using the Mac CLI	77
	Reinitialize the Virtual Drives on a Cisco DNA Center Appliance	78
	Install the Cisco DNA Center ISO Image	78
	Cisco DNA Center Appliance Configuration	79

---

<b>CHAPTER 5</b>	<b>Configure the Appliance Using the Maglev Wizard</b>	<b>81</b>
	Appliance Configuration Overview	81
	Configure the Primary Node Using the Maglev Wizard	81
	FIPS Mode Support	102
	Configure a Secondary Node Using the Maglev Wizard	103
	Upgrade to the Latest Cisco DNA Center Release	122

---

<b>CHAPTER 6</b>	<b>Configure the 44/56-Core Appliance Using the Browser-Based Wizard</b>	<b>123</b>
	Appliance Configuration Overview	123
	Browser-Based Configuration Wizards	123
	Browser-Based Wizard Prerequisites	124
	Configure an Appliance Using the Install Configuration Wizard	124
	Configure the Primary Node Using the Advanced Install Configuration Wizard	137
	Configure a Secondary Node Using the Advanced Install Configuration Wizard	156
	Upgrade to the Latest Cisco DNA Center Release	175

---

<b>CHAPTER 7</b>	<b>Configure the 112-Core Appliance Using the Browser-Based Wizard</b>	<b>177</b>
	Appliance Configuration Overview	177
	Browser-Based Configuration Wizards	177
	Browser-Based Wizard Prerequisites	178
	Configure an Appliance Using the Install Configuration Wizard	178
	Configure the Primary Node Using the Advanced Install Configuration Wizard	192
	Configure a Secondary Node Using the Advanced Install Configuration Wizard	209
	Upgrade to the Latest Cisco DNA Center Release	228

---

<b>CHAPTER 8</b>	<b>Complete First-Time Setup</b>	<b>229</b>
	First-Time Setup Workflow	229
	Compatible Browsers	229
	Complete the Quick Start Workflow	229
	Integrate Cisco ISE with Cisco DNA Center	235
	Group-Based Access Control: Policy Data Migration and Synchronization	238
	Configure Authentication and Policy Servers	241
	Configure SNMP Properties	244

---

<b>CHAPTER 9</b>	<b>Troubleshoot the Deployment</b>	<b>245</b>
	Troubleshooting Tasks	245
	Log Out	245
	Reconfigure the Appliance Using the Configuration Wizard	246
	Power Cycle the Appliance	247
	Using the Cisco IMC GUI	248
	Using SSH	248

---

<b>APPENDIX A</b>	<b>Review High Availability Cluster Deployment Scenarios</b>	<b>251</b>
	New HA Deployment	251
	Existing HA Deployment of the Primary Node with Standard Interface Configurations	252
	Existing HA Deployment of Primary Node with Nonstandard Interface Configurations	253
	Activate HA	253
	Additional HA Deployment Considerations	254
	Telemetry	254

Wireless Controller 254



## CHAPTER 1

# Review the Cisco DNA Center Appliance Features

- [Appliance Hardware Specifications, on page 1](#)
- [Front and Rear Panels, on page 5](#)
- [Physical Specifications, on page 18](#)
- [Environmental Specifications, on page 19](#)
- [Power Specifications, on page 20](#)

## Appliance Hardware Specifications

Cisco supplies Cisco Digital Network Architecture (DNA) Center in the form of a rack-mountable, physical appliance. The second-generation Cisco DNA Center appliance consists of either a Cisco Unified Computing System (UCS) C220 M5 small form-factor (SFF) chassis or Cisco UCS C480 M5 chassis, both with the addition of one Intel X710-DA2 network interface card (NIC) and one Intel X710-DA4 NIC. Six versions of the second-generation appliance are available:

- 44-core appliance: Cisco part number DN2-HW-APL
- 44-core promotional appliance: Cisco part number DN2-HW-APL-U
- 56-core appliance: Cisco part number DN2-HW-APL-L
- 56-core promotional appliance: Cisco part number DN2-HW-APL-L-U
- 112-core appliance: Cisco part number DN2-HW-APL-XL
- 112-core promotional appliance: Cisco part number DN2-HW-APL-XL-U

The following tables summarize the appliance's hardware specifications.

**Table 1: 44-Core Cisco DNA Center Appliance Hardware Specifications**

Feature	Description
Chassis	One rack-unit (1RU) chassis.
Processors	Two 22-core Intel 6238 2.1 GHz processors
Memory	Eight 32 GB DDR4 2933 MHz registered DIMMs (RDIMMs)

Feature	Description
Storage	<ul style="list-style-type: none"> <li>• 2 x 480 GB in RAID 1</li> <li>• 2 x 1.9 TB in RAID 1</li> <li>• 6 x 1.9 TB in RAID 10</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 10</li> </ul>
Network and Management I/O	<p>Supported connectors:</p> <ul style="list-style-type: none"> <li>• Two 10-Gbps Ethernet ports on the Intel X710-DA2 NIC</li> <li>• One 1-Gbps RJ-45 management port (Marvell 88E6176)</li> <li>• Two 10GBase-T LOM ports (Intel X550 controller embedded on the motherboard)</li> <li>• Four 1-Gbps/10-Gbps Ethernet ports on the Intel X710-DA4 NIC</li> </ul> <p><b>Note</b> These ports are active only when NIC bonding is enabled on the appliance. For more information, see <a href="#">NIC Bonding Overview, on page 67</a>.</p> <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 VGA (DB-15) 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 (DB-15), and one serial port (RS-232) RJ-45 connector.</li> </ul>
Power	Two 770 W AC power supplies. Redundant as 1+1.
Cooling	Seven 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 512 MB of video memory (8 MB is allocated by default).

Table 2: 56-Core Cisco DNA Center Appliance Hardware Specifications

Feature	Description
Chassis	One rack-unit (1RU) chassis.
Processors	Two 28-core Intel 8280 2.7 GHz processors



Feature	Description
Memory	Twelve 32 GB DDR4 2933 MHz RDIMMs
Storage	<ul style="list-style-type: none"> <li>• 2 x 480 GB in RAID 1</li> <li>• 2 x 1.9 TB in RAID 1</li> <li>• 6 x 1.9 TB in RAID 10</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 10</li> </ul>
Network and Management I/O	<p>Supported connectors:</p> <ul style="list-style-type: none"> <li>• Two 10-Gbps Ethernet ports on the Intel X710-DA2 NIC</li> <li>• One 1-Gbps RJ-45 management port (Marvell 88E6176)</li> <li>• Two 10GBase-T LOM ports (Intel X550 controller embedded on the motherboard)</li> <li>• Four 1-Gbps/10-Gbps Ethernet ports on the Intel X710-DA4 NIC</li> </ul> <p><b>Note</b> These ports are active only when NIC bonding is enabled on the appliance. For more information, see <a href="#">NIC Bonding Overview, on page 67</a>.</p> <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 VGA (DB-15) 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 (DB-15), and one serial port (RS-232) RJ-45 connector.</li> </ul>
Power	Two 770 W AC power supplies. Redundant as 1+1.
Cooling	Seven 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 512 MB of video memory (8 MB is allocated by default).

**Table 3: 112-Core Cisco DNA Center Appliance Hardware Specifications**

Feature	Description
Chassis	Four rack-unit (4RU) chassis.

Feature	Description
Processors	Two CPU modules, each with two 28-core Intel 8276 2.2 GHz processors
Memory	Twenty-four 32 GB DDR4 2933 MHz RDIMMs
Storage	<ul style="list-style-type: none"> <li>• 2 x 480 GB in RAID 1</li> <li>• 2 x 3.8 TB in RAID 1</li> <li>• 16 x 1.9 TB in RAID 10</li> </ul>
Disk Management (RAID)	<ul style="list-style-type: none"> <li>• RAID 1 on drive bays 1 and 2</li> <li>• RAID 10 on slots 3 through 18</li> <li>• RAID 1 on drive bays 19 and 20</li> </ul>
Network and Management I/O	<p>Supported connectors:</p> <ul style="list-style-type: none"> <li>• Two 10 Gbps Ethernet ports on the Intel X710-DA2 NIC</li> <li>• Two 10 Base-T Gbps Ethernet ports</li> <li>• One Gigabit Ethernet management port</li> <li>• Four 1-Gbps/10-Gbps Ethernet ports on the Intel X710-DA4 NIC</li> </ul> <p><b>Note</b> These ports are active only when NIC bonding is enabled on the appliance. For more information, see <a href="#">NIC Bonding Overview, on page 67</a>.</p> <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 VGA (DB-15) connector</li> <li>• Three 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 (DB-15), and one serial port (RS-232) RJ-45 connector.</li> </ul>
Power	<p>Four 1600 W AC power supplies.</p> <p>Redundant as 3+1 (must be configured via the Cisco Integrated Management Controller).</p>
Cooling	Four hot-swappable fan modules with two fans in each for front-to-rear cooling.
Video	VGA video resolution up to 1600 x 1200, 16 bpp at 60 Hz, and up to 256 MB of video memory.

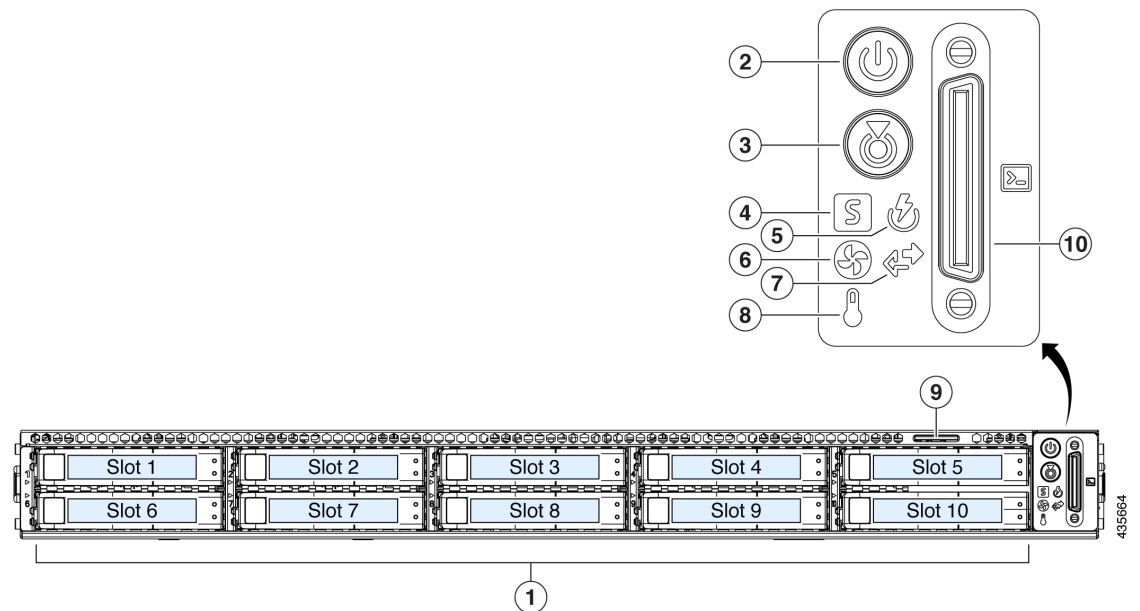
# Front and Rear Panels

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



**Note** If you are viewing this guide on Cisco.com, click any of its figures to view a full-sized version.

**Figure 1: 44 and 56-Core Appliance Front Panel**

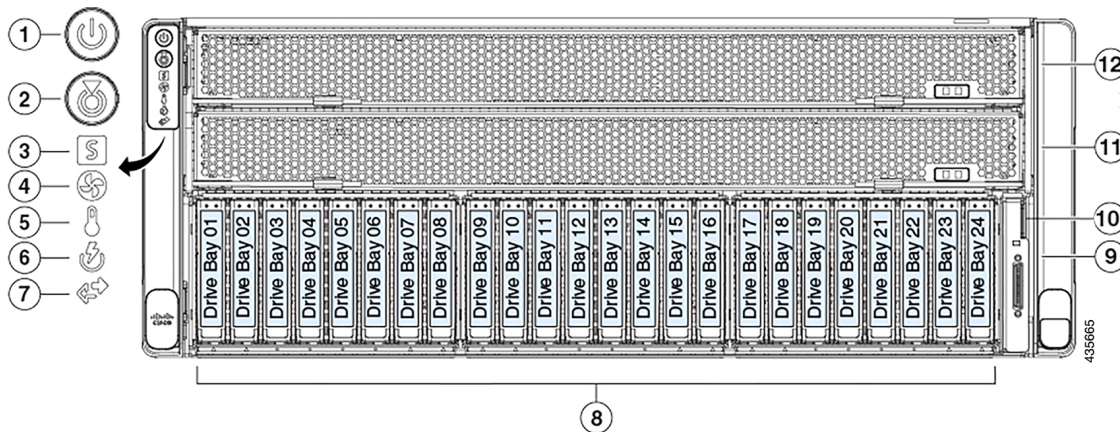


Component	Description
1	<p>A total of 10 drives are available on the appliance:</p> <ul style="list-style-type: none"> <li>• Two 480 GB SAS SSD (in slots 1 and 2).</li> <li>• Eight 1.9 TB SATA SSD (in slots 3 through 10).</li> </ul> <p>Each installed drive has a fault LED and an activity LED.</p> <p>When 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	<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 (Cisco IMC) and some motherboard functions.</li> <li>• Green: The appliance is in main power mode. Power is supplied to all the server components.</li> </ul>
3	<p>Unit identification button and LED. When the LED is:</p> <ul style="list-style-type: none"> <li>• Off: Unit identification is inactive.</li> <li>• Blue: Unit identification is active.</li> </ul>

Component	Description
4	<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, 2 blinks: There is a major fault with the system board.</li> <li>• Amber, 3 blinks: There is a major fault with the memory DIMMs.</li> <li>• Amber, 4 blinks: There is a major fault with the CPUs.</li> </ul>
5	<p>Power supply status LED. When the LED is:</p> <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>
6	<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>
7	<p>Network link activity LED. When the LED is:</p> <ul style="list-style-type: none"> <li>• Off: The Ethernet link is idle.</li> <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> </ul>
8	<p>Temperature status LED. When the LED is:</p> <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>

Component	Description
9	Pull-out asset tag.
10	KVM connector. Used with a KVM cable that provides two USB 2.0, one VGA, and one serial connector.

Figure 2: 112-Core Appliance Front Panel

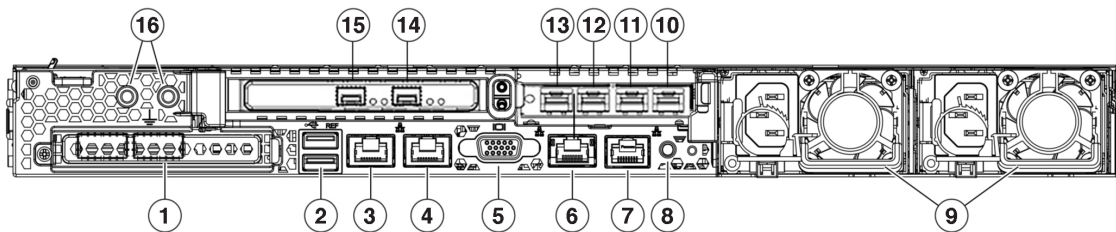


Component	Description
1	Power button/power status LED. When the LED is: <ul style="list-style-type: none"> <li>• Off: There is no AC power to the appliance.</li> <li>• Amber: The appliance is in standby power mode. Power is supplied only to the Cisco IMC and some motherboard functions.</li> <li>• Green: The appliance is in main power mode. Power is supplied to all the server components.</li> </ul>
2	Unit identification button and LED. When the LED is: <ul style="list-style-type: none"> <li>• Off: Unit identification is inactive.</li> <li>• Blue: Unit identification is active.</li> </ul>

Component	Description
3	<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>• 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 causes: <ul style="list-style-type: none"> <li>• Boot failure</li> <li>• Fatal processor and/or bus error detected</li> <li>• Over-temperature condition</li> </ul> </li> </ul>
4	<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: Fan modules are in a degraded state. One fan module has a fault.</li> <li>• Amber, blinking: Two or more fan modules have faults.</li> </ul>
5	<p>Temperature status LED. When the LED is:</p> <ul style="list-style-type: none"> <li>• Green: The appliance is operating at normal temperature. No error conditions detected.</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 non-recoverable threshold.</li> </ul>
6	<p>Power supply status LED. When the LED is:</p> <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>
7	<p>Network link activity LED. When the LED is:</p> <ul style="list-style-type: none"> <li>• Off: The Ethernet LOM port link is idle.</li> <li>• Green: One or more Ethernet LOM ports are link-active, but there is no activity.</li> <li>• Green, blinking: One or more Ethernet LOM ports are link-active, with activity.</li> </ul>

Component	Description
8	<p>A total of 20 drives are available on the appliance:</p> <ul style="list-style-type: none"> <li>• Two 480 GB SATA SSD (in drive bays 1 and 2).</li> <li>• Sixteen 1.9 TB SATA SSD (in slots 3 through 18).</li> <li>• Two 3.8 TB SATA SSD (in drive bays 19 and 20).</li> </ul> <p><b>Note</b> Drive bays 21 through 24 are not used by the appliance.</p> <p>Each installed drive 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>
9	KVM connector. Used with a KVM cable that provides two USB 2.0, one VGA, and one serial connector.
10	Pull-out asset tag.
11	CPU module bay 1.
12	CPU module bay 2.

**Figure 3: 44 and 56-Core Appliance Rear Panel**



**Note** If NIC bonding has been enabled on your Cisco DNA Center appliance, two instances of the Enterprise, Intracluster, Management, and Internet port are available to configure and use. See [NIC Bonding Overview, on page 67](#) for more information.



Callout	Description
1	Modular LAN-on-motherboard (mLOM) card bay (x16 PCIe lane)
2	Two USB 3.0 ports
3, 10	<p>1-Gbps/10-Gbps Management Port (Network Adapter 3): This Ethernet port can support 1 Gbps and 10 Gbps, depending on the link partner capability. It is identified as Network Adapter 3 in the Maglev Configuration wizard. Connect this port to a switch that provides access to your enterprise management network.</p> <ul style="list-style-type: none"> <li>• The primary instance (callout 3) is labeled <b>1</b> on the rear panel.</li> <li>• The secondary instance (callout 10) is the fourth port on the Intel X710-DA4 NIC in the appliance's PCIe riser 2/slot 2.</li> </ul> <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>• Off: No link is present.</li> <li>• Green, blinking: Traffic is present on the active link.</li> <li>• Green: Link is active, but there is no traffic present.</li> </ul> <p>When the speed LED is:</p> <ul style="list-style-type: none"> <li>• Off: Link speed is 10 Mbps or less.</li> <li>• Green: Link speed is 1 Gbps.</li> <li>• Amber: Link speed is 100 Mbps.</li> </ul>
4, 11	<p>1-Gbps/10-Gbps Internet Port (Network Adapter 4): This Ethernet port can support 1 Gbps and 10 Gbps, depending on the link partner capability. It is identified as Network Adapter 4 in the Maglev Configuration wizard. This port is optional and is used for connecting to the Internet when it is not possible to do so via the 10-Gbps Enterprise port. Connect to the Internet or a proxy server that has connections to the Internet.</p> <ul style="list-style-type: none"> <li>• The primary instance (callout 4) is labeled <b>2</b> on the rear panel.</li> <li>• The secondary instance (callout 11) is the third port on the Intel X710-DA4 NIC in the appliance's PCIe riser 2/slot 2.</li> </ul> <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>• Off: No link is present.</li> <li>• Green, blinking: Traffic is present on the active link.</li> <li>• Green: Link is active, but there is no traffic.</li> </ul> <p>When the speed LED is:</p> <ul style="list-style-type: none"> <li>• Off: Link speed is 10 Mbps or less.</li> <li>• Green: Link speed is 1 Gbps.</li> <li>• Amber: Link speed is 100 Mbps.</li> </ul>

Callout	Description
5	VGA video port (DB-15).
6	<p>1-Gbps Cisco IMC Port: This is the embedded port to the right of the VGA video port and to the left of the RJ45 serial port. It is assigned an IP address when you enable browser access to the appliance's Cisco IMC GUI (see <a href="#">Enable Browser Access to Cisco Integrated Management Controller</a>). This port is reserved for out-of-band management of the appliance chassis and software. Connect this port to a switch that provides access to your 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>• Off: No link is present.</li> <li>• Green, blinking: Traffic is present on the active link.</li> <li>• Green: Link is active, but there is no traffic present.</li> </ul> <p>When the speed LED is:</p> <ul style="list-style-type: none"> <li>• Off: Link speed is 10 Mbps or less.</li> <li>• Green: Link speed is 1 Gbps.</li> <li>• Amber: Link speed is 100 Mbps.</li> </ul>
7	Serial port (RJ-45 connector)
8	Rear unit identification button and LED
9	<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>• Off: There is no AC power to the power supply.</li> <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> </ul> <p>For more details, see <a href="#">Power Specifications</a>.</p>

Callout	Description
12, 15	<p>10-Gbps Enterprise Port (Network Adapter 1): This port is identified as Network Adapter 1 in the Maglev Configuration wizard. Connect it to a switch with connections to the Enterprise network.</p> <ul style="list-style-type: none"> <li>• The primary instance (callout 15) is the left-hand port on the Intel X710-DA2 NIC in the appliance's PCIe riser 1/slot 1.</li> <li>• The secondary instance (callout 12) is the second port on the Intel X710-DA4 NIC in the appliance's PCIe riser 2/slot 2.</li> </ul> <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>• Off: No link is present.</li> <li>• Green, blinking: Traffic is present on the active link.</li> <li>• Green: Link is active, but there is no traffic present.</li> </ul> <p>When the speed LED is:</p> <ul style="list-style-type: none"> <li>• Off: Link speed is 100 Mbps or less.</li> <li>• Green: Link speed is 10 Gbps.</li> <li>• Amber: Link speed is 1 Gbps.</li> </ul> <p><b>Note</b> Although capable of operating at lower speeds, this port is intended to operate at 10 Gbps only.</p>

Callout	Description
13, 14	<p>10-Gbps Intracluster Port (Network Adapter 2): This port is identified as Network Adapter 2 in the Maglev Configuration wizard. Connect this port to a switch with connections to the other nodes in the cluster.</p> <ul style="list-style-type: none"> <li>The primary instance (callout 14) is the right-hand port on the Intel X710-DA2 NIC in the appliance PCIe riser 1/slot 1.</li> <li>The secondary instance (callout 13) is first port on the Intel X710-DA4 NIC in the appliance's PCIe riser 2/slot 2.</li> </ul> <p>This port is located on the Intel X710-DA4 NIC, which is located in the appliance's PCIe riser 2/slot 2.</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>Off: No link is present.</li> <li>Green, blinking: Traffic is present on the active link.</li> <li>Green: Link is active, but there is no traffic present.</li> </ul> <p>When the link speed LED is:</p> <ul style="list-style-type: none"> <li>Off: Link speed is 100 Mbps or less.</li> <li>Green: Link speed is 10 Gbps.</li> <li>Amber: Link speed is 1 Gbps.</li> </ul> <p><b>Note</b> Although capable of operating at lower speeds, this port is intended to operate at 10 Gbps only.</p>
16	Threaded holes for dual-hole grounding lug.

Figure 4: 112-Core Appliance Rear Panel

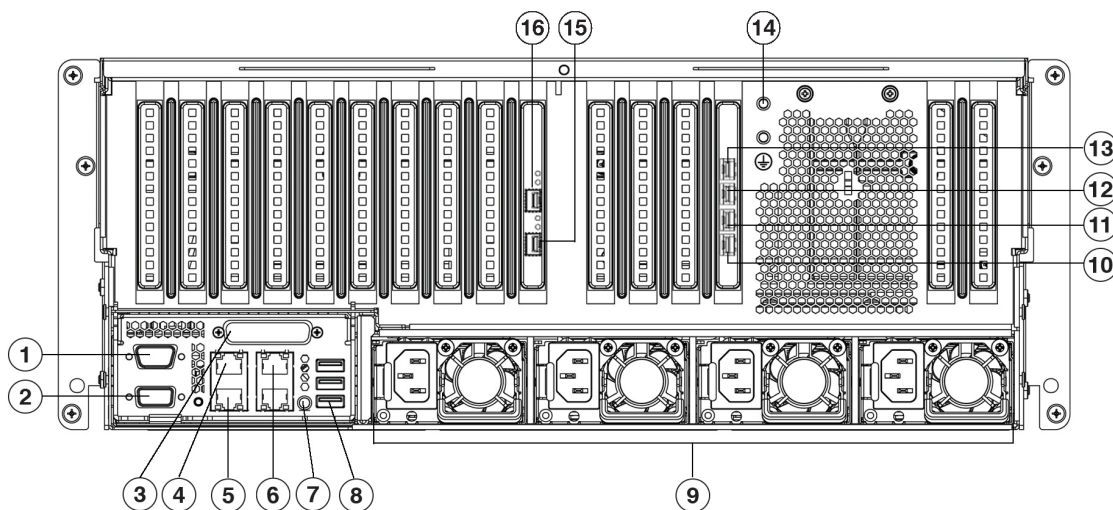
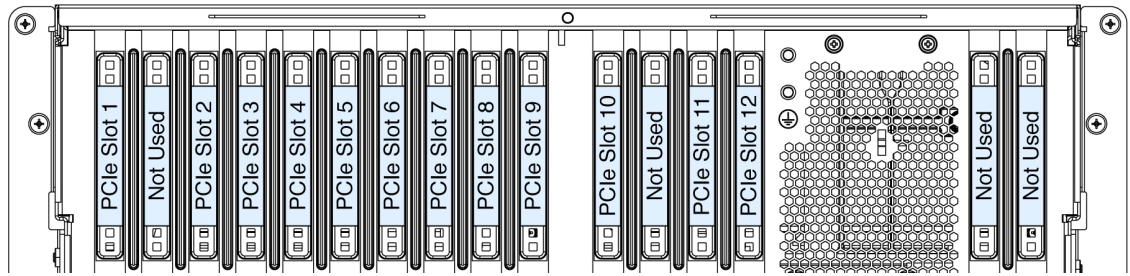


Figure 5: 112-Core Appliance Rear Panel Slots



**Note** If NIC bonding has enabled on your Cisco DNA Center appliance, two instances of the Enterprise, Intracluster, Management, and Internet port are available to configure and use. See [NIC Bonding Overview, on page 67](#) for more information.

Callout	Description
1	Serial port COM 1 (DB-9 connector)
2	VGA video port (DB-15 connector)
3	Not used at this time
4, 13	<p>1-Gbps/10-Gbps Management Port (Network Adapter 3): This Ethernet port can support 1 Gbps and 10 Gbps, depending on the link partner capability. It is identified as Network Adapter 3 in the Maglev Configuration wizard. Connect this port to a switch that provides access to your enterprise management network.</p> <ul style="list-style-type: none"> <li>The primary instance (callout 4) is labeled <b>1</b> on the rear panel.</li> <li>The secondary instance (callout 13) is the top port on the Intel X710-DA4 NIC in the appliance's PCIe riser 2/slot 12.</li> </ul> <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>Off: No link is present.</li> <li>Green, blinking: Traffic is present on the active link.</li> <li>Green: Link is active, but there is no traffic present.</li> </ul> <p>When the speed LED is:</p> <ul style="list-style-type: none"> <li>Off: Link speed is 10 Mbps or less.</li> <li>Green: Link speed is 1 Gbps.</li> <li>Amber: Link speed is 100 Mbps.</li> </ul>

Callout	Description
5, 12	<p>1-Gbps/10-Gbps Internet Port (Network Adapter 4): This Ethernet port can support 1 Gbps and 10 Gbps, depending on the link partner capability. It is identified as Network Adapter 4 in the Maglev Configuration wizard. This port is optional and is used for connecting to the Internet when it is not possible to do so via the 10-Gbps Enterprise port. Connect to the Internet or a proxy server that has connections to the Internet.</p> <ul style="list-style-type: none"> <li>• The primary instance (callout 5) is labeled <b>2</b> on the rear panel.</li> <li>• The secondary instance (callout 12) is the second port from the top on the Intel X710-DA4 NIC in the appliance's PCIe riser 2/slot 12.</li> </ul> <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>• Off: No link is present.</li> <li>• Green, blinking: Traffic is present on the active link.</li> <li>• Green: Link is active, but there is no traffic.</li> </ul> <p>When the speed LED is:</p> <ul style="list-style-type: none"> <li>• Off: Link speed is 10 Mbps or less.</li> <li>• Green: Link speed is 1 Gbps.</li> <li>• Amber: Link speed is 100 Mbps.</li> </ul>
6	<p>1-Gbps Cisco IMC Port: This is the 10/100/1000 Ethernet dedicated management port (Base-T), which is located to the right of the Management port. It is identified as <b>3</b> on the rear panel. This port is assigned an IP address when you enable browser access to the appliance's Cisco IMC GUI (see <a href="#">Enable Browser Access to Cisco Integrated Management Controller</a>). It is reserved for out-of-band management of the appliance chassis and software. Connect this port to a switch that provides access to your 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>• Off: No link is present.</li> <li>• Green, blinking: Traffic is present on the active link.</li> <li>• Green: Link is active, but there is no traffic present.</li> </ul> <p>When the speed LED is:</p> <ul style="list-style-type: none"> <li>• Off: Link speed is 10 Mbps or less.</li> <li>• Green: Link speed is 1 Gbps.</li> <li>• Amber: Link speed is 100 Mbps.</li> </ul>
7	Rear identification button/LED
8	Three USB 3.0 ports
9	<p>Power supplies 1 – 4: hot-swappable and redundant as 3+1 (configured in Cisco IMC).</p> <p>See <a href="#">Power Specifications</a> for more information.</p>

Callout	Description
10, 15	<p>10-Gbps Intracluster Port (Network Adapter 2): This port is identified as Network Adapter 2 in the Maglev Configuration wizard. Connect this port to a switch with connections to the other nodes in the cluster.</p> <ul style="list-style-type: none"> <li>• The primary instance (callout 15) is the bottom port on the Intel X710-DA2 NIC in the appliance PCIe riser 1/slot 9.</li> <li>• The secondary instance (callout 10) is the bottom port on the Intel X710-DA4 NIC in the appliance's PCIe riser 2/slot 12.</li> </ul> <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>• Off: No link is present.</li> <li>• Green, blinking: Traffic is present on the active link.</li> <li>• Green: Link is active, but there is no traffic present.</li> </ul> <p>When the link speed LED is:</p> <ul style="list-style-type: none"> <li>• Off: Link speed is 100 Mbps or less.</li> <li>• Green: Link speed is 10 Gbps.</li> <li>• Amber: Link speed is 1 Gbps.</li> </ul> <p><b>Note</b> Although capable of operating at lower speeds, this port is intended to operate at 10 Gbps only.</p>

Callout	Description
11, 16	<p>10-Gbps Enterprise Port (Network Adapter 1): This port is identified as Network Adapter 1 in the Maglev Configuration wizard. If NIC bonding is enabled on your appliance, connect this port to a switch with connections to the enterprise network.</p> <ul style="list-style-type: none"> <li>The primary instance (callout 16) is the top port on the Intel X710-DA2 NIC in the appliance PCIe riser 1/slot 9.</li> <li>The secondary instance (callout 11) is the third port from the top on the Intel X710-DA4 NIC in the appliance's PCIe riser 2/slot 12.</li> </ul> <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>Off: No link is present.</li> <li>Green, blinking: Traffic is present on the active link.</li> <li>Green: Link is active, but there is no traffic present.</li> </ul> <p>When the speed LED is:</p> <ul style="list-style-type: none"> <li>Off: Link speed is 100 Mbps or less.</li> <li>Green: Link speed is 10 Gbps.</li> <li>Amber: Link speed is 1 Gbps.</li> </ul> <p><b>Note</b> Although capable of operating at lower speeds, this port is intended to operate at 10 Gbps only.</p>
14	Threaded holes for dual-hole grounding lug.

## Physical Specifications

The following table lists the physical specifications for the appliance. Unless indicated, the specifications apply to the 44, 56, and 112-core appliances.

**Table 4: Physical Specifications**

Description	Specification
Height	44 and 56-core appliance: 1.7 in. (4.32 cm) 112-core appliance: 6.9 in. (17.6 cm)
Width	44 and 56-core appliance: <ul style="list-style-type: none"> <li>Without handles: 16.9 in. (43.0 cm)</li> <li>Including handles: 19.0 in. (48.3 cm)</li> </ul> 112-core appliance: 19.0 in. (48.3 cm)



Description	Specification
Depth (length)	44 and 56-core appliance: <ul style="list-style-type: none"> <li>• Without handles: 29.8 in. (75.6 cm)</li> <li>• Including handles: 30.98 in. (78.7 cm)</li> </ul> 112-core appliance: 32.7 in. (83.1 cm)
Front Clearance	3 in. (76 mm)
Side Clearance	1 in. (25 mm)
Rear Clearance	6 in. (152 mm)
Maximum weight (fully loaded chassis)	44 and 56-core appliance: 37.5 lb. (17.0 kg) 112-core appliance: 146 lb. (66.2 kg)

## Environmental Specifications

The following table lists the environmental specifications for the Cisco DNA Center appliance. Unless indicated, the specifications apply to the 44, 56, and 112-core appliances.

**Table 5: 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 (RH), nonoperating (when the appliance is stored or transported)	5 to 93% at 82°F (28°C)
Altitude, operating	0 to 10,000 ft. (0 to 3,048 m)
Altitude, nonoperating (when the appliance is stored or transported)	0 to 40,000 ft. (0 to 12,192 m)

Description	Specification
Sound power level, measure A-weighted per ISO7779 LwAd (Bels), operation at 73°F (23°C)	44 and 56-core appliance: 5.5 112-core appliance: <ul style="list-style-type: none"> <li>• Minimum configuration: 7.08</li> <li>• Typical configuration: 7.67</li> <li>• Maximum configuration: 8.24</li> </ul>
Sound pressure level, measure A-weighted per ISO7779 LpAm (dBA), Operation at 73°F (23°C)	44 and 56-core appliance: 40 112-core appliance: <ul style="list-style-type: none"> <li>• Minimum configuration: 57.6</li> <li>• Typical configuration: 63.5</li> <li>• Maximum configuration: 70.5</li> </ul>

## Power Specifications

The specifications for the power supplies provided with the Cisco DNA Center appliance are listed in the table below. The 44 and 56-core appliance ships with two 770 W power supplies (Cisco part number UCSC-PSU1-770W) and the 112-core appliance ships with four 1600 W AC power supplies (Cisco part number UCSC-PSU1-1600W). Unless indicated, the specifications apply to both power supplies.

**Table 6: AC Power Supply Specifications**

Description	Specification
AC input voltage	770 W: <ul style="list-style-type: none"> <li>• Nominal range: 100–120 VAC, 200–240 VAC</li> <li>• Range: 90–132 VAC, 180–264 VAC</li> </ul> 1600 W: <ul style="list-style-type: none"> <li>• Nominal range: 200–240 VAC</li> <li>• Range: 180–264 VAC</li> </ul>
AC input frequency	Nominal range: 50 to 60 Hz (Range: 47–63 Hz)

Description	Specification
Maximum AC input current	770 W: <ul style="list-style-type: none"> <li>• 9.5 A at 100 VAC</li> <li>• 4.5 A at 208 VAC</li> </ul> 1600 W: 9.5 A at 200 VAC
Maximum input volt-amperes	770 W: 950 VA at 100 VAC 1600 W: 1250 VA at 200 VAC
Maximum output power per PSU	770 W: 100–120 VAC 1600 W: 200–240 VAC
Maximum inrush current	770 W: 15 A at 35° C 1600 W: 30 A at 35° C
Maximum hold-up time	770 W: 12 ms 1600 W: 80 ms
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>





## CHAPTER 2

# Plan the Deployment

---

- [Planning Workflow](#), on page 23
- [Cisco DNA Center and Cisco Software-Defined Access](#), on page 24
- [Interface Cable Connections](#), on page 24
- [Required IP Addresses and Subnets](#), on page 29
- [Required Internet URLs and Fully Qualified Domain Names](#), on page 32
- [Provide Secure Access to the Internet](#), on page 35
- [Required Network Ports](#), on page 36
- [Required Ports and Protocols for Cisco Software-Defined Access](#), on page 37
- [Required Configuration Information](#), on page 44
- [Required First-Time Setup Information](#), on page 45

## 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 a switch that provides the following types of network access. At a minimum, you must configure the Enterprise and Intracluster port interfaces, as they are required for Cisco DNA Center functionality.

When NIC bonding is enabled on an appliance, a secondary instance of the Enterprise, Intracluster, Management, and Internet ports resides on the Intel X710-DA4 NIC. Connect these ports to a switch that's different from the one that you will connect the primary instance of these ports to (see [NIC Bonding Overview, on page 67](#)).

**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, assign the Intracluster port as the Cluster Link.
- 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 74](#).) 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 (Network Adapter 1):** The purpose of this port 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.

Primary instance:

- On the 44- and 56-core appliance, this is the left-hand port on the Intel X710-DA2 NIC that resides in PCIe slot 1.
- On the 112-core appliance, this is the top 10-Gbps port on the Intel X710-DA2 NIC that resides in PCIe slot 9.

Secondary instance:

- On the 44- and 56-core appliance, this is the second port on the Intel X710-DA4 NIC that resides in PCIe slot 2.
- On the 112-core appliance, this is the third 10-Gbps port from the top on the Intel X710-DA4 NIC that resides in PCIe slot 12.

- **(Required) 10-Gbps Intracluster Port (Network Adapter 2):** The purpose of this port is to enable communications among the primary and secondary nodes in a 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.

Primary instance:

- On the 44- and 56-core appliance, this is the right-hand port on the Intel X710-DA2 NIC that resides in PCIe slot 1.
- On the 112-core appliance, this is the bottom 10-Gbps port on the Intel X710-DA2 NIC that resides in PCIe slot 9.

Secondary instance:

- On the 44- and 56-core appliance, this is the first port on the Intel X710-DA4 NIC that resides in PCIe slot 2.
- On the 112-core appliance, this is the bottom 10-Gbps port on the Intel X710-DA4 NIC that resides in PCIe slot 12.

- **(Optional) 1-Gbps/10-Gbps Management Port (Network Adapter 3):** This port provides access to the Cisco DNA Center GUI, allowing 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.

Primary instance: Labeled **1** on the appliance's rear panel.

Secondary instance:

- On the 44- and 56-core appliance, this is the fourth port on the Intel X710-DA4 NIC that resides in PCIe slot 2.
- On the 112-core appliance, this is the top 10-Gbps port on the Intel X710-DA4 NIC that resides in PCIe slot 12.

- **(Optional) 1-Gbps/10-Gbps Internet Port (Network Adapter 4):** This port, labeled **2** on the rear panel, 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 (Network Adapter 1). If you need to use this port, connect it to a switch with connections to your Internet proxy server and configure one IP address with a subnet mask for the port.

Primary instance: Labeled **2** on the appliance's rear panel.

Secondary instance:

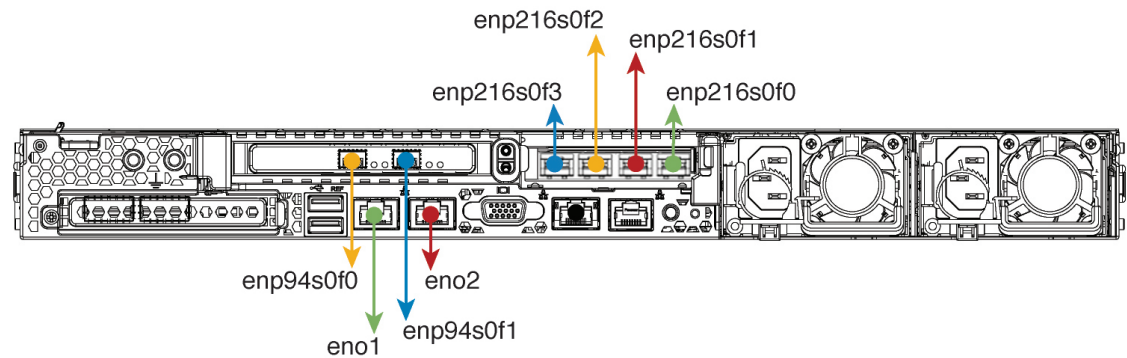
- On the 44- and 56-core appliance, this is the third port on the Intel X710-DA4 NIC that resides in PCIe slot 2.
- On the 112-core appliance, this is the second 10-Gbps port from the top on the Intel X710-DA4 NIC that resides in PCIe slot 12.

- **(Optional, but strongly recommended) 1-Gbps Cisco IMC Port:** This port provides browser access to the Cisco Integrated Management Controller (Cisco IMC) 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 figures show the recommended connections for a single-node Cisco DNA Center cluster, as well as the label that's assigned to each interface:



**Figure 6: Recommended Cabling for 44- and 56-Core Appliance**



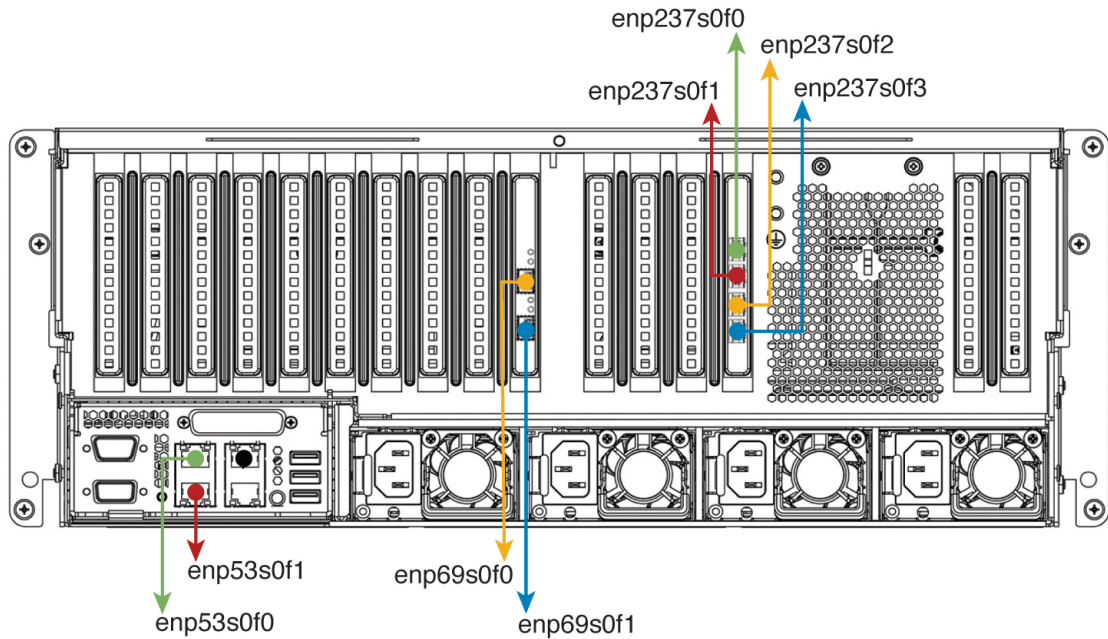
### Legend

- 10-Gbps Enterprise Port (Network Adapter 1)
- 10-Gbps Intracluster Port (Network Adapter 2)
- 1-Gbps/10-Gbps Management Port (Network Adapter 3)
- 1-Gbps/10-Gbps Internet Port (Network Adapter 4)
- 1-Gbps Cisco IMC Port



**Note** For both the Management and Internet interface, their primary instance has a bandwidth of 1 Gbps and their secondary instance 10 Gbps.

Figure 7: Recommended Cabling for 112-Core Appliance



#### Legend

- 10-Gbps Enterprise Port (Network Adapter 1)
- 10-Gbps Intracluster Port (Network Adapter 2)
- 1-Gbps/10-Gbps Management Port (Network Adapter 3)
- 1-Gbps/10-Gbps Internet Port (Network Adapter 4)
- 1-Gbps Cisco IMC Port



**Note** For both the Management and Internet interface, their primary instance has a bandwidth of 1 Gbps and their secondary instance 10 Gbps.

The connections for each node in a three-node Cisco DNA Center cluster are the same as those for a single-node cluster and use the same ports. Do the following when you cable a three-node cluster:

- Connect the primary instance of each node's Enterprise, Intracluster, Management, and Internet Port, as well as the Cisco IMC port, to the primary switch.
- Connect the secondary instance of each node's Enterprise, Intracluster, Management, and Internet Port to the secondary switch.



**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, note that the ports support only the following media types:

- SFP-10G-SR-S (Short range, MMF)
- 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.
- **Internet 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 Internet 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:

- **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 Internet. 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 VIP address. However, if you decide to do so, you must specify a VIP 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.
- **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](#).
- **DNS Server IP Addresses:** The IP address for one or more of your network's preferred Domain Name System (DNS) servers. During configuration, you can specify multiple DNS server IP addresses by entering them as a space-separated list.
- **(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 an 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 static routes where needed, to allow the appliance access to particular parts of the network that can be reached no other way.

- **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.

Specify these NTP servers during preflight hardware synchronization, and again during the configuration of the software on each appliance in the cluster. Time synchronization is critical to the accuracy of data and the coordination of processing across a multihost cluster. Before deploying the appliance in a production environment, make sure that the time on the appliance system clock is current and that the NTP servers you specified are keeping accurate time. If you are planning to integrate the appliance with ISE, you should also ensure that ISE is synchronizing with the same NTP servers as the appliance.

- **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 [Reimage the Appliance](#) for more information).

- 
- **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 [Reimage the Appliance](#) for more information).
- When entering an IP address for the Cluster port, container subnet, or cluster subnet, don't specify an address that falls within the 169.254.0.0/23 subnet.

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. The Cisco DNA Center internal services require a dedicated set of IP addresses to operate (a Cisco DNA Center microservice architecture requirement). To accommodate this requirement, you must allocate two dedicated subnets for each 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 forces the appliance to run Virtual Routing and Forwarding (VRF) FIBs internally. This leads to multiple encaps and 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 for each 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 running out of IP addresses 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 7: 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>• <a href="https://www.ciscoconnectdna.com">https://www.ciscoconnectdna.com</a></li> <li>• <a href="https://cdn.ciscoconnectdna.com">https://cdn.ciscoconnectdna.com</a></li> <li>• <a href="https://registry.ciscoconnectdna.com">https://registry.ciscoconnectdna.com</a></li> <li>• <a href="https://registry-cdn.ciscoconnectdna.com">https://registry-cdn.ciscoconnectdna.com</a></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>
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>

In order to...	...Cisco DNA Center must access these URLs and FQDNs
Integrate with Cisco Meraki.	Recommended: *.meraki.com:443 Customers who want to avoid wildcards can specify these URLs instead: <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
Integrate with cisco.com and Cisco Smart Licensing.	*.cisco.com:443 Customers who want to avoid wildcards can specify these URLs instead: <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



In order to...	...Cisco DNA Center must access these URLs and FQDNs
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.euc1.prd.kairos.ciscolabs.com">https://api.euc1.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 8: 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
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

Port Number	Permitted Traffic	Protocol (TCP or UDP)
21730	Application Visibility Service (used for CBAR device communication)	UDP
32767	NFS (used for Assurance backups)	TCP and UDP

Table 9: 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
443	HTTPS	TCP
5222, 8910	Cisco ISE XMP for PxGrid	TCP
9060	Cisco ISE ERS API traffic	TCP

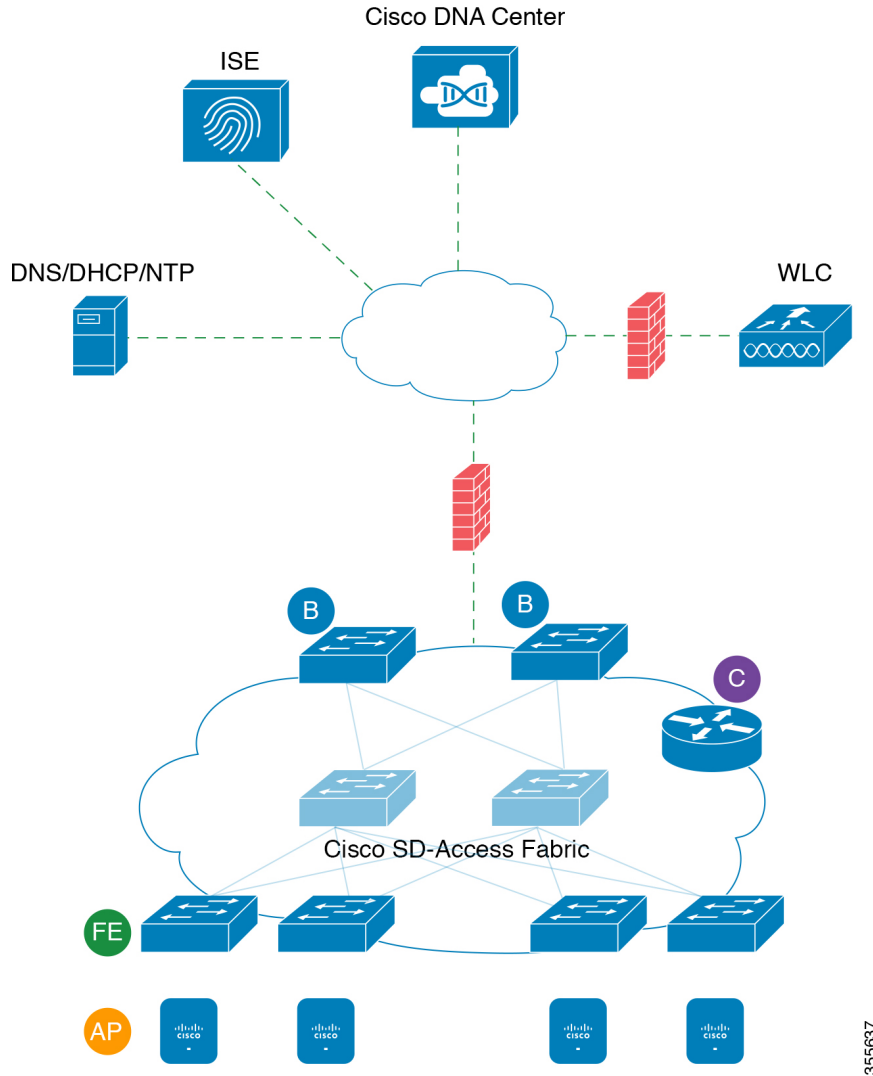


**Note** Additionally, you can configure your network to allow outgoing IP traffic from the appliance to the Cisco addresses at: <https://www.cisco.com/security/pki/>. The appliance uses the IP addresses listed at the above URL to access Cisco-supported certificates and trust pools.

## 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 8: 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 10: 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	From Cisco DNA Center to fabric switches for software upgrades (also to the internet if there is no proxy)
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 11: 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 12: 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 13: 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 14: 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 15: 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 16: 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 17: 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 18: 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 [Complete the Quick Start Workflow, on page 229](#)). 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.

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

The Cisco IMC 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 229](#).

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 241](#).

- **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 49
- [Unpack and Inspect the Appliance](#), on page 49
- [Review the Installation Warnings and Guidelines](#), on page 50
- [Review the Rack Requirements](#), on page 52
- [Connect and Power On the Appliance](#), on page 52
- [Check the LEDs](#), on page 53

## 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.

After you have completed all of these tasks successfully, continue with the steps described in [Preparation for Appliance Configuration Overview](#).

## 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



---

**Note** Before you install, operate, or service a server, review the [Regulatory Compliance and Safety Information for Cisco UCS C-Series Servers](#) for important safety information.

---



---

**Warning** **IMPORTANT SAFETY INSTRUCTIONS**

**This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.**

Statement 1071

---



---

**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

---





---

**Warning** This unit is intended for installation in restricted access areas. A restricted access area can be accessed only through the use of a special tool, lock, and key, or other means of security.

Statement 1017

---

The following four warnings are specific to the 112-core appliance:



---

**Warning** This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.

Statement 1024

---



---

**Warning** For Nordic countries (Norway, Finland, Sweden and Denmark) this system must be installed in a Restricted Access Location, where the voltage of the main ground connection of all equipment is the same (equipotential earth) and the system is connected to a grounded electrical outlet.

Statement 328

---



---

**Warning** High leakage current – earth connection essential before connection to system power supply.

Statement 342

---



---

**Warning** This equipment must be externally grounded using a customer-supplied ground wire before power is applied. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.

Statement 366

---



---

**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 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 UPS models that use ferroresonant technology. These UPS models can become unstable with systems such as the Cisco UCS, which can have substantial current-draw fluctuations because of fluctuating data traffic patterns.

---

When you install 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 the recommended site planning and preparation tasks.
- Ensure that there is adequate space around the appliance to enable servicing, and for adequate airflow. The airflow in this appliance is from front to back.
- Ensure that the site's air-conditioning meets the thermal requirements listed in [Environmental Specifications](#).
- Ensure that the cabinet or rack meets the requirements listed in [Review the Rack Requirements](#).
- Ensure that the site's power meets the requirements listed in [Power Specifications](#). If available, 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:
  - For the 44 and 56-core appliance, one RU, which equals 1.75 in. (44.45 mm).
  - For the 112-core appliance, four RUs, which equals 7.0 in. (177.8 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 a 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](#) for details.

**Note** For the 44 and 56-core appliance, you can use either one or both of the power supplies that come with the appliance. For the 112-core appliance, use at least 3 of its 4 power supplies.

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

The Power Status LED indicates the appliance's power status:

- 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 the appliance components.

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

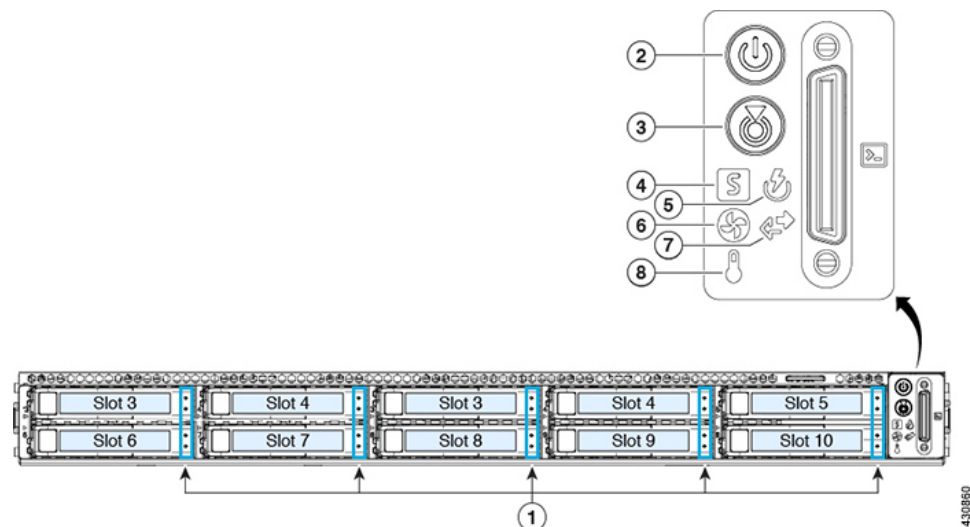
- Step 2** Connect a USB keyboard and VGA monitor to the server, using the supplied KVM cable connected to the KVM connector on the front panel. Alternatively, you can use the VGA and USB ports on the rear panel. You can only connect to one VGA interface at a time.

## Check the LEDs

After you have powered up the 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.

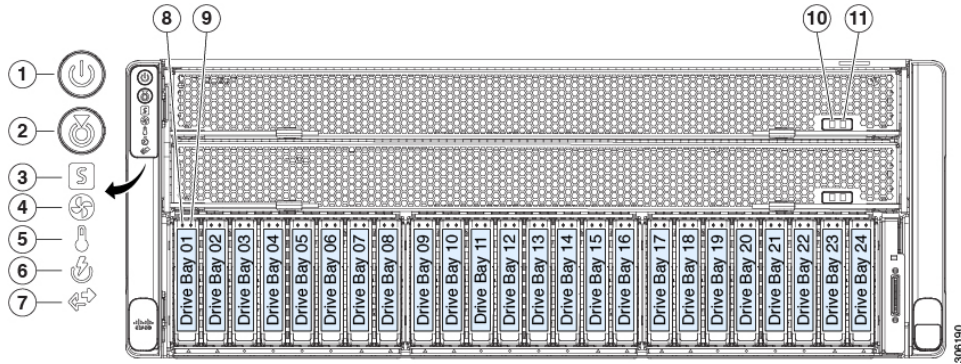
**Figure 9: 44 and 56-Core Appliance Front Panel LEDs**



LED	Desired Status Indicator
1	<ul style="list-style-type: none"> <li>• Drive Fault LEDs: Off</li> <li>• Drive Activity LEDs: Green</li> </ul>
2	Power Status: Green
3	Unit identification: Off
4	System Status: Green
5	Power Supply Status: Green
6	Fan Status: Green
7	Network Link Activity: Off

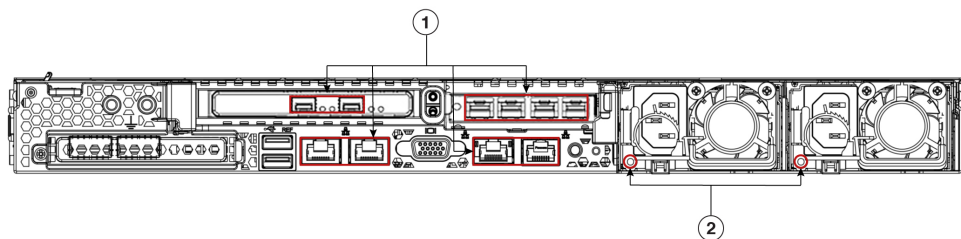
LED	Desired Status Indicator
8	Temperature Status: Green

Figure 10: 112-Core Appliance Front Panel LEDs



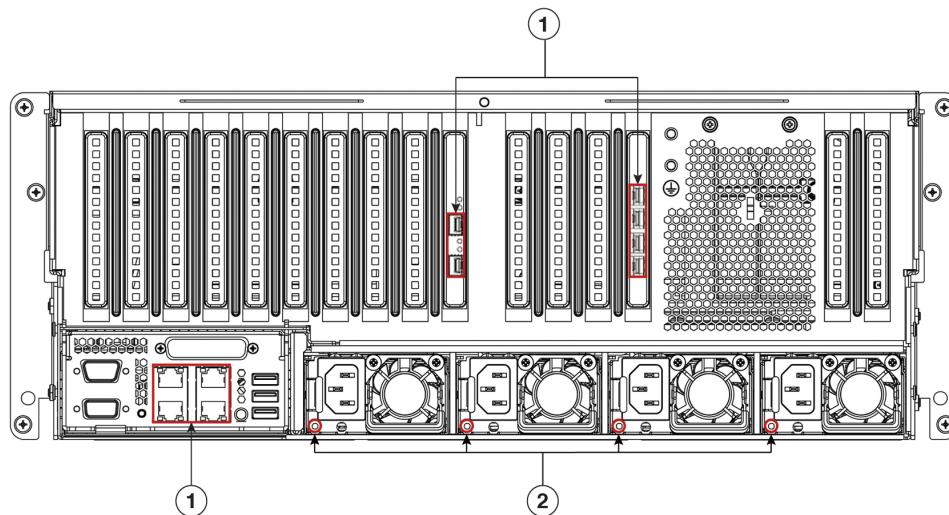
LED	Desired Status Indicator
1	Power Status: Green
2	Unit identification: Off
3	System Status: Green
4	Fan Status: Green
5	Temperature Status: Green
6	Power Supply Status: Green
7	Network Link Activity: Off
8	Drive Fault LEDs: Off
9	Drive Activity LEDs: Green
10	CPU module power status: Green
11	CPU module fault: Off

Figure 11: 44 and 56-Core Appliance Rear Panel LEDs



LED	Desired Status Indicator
1	After initial power-up, all the ports should have their Link Status and Link Speed LEDs showing as off.  After network settings are configured and tested using either the Maglev Configuration wizard (see <a href="#">Configure the Primary Node Using the Maglev Wizard</a> and <a href="#">Configure a Secondary Node Using the Maglev Wizard</a> ) or browser-based configuration wizard (see <a href="#">Configure the Primary Node Using the Advanced Install Configuration Wizard, on page 137</a> and <a href="#">Configure a Secondary Node Using the Advanced Install Configuration Wizard, on page 156</a> ), the Link Status and Link Speed LEDs for all <b>cabled</b> ports should be green. The LED for all <b>uncabled</b> ports should remain unchanged.
2	AC Power Supply Status LEDs: Green

Figure 12: 112-Core Appliance Rear Panel LEDs



LED	Desired Status Indicator
1	After initial power-up, all the ports should have their Link Status and Link Speed LEDs showing as off.  After network settings are configured and tested using either the Maglev Configuration wizard (see <a href="#">Configure the Primary Node Using the Maglev Wizard</a> and <a href="#">Configure a Secondary Node Using the Maglev Wizard</a> ) or browser-based configuration wizard (see <a href="#">Configure the Primary Node Using the Advanced Install Configuration Wizard, on page 192</a> and <a href="#">Configure a Secondary Node Using the Advanced Install Configuration Wizard, on page 209</a> ), the Link Status and Link Speed LEDs for all <b>cabled</b> ports should be green. All <b>uncabled</b> port LEDs should be unchanged.
2	AC Power Supply Status LEDs: Green

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 57
- [Enable Browser Access to Cisco Integrated Management Controller](#), on page 58
- [Execute Preconfiguration Checks](#), on page 63
- [NIC Bonding Overview](#), on page 67
- [Reimage the Appliance](#), on page 74
- [Cisco DNA Center Appliance Configuration](#), on page 79

## 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. If the Intel X710-DA4 network interface card (NIC) that shipped with your appliance is currently disabled, you need to enable it in order to make use of NIC bonding (see [Enable NIC on an Upgraded Appliance, on page 68](#)).
4. 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 the "Appliance Configuration Overview" topic specific to the configuration wizard you want to use:

- [Appliance Configuration Overview](#)
  - [Appliance Configuration Overview](#)
  - [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:

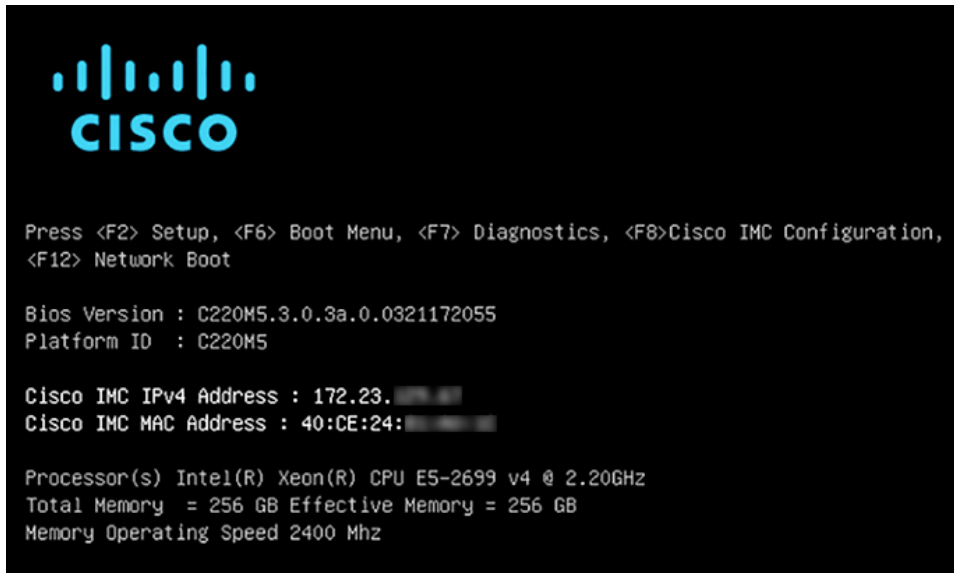
- A KVM cable to the KVM connector on the appliance's front panel (component 11 on the front panel illustrated in [Front and Rear Panels](#))
- A keyboard and monitor to the USB and VGA ports on the appliance's rear panel (components 2 and 5, respectively, on the rear panel illustrated in [Front and Rear Panels](#)).

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

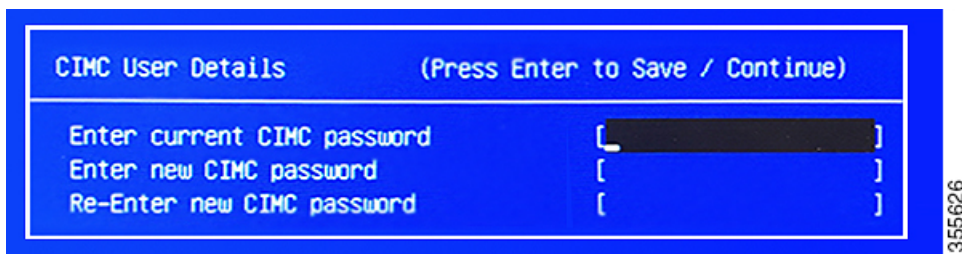
**Step 3** Press the **Power** button on the front panel to boot the appliance.

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





- 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.



- 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:
  Riser1:       [ ]                   Active-active:  [ ]
  Riser2:       [ ]                   VLAN (Advanced)
  MLom:         [ ]                   VLAN enabled:   [ ]
  Shared LOM Ext: [ ]                 VLAN ID:        1
                                           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:  G220-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.

Chassis / Summary

Server Properties

Product Name: FCH212

Serial Number: FCH212

PID: DN2-HW-APL

UUID: AF0FF4C-638C-4EC8-AB03

BIOS Version: C220M5.3.1.2b.0.1025170315

Description:

Asset Tag: Unknown

Cisco Integrated Management Controller (Cisco IMC) Information

Hostname: C220-FCH212

IP Address: 172.223

MAC Address: 70:69:48

Firmware Version: 3.1(2c)

Current Time (UTC): Thu May 16 51 2019

Local Time: Thu May 16 51 2019 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

Overall Utilization (%): N/A

CPU Utilization (%): N/A

Memory Utilization (%): N/A

IO Utilization (%): N/A

**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:

1. 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.
2. Reconfigure the switches connected to the 10-Gbps appliance ports to support higher throughput settings.

## 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 displays the Cisco IMC Chassis Summary page. At the top, the browser address bar shows the Cisco IMC URL and the user is logged in as admin@10.42.220-FCH212. The page title is "Chassis / Summary". Below the title, there are two main sections: "Server Properties" and "Cisco Integrated Management Controller (Cisco IMC) Information".

**Server Properties:**

- Product Name: FCH212
- Serial Number: FCH212
- PID: DN2-HW-APL
- UUID: AF0FFF4C-638C-4EC8-AB03-
- BIOS Version: C220M5.3.1.2b.0.1025170315
- Description: (empty field)
- Asset Tag: Unknown

**Cisco Integrated Management Controller (Cisco IMC) Information:**

- Hostname: C220-FCH212
- IP Address: 172.223
- MAC Address: 70:69:48
- Firmware Version: 3.1(2c)
- Current Time (UTC): Thu May 16 51 2019
- Local Time: Thu May 16 51 2019 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:**

- Overall Utilization (%): N/A
- CPU Utilization (%): N/A
- Memory Utilization (%): N/A
- IO Utilization (%): N/A

## Step 2

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

- a) From the top-left corner of the Cisco IMC GUI, click the **Toggle Navigation** icon (.
- b) From the Cisco IMC menu, select **Admin > Networking**, and then choose the **NTP Setting** tab.
- c) 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.

The screenshot shows the Cisco IMC interface for NTP configuration. The breadcrumb path is "/ ... / Networking / NTP Setting". The "NTP Properties" section includes:

- NTP Enabled:
- Server 1:
- Server 2:
- Server 3:
- Server 4:
- Status: NTP service disabled

At the bottom right, there are two buttons: "Save Changes" and "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**
- Unlike the previous generation of Cisco DNA Center appliances, second-generation appliances do not use a virtual interface card (VIC). You do not need to configure the network interface card (NIC) that comes installed on your second-generation appliance to support high throughput in Cisco IMC, as this is already enabled by default.
  - Cisco IMC does not support NTP authentication.

**Step 3** Reconfigure your switches to match the high-throughput settings on the appliance, as follows:

- Using a Secure Shell (SSH) client, log in to the switch to be configured and enter EXEC mode at the switch prompt.
- 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 mode access
MySwitch(config-if)#switchport access vlan 99
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)#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 the following:

- These commands are examples only.
  - The switch port on Cisco DNA Center second generation appliances must be set to access mode in order to function properly. Trunk mode is not supported, as it is on first generation appliances.
- 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 Intel X710-DA2 NIC ports are connected. For example:

```
MySwitch#show run interface tengigabitethernet 1/1/3
Building configuration...
Current configuration : 129 bytes
! interface TenGigabitEthernet1/1/3
  switchport access vlan 99
  ip device tracking maximum 10
end
```

MySwitch#

- e) 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  Te1/1/3
Total Mac Addresses for this criterion: 1

MySwitch#
```

**Step 4** In the **Configured Boot Mode** drop-down list, confirm that **Legacy** (the default mode) is set.

Running Version C220M5.4.1.3m.0.0708220050  
 UEFI Secure Boot   
 Actual Boot Mode Legacy  
 Configured Boot Mode Legacy  
 Last Configured Boot Order Source CIMC  
 Configured One time boot device

Save Changes

To access the **Configure Boot Order** tab, do the following:

- From the top-left corner of the Cisco IMC GUI, click the **Toggle Navigation** icon (.
- From the Cisco IMC menu, choose **Compute > BIOS > Configure Boot Order**.

Do *not* change the boot mode to **UEFI**. When this mode is set, your Cisco DNA Center appliance's interfaces may not be pingable.

### 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 the "Appliance Configuration Overview" topic specific to the configuration wizard you want to use:
  - [Appliance Configuration Overview](#)
  - [Appliance Configuration Overview](#)
  - [Appliance Configuration Overview](#)



# NIC Bonding Overview

On any given Cisco DNA Center appliance, you can configure the Enterprise, Intracluster, Management, and Internet interface. If you enable network interface controller (NIC) bonding on an appliance, each of these interfaces has two instances: The primary instance (located on either your appliance's motherboard or Intel X710-DA2 NIC) is connected to one switch, and the secondary instance (located on your appliance's Intel X710-DA4 NIC) is connected to a different switch. NIC bonding consolidates the two instances of each interface into a single logical interface, appearing as a single device with one MAC address. Depending on the bonding mode that you choose when configuring the interfaces on your appliance, this feature provides the following benefits when enabled:



---

**Note** Both single-node and three-node Cisco DNA Center clusters support NIC bonding.

---

- **Active-Backup mode:** By default, this is the bonding mode that's configured for your appliance's interfaces when this feature is enabled on your appliance. It enables high availability (HA) for the two interfaces that Cisco DNA Center has grouped together. When the interface that's currently active goes down, the other interface takes its place and becomes active.



---

**Note** When this mode is enabled on an interface that supports both 1-Gbps and 10-Gbps throughput, Cisco DNA Center automatically sets the throughput to 1-Gbps.

---

- **LACP mode:** When selected, the two interfaces that Cisco DNA Center has grouped together share the same speed and duplex settings. This provides load balancing and higher bandwidth for the interfaces. In order to enable this mode, the following items must first be in place:
  - The Linux utility `ethtool` must support the base drivers that are used to retrieve the speed and duplex mode of each interface.
  - The switch that is connected to the Enterprise port must support dynamic interface aggregation.
  - After you enable LACP on the switch, ensure that you have set the LACP mode to **active** (which places the switch port connected to your appliance into an active negotiating state, in which the port initiates negotiations with remote ports by sending LACP packets) and the LACP rate to **fast** (which changes the rate at which the LACP control packets are sent to an LACP-supported interface from the default every 30 seconds to once every second).



---

**Note** You can only enable LACP mode on your appliance's Enterprise and Intracluster interfaces. The Management and Internet Access interfaces only support Active-Backup mode.

---

Before you use NIC bonding in your production environment, you should do the following:

- Confirm that your appliance supports this feature. See [Appliance Support, on page 68](#).

- If the Intel X710-DA4 NIC that shipped with your appliance is currently disabled, you need to enable it in order to make use of NIC bonding (see [Enable NIC on an Upgraded Appliance, on page 68](#)).
- Determine where the secondary ports are located on your appliance's rear panel. See [Front and Rear Panels, on page 5](#).
- View the recommended appliance–switch cabling. See [Interface Cable Connections, on page 24](#).

## Appliance Support

All second-generation Cisco DNA Center appliances support NIC bonding:

- 44-core appliance: Cisco part number DN2-HW-APL
- 44-core promotional appliance: Cisco part number DN2-HW-APL-U
- 56-core appliance: Cisco part number DN2-HW-APL-L
- 56-core promotional appliance: Cisco part number DN2-HW-APL-L-U
- 112-core appliance: Cisco part number DN2-HW-APL-XL
- 112-core promotional appliance: Cisco part number DN2-HW-APL-XL-U

## Enable NIC on an Upgraded Appliance

In order to enable the Intel X710-DA4 NIC on an appliance that you plan to upgrade to Cisco DNA Center 2.3.4 from a previous version, complete the following procedure.

**Step 1** Confirm that your appliance has the Intel X710-DA4 NIC installed.

- Log in to the appliance's Cisco IMC.
- In the **Summary** window's **Server Properties** area, confirm that the following values are set:
  - PID: **DN2-HW-APL** for a 44-core appliance, **DN2-HW-APL-L** for a 56-core appliance, or **DN2-HW-APL-XL** for a 112-core appliance (see the following example).
  - BIOS Version: This value should start with either **C220M5** for a 44 and 56-core appliance or **C480M5** for a 112-core appliance (see the following example).

### Server Properties

Product Name: \_\_\_\_\_  
 Serial Number: FCH224-\_\_\_\_\_  
 PID: **DN2-HW-APL-XL**  
 UUID: 6FF202AA-EEF9-4DF4-9FE4-\_\_\_\_\_  
 BIOS Version: **C480M5** 4.0.1c.0.0706181854  
 Description:   
 Asset Tag:

### Cisco Integrated Management Controller

Hostname: C480-FCH224-\_\_\_\_\_  
 IP Address: 10.195.\_\_\_\_\_  
 MAC Address: A8:B4:56:\_\_\_\_\_  
 Firmware Version: 4.0(1a)  
 Current Time (UTC): Wed Nov 6 18:51:54 2019  
 Local Time: Wed Nov 6 10:51:54 2019 PST -08  
 Timezone: America/Los\_Angeles

- Choose  > **Chassis** > **Inventory** > **Network Adapters**.

- d) In the **Network Adapters** table, confirm that the Intel X710-DA4 Quad Port network adapter is listed for one of the following slots:
- For a 44 or 56-core appliance, **PCIe Slot 2**.
  - For a 112-core appliance, **PCIe Slot 12** (see the following example).

Cisco Integrated Management Controller


/ ... / Inventory / Network Adapters ★

CPU Memory PCI Adapters Power Supplies Cisco VIC Adapters **Network Adapters** Storage SAS Expan

Network Adapters Total 3 ⚙️

Slot	Product Name	Number Of Interfaces	External Ethernet Interfaces	
			ID	MAC Address
9	Intel X710-DA2 Dual Port 10Gb SFP+ conver...	2	1	3c:fd:fe:88:88:88
			2	3c:fd:fe:88:88:88
12	Intel X710-DA4 Quad Port 10Gb SFP+ conver...	4	4	3c:fd:fe:88:88:88
			3	3c:fd:fe:88:88:88
			1	3c:fd:fe:88:88:88
			2	3c:fd:fe:88:88:88
L	Cisco(R) LOM X550-T2	2	1	2c:f8:9b:88:88:88
			2	2c:f8:9b:88:88:88

**Step 2** Confirm that the your appliance's PCIe card is enabled:

- Choose  > **Compute**.  
The **BIOS > Configure BIOS > I/O** tab opens.
- If necessary, set the following parameters and then click **Save**:
  - For a 44 or 56-core appliance, set the **PCIe Slot 2 OptionROM** parameter to **Enabled** and the **PCIe Slot 2 Link Speed** parameter to **Auto**.
  - For a 112-core appliance, set the **PCIe Slot 12 OptionROM** parameter to **Enabled** and the **PCIe Slot 12 Link Speed** parameter to **Auto** (see the following example).

Cisco Integrated Management Controller

Home / Compute / BIOS

BIOS | Remote Management | Troubleshooting | Power Policies | PID Catalog

Enter BIOS Setup | Clear BIOS CMOS | Restore Manufacturing Custom Settings | Restore Defaults

Configure BIOS | Configure Boot Order | Configure BIOS Profile

I/O | Server Management | Security | Processor | Memory | Power/Performance

Note: Default values are shown in bold.

Reboot Host Immediately:

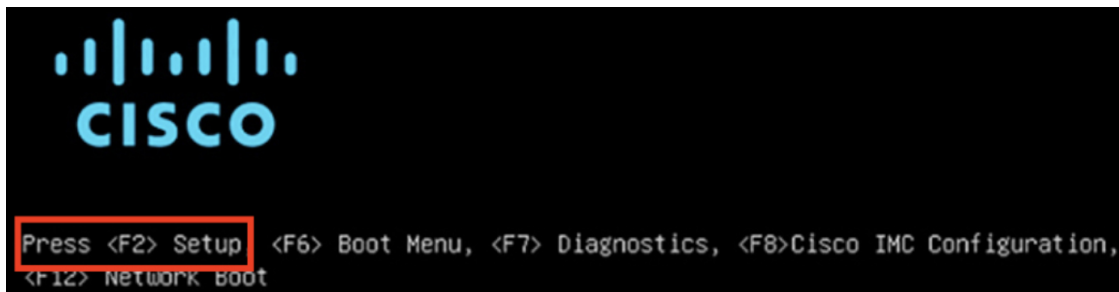
Intel VT for directed IO:	Enabled	Legacy USB Support:	Enabled
Intel VTD ATS support:	Enabled	Intel VTD coherency support:	Disabled
LOM Port 1 OptionRom:	Enabled	All Onboard LOM Ports:	Enabled
Pcie Slot 1 OptionRom:	Enabled	LOM Port 2 OptionRom:	Enabled
Pcie Slot 3 OptionRom:	Enabled	Pcie Slot 2 OptionRom:	Enabled
Pcie Slot 5 OptionRom:	Enabled	Pcie Slot 4 OptionRom:	Enabled
Pcie Slot 7 OptionRom:	Enabled	Pcie Slot 6 OptionRom:	Enabled
Pcie Slot 9 OptionRom:	Enabled	Pcie Slot 8 OptionRom:	Enabled
Pcie Slot 11 OptionRom:	Enabled	Pcie Slot 10 OptionRom:	Enabled
RAID OptionRom:	Enabled	<b>Pcie Slot 12 OptionRom:</b>	<b>Disabled</b>
Front NVME 2 OptionRom:	Enabled	Front NVME 1 OptionRom:	Enabled
Front NVME 12 OptionRom:	Enabled	Front NVME 11 OptionRom:	Enabled
Front NVME 14 OptionRom:	Enabled	Front NVME 13 OptionRom:	Enabled
Front NVME 16 OptionRom:	Enabled	Front NVME 15 OptionRom:	Enabled
Front NVME 18 OptionRom:	Enabled	Front NVME 17 OptionRom:	Enabled
Front NVME 20 OptionRom:	Enabled	<b>PCIe Slot 12 Link Speed:</b>	<b>Disabled</b>

c) Do one of the following:

- If you needed to set these two parameters for your appliance, reboot your appliance and then proceed with its configuration. You do not need to complete the rest of this procedure.
- If you have a 112-core appliance and only see one of these parameters displayed in the **I/O** tab, proceed to Step 3 and complete the rest of this procedure.

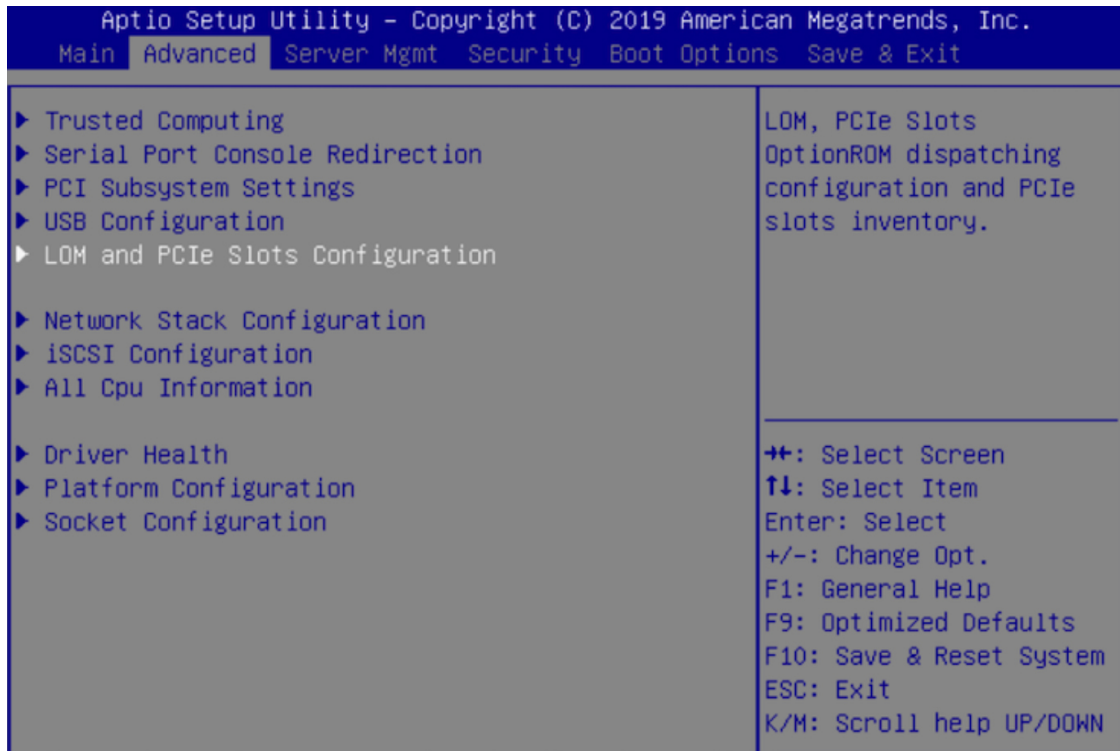
**Step 3** Boot into your appliance's BIOS:

- From Cisco IMC, start a KVM session.
- Power cycle the appliance by clicking the **Host Power** link and then choosing **Power Cycle**.
- During startup, press the **F2** key as soon as you see the following screen to boot into your appliance's BIOS and open the Aptio Setup Utility.

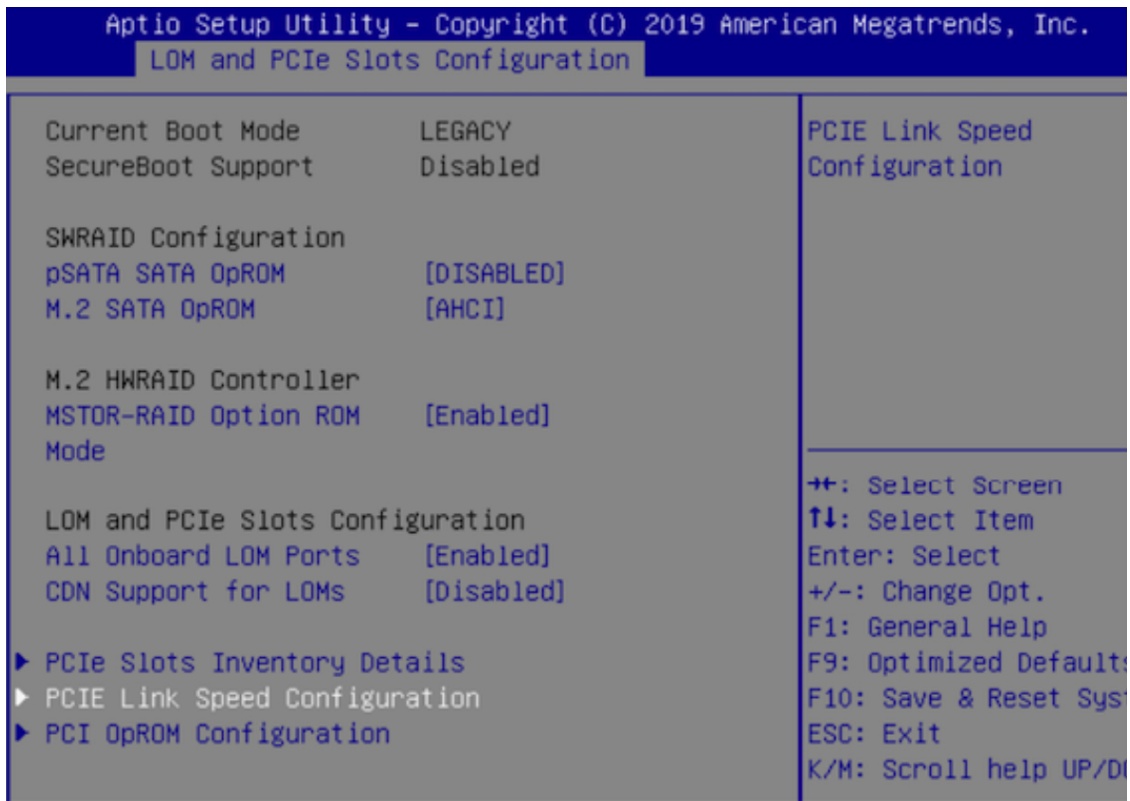


**Step 4** Enable the PCIe card:

- a) From the Aptio Setup Utility's **Main** tab, open the **Advanced** tab and then choose **LOM and PCIe Slots Configuration**.

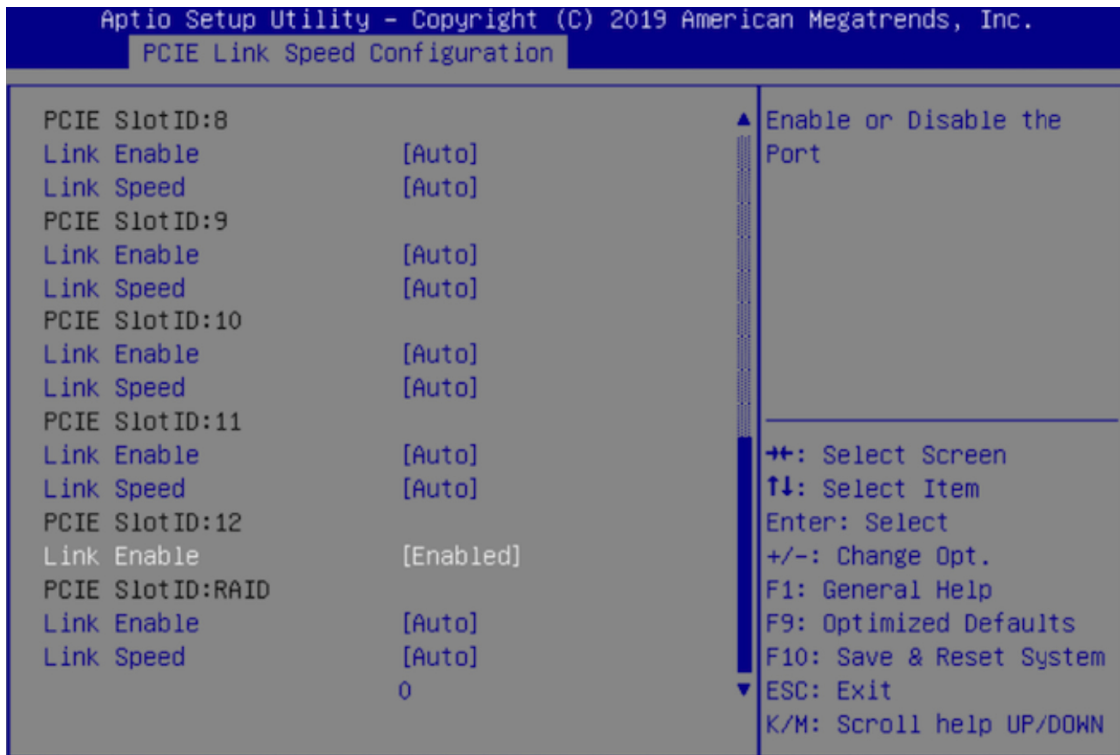


- b) In the **LOM and PCIe Slots Configuration** tab, choose **PCIE Link Speed Configuration**.

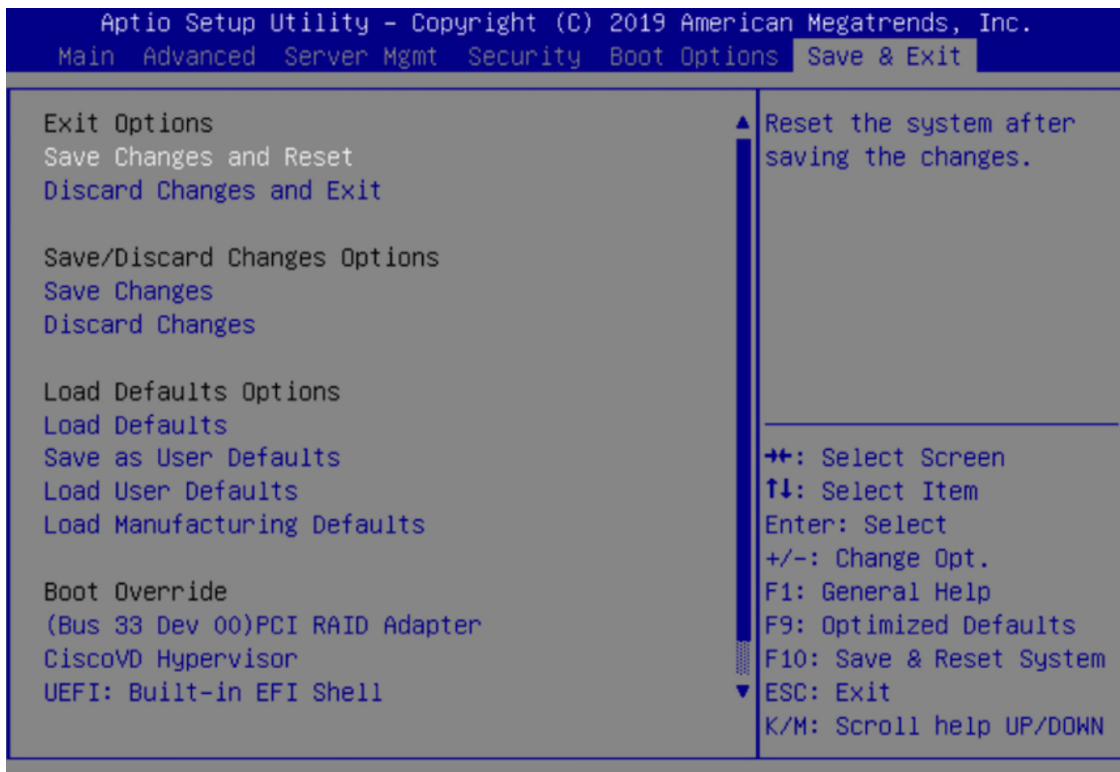


- c) In the **PCIe Link Speed Configuration** tab, scroll down to the **Link Enable** option for either PCIe SlotID: 2 (44 or 56-core appliance) or PCIe SlotID: 12 (112-core appliance), then press **Enter**.
- d) Choose **Enable**, then press **ENTER**.


Your screen should look like the following example:



- e) Press the **ESC** key twice to return to the main BIOS menu, then open the **Save & Exit** tab.
- f) Choose the **Save Changes and Reset** option, then press **Enter**.



Your appliance reboots and opens the configuration wizard. Proceed with the configuration of your appliance.

**Important** After you have enabled your appliance's NIC, if you reset your appliance to the default settings in Cisco IMC ( > **Admin** > **Utilities** > **Reset to factory Default**), you will need to complete this procedure again.

**Step 5** Upgrade to Cisco DNA Center 2.3.4.

In the *Cisco DNA Center Upgrade Guide*, complete the upgrade procedure specific to your current version.

During the upgrade, Cisco DNA Center will prepare your appliance to use the Intel X710-DA4 NIC. After the upgrade completes and your appliance reboots, Cisco IMC recognizes this NIC and the four interfaces that reside on it. Counting the four interfaces located on the Intel X710-DA2 NIC and appliance motherboard, that makes a total of eight interfaces on your appliance.

**Step 6** Complete the configuration wizard to finalize the use of the Intel X710-DA4 NIC on your appliance, as described in [Reconfigure the Appliance Using the Configuration Wizard, on page 246](#).

## Reimage the Appliance

Situations that require you to reimage your Cisco DNA Center appliance, such as recovering from a backup or changing your cluster link configuration, might arise. 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 ISO Image](#).

**Step 2** Create a bootable USB drive that contains the Cisco DNA Center ISO image.

See [Create a Bootable USB Flash Drive](#).

**Step 3** Reinitialize the virtual drives that are managed by your appliance's RAID controller: [Reinitialize the Virtual Drives on a Cisco DNA Center Appliance, on page 78](#).

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

See [Install the Cisco DNA Center ISO Image](#).

## Verify the Cisco DNA Center ISO Image

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

### Before you begin

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



- Step 1** Download the Cisco DNA Center ISO image (.iso) 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 ISO image from the location specified by Cisco.
- Step 4** Obtain the ISO 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 ISO image is corrupted due to a partial download.

Run one of the following commands (depending upon your operating system):

- On a Linux system: **sha512sum** *ISO-image-filename*
- On a Mac system: **shasum -a 512** *ISO-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 output of the command you run to the SHA512 checksum file that you downloaded. If the command output does not match, download the ISO 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 ISO image is genuine and from Cisco by verifying its signature:

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

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

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

- Step 7** After confirming that you have downloaded a Cisco ISO image, create a bootable USB drive that contains the Cisco DNA Center ISO 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 ISO 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:

- Click **Select drive**.
- 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.

## Reinitialize the Virtual Drives on a Cisco DNA Center Appliance

Complete the following procedure to reinitialize the virtual drives on your Cisco DNA Center appliance.

- 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](#).
- Step 2** From the top-left corner of the Cisco IMC GUI, click the **Toggle Navigation** icon (.
- Step 3** From the Cisco IMC menu, choose **Storage > Cisco 12G Modular Raid Controller**.
- Step 4** Click the **Virtual Drive Info** tab.
- Step 5** Check the check box for the first virtual drive that's listed (drive number 0), then click **Initialize**.
- Step 6** From the **Initialize Type** drop-down list, choose **Full Initialize**.
- Step 7** Click **Initialize VD**.
- Step 8** Repeat Step 5 through Step 7 for the appliance's other virtual drives, but choose **Fast Initialize**. (Only the first virtual drive requires full initialization. The second and third virtual drives don't require full initialization.)

## 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 Using the Maglev Wizard, on page 81](#) or [Configure a Secondary Node Using the Maglev Wizard, on page 103](#).

---

## Cisco DNA Center Appliance Configuration

When installation of the Cisco DNA Center ISO image completes, the installer reboots and opens the Maglev Configuration wizard's welcome screen. To complete the reimaging of your appliance, complete the steps described in [Configure the Appliance Using the Maglev Wizard, on page 81](#).





## CHAPTER 5

# Configure the Appliance Using the Maglev Wizard

---

- [Appliance Configuration Overview, on page 81](#)
- [Configure the Primary Node Using the Maglev Wizard, on page 81](#)
- [Configure a Secondary Node Using the Maglev Wizard, on page 103](#)
- [Upgrade to the Latest Cisco DNA Center Release, on page 122](#)

## 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. If you choose 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.
- **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 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. Configure the primary node in your cluster. See [Configure the Primary Node Using the Maglev Wizard, on page 81](#).
2. If you have installed three appliances and want to add the second and third nodes to your cluster, see [Configure a Secondary Node Using the Maglev Wizard, on page 103](#).

## Configure the Primary Node Using the Maglev Wizard

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 Using the Maglev Wizard](#), on page 103 instead.



---

**Important**

- 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.
  - 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 release 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 choose **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 choose **HTML-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)**.

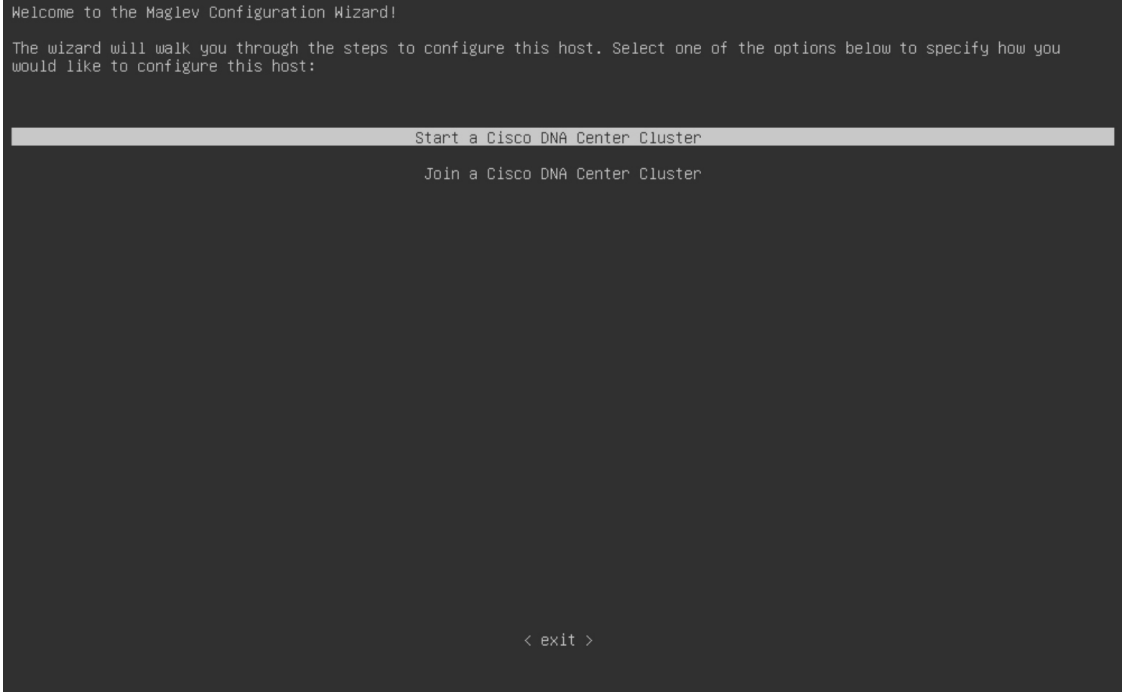
If you are asked to confirm your choice to reboot the appliance, click **OK**.

After displaying reboot messages, the KVM console displays the **Static IP Configuration** screen.



**Step 4** Click **Skip**.

The KVM console displays the Maglev Configuration wizard welcome screen.



**Note** Only users that want to configure their appliance using one of the browser-based wizards without using the IP address, subnet mask, and default gateway assigned to the appliance's Enterprise interface by a DHCP server need to complete this screen.

**Step 5** Click **Start a Cisco DNA Center Cluster** to begin configuring the primary node.

The screen updates.



**Step 6** Choose one of the following options:

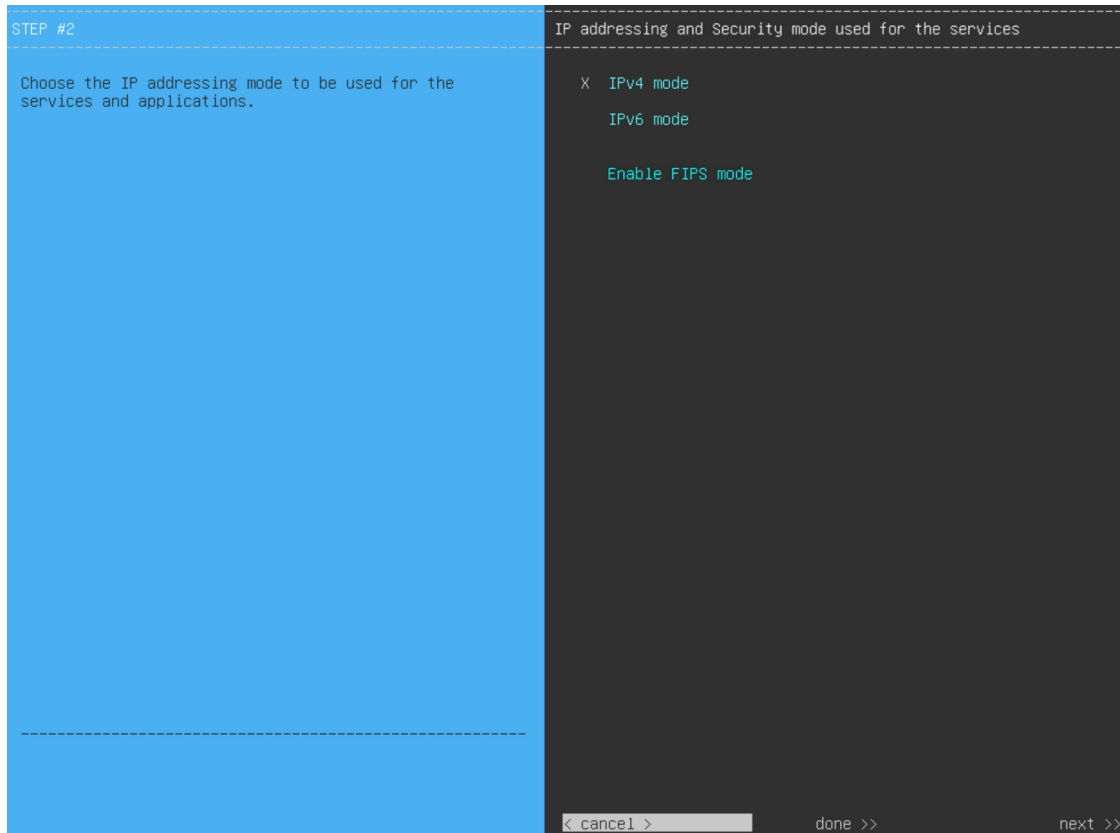
- **Start using DNAC pre manufactured cluster:** Choose this option to configure an appliance with its default settings in place:
  - Intracluster interface IP address: **169.254.6.66**
  - Intracluster interface subnet mask: **255.255.255.128**
  - Container subnet: **169.254.32.0/20**
  - Cluster subnet: **169.254.48.0/20**
  - IPv4 addressing
  - Admin superuser's password: **maglev1@3**

You will *not* be able to change any of these settings, so choose this option only if you want to use them.

**Important** This option is only available if you are configuring a new Cisco DNA Center appliance. If you are reimaging your appliance, the wizard proceeds with the **Start configuration of DNAC in advanced mode** option selected.

- **Start configuration of DNAC in advanced mode:** Choose this option to configure an appliance that doesn't use one or more of the default settings listed in the previous bullet. Also choose this option if you want to use IPv6 addressing on your appliance.

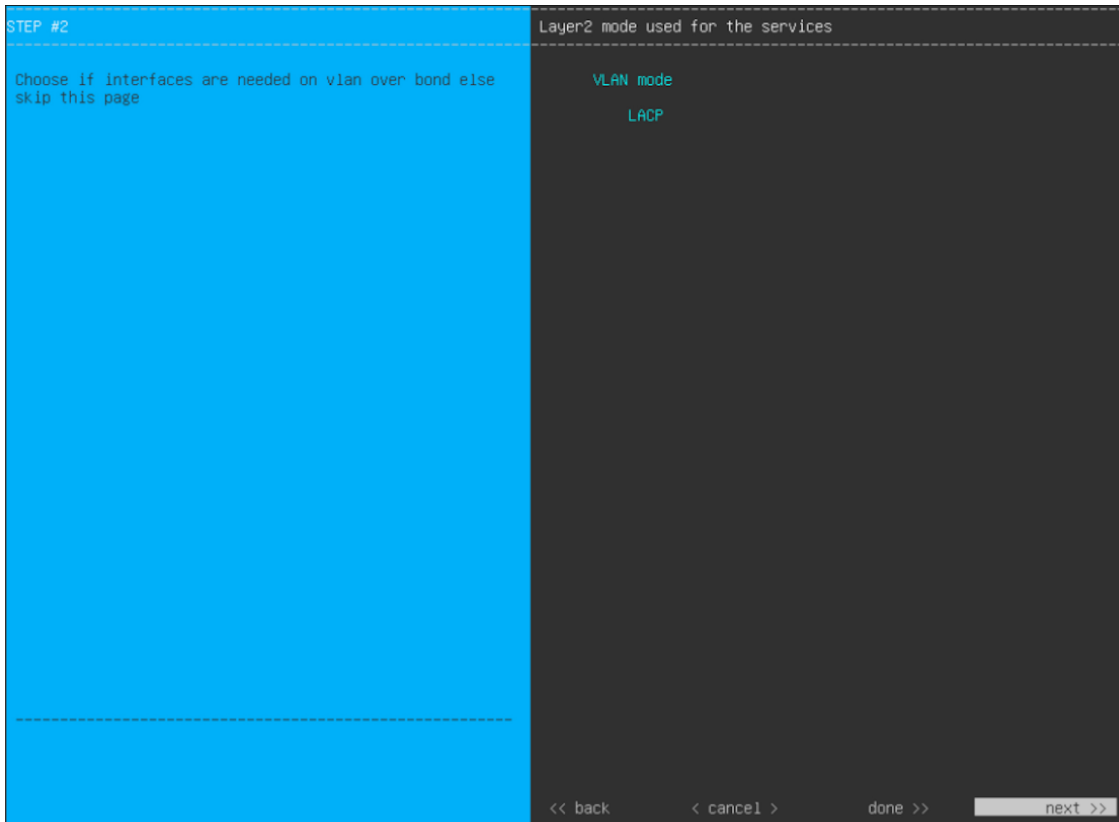
The screen updates.



**Step 7** Do the following, then click **next>>** to proceed:

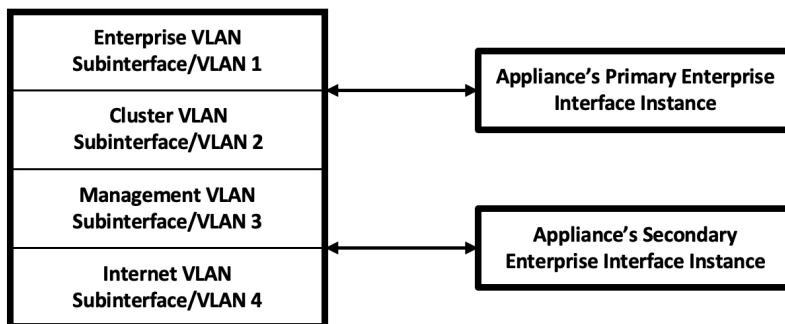
- Specify whether the applications and services running on your Cisco DNA Center appliance will use IPv4 or IPv6 addressing.
- (Optional) Check the **Enable FIPS Mode** check box to enable FIPS mode on your Cisco DNA Center appliance.  
See [FIPS Mode Support, on page 102](#) for things to keep in mind when enabling FIPS mode on an appliance.

**Step 8** (Optional) Do the following to enable Layer 2 portchannel mode (with VLAN tagging) for the appliance. This will create a single bonded interface that connects to your network using both the primary and secondary instance of your appliance's Enterprise interface. After making your selections, click **next>>** to proceed.



- a) Choose the **VLAN mode** option to enable dot1q/VLAN trunking and convert your appliance's Enterprise, Cluster, Management, and Internet interfaces into VLAN subinterfaces that reside on the bonded interface (as illustrated in the following figure). By default, this interface operates in Active-Backup mode (which enables HA).

**Bonded Interface**



- b) If you want this interface to operate in LACP mode instead (which enables load balancing and higher bandwidth), you must also choose the **LACP** option.
- c) When you enter the settings for your appliance's Enterprise and Cluster interfaces, ensure that you enter a unique VLAN ID in the **VLAN ID of Interface** field for the subinterfaces you want to configure on the virtual bonded interface.

- Important**
- The VLAN mode feature is not commonly used. Only enable it if it's required by your Cisco DNA Center deployment. If you just want to enable NIC bonding, you can do so in the next two wizard screens.
  - Even though one physical appliance interface (the Enterprise interface) is connected, you can configure all of the subinterfaces that reside on the virtual bonded interface.

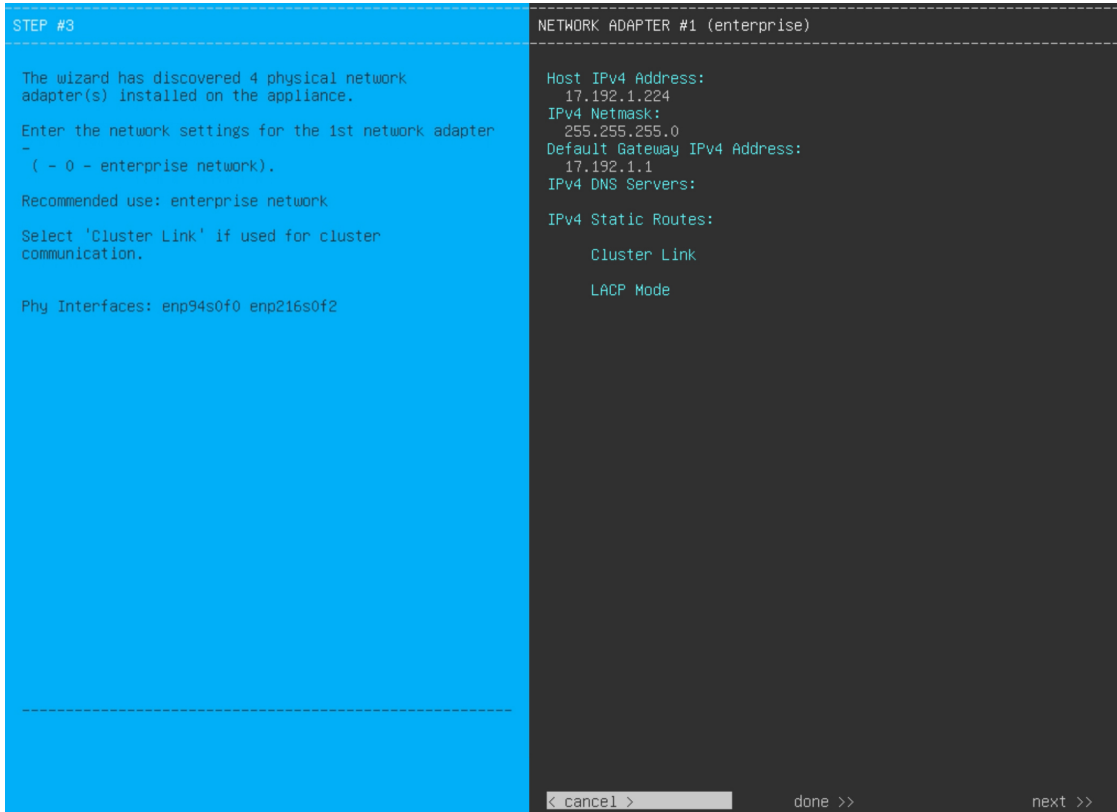
The wizard discovers all of the ports on the appliance and presents them to you one by one, in separate screens, in the following order:

- a. (Required) 10-Gbps Enterprise Port—Network Adapter #1
- b. (Required) 10-Gbps Cluster Port—Network Adapter #2
- c. (Optional) 1-Gbps/10-Gbps Management Port—Network Adapter #3
- d. (Optional) 1-Gbps/10-Gbps Internet Port—Network Adapter #4

If the wizard fails to display either or both of the Enterprise and Cluster ports during the course of configuration, it might indicate that these ports are nonfunctional or disabled. These two 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 contacting the Cisco Technical Assistance Center (for more information, see the "Get Assistance from the Cisco TAC" topic in the [Release Notes](#) document).

## Step 9

The wizard first presents the 10-Gbps Enterprise port as **NETWORK ADAPTER #1**. As explained in [Interface Cable Connections](#), this is a required port used 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 19: Primary Node Entries for Network Adapter #1: 10-Gbps Enterprise Port**

Host IPv4/IPv6 Address field	Enter the IP address for the Enterprise port. This is required.
IPv4 Netmask/IPv6 Prefix Length field	Do one of the following: <ul style="list-style-type: none"> <li>• If you selected IPv4 addressing, enter the netmask for the port's IP address. This is required.</li> <li>• If you selected IPv6 addressing, enter the prefix length (in bits). Valid values range from 10 through 127.</li> </ul>
Default Gateway IPv4/IPv6 Address field	Enter a default gateway IP address to use for the port. <p><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.</p>
IPv4/IPv6 DNS Servers field	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. <p><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.</p>

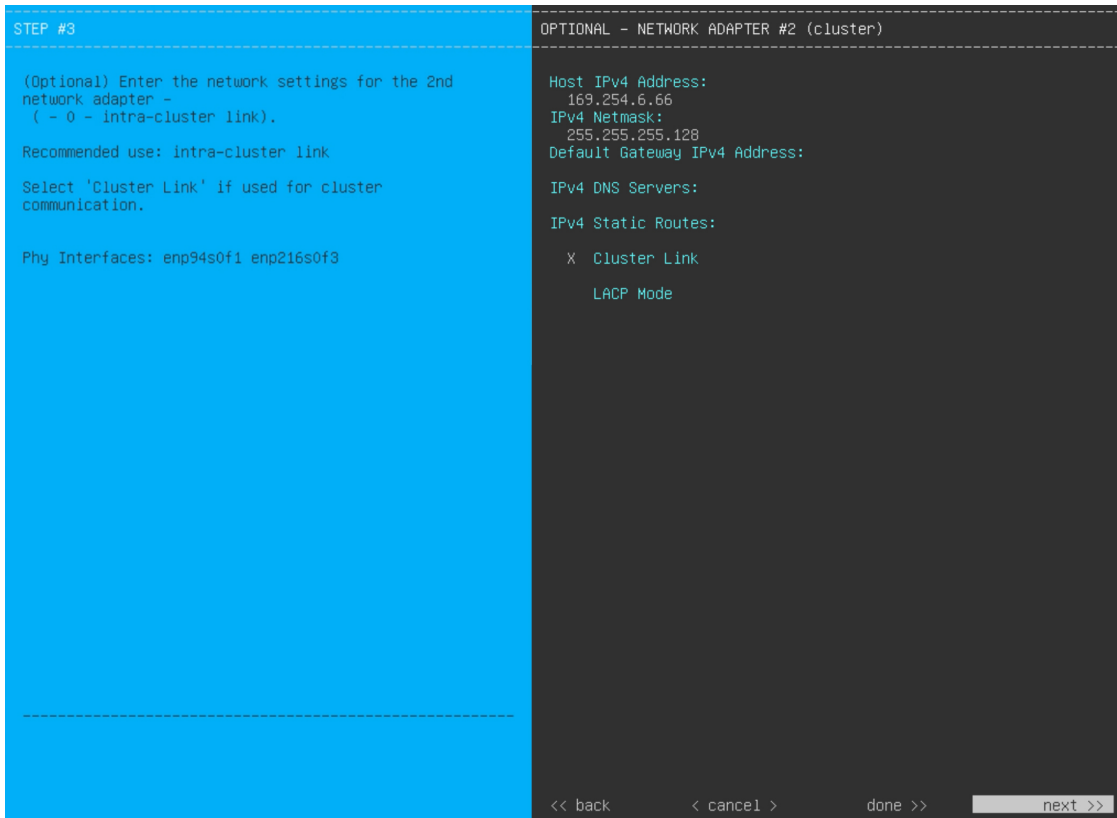
IPv4/IPv6 Static Routes field	Enter one or more static routes in the following format, separated by spaces: <code>&lt;network&gt;/&lt;netmask&gt;/&lt;gateway&gt;</code> . This is usually required on the Cisco DNA Center Management port only.
Vlan ID of Interface field	Enter the VLAN ID for the bonded interface you enabled in the previous step. If you didn't enable it, this field will not be displayed.
Cluster Link field	Leave this field blank. It is required on the Cluster port only.
LACP Mode field	<p>Do one of the following:</p> <ul style="list-style-type: none"> <li>• Leave this field blank and the port will operate in <b>Active-Backup</b> mode. This mode provides fault tolerance by aggregating two Ethernet interfaces into a single logical channel. When the interface that's currently active goes down, the other interface takes its place and becomes active.</li> <li>• Check the check box to enable <b>LACP</b> mode on this port. This mode aggregates two Ethernet interfaces that share the same speed and duplex settings into a single logical channel. This provides load balancing and higher bandwidth.</li> </ul> <p>For more information about Cisco DNA Center's implementation of NIC bonding, see <a href="#">NIC Bonding Overview, on page 67</a>.</p> <p><b>Note</b> This field is displayed if you didn't choose any of the options in the previous step.</p>

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 10

After successful validation of the Enterprise port values you entered, the wizard presents the 10-Gbps Cluster port and presents it 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 20: Primary Node Entries for Network Adapter #2: 10-Gbps Cluster Port**

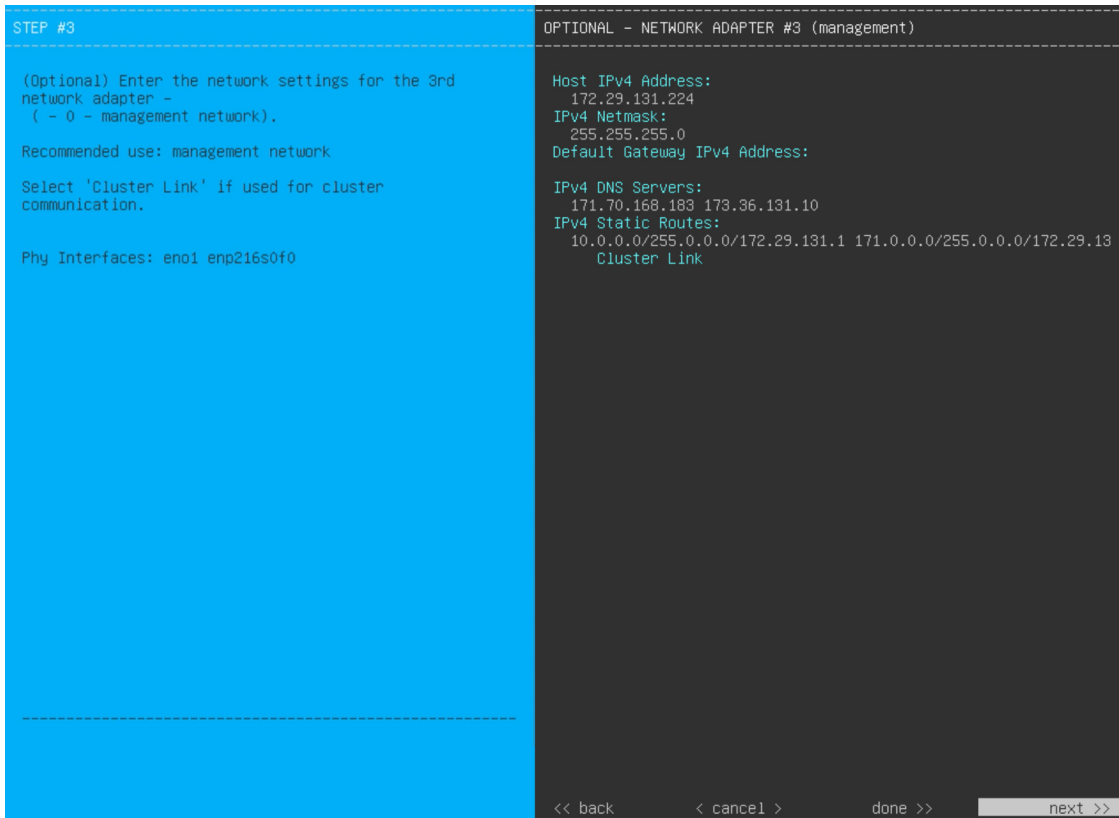
<p>Host IPv4/IPv6 address field</p>	<p>Enter the IP address for the Cluster port. This is required. Note that you cannot change the address of the Cluster port later.</p> <p><b>Note</b> If you selected the <b>Start using DNAC pre manufactured cluster</b> option previously, <b>169.254.6.66</b> will already be set in this field and you will not be able to enter a different address.</p>
<p>IPv4 Netmask/IPv6 Prefix Length field</p>	<p>Do one of the following:</p> <ul style="list-style-type: none"> <li>• If you selected IPv4 addressing, enter the netmask for the port's IP address. This is required.</li> </ul> <p><b>Note</b> If you selected the <b>Start using DNAC pre manufactured cluster</b> option previously, <b>255.255.255.128</b> will already be set in this field and you will not be able to enter a different netmask.</p> <ul style="list-style-type: none"> <li>• If you selected IPv6 addressing, enter the prefix length (in bits). Valid values range from 10 through 127.</li> </ul>

Default Gateway IPv4/IPv6 address field	<p>Enter a default gateway IP address to use for the port.</p> <p><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.</p>
IPv4/IPv6 DNS Servers field	<p>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.</p> <p><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.</p>
IPv4/IPv6 Static Routes field	<p>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 Management port only.</p>
Vlan ID of Interface field	<p>Enter the VLAN ID for the bonded interface you enabled previously. If you didn't enable it, this field will not be displayed.</p>
Cluster Link field	<p>Check the check box to set this port as the link to a Cisco DNA Center cluster. This is required on the Cluster port only.</p>
LACP Mode field	<p>Do one of the following:</p> <ul style="list-style-type: none"> <li>• Leave this field blank and the port will operate in <b>Active-Backup</b> mode. This mode provides fault tolerance by aggregating two Ethernet interfaces into a single logical channel. When the interface that's currently active goes down, the other interface takes its place and becomes active.</li> <li>• Check the check box to enable <b>LACP</b> mode on this port. This mode aggregates two Ethernet interfaces that share the same speed and duplex settings into a single logical channel. This provides load balancing and higher bandwidth.</li> </ul> <p>For more information about Cisco DNA Center's implementation of NIC bonding, see <a href="#">NIC Bonding Overview, on page 67</a>.</p> <p><b>Note</b> This field is displayed if you didn't choose any of the options in Step 8.</p>

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 11

After successful validation of the Cluster port values you entered, the wizard presents the 1-Gbps/10-Gbps Management port and presents it 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 21: Primary Node Entries for Network Adapter #3: 1-Gbps/10-Gbps Management Port**

Host IPv4/IPv6 address field	Enter the IP address for the Management Port. This is required only if you are using this port to access the Cisco DNA Center GUI from your management network; otherwise, you can leave it blank.
IPv4 Netmask/IPv6 Prefix Length field	Do one of the following if you entered an IP address: <ul style="list-style-type: none"> <li>• If you selected IPv4 addressing, enter the netmask for the port's IP address. This is required.</li> <li>• If you selected IPv6 addressing, enter the prefix length (in bits). Valid values range from 10 through 127.</li> </ul>
Default Gateway IPv4/IPv6 address field	Enter a default gateway IP address to use for the port. <p><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.</p>

IPv4/IPv6 DNS Servers field	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>
IPv4/IPv6 Static Routes field	Enter one or more static routes in the following format, separated by spaces: <network>/<netmask>/<gateway>.
Cluster Link field	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 12

After successful validation of the Management port values you entered, the wizard presents the 1-Gbps/10-Gbps Internet port 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. 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).

```

STEP #3
-----
(Optional) Enter the network settings for the 4th
network adapter -
( - 0 - internet-access network).

Recommended use: internet-access network
Cable status: disconnected
Select 'Cluster Link' if used for cluster
communication.

Phy Interfaces: eno2 enp216s0f1

OPTIONAL - NETWORK ADAPTER #4 (internet)
-----
Host IPv4 Address:
IPv4 Netmask:
Default Gateway IPv4 Address:
IPv4 DNS Servers:
IPv4 Static Routes:
Cluster Link

<< back      < cancel >      done >>      next >>

```

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

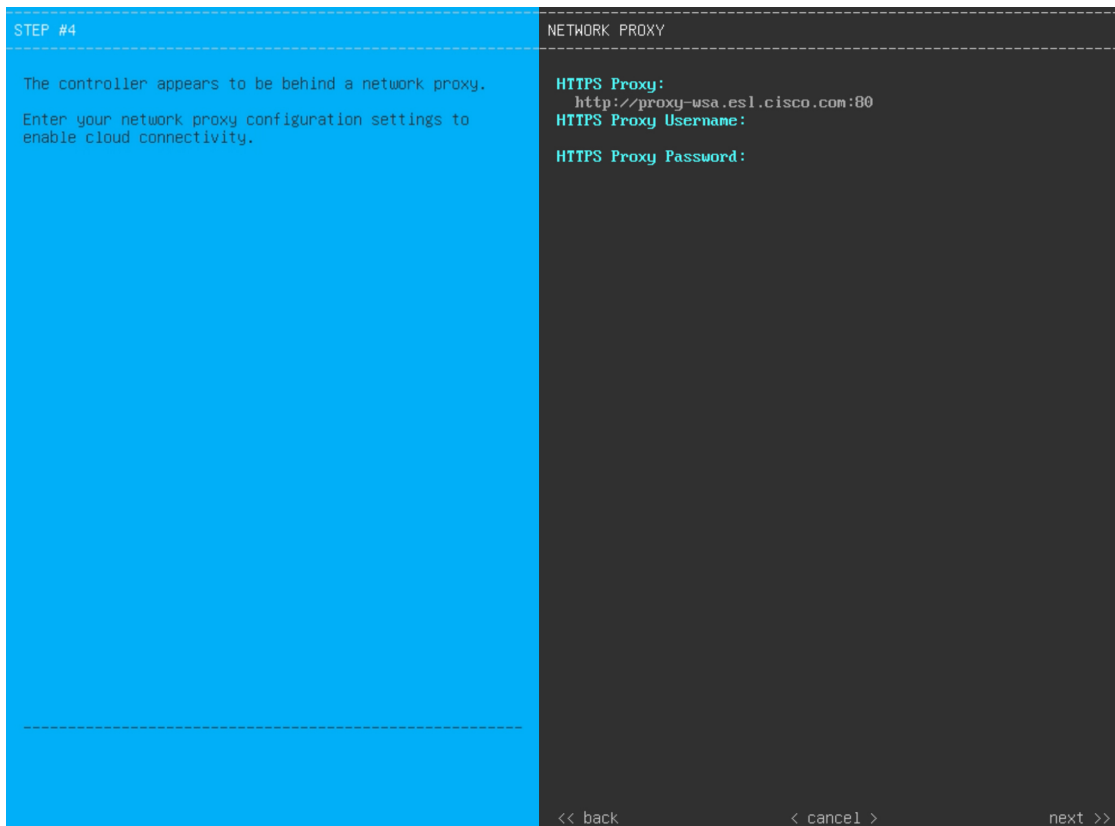
**Table 22: Primary Node Entries for Network Adapter #4: 1-Gbps/10-Gbps Internet Port**

Host IPv4/IPv6 address field	Enter the IP address for the Internet port. This is required only if you are using the Internet port for internet connection; otherwise, you can leave it blank.
IPv4 Netmask/IPv6 Prefix Length field	Do one of the following if you entered an IP address: <ul style="list-style-type: none"> <li>• If you selected IPv4 addressing, enter the netmask for the port's IP address. This is required.</li> <li>• If you selected IPv6 addressing, enter the prefix length (in bits). Valid values range from 10 through 127.</li> </ul>
Default Gateway IPv4/IPv6 address field	Enter a default gateway IP address to use for the Internet 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.
IPv4/IPv6 DNS Servers field	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.
IPv4/IPv6 Static Routes field	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 Management port only.
Cluster Link field	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 13**

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.

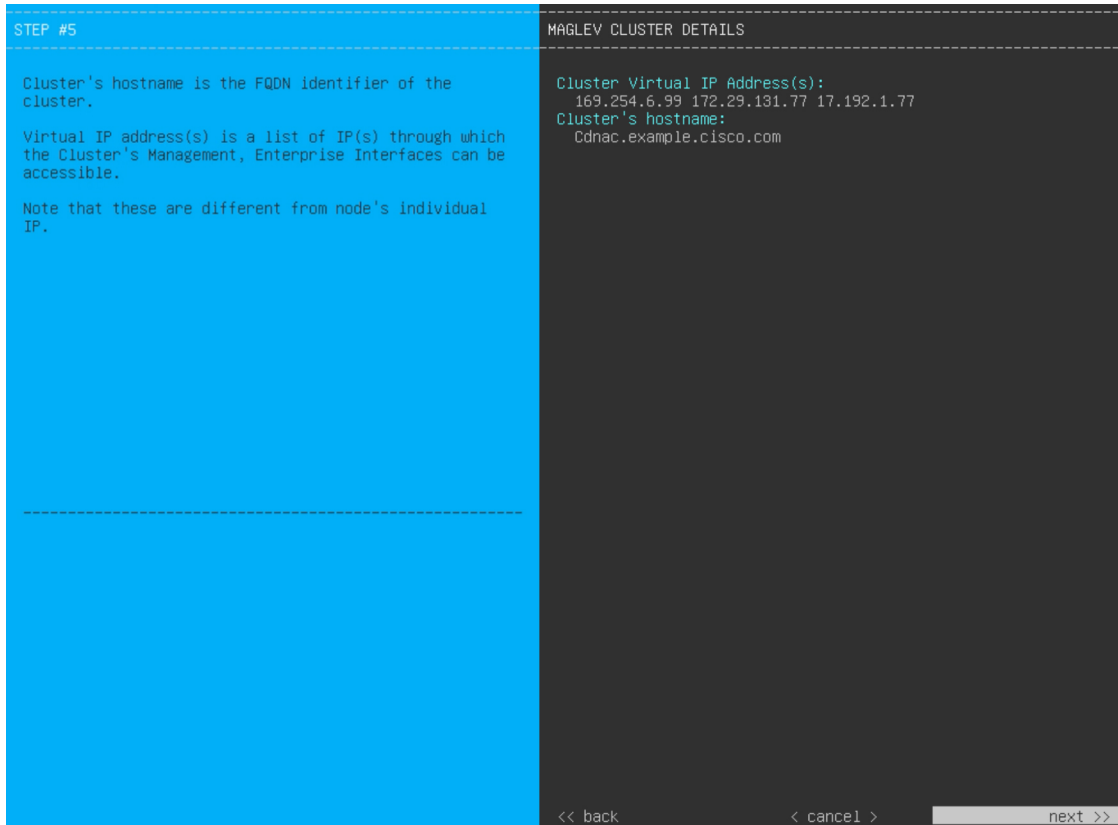
**Table 23: Primary Node Entries for Network Proxy**

<p>HTTPS Proxy field</p>	<p>Enter the URL or host name of an HTTPS network proxy used to access the Internet.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• Connection from Cisco DNA Center to the HTTPS proxy is supported only through HTTP in this release.</li> <li>• If you enter an IPv6 URL that contains a port number, enclose the IP address portion of the URL in square brackets. In this example, 443 is the port number: http://[2001:db8:85a3:8d3:1319:8a2e:370:7348]:443/</li> </ul>
<p>HTTPS Proxy Username field</p>	<p>Enter the user name used to access the network proxy. If no proxy login is required, leave this field blank.</p>
<p>HTTPS Proxy Password field</p>	<p>Enter the password used to access the network proxy. If no proxy login is required, leave this field blank.</p>

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

**Step 14**

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 the next step.

**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.

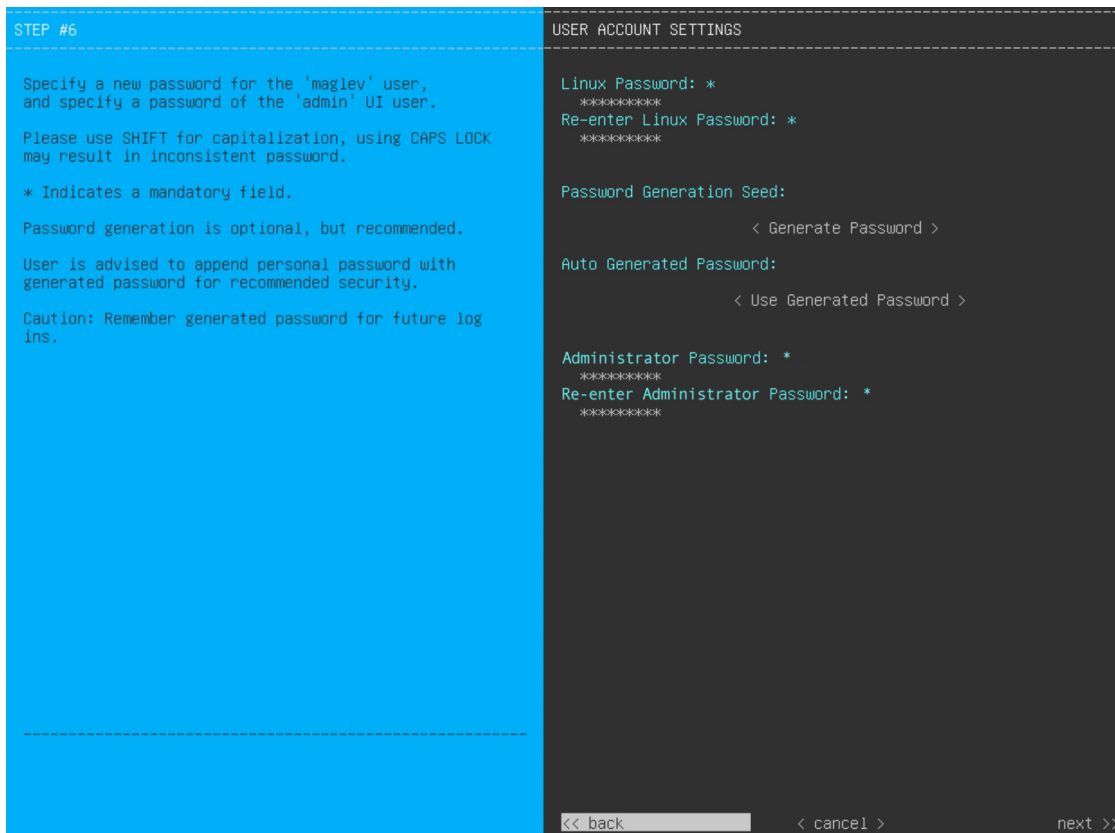
You also have the option to specify the fully qualified domain name (FQDN) for your cluster. Cisco DNA Center uses this domain name to do the following:

- 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 15**

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



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

**Table 24: Primary Node Entries for User Account Settings**

Linux Password field	Enter a Linux password for the maglev user that's a minimum of 8 characters long.
Re-enter Linux Password field	Confirm the Linux password by entering it a second time.
Password Generation Seed field	If you do not want to create the Linux password yourself, enter a seed phrase in this field and then press <b>&lt;Generate Password&gt;</b> to generate the password.
Auto Generated Password field	(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>&lt;Use Generated Password&gt;</b> to save the password.

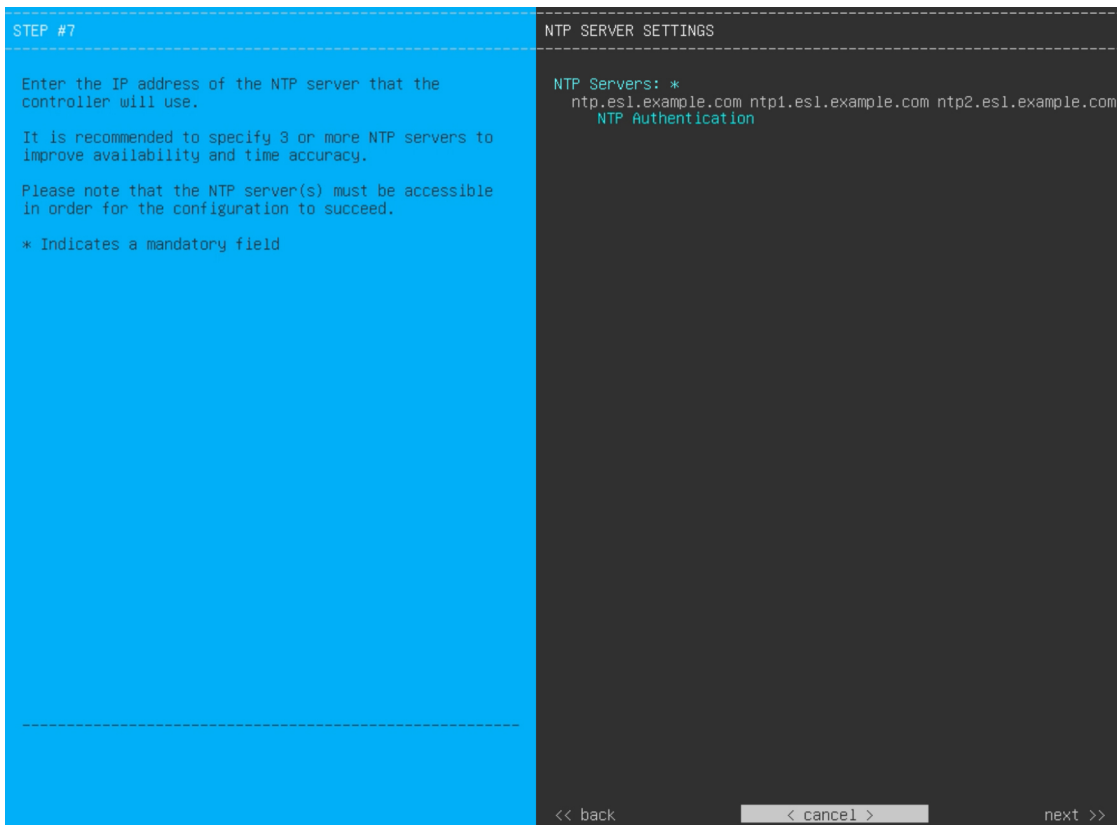


<p>Administrator Password field</p>	<p>Enter a password for the default admin superuser, used to log in to Cisco DNA Center for the first time.</p> <p>Note the following points:</p> <ul style="list-style-type: none"> <li>• If you enabled FIPS mode earlier in the wizard, ensure that this password is at least 8 characters long.</li> <li>• If you chose the <b>Start using DNAC pre manufactured cluster</b> option previously, the default password (<b>maglev1@3</b>) has already been set for the appliance and cannot be changed in the configuration wizard. As a result, this and the following field are not displayed in this screen.</li> </ul>
<p>Re-enter Administrator Password field</p>	<p>Confirm the administrator password by entering it a second time.</p>

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

**Step 16**

After you have entered the user account details, the wizard prompts you to enter **NTP SERVER SETTINGS** values.



Enter the values for **NTP SERVER SETTINGS**, as shown in the table below.

<p>NTP Servers field</p>	<p>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.</p>
--------------------------	---

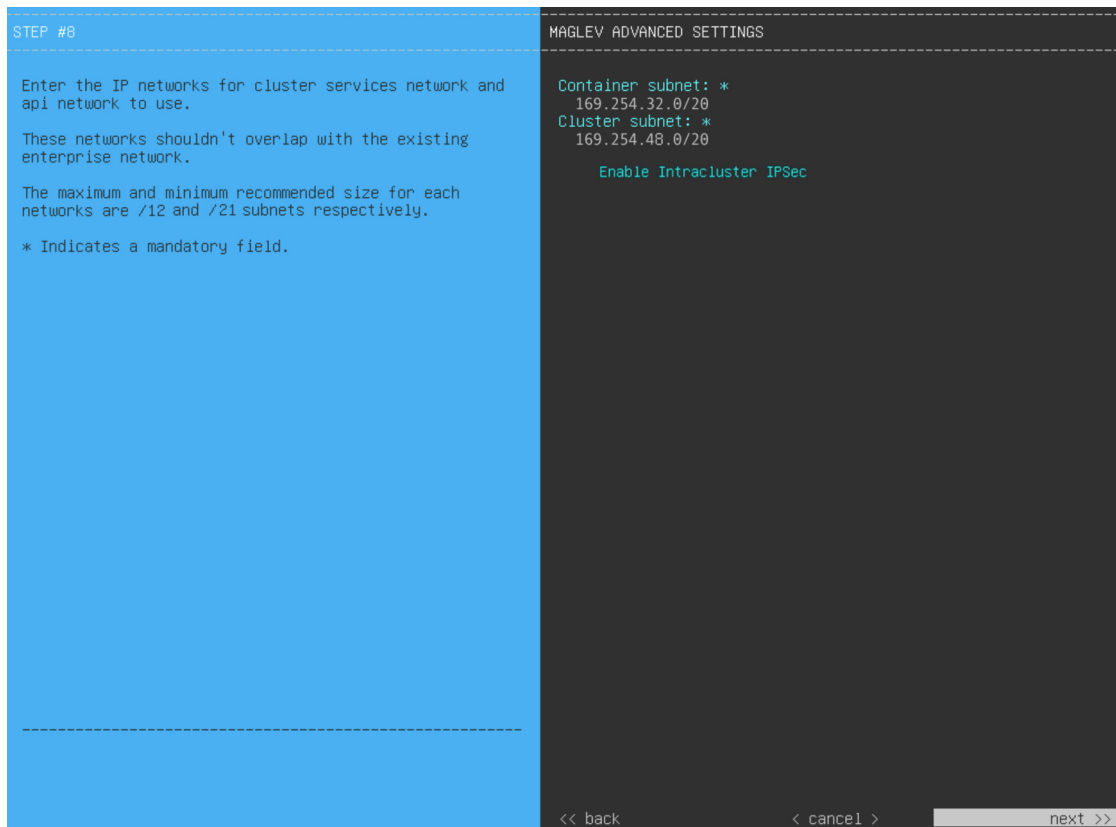
<p>NTP Authentication check box</p>	<p>To enable the authentication of your NTP server before it's synchronized with Cisco DNA Center, check this check box and then enter the following information:</p> <ul style="list-style-type: none"> <li>• The NTP server's key ID. Valid values range between 1 and 4294967295 (2<sup>32</sup>-1). This value corresponds to the key ID that's defined in the NTP server's key file.</li> <li>• The SHA-1 key value associated with the NTP server's key ID. This 40-character hex string resides in the NTP server's key file.</li> </ul> <p><b>Note</b> Ensure that you enter a key ID and key value for each NTP server that you configured in the previous field.</p>
-------------------------------------	--

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 17**

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

**Note** If you chose the **Start using DNAC pre manufactured cluster** option previously, the default Container and Cluster subnets have already been set for the appliance and cannot be changed in the configuration wizard. As a result, you will not see the following wizard screen. Proceed to Step 17.



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

**Table 25: Primary Node Entries for Maglev Advanced Settings**

Container Subnet field	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 29</a> .
Cluster Subnet field	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 29</a> .
Enable Intracluster IPsec check box	Check to enable IPsec connections between the nodes in a three-node high HA cluster.

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

**Step 18**

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.

```

CONFIGURATION SUCCEEDED
The configuration wizard has completed successfully!
To access the Maglev Web UI, please point your browser to one of the following URLs:

To access the Maglev Web Console, please point your browser to one of the following URLs:
https://17.192.1.224
https://169.254.6.66
https://172.29.131.224

The wizard will automatically close in 30 seconds

```

### 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 Using the Maglev Wizard, on page 103](#).

## FIPS Mode Support

Cisco DNA Center supports the Federal Information Processing Standard (FIPS), a government certification standard that specifies best practices for implementing cryptographic algorithms, handling key material and data buffers, and working with the operating system. Note the following points if you plan to enable FIPS mode on an appliance:

- You cannot enable FIPS mode on an appliance that has been upgraded from a previous Cisco DNA Center version. You can only enable it on an appliance that came with the latest version already installed.
- When FIPS mode is enabled, you cannot import images from a URL. You can only import images from either your computer or cisco.com.
- You will need to enter a password that's at least 8 characters long for the default admin superuser in the **USER ACCOUNT SETTINGS** screen.
- When FIPS mode is enabled on an appliance, you cannot enable external authentication.
- If you selected the **Start using DNAC pre manufactured cluster** option while completing the Maglev Configuration wizard, you will not see the **IP addressing and Security mode used for the services** screen. As a result, you will not be able to enable FIPS mode.
- Cisco DNA Center does not support SNMPv2c device credentials when FIPS mode is enabled. You must specify SNMPv3 credentials instead.
- After FIPS mode has been enabled on an appliance, the only way you can disable it is to reimage your appliance (to erase all existing data). You can then reconfigure the appliance with FIPS mode disabled. See [Reimage the Appliance, on page 74](#) for more information.
- When FIPS mode is enabled, you can only enable KeyWrap if Cisco DNA Center and Cisco ISE haven't already been integrated. See [Configure Authentication and Policy Servers, on page 241](#) for more information.

- After configuring your appliance, you can do the following to confirm whether FIPS mode is enabled:
  1. Open an SSH console to the appliance and run the `ssh -p 2222 maglev@appliance's-IP-address` command.
  2. Enter the default admin superuser's password to log in to the appliance.
  3. Run the `magctl fips status` command.
- The Cisco Wide Area Bonjour application does not support FIPS mode. As a result, you cannot install this application from either the Cisco DNA Center GUI or CLI.
- When FIPS mode is enabled, some of the functions related to Endpoint Analytics are unavailable in the Cisco DNA Center GUI.
- FIPS mode affects the export and import of map archives.

When FIPS mode is *enabled*:

- Exported map archives are unencrypted.
- Only unencrypted map archives can be imported.

When FIPS mode is *disabled*:

- Exported map archives are encrypted.
- Both encrypted and unencrypted map archives can be imported.

## Configure a Secondary Node Using the Maglev Wizard

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.
- 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.
- 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.

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://172.29.131.224:443]
```

NAME	DISPLAY_NAME	DEPLOYED	AVAILABLE	STATUS	PROGRESS
access-control-application	Access Control Application	2.1.388.60364	-	DEPLOYED	
ai-network-analytics	AI Network Analytics	2.7.8.528	-	DEPLOYED	
app-hosting	Application Hosting	1.7.0.2108120753	-	DEPLOYED	
application-policy	Application Policy	2.1.388.170155	-	DEPLOYED	
application-registry	Application Registry	2.1.388.170155	-	DEPLOYED	
application-visibility-service	Application Visibility Service	2.1.388.170155	-	DEPLOYED	
assurance	Assurance - Base	2.2.3.337	-	DEPLOYED	
automation-core	NCP - Services	2.1.388.60364	-	DEPLOYED	
base-provision-core	Automation - Base	2.1.388.60364	-	DEPLOYED	
cloud-connectivity-contextual-content	Cloud Connectivity - Contextual Content	1.3.1.364	-	DEPLOYED	DEPLOYED
cloud-connectivity-data-hub	Cloud Connectivity - Data Hub	1.6.0.380	-	DEPLOYED	
cloud-connectivity-tethering	Cloud Connectivity - Tethering	2.1.1.43	-	DEPLOYED	
cloud-provision-core	Cloud Device Provisioning Application	2.1.388.60364	-	DEPLOYED	
command-runner	Command Runner	2.1.388.60364	-	DEPLOYED	
device-onboarding	Device Onboarding	2.1.388.60364	-	DEPLOYED	
disaster-recovery	Disaster Recovery	2.1.388.3600024	-	DEPLOYED	
dna-core-apps	Network Experience Platform - Core	2.1.388.60364	-	DEPLOYED	
dnac-platform	Cisco DNA Center Platform	1.6.1.126	-	DEPLOYED	
dnac-search	Cisco DNA Center Global Search	1.6.99.10	-	DEPLOYED	
endpoint-analytics	AI Endpoint Analytics	1.5.0.226	-	DEPLOYED	
group-based-policy-analytics	Group-Based Policy Analytics	2.2.3.55	-	DEPLOYED	
icap-automation	Automation - Intelligent Capture	2.1.388.60364	-	DEPLOYED	
image-management	Image Management	2.1.388.60364	-	DEPLOYED	
machine-reasoning	Machine Reasoning	2.1.388.210008	-	DEPLOYED	
ncp-system	NCP - Base	2.1.388.60364	-	DEPLOYED	
ndp-base-analytics	Network Data Platform - Base Analytics	1.6.1686	-	DEPLOYED	
ndp-platform	Network Data Platform - Core	1.6.1705	-	DEPLOYED	
ndp-ui	Network Data Platform - Manager	1.6.1662	-	DEPLOYED	
network-visibility	Network Controller Platform	2.1.388.60364	-	DEPLOYED	
path-trace	Path Trace	2.1.388.60364	-	DEPLOYED	
platform-ui	Cisco DNA Center UI	1.6.3.155	-	DEPLOYED	
rbac-extensions	RBAC Extensions	2.1.388.190003	-	DEPLOYED	
rogue-management	Rogue and aWIPS	2.3.0.24	-	DEPLOYED	
sd-access	SD Access	2.1.388.60364	-	DEPLOYED	
sensor-assurance	Assurance - Sensor	2.2.3.317	-	DEPLOYED	
sensor-automation	Automation - Sensor	2.1.388.60364	-	DEPLOYED	
ssa	Stealthwatch Security Analytics	2.1.388.1090064	-	DEPLOYED	
system	System	1.6.551	-	DEPLOYED	
system-commons	System Commons	2.1.388.60364	-	DEPLOYED	
umbrella	Cisco Umbrella	2.1.388.590077	-	DEPLOYED	
wide-area-bonjour	Wide Area Bonjour	2.4.364.75035	-	DEPLOYED	

- 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 Using the Maglev Wizard, on page 81](#).
- 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.

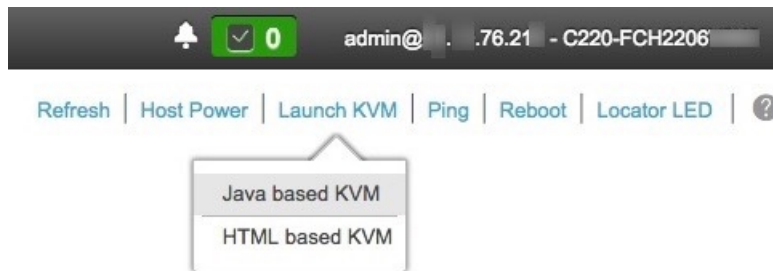
You can also access this information from the Cisco DNA Center GUI by clicking the **Help** icon (🔍) and choosing **About > Packages**.

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 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)**.

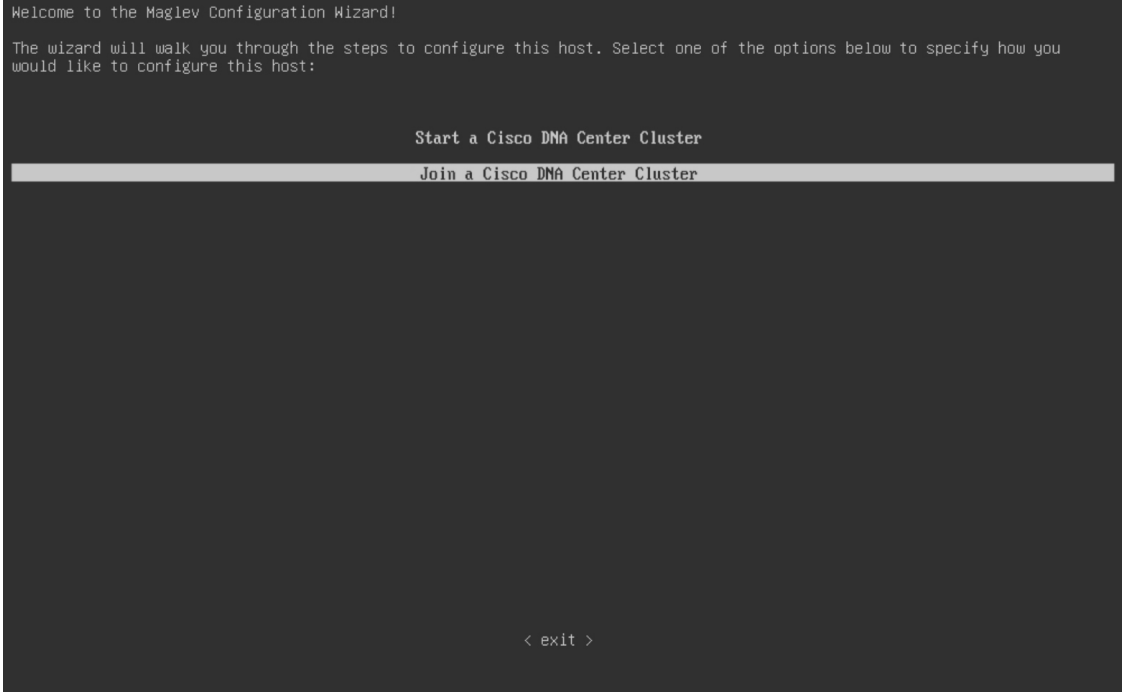
If you are asked to confirm your choice to reboot the appliance, click **OK**.

After displaying reboot messages, the KVM console displays the **Static IP Configuration** screen.



**Step 4** Click **Skip**.

The KVM console displays the Maglev Configuration wizard welcome screen.

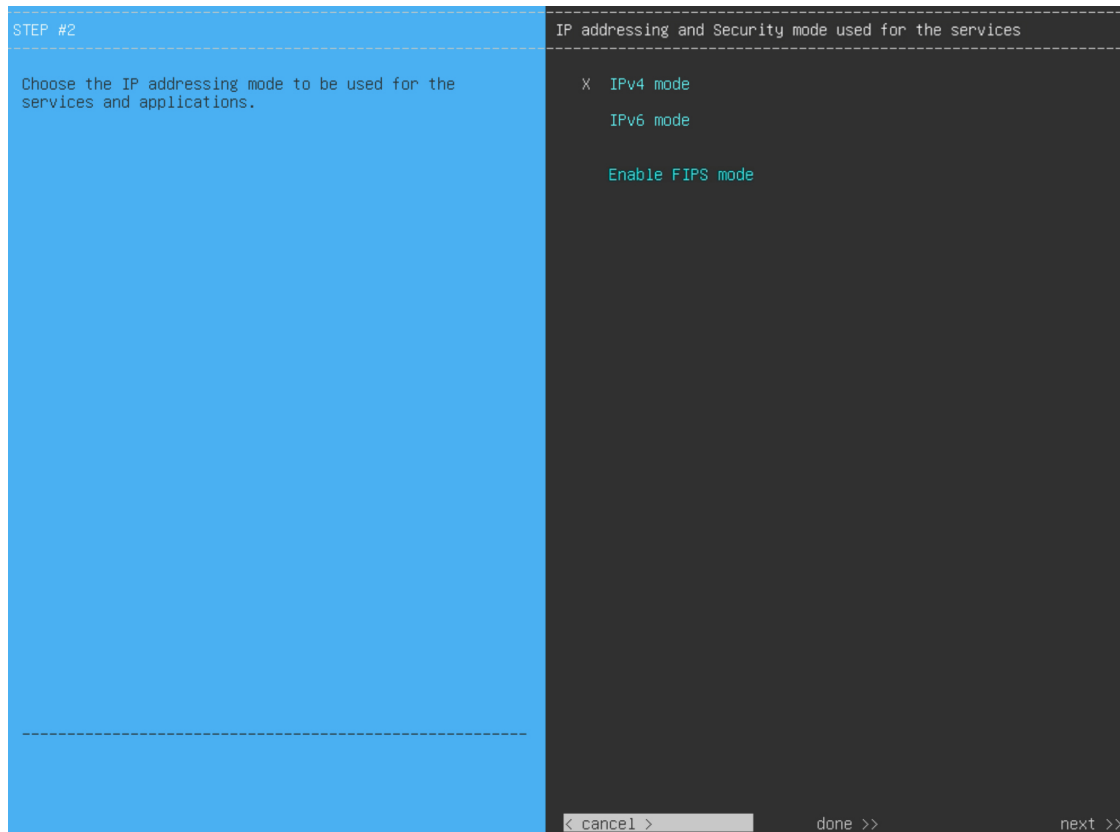




**Note** Only users that want to configure their appliance using one of the browser-based wizards without using the IP address, subnet mask, and default gateway assigned to the appliance's Enterprise interface by a DHCP server need to complete this screen.

**Step 5** Click **Join a Cisco DNA Center Cluster** to begin configuring the secondary node.

The screen updates.

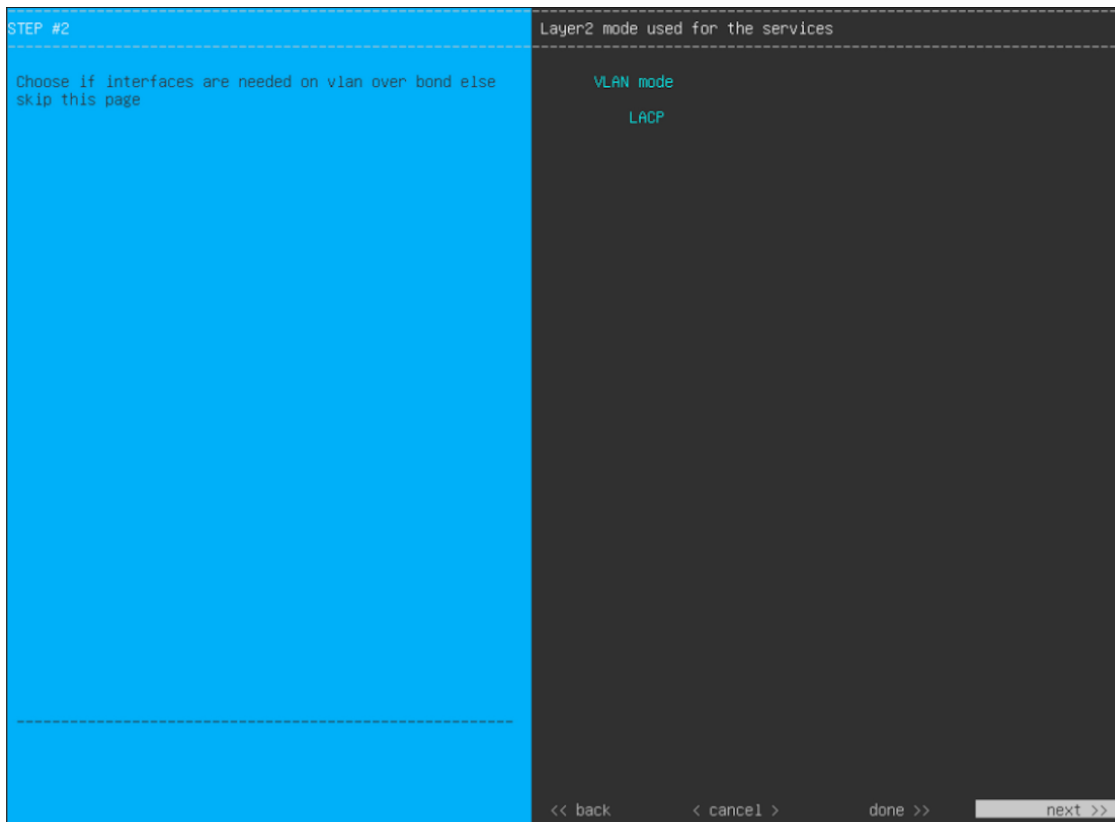


**Step 6** Do the following, then click **next>>** to proceed:

- Specify whether the applications and services running on your Cisco DNA Center appliance will use IPv4 or IPv6 addressing.
- (Optional) Check the **Enable FIPS Mode** check box to enable FIPS mode on your Cisco DNA Center appliance.

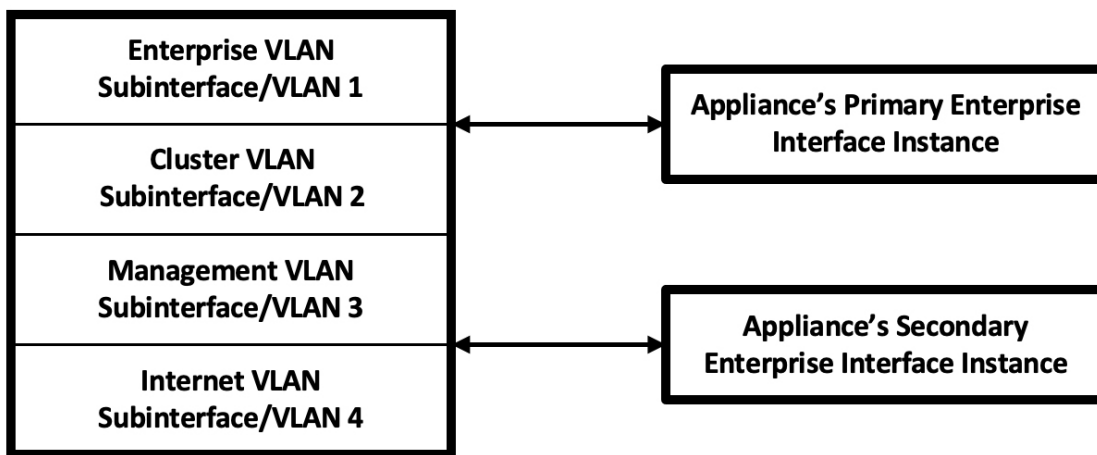
See [FIPS Mode Support, on page 102](#) for things to keep in mind when enabling FIPS mode on an appliance.

**Step 7** (Optional) Do the following to enable Layer 2 port channel mode (with VLAN tagging) for the appliance. This will create a single bonded interface that connects to your network using both the primary and secondary instance of your appliance's Enterprise interface. After making your selections, click **next>>** to proceed.



- a) Choose the **VLAN mode** option to enable dot1q/VLAN trunking and convert your appliance's Enterprise, Cluster, Management, and Internet interfaces into VLAN subinterfaces that reside on the bonded interface (as illustrated in the following figure). By default, this interface operates in Active-Backup mode (which enables HA).

**Bonded Interface**



- b) If you want this interface to operate in LACP mode instead (which enables load balancing and higher bandwidth), you must also choose the **LACP** option.
- c) When you enter the settings for your appliance's Enterprise and Cluster interfaces, ensure that you enter a unique VLAN ID in the **VLAN ID of Interface** field for the subinterfaces you want to configure on the virtual bonded interface.

- Important**
- The VLAN mode feature is not commonly used. Only enable it if it's required by your Cisco DNA Center deployment. If you just want to enable NIC bonding, you can do so in the next two wizard screens.
  - Even though one physical appliance interface (the Enterprise interface) is connected, you can configure all of the subinterfaces that reside on the virtual bonded interface.

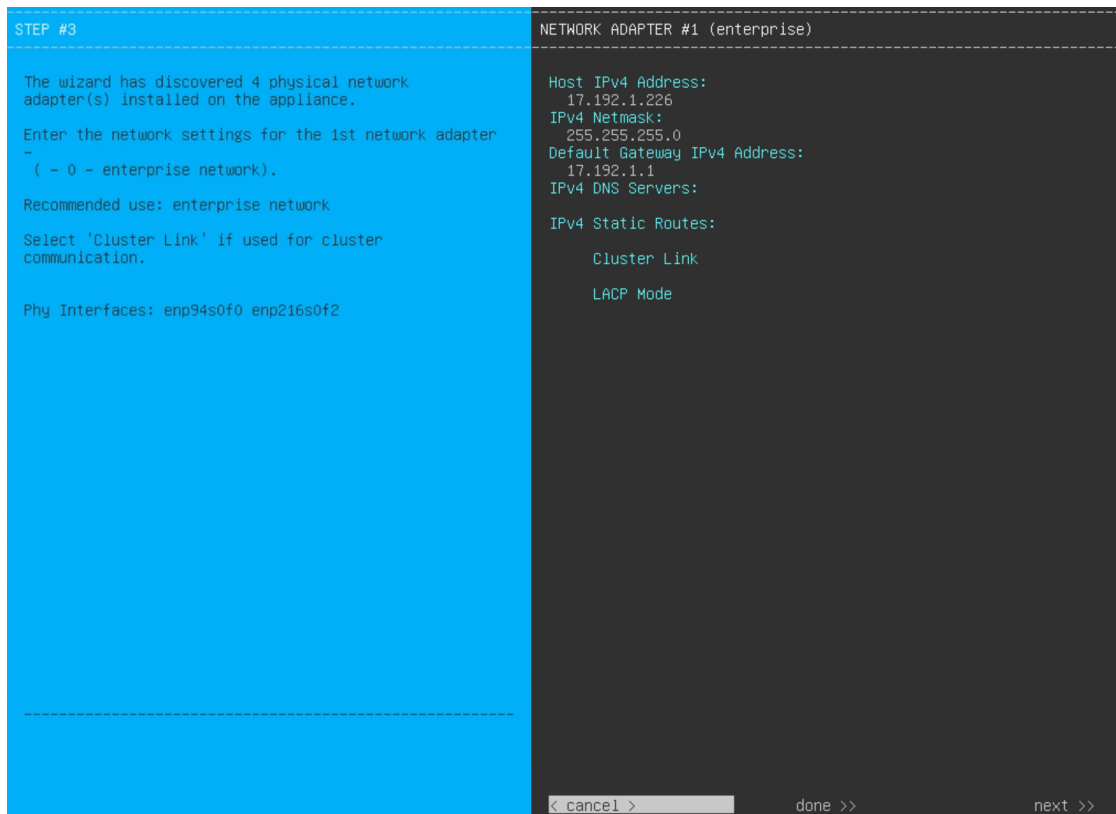
The wizard discovers all of the ports on the appliance and presents them to you one by one, in separate screens, in the following order:

- a. (Required) 10-Gbps Enterprise Port—Network Adapter #1
- b. (Required) 10-Gbps Cluster Port—Network Adapter #2
- c. (Optional) 1-Gbps/10-Gbps Management Port—Network Adapter #3
- d. (Optional) 1-Gbps/10-Gbps Internet Port—Network Adapter #4

If the wizard fails to display either or both of the Enterprise and Cluster ports during the course of configuration, it might indicate that these ports are nonfunctional or disabled. These two 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 contacting the Cisco Technical Assistance Center (for more information, see the "Get Assistance from the Cisco TAC" topic in the [Release Notes](#) document).

### Step 8

The wizard first presents the 10-Gbps Enterprise port as **NETWORK ADAPTER #1**. As explained in [Interface Cable Connections](#), this is a required port used 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 26: Secondary Node Entries for Network Adapter #1: 10-Gbps Enterprise Port**

Host IPv4/IPv6 Address field	Enter the IP address for the Enterprise port. This is required.
IPv4 Netmask/IPv6 Prefix Length field	Do one of the following if you entered an IP address: <ul style="list-style-type: none"> <li>• If you selected IPv4 addressing, enter the netmask for the port's IP address. This is required.</li> <li>• If you selected IPv6 addressing, enter the prefix length (in bits). Valid values range from 10 through 127.</li> </ul>
Default Gateway IPv4/IPv6 address field	Enter a default gateway IP address to use for the port. <p><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.</p>
IPv4/IPv6 DNS Servers field	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. <p><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.</p>

IPv4/IPv6 Static Routes field	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 Management port only.
Vlan Id of Interface field	Enter the VLAN ID that will be tagged over the LACP link to be created for the appliance you are configuring.  <b>Note</b> This field is displayed only if you set Layer 2 LACP portchannel mode for the appliance by choosing both options in the previous step.
Cluster Link field	Leave this field blank. It is required on the Cluster port only.
LACP Mode field	Do one of the following: <ul style="list-style-type: none"> <li>• Leave this field blank and the port will operate in <b>Active-Backup</b> mode. This mode provides fault tolerance by aggregating two Ethernet interfaces into a single logical channel. When the interface that's currently active goes down, the other interface takes its place and becomes active.</li> <li>• Check the check box to enable <b>LACP</b> mode on this port. This mode aggregates two Ethernet interfaces that share the same speed and duplex settings into a single logical channel. This provides load balancing and higher bandwidth.</li> </ul> <p>For more information about Cisco DNA Center's implementation of NIC bonding, see <a href="#">NIC Bonding Overview, on page 67</a>.</p> <b>Note</b> This field is displayed if you didn't choose any of the options in the previous step.

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 9

After successful validation of the Enterprise port values you entered, the wizard presents the 10-Gbps Cluster port and presents it 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).

STEP #3	OPTIONAL - NETWORK ADAPTER #2 (cluster)
<p>(Optional) Enter the network settings for the 2nd network adapter - (- 0 - intra-cluster link).</p> <p>Recommended use: Intra-cluster link</p> <p>Select 'Cluster Link' if used for cluster communication.</p> <p>Phy Interfaces: enp94s0f1 enp216s0f3</p>	<p>Host IPv4 Address: 169.254.6.64</p> <p>IPv4 Netmask: 255.255.255.128</p> <p>Default Gateway IPv4 Address:</p> <p>IPv4 DNS Servers:</p> <p>IPv4 Static Routes:</p> <p><input checked="" type="checkbox"/> Cluster Link</p> <p>LACP Mode</p>
<p>&lt;&lt; back      &lt; cancel &gt;      done &gt;&gt;      next &gt;&gt;</p>	

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

**Table 27: Secondary Node Entries for Network Adapter #2: 10-Gbps Cluster Port**

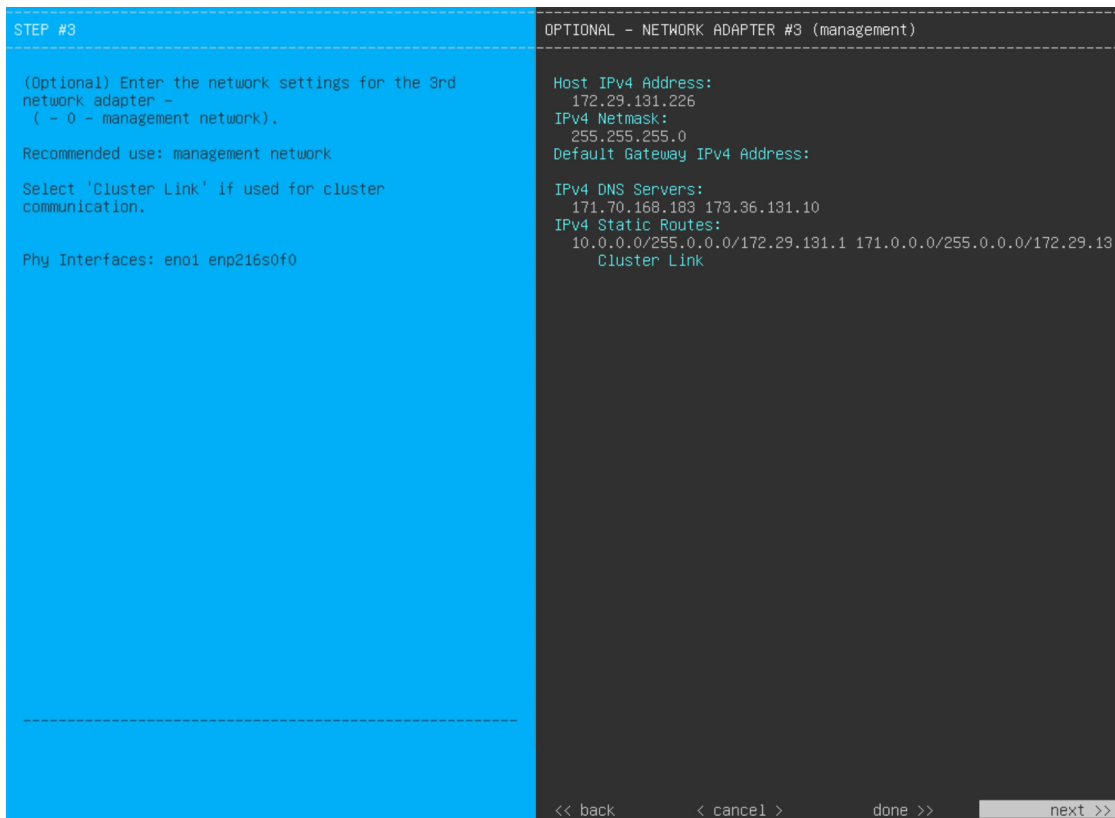
Host IPv4/IPv6 address field	Enter the IP address for the Cluster port. This is required. Note that you cannot change the address of the Cluster port later.
IPv4 Netmask/IPv6 Prefix Length field	Do one of the following if you entered an IP address: <ul style="list-style-type: none"> <li>• If you selected IPv4 addressing, enter the netmask for the port's IP address. This is required.</li> <li>• If you selected IPv6 addressing, enter the prefix length (in bits). Valid values range from 10 through 127.</li> </ul>
Default Gateway IPv4/IPv6 address field	Enter a default gateway IP address to use for the port. <p><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.</p>
IPv4/IPv6 DNS Servers field	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. <p><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.</p>

IPv4/IPv6 Static Routes field	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 Management port only.
Vlan Id of Interface field	Enter the VLAN ID that will be tagged over the LACP link to be created for the appliance you are configuring.  <b>Note</b> This field is displayed only if you set Layer 2 LACP portchannel mode for the appliance by choosing both options in Step 7.
Cluster Link field	Check the check box to set this port as the link to a Cisco DNA Center cluster. This is required on the Cluster port only.
LACP Mode field	Do one of the following: <ul style="list-style-type: none"> <li>• Leave this field blank and the port will operate in <b>Active-Backup</b> mode. This mode provides fault tolerance by aggregating two Ethernet interfaces into a single logical channel. When the interface that's currently active goes down, the other interface takes its place and becomes active.</li> <li>• Check the check box to enable <b>LACP</b> mode on this port. This mode aggregates two Ethernet interfaces that share the same speed and duplex settings into a single logical channel. This provides load balancing and higher bandwidth.</li> </ul> <p>For more information about Cisco DNA Center's implementation of NIC bonding, see <a href="#">NIC Bonding Overview, on page 67</a>.</p> <p><b>Note</b> This field is displayed if you didn't choose any of the options in Step 7.</p>

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 10

After successful validation of the Cluster port values you entered, the wizard presents the 1-Gbps/10-Gbps Management port and presents it 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 28: Secondary Node Entries for Network Adapter #3: 1-Gbps/10-Gbps Management Port**

Host IPv4/IPv6 address field	Enter the IP address for the Management Port. This is required only if you are using this port to access the Cisco DNA Center GUI from your management network; otherwise, you can leave it blank.
IPv4 Netmask/IPv6 Prefix Length field	Do one of the following: <ul style="list-style-type: none"> <li>• If you selected IPv4 addressing, enter the netmask for the port's IP address. This is required.</li> <li>• If you selected IPv6 addressing, enter the prefix length (in bits). Valid values range from 10 through 127.</li> </ul>
Default Gateway IPv4/IPv6 address field	Enter a default gateway IP address to use for the port. <p><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.</p>

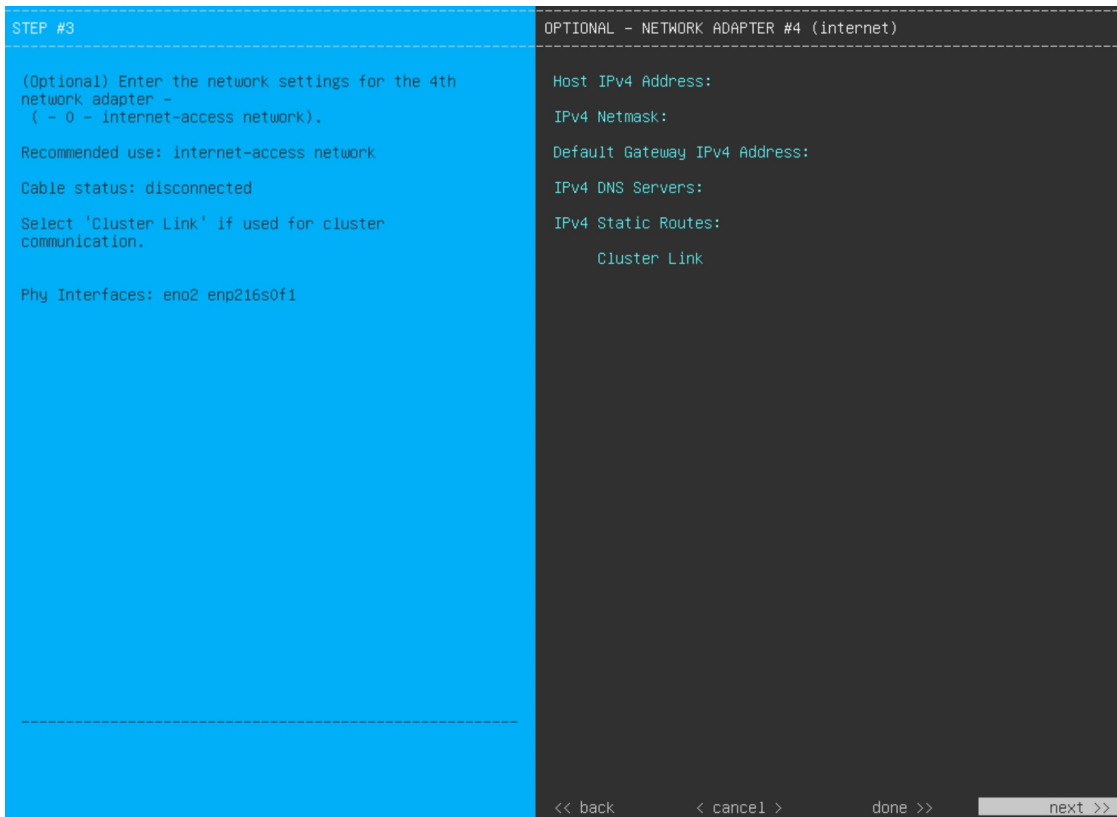


IPv4/IPv6 DNS Servers field	<p>Enter the IP address of the preferred DNS server. If you are entering multiple DNS servers, separate the IP addresses in the list with spaces.</p> <p><b>Important</b></p> <ul style="list-style-type: none"> <li>• For NTP, ensure port 123 (UDP) is open between Cisco DNA Center 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>
IPv4/IPv6 Static Routes field	<p>Enter one or more static routes in the following format, separated by spaces: <i>&lt;network&gt;/&lt;netmask&gt;/&lt;gateway&gt;</i>.</p>
Cluster Link field	<p>Leave this field blank. It is required on the Cluster port only.</p>

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 11**

After successful validation of the Management port values you entered, the wizard presents the 1-Gbps/10-Gbps Internet port 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. 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.

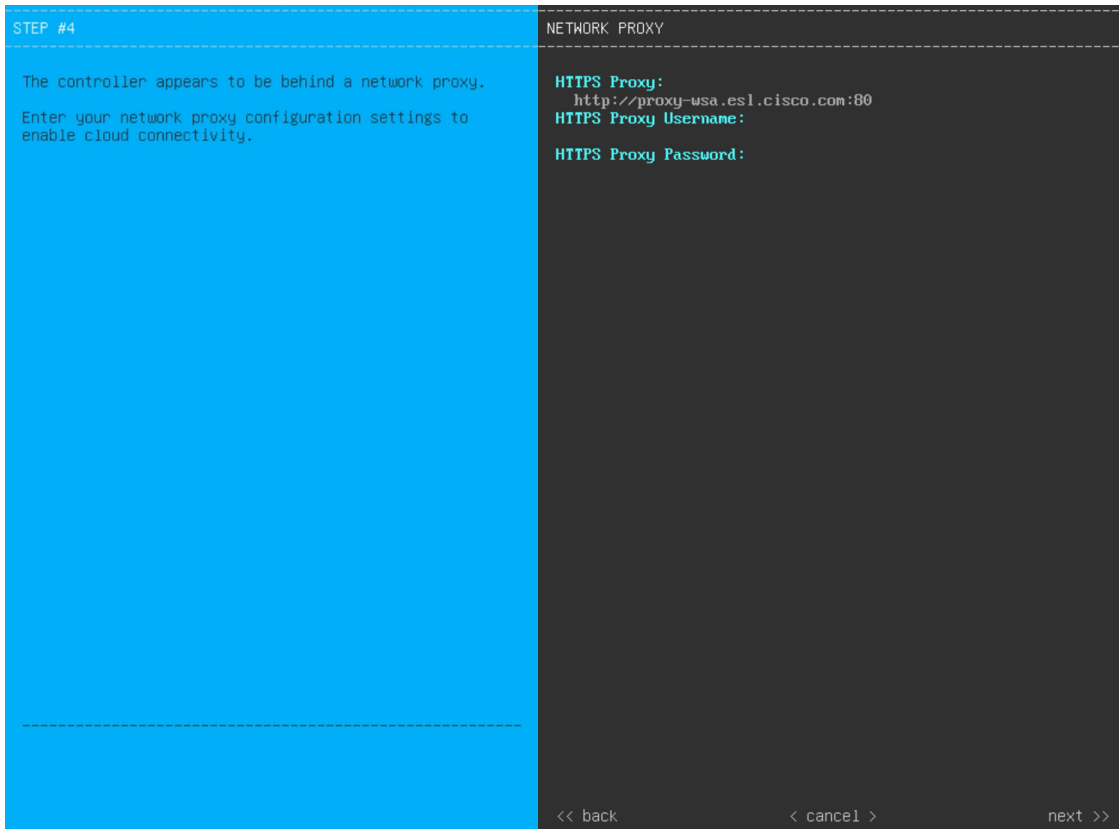
Table 29: Secondary Node Entries for Network Adapter #4: 1-Gbps/10-Gbps Internet Port

Host IPv4/IPv6 address field	Enter the IP address for the Internet port. This is required only if you are using the Internet port for internet connection; otherwise, you can leave it blank.
IPv4 Netmask/IPv6 Prefix Length field	Do one of the following: <ul style="list-style-type: none"> <li>• If you selected IPv4 addressing, enter the netmask for the port's IP address. This is required.</li> <li>• If you selected IPv6 addressing, enter the prefix length (in bits). Valid values range from 10 through 127.</li> </ul>
Default Gateway IPv4/IPv6 address field	Enter a default gateway IP address to use for the Internet 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.
IPv4/IPv6 DNS Servers field	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.
IPv4/IPv6 Static Routes field	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 Management port only.
Cluster Link field	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 12**

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.



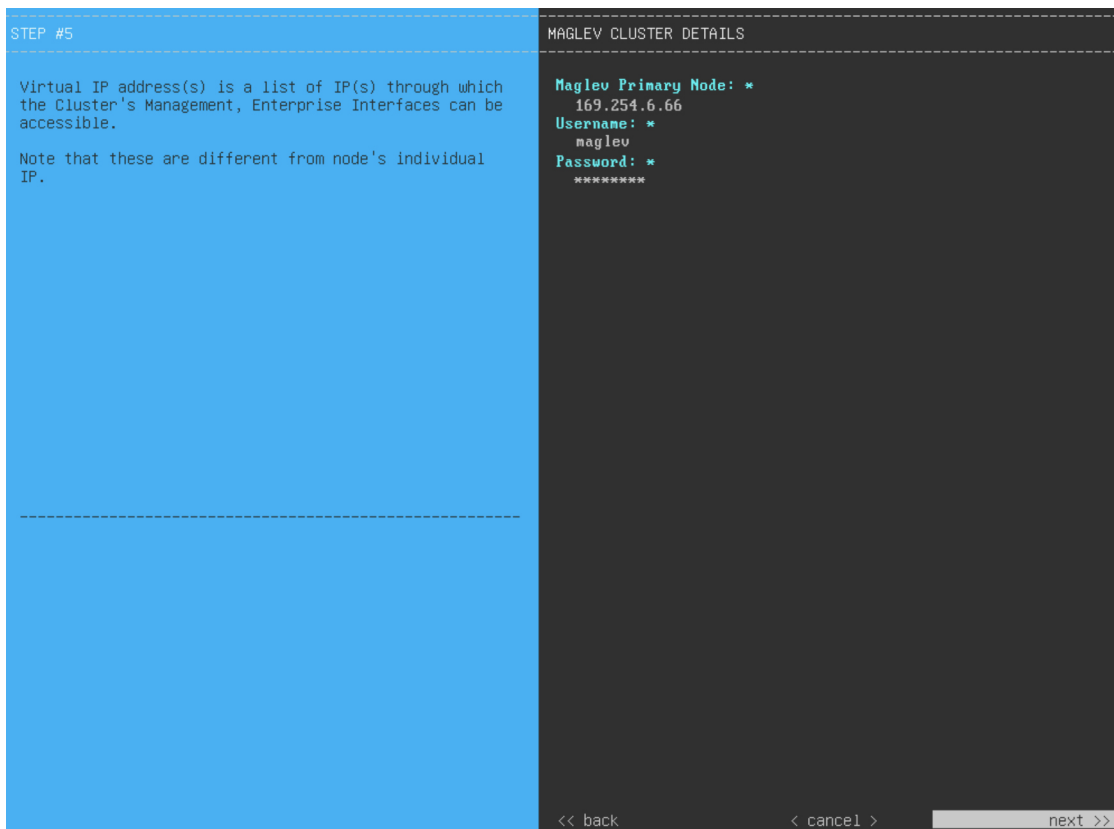
Enter the configuration values for the **NETWORK PROXY**, as shown in the table below.

**Table 30: Secondary Node Entries for Network Proxy**

HTTPS Proxy field	<p>Enter the URL or host name of an HTTPS network proxy used to access the Internet.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• Connection from Cisco DNA Center to the HTTPS proxy is supported only through HTTP in this release.</li> <li>• If you enter an IPv6 URL that contains a port number, enclose the IP address portion of the URL in square brackets. In this example, 443 is the port number: http://[2001:db8:85a3:8d3:1319:8a2e:370:7348]:443/</li> </ul>
HTTPS Proxy Username field	Enter the user name used to access the network proxy. If no proxy login is required, leave this field blank.
HTTPS Proxy Password field	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 13** 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).



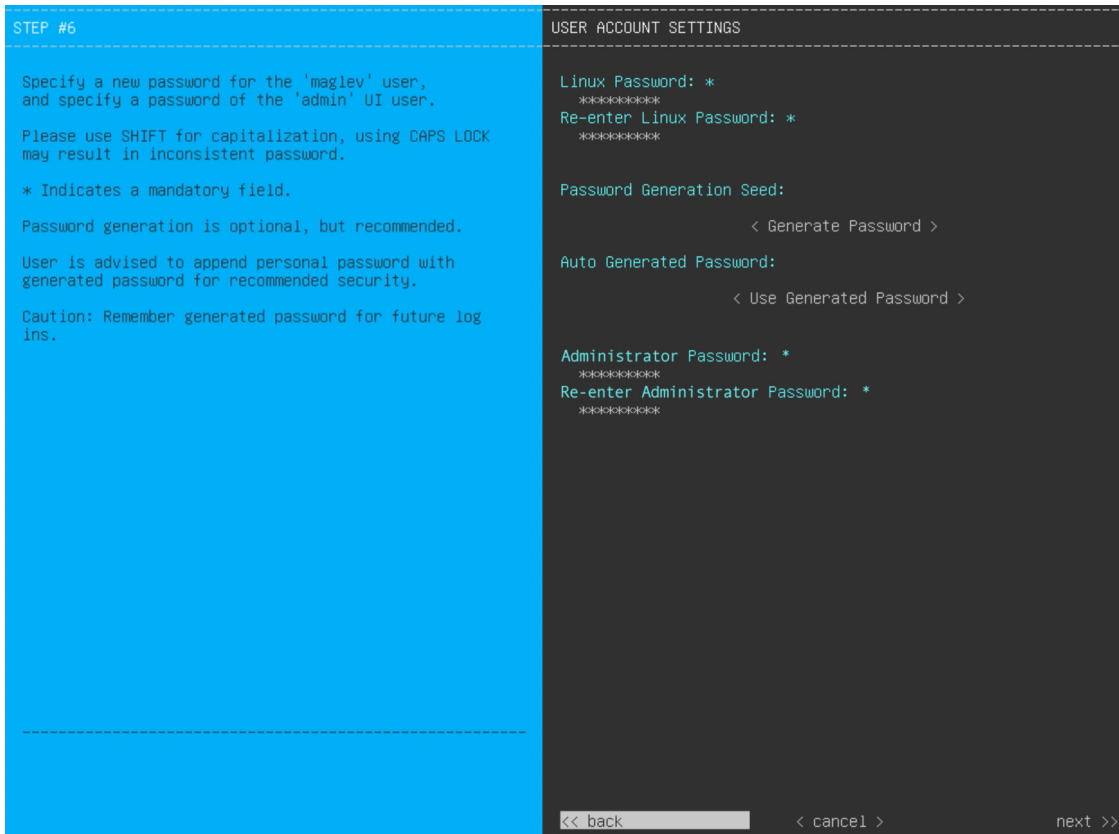
Enter the values for **MAGLEV CLUSTER DETAILS**, as shown in the table below.

**Table 31: Secondary Node Entries for Maglev Cluster Details**

Maglev Primary Node field	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 Network Adapter #2 on the primary node.
Username field	Enter <b>maglev</b> .
Password field	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 14** After you have entered the cluster details, the wizard prompts you to enter **USER ACCOUNT SETTINGS** values, as shown below.



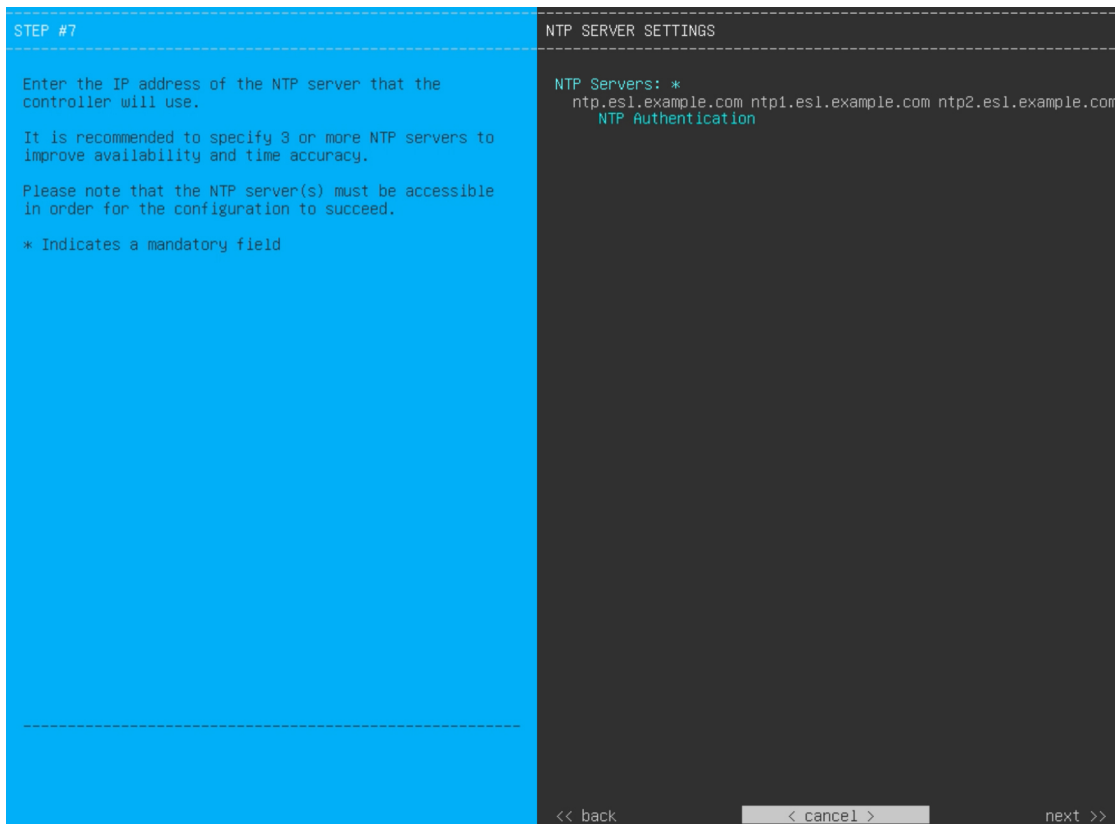
Enter the values for **USER ACCOUNT SETTINGS**, as shown in the table below.

**Table 32: Secondary Node Entries for User Account Settings**

Linux Password field	Enter a Linux password for the maglev user.
Re-enter Linux Password field	Confirm the Linux password by entering it a second time.
Password Generation Seed field	If you do not want to create the Linux password yourself, enter a seed phrase in this field and then press <b>&lt;Generate Password&gt;</b> to generate the password.
Auto Generated Password field	(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>&lt;Use Generated Password&gt;</b> to save the password.
Administrator Password field	Enter a password for the default admin superuser, used to log in to Cisco DNA Center for the first time.
Re-enter Administrator Password field	Confirm the administrator password 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 15** After you have entered the user account details, the wizard prompts you to enter **NTP SERVER SETTINGS** values.



Enter the values for **NTP SERVER SETTINGS**, as shown in the table below.

NTP Servers field	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.
NTP Authentication check box	<p>To enable the authentication of your NTP server before it's synchronized with Cisco DNA Center, check this check box and then enter the following information:</p> <ul style="list-style-type: none"> <li>• The NTP server's key ID. Valid values range between 1 and 4294967295 (2<sup>32</sup>-1). This value corresponds to the key ID that's defined in the NTP server's key file.</li> <li>• The SHA-1 key value associated with the NTP server's key ID. This 40-character hex string resides in the NTP server's key file.</li> </ul> <p><b>Note</b> Ensure that you enter a key ID and key value for each NTP server that you configured in the previous field.</p>

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 16** 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.

```
CONFIGURATION SUCCEEDED
The configuration wizard has completed successfully!
To access the Maglev Web UI, please point your browser to one of the following URLs:
To access the Maglev Web Console, please point your browser to one of the following URLs:
  https://17.192.1.226
  https://169.254.6.64
  https://172.29.131.226
The wizard will automatically close in 30 seconds
```

### 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

# Configure the 44/56-Core Appliance Using the Browser-Based Wizard

---

- [Appliance Configuration Overview](#), on page 123
- [Configure an Appliance Using the Install Configuration Wizard](#), on page 124
- [Configure the Primary Node Using the Advanced Install Configuration Wizard](#), on page 137
- [Configure a Secondary Node Using the Advanced Install Configuration Wizard](#), on page 156
- [Upgrade to the Latest Cisco DNA Center Release](#), on page 175

## Appliance Configuration Overview

You can deploy the 44 or 56-core appliance in your network in one of the following 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. If you choose Standalone mode for your initial deployment, this will be your first, or primary, node. Note that you can add more appliances later to form a cluster.
- **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 Cluster mode for your initial deployment, be sure to finish configuring the primary node before configuring the secondary nodes.

To proceed, first configure the primary node in your cluster. Then, if you have installed three appliances and want to add the second and third nodes to your cluster, configure the secondary nodes.

## Browser-Based Configuration Wizards

Cisco DNA Center offers two browser-based wizards that you can use to configure your appliance. Read their descriptions to determine which of these wizards you should complete.



---

**Important**

These wizards are available for use if you are configuring a new appliance that came with Cisco DNA Center 2.3.4 already installed. If you upgraded from a previous version and want to use these wizards, contact Cisco TAC for assistance.

---

### Install Configuration Wizard

This wizard streamlines the appliance configuration process by setting default values for the Enterprise, Management, and Internet Access interfaces (which all reside on the appliance's Enterprise port) as well as the Intracluster interface. Use this wizard if you are okay with using the default interface settings and want to get your appliance up and running as quickly as possible. Note that you cannot use this wizard to do the following:

- To configure a cluster's secondary nodes.
- To configure a first-generation 44-core Cisco DNA Center appliance.

### Advanced Install Configuration Wizard

This wizard provides access to all of the available appliance settings that you can modify. Use this wizard if you want to specify interface settings that are different from the default settings. Also use this wizard if you are configuring the second or third node in your cluster.

## Browser-Based Wizard Prerequisites

To use either of the browser-based wizards and ensure that it configures your appliance properly, complete the following tasks:

- Designate the Enterprise interface on your appliance to use the IP address, subnet mask, and default gateway that a DHCP server assigns to it. When you configure this interface in the wizard, you will not be able to change the IP address or subnet mask that have been assigned to it. You will only be able to change its default gateway. The topics in this chapter assume that the Enterprise interface was chosen for this purpose.
- Confirm that the IP address assigned by the DHCP server is reachable by the machine from which you will complete the wizard.
- For the Enterprise and Intracluster interfaces, verify that both interfaces are connected and in the **UP** state.

If you want to specify your own IP address, subnet mask, and default gateway for your appliance's Enterprise interface (and not use the values assigned by a DHCP server), ensure that you complete the Static IP Address Settings screen.

## Configure an Appliance Using the Install Configuration Wizard

Perform this procedure to configure either a three-node cluster's primary node or a standalone node using the Install configuration wizard. The wizard simplifies the configuration process by setting up the Enterprise, Management, and Internet interfaces on the same port using default settings. The following second generation Cisco DNA Center appliances support configuration using this wizard:

- 44-core appliance: Cisco part number DN2-HW-APL
- 44-core promotional appliance: Cisco part number DN2-HW-APL-U
- 56-core appliance: Cisco part number DN2-HW-APL-L
- 56-core promotional appliance: Cisco part number DN2-HW-APL-L-U

The first generation 44-core Cisco DNA Center appliance (Cisco part number DN1-HW-APL) *cannot* be configured using this wizard.



---

**Important**

- You can only use this wizard to complete the initial configuration of a new Cisco DNA Center appliance. To reimage an appliance that's been configured previously, you will need to use the Maglev Configuration wizard (see [Configure the Appliance Using the Maglev Wizard, on page 81](#)).
  - You cannot use this wizard to configure the second or third appliance in a three-node cluster. To do so, complete the steps described in [Configure a Secondary Node Using the Advanced Install Configuration Wizard, on page 156](#). Also, you cannot use this wizard to enable LACP mode on your appliance's Enterprise and Intracluster interfaces.
  - Before you configure any of 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.
  - 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.
- 

**Before you begin**

Ensure that you:

- Installed the Cisco DNA Center software image onto your appliance, as described in [Reimage the Appliance, on page 74](#).



---

**Important**

This is only applicable if you are going to configure a promotional appliance, because the Cisco DNA Center software image is not preinstalled on the following appliances:

- 44-core promotional appliance (Cisco part number DN2-HW-APL-U)
  - 56-core promotional appliance: (Cisco part number DN2-HW-APL-L-U)
- 
- Collected all of the information called for in [Required IP Addresses and Subnets, on page 29](#) and [Required Configuration Information](#).
  - Installed the appliance as described in [Appliance Installation Workflow](#).
  - Configured Cisco IMC browser access on this appliance, as described in [Enable Browser Access to Cisco Integrated Management Controller](#).
  - Checked that the appliance's ports and the switches it uses are properly configured, as described in [Execute Preconfiguration Checks](#).
  - Are using a browser that is compatible with Cisco IMC and Cisco DNA Center. For a list of compatible browsers, see the [Release Notes](#) for the version of Cisco DNA Center you are installing.

- Enabled ICMP on the firewall between Cisco DNA Center and the DNS servers you will specify in the following procedure. This wizard uses Ping to verify the DNS server you specify. This ping can be blocked if there is a firewall between Cisco DNA Center and the DNS server and ICMP is not enabled on that firewall. When this happens, you will not be able to complete the wizard.

**Step 1**

Start the Install configuration wizard:

- Point your browser to the Cisco IMC IP address you set during the Cisco IMC GUI configuration you performed, then 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 blue link menu at the upper right, as shown below.



- From the blue link menu, choose **Launch KVM** and then select either **Java based KVM** or **HTML based KVM**. If you select the 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 the HTML-based KVM, it will launch the KVM console in a separate browser 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 Maglev Configuration Wizard prompts.

- 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**. Then switch to the KVM console to continue.
  - In the KVM console: Choose **Power > Power Cycle System (cold boot)**.

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

After displaying reboot messages, the KVM console displays the **Static IP Configuration** screen.

```

STEP #None
-----
Welcome to the Maglev Configuration Wizard!

Please Enter Static IP Information for Enterprise Interface Configuration,
Static IP is configured as an alternative to DHCP for web UI Configuration.
- Click Configure after entering Information for configuring IP which will
be configured on Enterprise Interface
- Click Skip to move to config wizard

NOTE: Default Configuration mode is IPv4, Please select IPv6 mode for Ipv6
Configuration

-----

STATIC IP CONFIGURATION

IPv6 mode

IP Address:
Netmask:
Default Gateway Address:
Static Routes:

Web installation:
https://10.106.172.47:9004/

-----
< cancel >      skip >>      configure >>

```

Note the URL listed in the **Web Installation** field.

d) Do one of the following:

- If you want a DHCP server to assign an IP address, subnet mask, and default gateway to your appliance's Enterprise interface, click **Skip**.
- If you want to assign your own IP address, subnet mask, and default gateway to your appliance's Enterprise interface, enter the information described in the following table and then click **Configure**.

IPv6 Mode check box	If you want to configure an IPv6 address, check this check box.
IP Address field	Enter the static IP address you want to use.
Netmask field	Enter the netmask for the IP address you specified in the previous field: <ul style="list-style-type: none"> <li>• If you entered an IPv4 address, you can enter either a netmask or CIDR address.</li> <li>• If you entered an IPv6 address, you can only enter a CIDR address.</li> </ul>
Default Gateway Address field	Specify the default gateway that will be used to route traffic.
Static Routes field	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 Management port only.

The KVM console displays the Maglev Configuration wizard welcome screen.

```
Welcome to the Maglev Configuration Wizard!  
The wizard will walk you through the steps to configure this host. Select one of the options below to specify how you  
would like to configure this host:  
  
Start a Cisco DNA Center Cluster  
Join a Cisco DNA Center Cluster  
  
< exit >
```

- e) To bring up the **Appliance Configuration** screen, open the URL that was displayed in the **Static IP Configuration** screen.

Cisco DNA Center Appliance Configuration

Welcome to Cisco DNA Center


Are you starting a new Cisco DNA Center Cluster or joining an existing one?

Start A Cisco DNA Center Cluster

This appliance will be the primary node of a cluster.

Join A Cisco DNA Center Cluster

This appliance will be added as a node to the primary node of a cluster.



Next

- f) Click the **Start a Cisco DNA Center Cluster** radio button, then click **Next**.

Cisco DNA Center

Appliance Configuration

Welcome to Cisco DNA Center

Before you can use Cisco DNA Center, first complete the appropriate appliance configuration workflow. Which workflow matches your needs?

**Install**


Configure a standalone node or **cluster's primary node**.

Use this quick, simplified wizard to set up the Enterprise, Management, and Internet interfaces on the same interface with default settings.

**Advanced Install**

Configure a standalone node or **any node in a cluster**.

Use this wizard to access all of the available appliance configuration options.



Back
Start

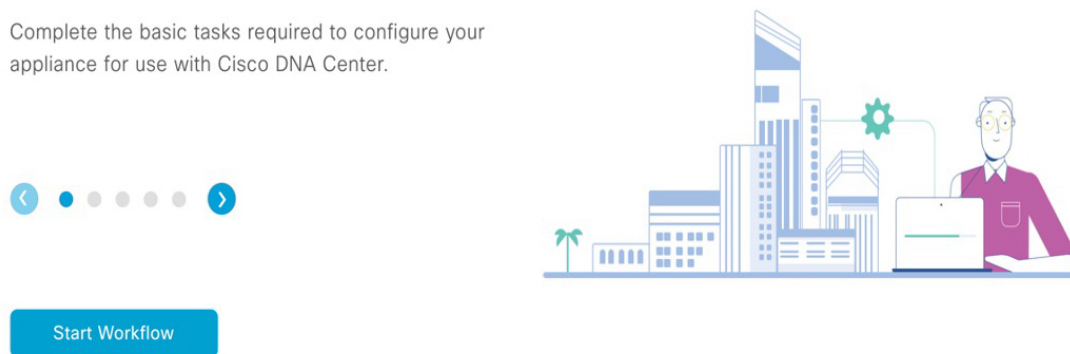
- g) Click the **Install** radio button, then click **Start**.

The **Overview** slider opens. Click > to view a summary of the tasks that the wizard will help you complete.

✕

## Overview

Complete the basic tasks required to configure your appliance for use with Cisco DNA Center.



- h) Click **Start Workflow** to start the wizard.

The **Appliance Interface Overview** screen opens, providing a description of the four interfaces that are available on your Cisco DNA Center appliance:



Cisco DNA Center
Install

## Appliance Interface Overview

In order for Cisco DNA Center to operate properly, you need to configure four interfaces on your appliance:

1. **Enterprise Network Interface:** Connects your appliance to the Enterprise network.
2. **Intracluster Link Interface:** Connects your appliance to your cluster.
3. **Management Network Interface:** (Optional) Accesses the Cisco DNA GUI from your Management network.
4. **Internet Access Interface:** (Optional) Accesses the internet.

In this workflow, the Intracluster Link Interface is predefined. The other 3 interfaces will be configured together on the Enterprise port.

Exit
Next

The wizard will help you configure the Enterprise and Intracluster ports, which are required for Cisco DNA Center functionality. If the wizard fails to display either or both of these ports in the next screen, they may be non-functional or disabled. If you discover that they are non-functional, choose **Exit** to exit the wizard 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 2 Complete the Install configuration wizard:

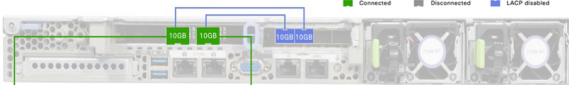
a) Click **Next**.

The **Configure The Enterprise Port** screen opens.

Cisco DNA Center
Install

## Configure the Enterprise Port

In this workflow, the Management Network and Internet Access Interfaces are on the same port as the Enterprise Network Interface. You can enter up to three DNS addresses. If your network resides behind a firewall, you must [allow access to these URLs](#) and [open these ports](#). If you are setting up a multinode cluster, the cluster's second and third nodes must reside in the same subnet as the primary node. [Download the Intracluster Link interface's information](#)



**Enterprise & Management Network & Internet Access Interface**

LACP Mode: Disabled

IP Address: 10.106.172.47

Netmask: 255.255.255.128

Default Gateway: 10.106.172.1

**Intracluster Link Interface**

Interface Name: cluster

LACP Mode: Disabled

IP Address: 169.254.6.66

Subnet Mask: 255.255.255.128

Exit
Next

The configuration wizard sets up the Enterprise, Management, and Internet Access interfaces on the Enterprise port. The wizard also prepopulates values for almost all of the listed parameters.

If your network resides behind a firewall, do the following:

- Click the **allow access to these URLs** link to view a popup window that lists the URLs that Cisco DNA Center must be able to access.
- Click the **open these ports** link to view a popup window that lists the network service ports that must be available for Cisco DNA Center to use.

b) Click **Next**.

The **DNS Configuration** screen opens.

c) In the **DNS** field, enter the IP address of the preferred DNS server. To enter additional DNS servers, click the **Add (+)** icon.

**Important** You can configure a maximum of three DNS servers. Problems can occur if you configure more than three DNS servers for an appliance.

d) Click **Next**.

The wizard validates the information you have entered, confirms that the port is up, and notifies you of any settings that need to be changed before you can proceed with the wizard. If the settings you have entered are valid and the port is up, the wizard's **Interface to Port Configuration** screen opens.

Cisco DNA Center Install

### Interface to Port Configuration

We are going to configure the following interfaces. Click Configure and wait for configuration to be done before proceeding to the next step.

[Configure](#)

**Enterprise & Management Network & Internet Access Interface**

Interface Name	enterprise
LACP Mode	Disabled
IP Address	10.106.172.47
Netmask	255.255.255.128
Default Gateway	10.106.172.1

**Intracluster Link Interface**

Interface Name	cluster
LACP Mode	Disabled
IP Address	169.254.6.66
Subnet Mask	255.255.255.128

[Exit](#) [Back](#) [Next](#)

- e) Review the interface settings that have been set, then click **Configure**.
- f) After initial interface configuration has completed, click **Next** to proceed to the next wizard screen.

The **Configure Proxy Server Information** screen opens.

Cisco DNA Center Install

### Configure Proxy Server Information

Does your network use a proxy server to access the internet?

Yes  No

Proxy Server\*  
 E.g. http://example.com

Port\*  
 Enter port number between 0 to 65535.

[Exit](#) [Review](#) [Back](#) [Next](#)

- g) Do one of the following:
- If your network does *not* use a proxy server to access the internet, click the **No** radio button and then click **Next**.
  - If your network does use a proxy server to access the internet, enter the values described in the following table:

**Table 33: Primary Node Entries for Proxy Server Settings**

Proxy Server field	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.
Port field	Enter the port your appliance used to access the network proxy.
Username field	Enter the user name used to access the network proxy. If no proxy login is required, leave this field blank.
Password field	Enter the password used to access the network proxy. If no proxy login is required, leave this field blank.

The wizard validates the information you have entered and notifies you of any settings that need to be changed before you can proceed with the wizard. If the settings you have entered are valid, the wizard's **Advanced Appliance Settings** screen opens.

- h) Enter configuration values for your cluster, then click **Next**.

**Table 34: Primary Node Entries for Advanced Appliance Settings**

Cluster Virtual IP Addresses	
To access from Enterprise Network and For Intracluster Access fields	Enter the virtual IP address that will be used for traffic between the cluster and both the Enterprise and Intracluster interfaces on your appliance. This is required for single-node clusters that will be converted into a three-node cluster in the future. If you have a single-node cluster setup and don't plan to move to a three-node cluster setup, you can leave the fields in this section blank.  <b>Important</b> If you choose to configure a virtual IP address, you must enter one 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 <b>UP</b> state.

Fully Qualified Domain Name (FQDN) field	<p>Enter the fully qualified domain name (FQDN) for your cluster. Cisco DNA Center does the following with this hostname:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> </ul>
<b>NTP Server Settings</b>	
NTP Server field	<p>Enter at least one NTP server address or hostname. To enter additional NTP server addresses or hostnames, click the <b>Add (+)</b> icon.</p> <p>For a production deployment, Cisco recommends that you configure a minimum of three NTP servers.</p>
<b>Subnet Settings</b>	
Container Subnet field	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 you cannot enter another subnet.
Cluster Subnet field	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 you cannot enter another subnet.

The **Enter CLI Password** screen opens.

Cisco DNA Center Install

Enter CLI Password

CLI Password: Identifies the password for the CLI username maglev. This password ensures secure access to each appliance using the CLI command line. If required, you can assign a different CLI password for each maglev CLI username on each appliance in a cluster.

Username\*  
maglev

Password\*  
..... [SHOW](#)

[View Password Criteria](#)

Retype to Confirm\*  
..... [SHOW](#)

[Exit](#) [Review](#) [Back](#) [Next](#)

- i) Enter and confirm the password for the `maglev` user, then click **Next**.

The wizard validates the information you have entered and notifies you of any settings that need to be changed before you can proceed with the wizard. If the settings you have entered are valid, the wizard's **Summary** screen opens.

Cisco DNA Center Install

### Summary

Please review the settings that you have entered. If you need to make any changes, click the appropriate [Edit](#) link and make the necessary updates. You can download the generated configuration in JSON format from [here](#). When you are happy with your settings, click [Start Configuration](#).

Enterprise Port [Edit](#)

**Enterprise & Management Network & Internet Access Interface**

Interface Name: enterprise

LACP Mode: Disabled

IP Address: 10.106.172.47

Netmask: 255.255.255.128

Default Gateway: 10.106.172.1

**Intracluster Link Interface**

Interface Name: cluster

LACP Mode: Disabled

IP Address: 169.254.6.66

Subnet Mask: 255.255.255.128

**Note** To download the appliance configuration as a JSON file, click the [here](#) link.

- j) Scroll to the bottom of the screen and review all of the settings that you have entered while completing the wizard. If necessary, click the appropriate **Edit** link to open the wizard screen in which you want to make updates.
- k) To complete the configuration of your Cisco DNA Center appliance, click **Start Configuration**.

The wizard screen continuously updates during the process, indicating the tasks that are currently being completed and their progress, as well as any errors that have occurred. To save a local copy of this information as a text file, click the **Download** link.

Cisco DNA Center Install

## Appliance Configuration In Progress

It should take about 30 minutes to configure the appliance. **Do not press your browser's back button or refresh this page.** The page will update after configuration completes.

Initializing the cluster using kubeadm 30%

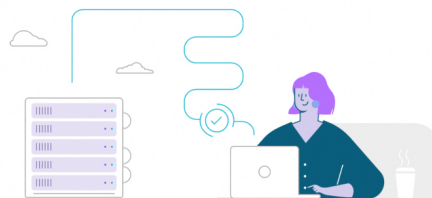
Started: 04/09/2020 12:15:36

[Download](#)

```

17:40:20 2021 GMT
2021-12-03T05:37:06.616Z14 | kubelet.conf Apr
13 12:12:14 2020 GMT Apr 13 17:40:21 2021 GMT
2021-12-03T05:37:06.616Z15 | admin.conf Apr 13
12:12:14 2020 GMT Apr 13 17:40:21 2021 GMT
2021-12-03T05:37:06.616Z16 | scheduler.conf Apr
13 12:12:14 2020 GMT Apr 13 17:40:22 2021 GMT
2021-12-03T05:37:06.616Z17 | controller-
manager.conf Apr 13 12:12:14 2020 GMT Apr 13
17:40:22 2021 GMT
2021-12-03T05:37:06.616Z18 | -----
-----
-----

```




- Step 3** After appliance configuration completes, click the copy icon in the **Cisco DNA Center - Admin Credential** area to copy the default admin superuser password.

Cisco DNA Center

Install

## Appliance Configuration Complete!

**Important:** Take note of the credentials displayed below. You can click the copy icon  if you want to save them locally. You will use these credentials to log in to Cisco DNA Center for the first time. After logging in, you will be prompted to change the password.



CISCO DNA CENTER - ADMIN CREDENTIAL	
Username	admin
password	maglev1@3

What's Next?

[Open Cisco DNA Center](#)

**Important** Cisco DNA Center automatically sets this password when you complete the Install configuration wizard. Ensure that you click the copy icon before you proceed. Otherwise, you will not be able to log in to Cisco DNA Center for the first time.

**Note** As a security measure, you'll be prompted to change this password after you log in. For more information, see [Complete the Quick Start Workflow, on page 229](#).

### What to do next

As you are deploying this appliance in standalone mode, continue by performing first-time setup: [First-Time Setup Workflow](#).

# Configure the Primary Node Using the Advanced Install Configuration Wizard

Perform the following steps to configure the first installed appliance as the primary node using the Advanced Install configuration wizard. You must always configure the first appliance as the primary node, whether it will operate standalone or as part of a cluster.

**Important**

- The following second generation Cisco DNA Center appliances support configuration using this wizard:
  - 44-core appliance: Cisco part number DN2-HW-APL
  - 44-core promotional appliance: Cisco part number DN2-HW-APL-U
  - 56-core appliance: Cisco part number DN2-HW-APL-L
  - 56-core promotional appliance: Cisco part number DN2-HW-APL-L-U

The first generation 44-core Cisco DNA Center appliance (Cisco part number DN1-HW-APL) *cannot* be configured using this wizard.

- You can only use this wizard to complete the initial configuration of a new Cisco DNA Center appliance. To reimage an appliance that's been configured previously, you will need to use the Maglev Configuration wizard (see [Configure the Appliance Using the Maglev Wizard, on page 81](#)).
- 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.
- 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.

If you are configuring the installed appliance as a secondary node for an existing cluster that already has a primary node, follow the steps in [Configure a Secondary Node Using the Advanced Install Configuration Wizard, on page 156](#) instead.

**Before you begin**

Ensure that you:

- Installed the Cisco DNA Center software image onto your appliance, as described in [Reimage the Appliance, on page 74](#).

**Important**

This is only applicable if you are going to configure a promotional appliance, because the Cisco DNA Center software image is not preinstalled on the following appliances:

- 44-core promotional appliance (Cisco part number DN2-HW-APL-U)
  - 56-core promotional appliance: (Cisco part number DN2-HW-APL-L-U)
- 
- Collected all of the information called for in [Required IP Addresses and Subnets, on page 29](#) 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's ports and the switches it uses are properly configured, as described in [Execute Preconfiguration Checks](#).
- Are using a browser that is compatible with Cisco IMC and Cisco DNA Center. For a list of compatible browsers, see the [Release Notes](#) 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 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**

Start the Advanced Install configuration wizard:

- Point your browser to the Cisco IMC IP address you set during the Cisco IMC GUI configuration you performed, then 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 blue link menu at the upper right, as shown below.



- From the blue link menu, choose **Launch KVM** and then select either **Java based KVM** or **HTML based KVM**. If you select the 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 the HTML-based KVM, it will launch the KVM console in a separate browser 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 Maglev Configuration Wizard prompts.

- 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**. Then switch to the KVM console to continue.
  - In the KVM console: Choose **Power > Power Cycle System (cold boot)**.

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

After displaying reboot messages, the KVM console displays the **Static IP Configuration** screen.

```

STEP #None
-----
Welcome to the Maglev Configuration Wizard!

Please Enter Static IP Information for Enterprise Interface Configuration,
Static IP is configured as an alternative to DHCP for web UI Configuration.
- Click Configure after entering Information for configuring IP which will
be configured on Enterprise Interface
- Click Skip to move to config wizard

NOTE: Default Configuration mode is IPv4,
Please select IPv6 mode for Ipv6 Configuration

-----
STATIC IP CONFIGURATION

IPv6 mode

IP Address:

Netmask:

Default Gateway Address:

Static Routes:

Web installation:
https://10.106.172.47:9004/

-----
< cancel >      skip >>      configure >>

```

Note the URL listed in the **Web Installation** field.

d) Do one of the following:

- If you want a DHCP server to assign an IP address, subnet mask, and default gateway to your appliance's Enterprise interface, click **Skip**.
- If you want to assign your own IP address, subnet mask, and default gateway to your appliance's Enterprise interface, enter the information described in the following table and then click **Configure**.

IPv6 Mode check box	If you want to configure an IPv6 address, check this check box.
IP Address field	Enter the static IP address you want to use.
Netmask field	Enter the netmask for the IP address you specified in the previous field: <ul style="list-style-type: none"> <li>• If you entered an IPv4 address, you can enter either a netmask or CIDR address.</li> <li>• If you entered an IPv6 address, you can only enter a CIDR address.</li> </ul>
Default Gateway Address field	Specify the default gateway that will be used to route traffic.
Static Routes field	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 Management port only.

The KVM console displays the Maglev Configuration wizard welcome screen.

```
Welcome to the Maglev Configuration Wizard!

The wizard will walk you through the steps to configure this host. Select one of the options below to specify how you
would like to configure this host:

Start a Cisco DNA Center Cluster
Join a Cisco DNA Center Cluster

< exit >
```

- e) To bring up the **Appliance Configuration** screen, open the URL that was displayed in the **Static IP Configuration** screen.

Cisco DNA Center

Appliance Configuration

Welcome to Cisco DNA Center

Are you starting a new Cisco DNA Center Cluster or joining an existing one?

Start A Cisco DNA  
Center Cluster

This appliance will be the primary  
node of a cluster.

Join A Cisco DNA  
Center Cluster

This appliance will be added as a  
node to the primary node of a cluster.



Next

- f) Click the **Start a Cisco DNA Center Cluster** radio button, then click **Next**.

Cisco DNA Center Appliance Configuration

Welcome to Cisco DNA Center

Before you can use Cisco DNA Center, first complete the appropriate appliance configuration workflow. Which workflow matches your needs?

**Install**


Configure a standalone node or cluster's **primary node**.

Use this quick, simplified wizard to set up the Enterprise, Management, and Internet interfaces on the same interface with default settings.

**Advanced Install**

Configure a standalone node or **any node in a cluster**.

Use this wizard to access all of the available appliance configuration options.



- g) Click the **Advanced Install** radio button, then click **Start**.

The **Advanced Install Overview** slider opens. Click > to view a summary of the tasks that the wizard will help you complete.

### Advanced Install Overview

Prepare your appliance for use with Cisco DNA Center by configuring its interfaces and entering cluster and other required information.



- h) Click **Start Workflow** to start the wizard.

The **Appliance Interface Overview** screen opens, providing a description of the four appliance interfaces that you can configure.

The screenshot shows the 'Cisco DNA Center' interface with 'Advanced Install' selected. The main heading is 'Appliance Interface Overview'. Below it, a note states: 'In order for Cisco DNA Center to operate properly, you need to configure four interfaces on your appliance:'. A numbered list follows:

1. **Enterprise Network Interface:** Connects your appliance to the Enterprise network.
2. **Intracenter Link Interface:** Connects your appliance to your cluster.
3. **Management Network Interface:** (Optional) Accesses the Cisco DNA Center GUI from your Management network.
4. **Internet Access Interface:** (Optional) Accesses the internet.

Below the list, a paragraph explains: 'In this workflow, the Enterprise Network Interface and the Intracenter Link Interface will each have their own dedicated port. You can choose to have either Management Network Interface and/or Internet Access Interface be on the same port as the Enterprise Network Interface or assign them to a separate designated port.' At the bottom of the screen, there are two buttons: 'Exit' on the left and 'Next' on the right.

**Important** At a minimum, you must configure the interfaces on your appliance's Enterprise and Cluster ports, as they are required for Cisco DNA Center functionality. If the wizard fails to display either or both of these ports during the course of configuration, they may be non-functional or disabled. If you discover that they are non-functional, choose **Exit** to exit the wizard 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 2** Complete the Advanced Install configuration wizard:


a) Click **Next**.

The **Will this appliance join a cluster?** screen opens.

Cisco DNA Center Advanced Install

Will this appliance join a cluster?

This appliance is running on [software version] *N/A*.



Yes, This appliance will be added as a node to the primary node of a cluster.  
 No, This appliance will be the primary node of a cluster.


Exit Back Next

- b) Click the **No** radio button (as you are configuring your cluster's primary node), then click **Next**. The **How would you like to set up your appliance interfaces?** screen opens.

Cisco DNA Center Advanced Install

How would you like to set up your appliance interfaces?

Both Enterprise Network and Intracluster Link Interfaces have their own designated port. You can decide whether to have a separate dedicated port for either Management Network Interface and Internet Access Interface. Before you start, reserve the IP addresses necessary for configuration. If your network resides behind a firewall, be sure to [allow access to these URLs](#) and [open these ports](#).



Enterprise Network Interface  Intracluster Link Network

The Enterprise Network Interface and Intracluster Link Interface will be configured using the two 10-Gbps ports as shown above.

Would you like to have a dedicated Management Network Interface?

Yes  No

Would you like to have a dedicated Internet Access Interface?

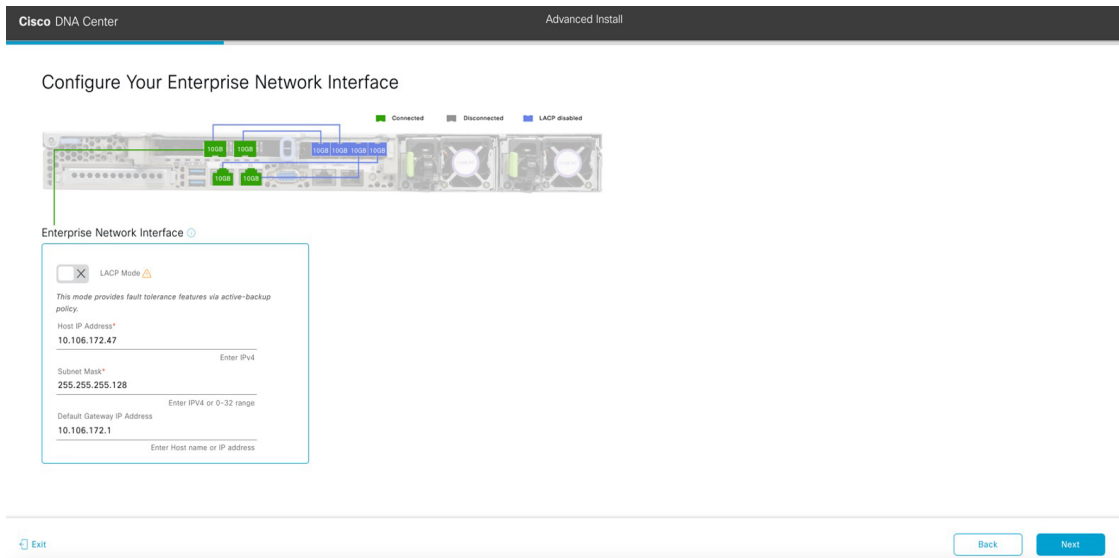
Yes  No

Exit Back Next

If your network resides behind a firewall, do the following:

- Click the **allow access to these URLs** link to view a popup window that lists the URLs that Cisco DNA Center must be able to access.
- Click the **open these ports** link to view a popup window that lists the network service ports that must be available for Cisco DNA Center to use.

- c) Indicate whether you want to configure dedicated Management and Internet Access interfaces, then click **Next**. The **Configure Your Enterprise Network Interface** screen opens.



- d) Enter configuration values for the Enterprise interface, then click **Next**.

As explained in [Interface Cable Connections](#), this is a required interface used to link the appliance to the enterprise network. See [Required IP Addresses and Subnets, on page 29](#) and [Required Configuration Information](#) for a more detailed description of the values you need to enter.

**Table 35: Primary Node Entries for the Enterprise Interface**

LACP Mode slider	<p>Choose one of the following network interface controller (NIC) bonding modes for the Enterprise interface:</p> <ul style="list-style-type: none"> <li>• <b>Active-Backup mode:</b> This mode provides fault tolerance by aggregating two Ethernet interfaces into a single logical channel. When the interface that's currently active goes down, the other interface takes its place and becomes active.</li> <li>• <b>LACP mode:</b> This mode aggregates two Ethernet interfaces that share the same speed and duplex settings into a single logical channel. This provides load balancing and higher bandwidth.</li> </ul> <p>For more information about Cisco DNA Center's implementation of NIC bonding, see <a href="#">NIC Bonding Overview, on page 67</a>.</p>
Host IP Address field	Enter the IP address for the Enterprise port. This is required.
Subnet Mask field	Enter the netmask for the port's IP address. This is required.



Default Gateway IP Address field	<p>Enter a default gateway IP address to use for the port.</p> <p><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.</p> <p><b>Note</b> You designated this interface to use the default gateway assigned to it by a DHCP server. Complete the following steps to specify a different gateway:</p> <ol style="list-style-type: none"> <li>1. Delete the IP address that is currently listed in this field and then click <b>Exit</b>.  This will bring you back to the first wizard screen.</li> <li>2. Return to the Enterprise port's wizard screen and enter the gateway IP address you want to use.</li> </ol>
----------------------------------	--

The wizard validates the information you have entered, confirms that the port is up, and notifies you of any settings that need to be changed before you can proceed with the wizard. If the settings you have entered are valid and the port is up, the wizard's **Configure Your Intracluster Interface** screen opens.

- e) Enter configuration values for your Intracluster interface, then click **Next**.

As explained in [Interface Cable Connections](#), this required port is used to link the appliance to your cluster. See [Required IP Addresses and Subnets, on page 29](#) and [Required Configuration Information](#) for a more detailed description of the values you need to enter.

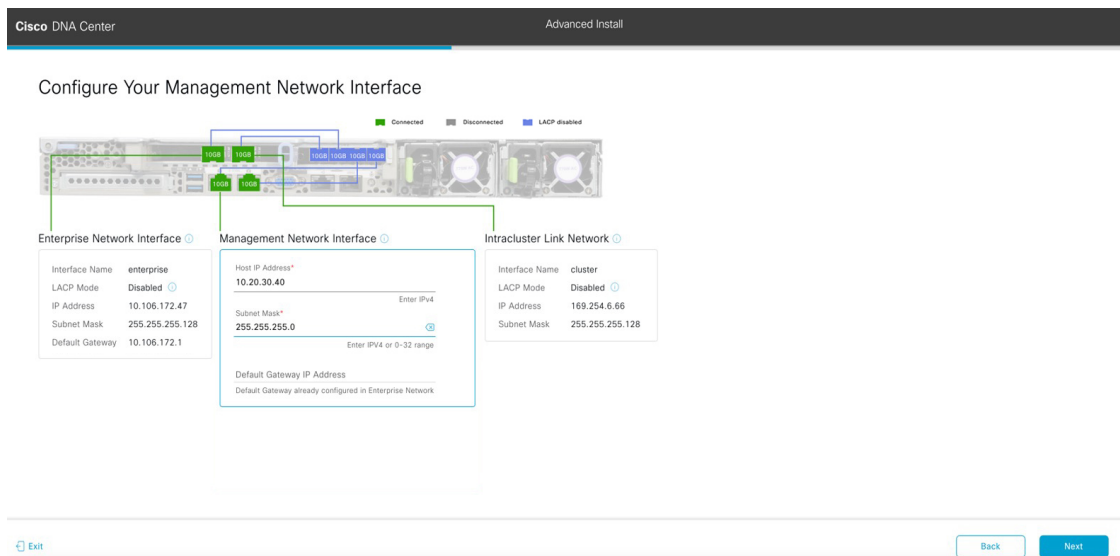
**Note**

- If you opted to configure the Enterprise and Internet Access interfaces on the same port, complete this step and then proceed to Step 2f (which describes how to configure your Management interface).
- If you opted to configure the Enterprise and Management interfaces on the same port, complete this step and then skip ahead to Step 2g (which describes how to configure your Internet Access interface).
- If you opted to configure the Enterprise, Management, and Internet Access interfaces on the same port, complete this step and then skip ahead to Step 2h.

**Table 36: Primary Node Entries for the Intracluster Interface**

LACP Mode slider	<p>Choose one of the following NIC bonding modes for the Intracluster interface:</p> <ul style="list-style-type: none"> <li>• <b>Active-Backup mode:</b> This mode provides fault tolerance by aggregating two Ethernet interfaces into a single logical channel. When the interface that's currently active goes down, the other interface takes its place and becomes active.</li> <li>• <b>LACP mode:</b> This mode aggregates two Ethernet interfaces that share the same speed and duplex settings into a single logical channel. This provides load balancing and higher bandwidth.</li> </ul> <p>For more information about Cisco DNA Center's implementation of NIC bonding, see <a href="#">NIC Bonding Overview</a>, on page 67.</p>
Host IP Address field	Enter the IP address for the Cluster port. This is required. Note that you cannot change the address of the Cluster port later.
Subnet Mask field	Enter the netmask for the port's IP address. This is required.

The wizard validates the information you have entered, confirms that the port is up, and notifies you of any settings that need to be changed before you can proceed with the wizard. If the settings you have entered are valid and the port is up, the wizard's **Configure Your Management Network Interface** screen opens.



- f) (Optional) Enter configuration values for the Management port, then click **Next**.

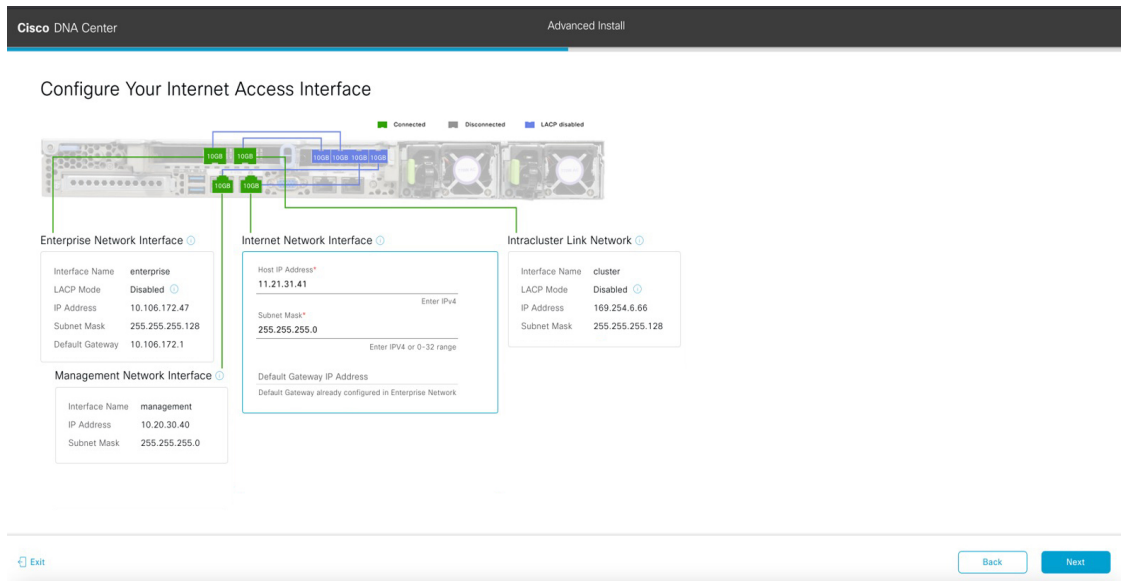
As explained in [Interface Cable Connections](#), this port is used to access the Cisco DNA Center GUI from your management network. If you chose to configure a dedicated Management interface, enter the information described in the following table. (See [Required IP Addresses and Subnets](#), on page 29 and [Required Configuration Information](#) for a more detailed description of the values you need to enter.)

**Note** If you opted to configure the Enterprise and Internet Access interfaces on the same port, complete this step and then skip ahead to Step 2h.

**Table 37: Primary Node Entries for the Management Port**

Host IP Address field	Enter the IP address for the Management port.
Subnet Mask field	Enter the netmask for the port's IP address.
Default Gateway IP Address field	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.

The wizard validates the information you have entered, confirms that the port is up, and notifies you of any settings that need to be changed before you can proceed with the wizard. If the settings you have entered are valid and the port is up, the wizard's **Configure Your Internet Access Interface** screen opens.



g) (Optional) Enter configuration values for the Internet Access interface, then click **Next**.

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 Enterprise port. If you chose to configure a dedicated Internet Access interface, enter the information described in the following table. (See [Required IP Addresses and Subnets](#), on page 29 and [Required Configuration Information](#) for a more detailed description of the values you need to enter.)

**Table 38: Primary Node Entries for the Internet Access Port**

Host IP Address field	Enter the IP address for the Internet Access port.
-----------------------	--

Subnet Mask field	Enter the netmask for the port's IP address. This is required if you entered an IP address in the previous field.
Default Gateway IP Address field	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.

The wizard validates the information you have entered, confirms that the port is up, and notifies you of any settings that need to be changed before you can proceed with the wizard. If the settings you have entered are valid and the port is up, the wizard's **Interface to Port Configuration** screen opens.

Cisco DNA Center Advanced Install

### Interface to Port Configuration

We are going to configure the following interfaces. Click Configure and wait for configuration to be done before proceeding to the next step.

[Configure](#)

**Enterprise Network Interface**

Interface Name	enterprise
LACP Mode	Disabled
IP Address	10.106.172.47
Subnet Mask	255.255.255.128
Default Gateway	10.106.172.1

**Internet Network Interface**

Interface Name	internet
IP Address	11.21.31.41
Subnet Mask	255.255.255.0

**Intracluster Link Network**

Interface Name	cluster
LACP Mode	Disabled
IP Address	169.254.6.66
Subnet Mask	255.255.255.128

**Management Network Interface**

Interface Name	management
IP Address	10.20.30.40
Subnet Mask	255.255.255.0

[Exit](#) [Back](#) [Next](#)

- h) Review the settings that you have entered for the primary node's interfaces.  
If you need to make any changes, click the **Edit** link for the relevant interface.
- i) When you are happy with the interface settings, click **Configure**.
- j) After initial interface configuration has completed, click **Next**.

The **DNS Configuration** screen opens.

- k) Enter the IP address of the preferred DNS server, then click **Next**. To enter additional DNS servers, click the **Add (+)** icon.

**Important**

- For each node in your cluster, configure a maximum of three DNS servers. Problems can occur if you configure more than three DNS servers for an appliance.
- For NTP, ensure port 123 (UDP) is open between Cisco DNA Center and your NTP server.

The **Configure Proxy Server Information** screen opens.

- l) Do one of the following and then click **Next**:
- If your network does *not* use a proxy server to access the internet, click the **No** radio button.
  - If your network does use a proxy server to access the internet, enter the values described in the following table:

**Table 39: Primary Node Entries for Proxy Server Settings**

Proxy Server field	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.
Port field	Enter the port your appliance used to access the network proxy.
Username field	Enter the user name used to access the network proxy. If no proxy login is required, leave this field blank.
Password field	Enter the password used to access the network proxy. If no proxy login is required, leave this field blank.

The wizard validates the information you have entered and notifies you of any settings that need to be changed before you can proceed with the wizard. If the settings you have entered are valid and the port is up, the wizard's **Advanced Appliance Settings** screen opens.

Cisco DNA Center Advanced Install

### Advanced Appliance Settings

**CLUSTER VIRTUAL IP ADDRESSES**  
Virtual IP addresses are used for traffic between the cluster and your network. VIPs are required for three-node clusters and for single-node clusters that might be converted to three node later. If you're using a single-node cluster, you can skip the VIP addresses and hostname.

To access from Enterprise Network: IP should be within the range 10.106.172.47/25  
To access from Management Network: IP should be within the range 10.20.30.40/24  
For Internet Access: IP should be within the range 11.21.31.41/24  
For Intracluster Access: IP should be within the range 169.254.6.66/25

Fully Qualified Domain Name (FQDN)  
Enter FQDN for Enterprise Network

**NTP SERVER SETTINGS**  
NTP Server: ntp.esl.cisco.com  
Enter an IP address or FQDN

Turn On NTP Authentication

**SUBNET SETTINGS**  
Cisco DNA Center requires a dedicated, nonrouted IP subnet to manage internal and cluster services.

Container Subnet: 169.254.32.0/20 (Minimum subnet size is 21 bits. Slash notation is allowed.)  
Cluster Subnet: 169.254.48.0/20 (Minimum subnet size is 21 bits. Slash notation is allowed.)

Exit Review Back Next

m) Enter configuration values for your cluster, then click **Next**.

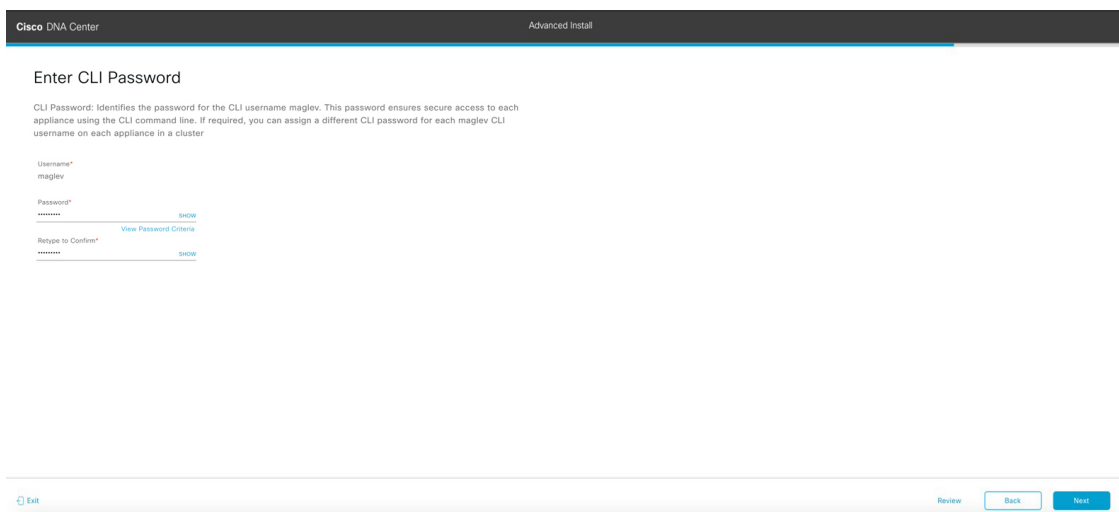
**Table 40: Primary Node Entries for Advanced Appliance Settings**

<b>Cluster Virtual IP Addresses</b>
-------------------------------------

<p>To access from Enterprise Network, To access from Management Network, For Internet Access, and For Intracluster Access fields</p> <p><b>Note</b> If you configured the Management or Internet Access interface on the same port as the Enterprise interface, its corresponding field is not displayed in this section.</p>	<p>Enter the virtual IP address that will be used for traffic between the cluster and the interfaces that you have configured on your primary node. 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 don't plan to move to a three-node cluster setup, you can leave the fields in this section blank.</p> <p><b>Important</b> If you choose to configure a virtual IP address, you must enter one 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 <b>UP</b> state.</p>
<p>Fully Qualified Domain Name (FQDN) field</p>	<p>Enter the fully qualified domain name (FQDN) for your cluster. Cisco DNA Center does the following with this hostname:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> </ul>
<p><b>NTP Server Settings</b></p>	
<p>NTP Server field</p>	<p>Enter at least one NTP server address or hostname. To enter additional NTP server addresses or hostnames, click the <b>Add (+)</b> icon.</p> <p>For a production deployment, Cisco recommends that you configure a minimum of three NTP servers.</p>

Turn On NTP Authentication check box	<p>To enable the authentication of your NTP server before it's synchronized with Cisco DNA Center, check this check box and then enter the following information:</p> <ul style="list-style-type: none"> <li>The NTP server's key ID. Valid values range between 1 and 4294967295 (<math>2^{32}-1</math>).</li> </ul> <p>This value corresponds to the key ID that's defined in the NTP server's key file.</p> <ul style="list-style-type: none"> <li>The SHA-1 key value associated with the NTP server's key ID. This 40-character hex string resides in the NTP server's key file.</li> </ul> <p><b>Note</b> Ensure that you enter a key ID and key value for each NTP server that you configured in the previous field.</p>
<b>Subnet Settings</b>	
Container Subnet field	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.
Cluster Subnet field	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.

The **Enter CLI Password** screen opens.



Cisco DNA Center Advanced Install

### Enter CLI Password

CLI Password: Identifies the password for the CLI username maglev. This password ensures secure access to each appliance using the CLI command line. If required, you can assign a different CLI password for each maglev CLI username on each appliance in a cluster

Username\*  
maglev

Password\*  
..... [SHOW](#)

[View Password Criteria](#)

Retype to Confirm\*  
..... [SHOW](#)

[Exit](#) [Review](#) [Back](#) [Next](#)

- n) Enter and confirm the password for the `maglev` user, then click **Next**.

The wizard validates the information you have entered and notifies you of any settings that need to be changed before you can proceed with the wizard. If the settings you have entered are valid, the wizard's **Summary** screen opens.



Cisco DNA Center Advanced Install

### Summary

Please review the settings that you have entered. If you need to make any changes, click the appropriate Edit link and make the necessary updates. You can download the generated configuration in JSON format from [here](#). When you are happy with your settings, click Start Configuration.

Ports Configuration Completed

Interface Name	IP Address	Subnet Mask	Default Gateway	LACP Mode
enterprise	10.106.172.47	255.255.255.128	10.106.172.1	Disabled
internet	11.21.31.41	255.255.255.0		
cluster	169.254.6.66	255.255.255.128		Disabled
management	10.20.30.40	255.255.255.0		

[Exit](#) [Start Configuration](#)

**Note** To download the appliance configuration as a JSON file, click the [here](#) link.

- o) Review all of the settings that you have entered while completing the wizard. If necessary, click the appropriate **Edit** link to open the wizard screen in which you want to make updates.
- p) To complete the configuration of your Cisco DNA Center appliance, click **Start Configuration**.

The wizard screen continuously updates during the process, indicating the tasks that are currently being completed and their progress, as well as any errors that have occurred. To save a local copy of this information as a text file, click the download icon.

Cisco DNA Center Configuration

### Appliance Configuration In Progress

It should take about 90 minutes to complete the configuration of your appliance. As you wait, you can view a video that explains the next steps in the Cisco DNA Center setup process.

Initializing the cluster using kubeadm 30%

ABOUT STARTING CISCO DNA CENTER

Started: 04/09/2020 12:15:36

```

2021-05-05T16:56:59.32526 | -----
2021-05-05T16:56:59.32525 | credentialmanager.pem Apr 13 16:49:52 2020 GMT Apr 13 16:49:52 2021 GMT
2021-05-05T16:56:59.32526 | kong.pem Apr 13 16:49:51 2020 GMT Apr 13 16:49:51 2021 GMT
2021-05-05T16:56:59.32527 | kube-admin.pem Apr 13 16:49:50 2020 GMT Apr 13 16:49:50 2021 GMT
2021-05-05T16:56:59.32528 | kube-worker-1.pem Apr 13 16:49:50 2020 GMT Apr 13 16:49:50 2021 GMT
2021-05-05T16:56:59.32529 | maglev-registry.pem Apr 13 16:49:52 2020 GMT Apr 13 16:49:52 2021 GMT
2021-05-05T16:56:59.325210 | apiserver-kubelet-client.crt Apr 13 12:12:14 2020 GMT Apr 13 17:40:20 2021 GMT
2021-05-05T16:56:59.325211 | apiserver-kubelet-client.crt Apr 13 12:12:14 2020 GMT Apr 13 17:40:20 2021 GMT
2021-05-05T16:56:59.325212 | front-proxy-ca.crt Apr 13 17:40:20 2020 GMT Apr 11 17:40:20 2030 GMT
2021-05-05T16:56:59.325213 | front-proxy-client.crt Apr 13 17:40:20 2020 GMT Apr 13 17:40:20 2021 GMT
2021-05-05T16:56:59.325214 | kubelet.conf Apr 13 12:12:14 2020 GMT Apr 13 17:40:21 2021 GMT
2021-05-05T16:56:59.325215 | admin.conf Apr 13 12:12:14 2020 GMT Apr 13 17:40:21 2021 GMT
2021-05-05T16:56:59.325216 | scheduler.conf Apr 13 12:12:14 2020 GMT Apr 13 17:40:22 2021 GMT
2021-05-05T16:56:59.325217 | controller-manager.conf Apr 13 12:12:14 2020 GMT Apr 13 17:40:22 2021 GMT
2021-05-05T16:56:59.325218 | -----
                    
```

### What to do next

When this task is complete:

- If you are deploying this appliance in standalone mode only, continue by performing 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 Using the Advanced Install Configuration Wizard, on page 156](#).

## Configure a Secondary Node Using the Advanced Install Configuration Wizard

Perform the following steps to configure the second and third nodes in the cluster using the Advanced Install configuration wizard.



### 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.
- The following second generation Cisco DNA Center appliances support configuration using the Advanced Install configuration wizard:
  - 44-core appliance: Cisco part number DN2-HW-APL
  - 44-core promotional appliance: Cisco part number DN2-HW-APL-U
  - 56-core appliance: Cisco part number DN2-HW-APL-L
  - 56-core promotional appliance: Cisco part number DN2-HW-APL-L-U

The first generation 44-core Cisco DNA Center appliance (Cisco part number DN1-HW-APL) *cannot* be configured using this wizard.

- You can only use this wizard to complete the initial configuration of a new Cisco DNA Center appliance. To reimage an appliance that's been configured previously, you will need to use the Maglev Configuration wizard (see [Configure the Appliance Using the Maglev Wizard, on page 81](#)).
- 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.
- 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.

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

- 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://172.29.131.224:443]
```

NAME	DISPLAY_NAME	DEPLOYED	AVAILABLE	STATUS	PROGRESS
access-control-application	Access Control Application	2.1.388.60364	-	DEPLOYED	
ai-network-analytics	AI Network Analytics	2.7.8.528	-	DEPLOYED	
app-hosting	Application Hosting	1.7.0.2108120753	-	DEPLOYED	
application-policy	Application Policy	2.1.388.170155	-	DEPLOYED	
application-registry	Application Registry	2.1.388.170155	-	DEPLOYED	
application-visibility-service	Application Visibility Service	2.1.388.170155	-	DEPLOYED	
assurance	Assurance - Base	2.2.3.337	-	DEPLOYED	
automation-core	NCP - Services	2.1.388.60364	-	DEPLOYED	
base-provision-core	Automation - Base	2.1.388.60364	-	DEPLOYED	
cloud-connectivity-contextual-content	Cloud Connectivity - Contextual Content	1.3.1.364	-	DEPLOYED	DEPLOYED
cloud-connectivity-data-hub	Cloud Connectivity - Data Hub	1.6.0.380	-	DEPLOYED	
cloud-connectivity-tethering	Cloud Connectivity - Tethering	2.1.1.43	-	DEPLOYED	
cloud-provision-core	Cloud Device Provisioning Application	2.1.388.60364	-	DEPLOYED	
command-runner	Command Runner	2.1.388.60364	-	DEPLOYED	
device-onboarding	Device Onboarding	2.1.388.60364	-	DEPLOYED	
disaster-recovery	Disaster Recovery	2.1.388.3600024	-	DEPLOYED	
dna-core-apps	Network Experience Platform - Core	2.1.388.60364	-	DEPLOYED	
dnac-platform	Cisco DNA Center Platform	1.6.1.126	-	DEPLOYED	
dnac-search	Cisco DNA Center Global Search	1.6.99.10	-	DEPLOYED	
endpoint-analytics	AI Endpoint Analytics	1.5.0.226	-	DEPLOYED	
group-based-policy-analytics	Group-Based Policy Analytics	2.2.3.55	-	DEPLOYED	
icap-automation	Automation - Intelligent Capture	2.1.388.60364	-	DEPLOYED	
image-management	Image Management	2.1.388.60364	-	DEPLOYED	
machine-reasoning	Machine Reasoning	2.1.388.210008	-	DEPLOYED	
ncp-system	NCP - Base	2.1.388.60364	-	DEPLOYED	
ndp-base-analytics	Network Data Platform - Base Analytics	1.6.1686	-	DEPLOYED	
ndp-platform	Network Data Platform - Core	1.6.1705	-	DEPLOYED	
ndp-ui	Network Data Platform - Manager	1.6.1662	-	DEPLOYED	
network-visibility	Network Controller Platform	2.1.388.60364	-	DEPLOYED	
path-trace	Path Trace	2.1.388.60364	-	DEPLOYED	
platform-ui	Cisco DNA Center UI	1.6.3.155	-	DEPLOYED	
rbac-extensions	RBAC Extensions	2.1.388.190003	-	DEPLOYED	
rogue-management	Rogue and aWIPS	2.3.0.24	-	DEPLOYED	
sd-access	SD Access	2.1.388.60364	-	DEPLOYED	
sensor-assurance	Assurance - Sensor	2.2.3.317	-	DEPLOYED	
sensor-automation	Automation - Sensor	2.1.388.60364	-	DEPLOYED	
ssa	Stealthwatch Security Analytics	2.1.388.1090064	-	DEPLOYED	
system	System	1.6.551	-	DEPLOYED	
system-commons	System Commons	2.1.388.60364	-	DEPLOYED	
umbrella	Cisco Umbrella	2.1.388.590077	-	DEPLOYED	
wide-area-bonjour	Wide Area Bonjour	2.4.364.75035	-	DEPLOYED	

- 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, as doing so will result in unpredictable behavior.
- 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:

- Installed the Cisco DNA Center software image onto your appliance, as described in [Reimage the Appliance, on page 74](#).

**Important**

This is only applicable if you are going to configure a promotional appliance, because the Cisco DNA Center software image is not preinstalled on the following appliances:

- 44-core promotional appliance (Cisco part number DN2-HW-APL-U)
- 56-core promotional appliance: (Cisco part number DN2-HW-APL-L-U)

- 
- Configured the first appliance in the cluster, following the steps in [Configure the Primary Node Using the Advanced Install Configuration Wizard, on page 137](#).
  - Collected all of the information called for in [Required IP Addresses and Subnets, on page 29](#) 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 nodes as described in [Enable Browser Access to Cisco Integrated Management Controller](#).
  - Checked that both secondary nodes' ports and the switches they use are properly configured, as described in [Execute Preconfiguration Checks](#).
  - Are using a compatible browser. For a list of compatible browsers, see the [Release Notes](#) 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 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**

Start the Advanced Install configuration wizard:

- a) Point your browser to the Cisco IMC IP address you set during the Cisco IMC GUI configuration you performed, then 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 blue link menu at the upper right, as shown below.



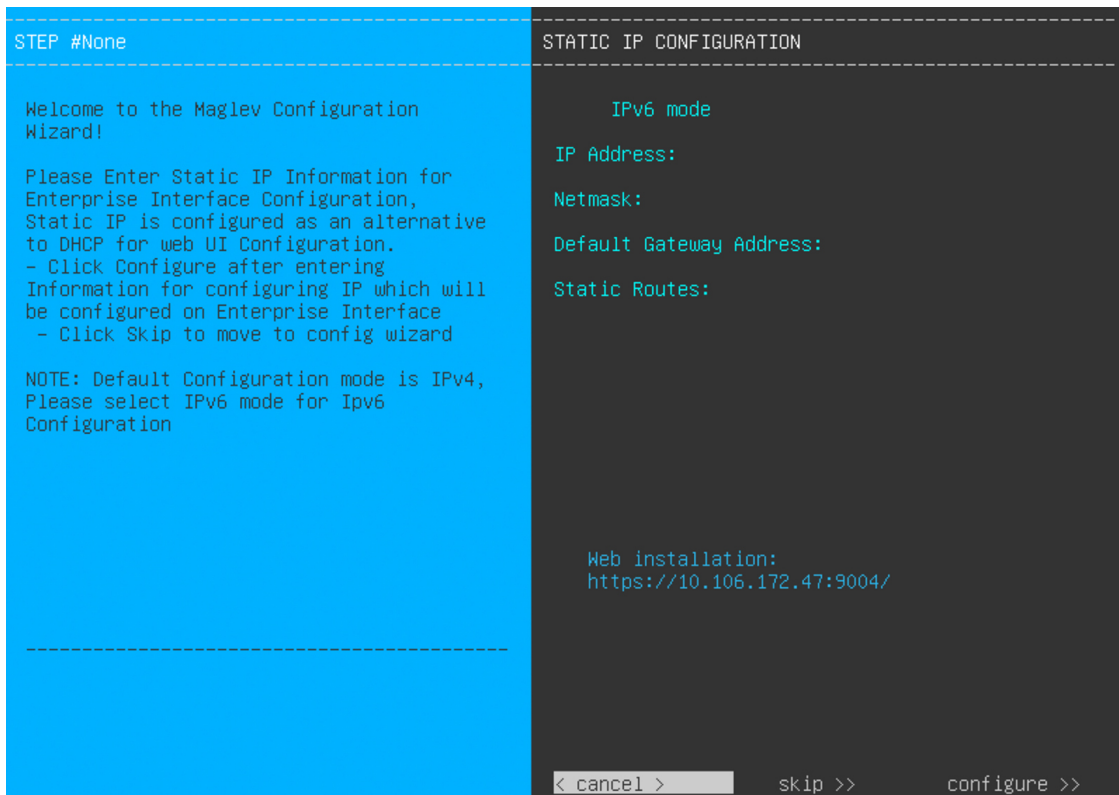
- b) From the blue link menu, choose **Launch KVM** and then select either **Java based KVM** or **HTML based KVM**. If you select the Java-based KVM, you will need to launch the Java startup file from your browser or file manager in order to view the KVM console in its own window. If you select the HTML-based KVM, it will launch the KVM console in a separate browser 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 Maglev Configuration Wizard prompts.

- c) 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**. Then switch to the KVM console to continue.
  - In the KVM console: Choose **Power > Power Cycle System (cold boot)**.

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

After displaying reboot messages, the KVM console displays the **Static IP Configuration** screen.



Note the URL listed in the **Web Installation** field.

d) Do one of the following:

- If you want a DHCP server to assign an IP address, subnet mask, and default gateway to your appliance's Enterprise interface, click **Skip**.
- If you want to assign your own IP address, subnet mask, and default gateway to your appliance's Enterprise interface, enter the information described in the following table and then click **Configure**.

IPv6 Mode check box	If you want to configure an IPv6 address, check this check box.
IP Address field	Enter the static IP address you want to use.
Netmask field	Enter the netmask for the IP address you specified in the previous field: <ul style="list-style-type: none"> <li>• If you entered an IPv4 address, you can enter either a netmask or CIDR address.</li> <li>• If you entered an IPv6 address, you can only enter a CIDR address.</li> </ul>
Default Gateway Address field	Specify the default gateway that will be used to route traffic.
Static Routes field	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 Management port only.

The KVM console displays the Maglev Configuration wizard welcome screen.



- e) To bring up the **Appliance Configuration** screen, open the URL that was displayed in the **Static IP Configuration** screen.

Cisco DNA Center

Appliance Configuration

Welcome to Cisco DNA Center

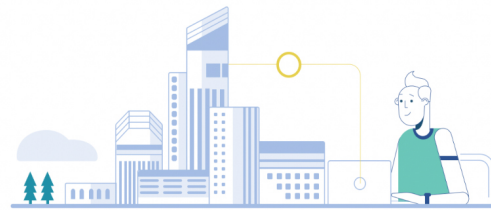
Are you starting a new Cisco DNA Center Cluster or joining an existing one?

Start A Cisco DNA  
Center Cluster

This appliance will be the primary  
node of a cluster.

Join A Cisco DNA  
Center Cluster

This appliance will be added as a  
node to the primary node of a cluster.



Next

- f) Click the **Join a Cisco DNA Center Cluster** radio button, then click **Next**.



Welcome to Cisco DNA Center

Before you can use Cisco DNA Center, first complete the appropriate appliance configuration workflow.  
Which workflow matches your needs?

**Advanced Install** +

---

Configure a standalone node or **any node in a cluster**.

Use this wizard to access all of the available appliance configuration options.



Back

Start

- g) Click the **Advanced Install** radio button, then click **Start**.

The **Advanced Install Overview** slider opens. Click > to view a summary of the tasks that the wizard will help you complete.

## Advanced Install Overview

Prepare your appliance for use with Cisco DNA Center by configuring its interfaces and entering cluster and other required information.



Start Workflow



- h) Click **Start Workflow** to start the wizard.

The **Appliance Interface Overview** screen opens, providing a description of the four appliance interfaces that you can configure.

Cisco DNA Center
Advanced Install

---

### Appliance Interface Overview

In order for Cisco DNA Center to operate properly, you need to configure four interfaces on your appliance:

1. **Enterprise Network Interface:** Connects your appliance to the Enterprise network.
2. **Intracenter Link Interface:** Connects your appliance to your cluster.
3. **Management Network Interface:** (Optional) Accesses the Cisco DNA Center GUI from your Management network.
4. **Internet Access Interface:** (Optional) Accesses the internet.

In this workflow, the Enterprise Network Interface and the Intracenter Link Interface will each have their own dedicated port. You can choose to have either Management Network Interface and/or Internet Access Interface be on the same port as the Enterprise Network Interface or assign them to a separate designated port.

---

Exit
Next

**Important** At a minimum, you must configure the interfaces on your appliance's Enterprise and Cluster ports, as they are required for Cisco DNA Center functionality. If the wizard fails to display either or both of these ports during the course of configuration, they may be non-functional or disabled. If you discover that they are non-functional, choose **Exit** to exit the wizard 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 2** Complete the Advanced Install configuration wizard:


a) Click **Next**.

The **Will this appliance join a cluster?** screen opens.

Cisco DNA Center Advanced Install

Will this appliance join a cluster?

This appliance is running on [software version] *N/A*.



Yes, This appliance will be added as a node to the primary node of a cluster.  
 No, This appliance will be the primary node of a cluster.

Exit Back Next


b) Click the **Yes** radio button, then click **Next**.

The **How would you like to set up your appliance interfaces?** screen opens.

Cisco DNA Center Advanced Install

How would you like to set up your appliance interfaces?

Both Enterprise Network and Intracluster Link Interfaces have their own designated port. You can decide whether to have a separate dedicated port for either Management Network Interface and Internet Access Interface. Before you start, reserve the IP addresses necessary for configuration. If your network resides behind a firewall, be sure to [allow access to these URLs](#) and [open these ports](#).



Enterprise Network Interface  Intracluster Link Network

The Enterprise Network Interface and Intracluster Link Interface will be configured using the two 10-Gbps ports as shown above.

Would you like to have a dedicated Management Network Interface?

Yes  No

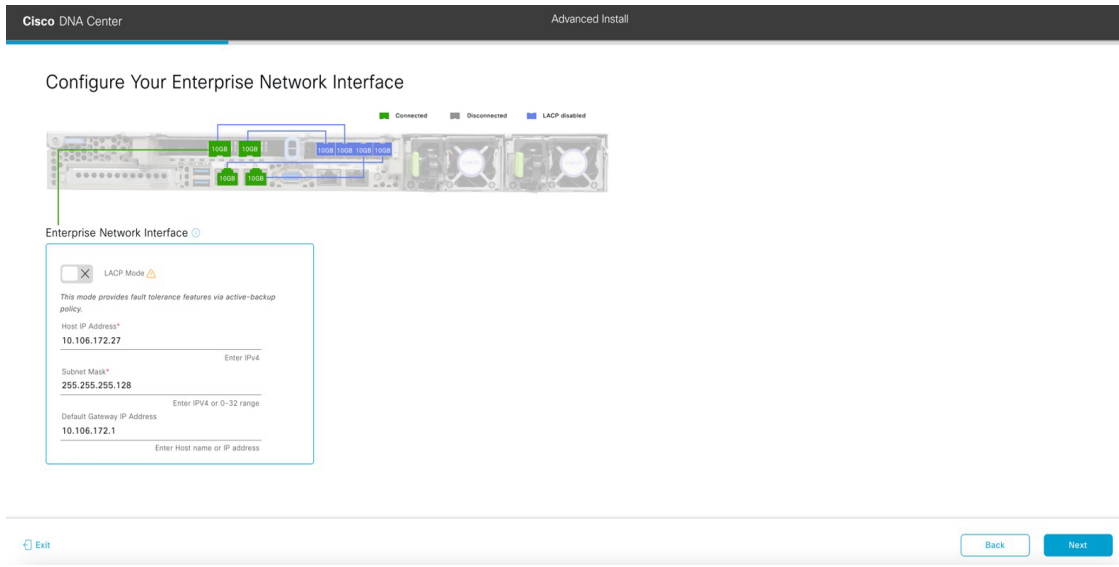
Would you like to have a dedicated Internet Access Interface?

Yes  No

Exit Back Next

c) Indicate whether you want to configure dedicated Management and Internet Access interfaces, then click **Next**.

The **Configure Your Enterprise Network Interface** screen opens.



- d) Enter configuration values for the Enterprise interface, then click **Next**.

As explained in [Interface Cable Connections](#), this is a required interface used to link the appliance to the enterprise network. See [Required IP Addresses and Subnets, on page 29](#) and [Required Configuration Information](#) for a more detailed description of the values you need to enter.

**Table 41: Secondary Node Entries for the Enterprise Interface**

LACP Mode slider	<p>Choose one of the following network interface controller (NIC) bonding modes for the Enterprise interface:</p> <ul style="list-style-type: none"> <li>• <b>Active-Backup mode:</b> This mode provides fault tolerance by aggregating two Ethernet interfaces into a single logical channel. When the interface that's currently active goes down, the other interface takes its place and becomes active.</li> <li>• <b>LACP mode:</b> This mode aggregates two Ethernet interfaces that share the same speed and duplex settings into a single logical channel. This provides load balancing and higher bandwidth.</li> </ul> <p>For more information about Cisco DNA Center's implementation of NIC bonding, see <a href="#">NIC Bonding Overview, on page 67</a>.</p>
Host IP Address field	Enter the IP address for the Enterprise port. This is required.
Subnet Mask field	Enter the netmask for the port's IP address. This is required.

Default Gateway IP Address field	<p>Enter a default gateway IP address to use for the port.</p> <p><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.</p> <p><b>Note</b> You designated this interface to use the default gateway assigned to it by a DHCP server. Complete the following steps to specify a different gateway:</p> <ol style="list-style-type: none"> <li>1. Delete the IP address that is currently listed in this field and then click <b>Exit</b>.  This will bring you back to the first wizard screen.</li> <li>2. Return to the Enterprise port's wizard screen and enter the gateway IP address you want to use.</li> </ol>
----------------------------------	--

The wizard validates the information you have entered, confirms that the port is up, and notifies you of any settings that need to be changed before you can proceed with the wizard. If the settings you have entered are valid and the port is up, the wizard's **Configure Your Intracluster Interface** screen opens.

e) Enter configuration values for your Intracluster interface, then click **Next**.

As explained in [Interface Cable Connections](#), this required port is used to link the appliance to your cluster. See [Required IP Addresses and Subnets, on page 29](#) and [Required Configuration Information](#) for a more detailed description of the values you need to enter.

## Configure a Secondary Node Using the Advanced Install Configuration Wizard

- Note**
- If you opted to configure the Enterprise and Internet Access interfaces on the same port, complete this step and then proceed to Step 2f (which describes how to configure your Management interface).
  - If you opted to configure the Enterprise and Management interfaces on the same port, complete this step and then skip ahead to Step 2g (which describes how to configure your Internet Access interface).
  - If you opted to configure the Enterprise, Management, and Internet Access interfaces on the same port, complete this step and then skip ahead to Step 2h.

**Table 42: Secondary Node Entries for the Intracluster Interface**

LACP Mode slider	<p>Choose one of the following NIC bonding modes for the Intracluster interface:</p> <ul style="list-style-type: none"> <li>• <b>Active-Backup mode:</b> This mode provides fault tolerance by aggregating two Ethernet interfaces into a single logical channel. When the interface that's currently active goes down, the other interface takes its place and becomes active.</li> <li>• <b>LACP mode:</b> This mode aggregates two Ethernet interfaces that share the same speed and duplex settings into a single logical channel. This provides load balancing and higher bandwidth.</li> </ul> <p>For more information about Cisco DNA Center's implementation of NIC bonding, see <a href="#">NIC Bonding Overview, on page 67</a>.</p>
Host IP Address field	Enter the IP address for the Cluster port. This is required. Note that you cannot change the address of the Cluster port later.
Subnet Mask field	Enter the netmask for the port's IP address. This is required.

The wizard validates the information you have entered, confirms that the port is up, and notifies you of any settings that need to be changed before you can proceed with the wizard. If the settings you have entered are valid and the port is up, the wizard's **Configure Your Management Network Interface** screen opens.

Cisco DNA Center
Advanced Install

### Configure Your Management Network Interface

**Enterprise Network Interface**

Interface Name: enterprise

LACP Mode: Disabled

IP Address: 10.106.172.27

Subnet Mask: 255.255.255.128

Default Gateway: 10.106.172.1

**Management Network Interface**

Host IP Address\*: 11.22.33.44 Enter IPv4

Subnet Mask\*: 255.255.255.0 Enter IPv4 or 0-32 range

Default Gateway IP Address  
Default Gateway already configured in Enterprise Network

**Intracluster Link Network**

Interface Name: cluster

LACP Mode: Disabled

IP Address: 169.254.6.64

Subnet Mask: 255.255.255.128

Exit
Back
Next

- f) (Optional) Enter configuration values for the Management port, then click **Next**.

As explained in [Interface Cable Connections](#), this port is used to access the Cisco DNA Center GUI from your management network. If you chose to configure a dedicated Management interface, enter the information described in the following table. (See [Required IP Addresses and Subnets, on page 29](#) and [Required Configuration Information](#) for a more detailed description of the values you need to enter.)

**Note** If you opted to configure the Enterprise and Internet Access interfaces on the same port, complete this step and then skip ahead to Step 2h.

**Table 43: Secondary Node Entries for the Management Port**

Host IP Address field	Enter the IP address for the Management port. This is required.
Subnet Mask field	Enter the netmask for the port's IP address. This is required.
Default Gateway IP Address field	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.

The wizard validates the information you have entered, confirms that the port is up, and notifies you of any settings that need to be changed before you can proceed with the wizard. If the settings you have entered are valid and the port is up, the wizard's **Configure Your Internet Access Interface** screen opens.

- g) (Optional) Enter configuration values for the Internet Access interface, then click **Next**.

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 Enterprise port. If you chose to configure a dedicated Internet Access interface, enter the information described in the following table. (See [Required IP Addresses and Subnets, on page 29](#) and [Required Configuration Information](#) for a more detailed description of the values you need to enter.)

Table 44: Secondary Node Entries for the Internet Access Port

Host IP Address field	Enter the IP address for the Internet Access port.
Subnet Mask field	Enter the netmask for the port's IP address. This is required if you enter an IP address.
Default Gateway IP Address field	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.

The wizard validates the information you have entered, confirms that the port is up, and notifies you of any settings that need to be changed before you can proceed with the wizard. If the settings you have entered are valid and the port is up, the wizard's **Interface to Port Configuration** screen opens.

Cisco DNA Center Advanced Install

### Interface to Port Configuration

We are going to configure the following interfaces. Click Configure and wait for configuration to be done before proceeding to the next step.

[Configure](#)

Legend: ■ Connected ■ Disconnected ■ LACP disabled

**Enterprise Network Interface**

Interface Name: enterprise  
LACP Mode: Disabled  
IP Address: 10.106.172.27  
Subnet Mask: 255.255.255.128  
Default Gateway: 10.106.172.1

[Edit](#)

**Internet Network Interface**

Interface Name: internet  
IP Address: 10.20.30.40  
Subnet Mask: 255.255.255.0

[Edit](#)

**Intracluster Link Network**

Interface Name: cluster  
LACP Mode: Disabled  
IP Address: 169.254.6.64  
Subnet Mask: 255.255.255.128

[Edit](#)

**Management Network Interface**

Interface Name: management  
IP Address: 11.22.33.44  
Subnet Mask: 255.255.255.0

[Edit](#)

[Exit](#) [Back](#) [Next](#)

h) Review the settings that you have entered for the secondary node's interfaces.

If you need to make any changes, click the **Edit** link for the relevant interface to return to its wizard screen.

i) When you are happy with the interface settings, click **Configure**.

j) After initial interface configuration has completed, click **Next** to proceed to the next wizard screen.

The **DNS Configuration** screen opens.



- k) Enter the IP address of the preferred DNS server, then click **Next**. To enter additional DNS servers, click the **Add (+)** icon.

**Important**

- For each node in your cluster, configure a maximum of three DNS servers. Problems can occur if you configure more than three DNS servers for an appliance.
- For NTP, ensure port 123 (UDP) is open between Cisco DNA Center and your NTP server.

The **Configure Proxy Server Information** screen opens.

- l) Do one of the following and then click **Next**:
- If your network does *not* use a proxy server to access the internet, click the **No** radio button.
  - If your network does use a proxy server to access the internet, enter the values described in the following table:

**Table 45: Secondary Node Entries for Proxy Server Settings**

Proxy Server field	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.
Port field	Enter the port your appliance used to access the network proxy.
Username field	Enter the user name used to access the network proxy. If no proxy login is required, leave this field blank.
Password field	Enter the password used to access the network proxy. If no proxy login is required, leave this field blank.

The wizard validates the information you have entered and notifies you of any settings that need to be changed before you can proceed with the wizard. If the settings you have entered are valid, the wizard's **Primary Node Details** screen opens.

Cisco DNA Center Advanced Install

### Primary Node Details

This appliance is getting added as a node for the multi-node setup with software version *N/A*. This information will be used when you need to log into the Maglev CLI.

Primary Node IP\*  
IP should be within Intra-Cluster's 169.254.6.66/25

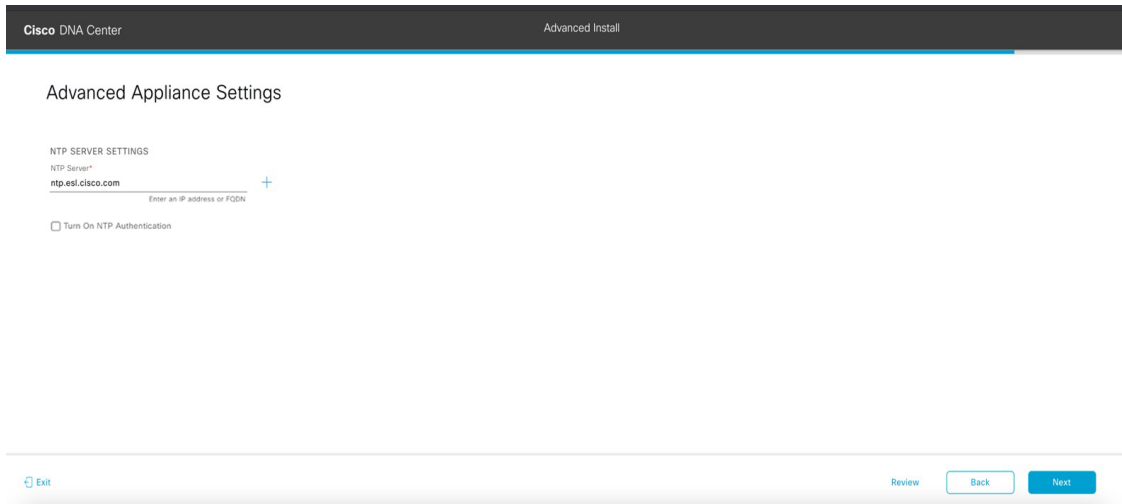
CLI Username  
maglev

CLI Password\*  
Enter CLI Password

Exit Review Back Next

- m) To establish a connection with your cluster's primary node, enter its IP address and login credentials, and then click **Next**.

The **Advanced Appliance Settings** screen opens.



n) Enter configuration values for your cluster, then click **Next**.

**Table 46: Secondary Node Entries for Advanced Appliance Settings**

NTP Server Settings	
NTP Server field	<p>Enter at least one NTP server address or hostname. To enter additional NTP server addresses or hostnames, click the <b>Add (+)</b> icon.</p> <p>For a production deployment, Cisco recommends that you configure a minimum of three NTP servers.</p>
Turn On NTP Authentication check box	<p>To enable the authentication of your NTP server before it's synchronized with Cisco DNA Center, check this check box and then enter the following information:</p> <ul style="list-style-type: none"> <li>• The NTP server's key ID. Valid values range between 1 and 4294967295 (2<sup>32</sup>-1). This value corresponds to the key ID that's defined in the NTP server's key file.</li> <li>• The SHA-1 key value associated with the NTP server's key ID. This 40-character hex string resides in the NTP server's key file.</li> </ul> <p><b>Note</b> Ensure that you enter a key ID and key value for each NTP server that you configured in the previous field.</p>

The **Enter CLI Password** screen opens.

## Configure a Secondary Node Using the Advanced Install Configuration Wizard

Cisco DNA Center Advanced Install

### Enter CLI Password

CLI Password: Identifies the password for the CLI username maglev. This password ensures secure access to each appliance using the CLI command line. If required, you can assign a different CLI password for each maglev CLI username on each appliance in a cluster

Username\*  
maglev

Password\*  
 [SHOW](#)  
[View Password Criteria](#)

Retype to Confirm\*  
 [SHOW](#)

[Exit](#) [Review](#) [Back](#) [Next](#)

- o) Enter and confirm the password for the `maglev` user, then click **Next**.

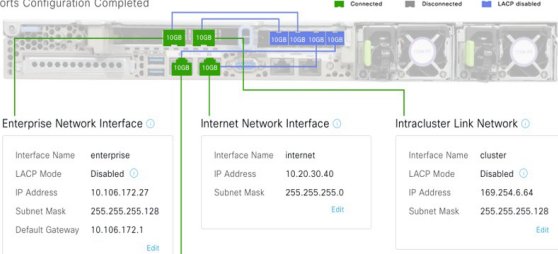
The wizard validates the information you have entered, confirms that the port is up, and notifies you of any settings that need to be changed before you can proceed with the wizard. If the settings you have entered are valid, the wizard's **Summary** screen opens.

Cisco DNA Center Advanced Install

### Summary

Please review the settings that you have entered. If you need to make any changes, click the appropriate Edit link and make the necessary updates. You can download the generated configuration in JSON format from [here](#). When you are happy with your settings, click Start Configuration.

Ports Configuration Completed Connected Disconnected LACP disabled



**Enterprise Network Interface**

Interface Name enterprise

LACP Mode Disabled

IP Address 10.106.172.27

Subnet Mask 255.255.255.128

Default Gateway 10.106.172.1

[Edit](#)

**Internet Network Interface**

Interface Name internet

IP Address 10.20.30.40

Subnet Mask 255.255.255.0

[Edit](#)

**Intracluster Link Network**

Interface Name cluster

LACP Mode Disabled

IP Address 169.254.6.64

Subnet Mask 255.255.255.128

[Edit](#)

**Management Network Interface**

Interface Name management

IP Address 11.22.33.44

Subnet Mask 255.255.255.0

[Exit](#) [Start Configuration](#)

**Note** To download the appliance configuration as a JSON file, click the [here](#) link.

- p) Review all of the settings that you have entered while completing the wizard. If necessary, click the appropriate **Edit** link to open the wizard screen in which you want to make updates.
- q) To complete the configuration of your Cisco DNA Center appliance, click **Start Configuration**.

The wizard screen continuously updates during the process, indicating the tasks that are currently being completed and their progress, as well as any errors that have occurred. To save a local copy of this information as a text file, click the download icon.

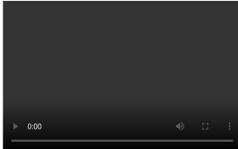
Cisco DNA Center
Configuration

### Appliance Configuration In Progress

It should take about 90 minutes to complete the configuration of your appliance. As you wait, you can view a video that explains the next steps in the Cisco DNA Center setup process.

Initializing the cluster using kubeadm 30%

ABOUT STARTING CISCO DNA CENTER



Started: 04/09/2020 12:15:36

```

2021-05-05T16:56:59.32524 | .....
2021-05-05T16:56:59.32525 | credentialmanager.pem Apr 13 16:49:52 2020 GMT Apr 13 16:49:52 2021 GMT
2021-05-05T16:56:59.32526 | kong.pem Apr 13 16:49:51 2020 GMT Apr 13 16:49:51 2021 GMT
2021-05-05T16:56:59.32527 | kube-admin.pem Apr 13 16:49:50 2020 GMT Apr 13 16:49:50 2021 GMT
2021-05-05T16:56:59.32528 | kube-worker-1.pem Apr 13 16:49:52 2020 GMT Apr 13 16:49:52 2021 GMT
2021-05-05T16:56:59.32529 | maglev-registry.pem Apr 13 16:49:52 2020 GMT Apr 13 16:49:52 2021 GMT
2021-05-05T16:56:59.325210 | apiserver.crt Apr 13 12:12:14 2020 GMT Apr 13 17:40:20 2021 GMT
2021-05-05T16:56:59.325211 | apiserver-kubeler-client.crt Apr 13 12:12:14 2020 GMT Apr 13 17:40:20 2021 GMT
2021-05-05T16:56:59.325212 | front-proxy-ca.crt Apr 13 17:40:20 2020 GMT Apr 13 17:40:20 2020 GMT
2021-05-05T16:56:59.325213 | front-proxy-client.crt Apr 13 17:40:20 2020 GMT Apr 13 17:40:20 2021 GMT
2021-05-05T16:56:59.325214 | kubelet.conf Apr 13 12:12:14 2020 GMT Apr 13 17:40:21 2021 GMT
2021-05-05T16:56:59.325215 | admin.conf Apr 13 12:12:14 2020 GMT Apr 13 17:40:21 2021 GMT
2021-05-05T16:56:59.325216 | scheduler.conf Apr 13 12:12:14 2020 GMT Apr 13 17:40:22 2021 GMT
2021-05-05T16:56:59.325217 | controller-manager.conf Apr 13 12:12:14 2020 GMT Apr 13 17:40:22 2021 GMT
2021-05-05T16:56:59.325218 | .....

```

### What to do next

When this task is complete:

- If you have an additional appliance to deploy as the third and final node in the cluster, repeat this procedure.
- If you are finished adding nodes to the cluster, continue by performing 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 7

# Configure the 112-Core Appliance Using the Browser-Based Wizard

---

- [Appliance Configuration Overview](#), on page 177
- [Configure an Appliance Using the Install Configuration Wizard](#), on page 178
- [Configure the Primary Node Using the Advanced Install Configuration Wizard](#), on page 192
- [Configure a Secondary Node Using the Advanced Install Configuration Wizard](#), on page 209
- [Upgrade to the Latest Cisco DNA Center Release](#), on page 228

## Appliance Configuration Overview

You can deploy the 112-core appliance in your network in one of the following 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. If you choose Standalone mode for your initial deployment, this will be your first, or primary, node. Note that you can add more appliances later to form a cluster.
- **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 Cluster mode for your initial deployment, be sure to finish configuring the primary node before configuring the secondary nodes.

To proceed, first configure the primary node in your cluster. Then, if you have installed three appliances and want to add the second and third nodes to your cluster, configure the secondary nodes.

## Browser-Based Configuration Wizards

Cisco DNA Center offers two browser-based wizards that you can use to configure your appliance. Read their descriptions to determine which of these wizards you should complete.



---

**Important**

These wizards are available for use if you are configuring a new appliance that came with Cisco DNA Center 2.3.4 already installed. If you upgraded from a previous version and want to use these wizards, contact Cisco TAC for assistance.

---

### Install Configuration Wizard

This wizard streamlines the appliance configuration process by setting default values for the Enterprise, Management, and Internet Access interfaces (which all reside on the appliance's Enterprise port) as well as the Intracluster interface. Use this wizard if you are okay with using the default interface settings and want to get your appliance up and running as quickly as possible. Note that you cannot use this wizard to configure a cluster's secondary nodes.

### Advanced Install Configuration Wizard

This wizard provides access to all of the available appliance settings that you can modify. Use this wizard if you want to specify interface settings that are different from the default settings. Also use this wizard if you are configuring the second or third node in your cluster.

## Browser-Based Wizard Prerequisites

To use either of the browser-based wizards and ensure that it configures your appliance properly, complete the following tasks:

- Designate the Enterprise interface on your appliance to use the IP address, subnet mask, and default gateway that a DHCP server assigns to it. When you configure this interface in the wizard, you will not be able to change the IP address or subnet mask that have been assigned to it. You will only be able to change its default gateway. The topics in this chapter assume that the Enterprise interface was chosen for this purpose.
- Confirm that the IP address assigned by the DHCP server is reachable by the machine from which you will complete the wizard.
- For the Enterprise and Intracluster interfaces, verify that both interfaces are connected and in the **UP** state.

If you want to specify your own IP address, subnet mask, and default gateway for your appliance's Enterprise interface (and not use the values assigned by a DHCP server), ensure that you complete the Static IP Address Settings screen.

## Configure an Appliance Using the Install Configuration Wizard

Perform this procedure to configure either a three-node cluster's primary node or a standalone node using the Install configuration wizard. The wizard simplifies the configuration process by setting up the Enterprise, Management, and Internet interfaces on the same port using default settings. The following second generation Cisco DNA Center appliances support configuration using this wizard:

- 112-core appliance: Cisco part number DN2-HW-APL-XL
- 112-core promotional appliance: Cisco part number DN2-HW-APL-XL-U



**Important**

- You cannot use this wizard to configure the second or third appliance in a three-node cluster. To do so, complete the steps described in [Configure a Secondary Node Using the Advanced Install Configuration Wizard, on page 209](#). Also, you cannot use this wizard to enable LACP mode on your appliance's Enterprise and Intracluster interfaces.
- Before you configure any of 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.
- 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.

You can only use this wizard to complete the initial configuration of a new Cisco DNA Center appliance. To reimage an appliance that's been configured previously, you will need to use the Maglev Configuration wizard (see [Configure the Appliance Using the Maglev Wizard, on page 81](#)).

**Before you begin**

Ensure that you:

- Installed the Cisco DNA Center software image onto your appliance, as described in [Reimage the Appliance, on page 74](#).

**Important**

This is only applicable if you are going to configure a promotional appliance, because the Cisco DNA Center software image is not preinstalled on the 112-core promotional appliance (Cisco part number DN2-HW-APL-XL-U).

- Collected all of the information called for in [Required IP Addresses and Subnets, on page 29](#) and [Required Configuration Information](#).
- Installed the appliance as described in [Appliance Installation Workflow](#).
- Configured Cisco IMC browser access on this appliance, as described in [Enable Browser Access to Cisco Integrated Management Controller](#).
- Checked that the appliance's ports and the switches it uses are properly configured, as described in [Execute Preconfiguration Checks](#).
- Are using a browser that is compatible with Cisco IMC and Cisco DNA Center. For a list of compatible browsers, see the [Release Notes](#) for the version of Cisco DNA Center you are installing.
- Enabled ICMP on the firewall between Cisco DNA Center and the DNS servers you will specify in the following procedure. This wizard uses Ping to verify the DNS server you specify. This ping can be blocked if there is a firewall between Cisco DNA Center and the DNS server and ICMP is not enabled on that firewall. When this happens, you will not be able to complete the wizard.

**Step 1**

Start the Install configuration wizard:

- a) Point your browser to the Cisco IMC IP address you set during the Cisco IMC GUI configuration you performed, then 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 blue link menu at the upper right, as shown below.



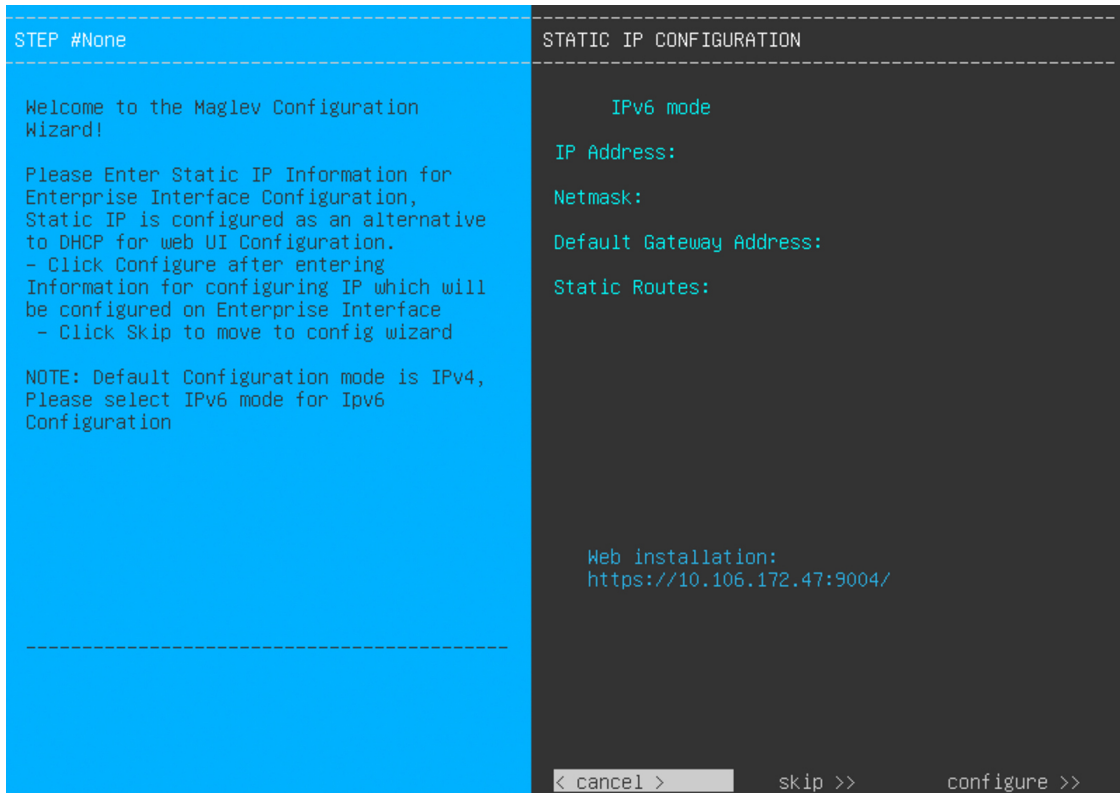
- b) From the blue link menu, choose **Launch KVM** and then select either **Java based KVM** or **HTML based KVM**. If you select the Java-based KVM, you will need to launch the Java startup file from your browser or file manager in order to view the KVM console in its own window. If you select the HTML-based KVM, it will launch the KVM console in a separate browser 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 Maglev Configuration Wizard prompts.

- c) 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**. Then switch to the KVM console to continue.
  - In the KVM console: Choose **Power > Power Cycle System (cold boot)**.

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

After displaying reboot messages, the KVM console displays the **Static IP Configuration** screen.



Note the URL listed in the **Web Installation** field.

d) Do one of the following:

- If you want a DHCP server to assign an IP address, subnet mask, and default gateway to your appliance's Enterprise interface, click **Skip**.
- If you want to assign your own IP address, subnet mask, and default gateway to your appliance's Enterprise interface, enter the information described in the following table and then click **Configure**.

IPv6 Mode check box	If you want to configure an IPv6 address, check this check box.
IP Address field	Enter the static IP address you want to use.
Netmask field	Enter the netmask for the IP address you specified in the previous field: <ul style="list-style-type: none"> <li>• If you entered an IPv4 address, you can enter either a netmask or CIDR address.</li> <li>• If you entered an IPv6 address, you can only enter a CIDR address.</li> </ul>
Default Gateway Address field	Specify the default gateway that will be used to route traffic.
Static Routes field	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 Management port only.

The KVM console displays the Maglev Configuration wizard welcome screen.

```
Welcome to the Maglev Configuration Wizard!

The wizard will walk you through the steps to configure this host. Select one of the options below to specify how you
would like to configure this host:

Start a Cisco DNA Center Cluster
Join a Cisco DNA Center Cluster

< exit >
```

- e) To bring up the **Appliance Configuration** screen, open the URL that was displayed in the **Static IP Configuration** screen.

Cisco DNA Center

Appliance Configuration

Welcome to Cisco DNA Center

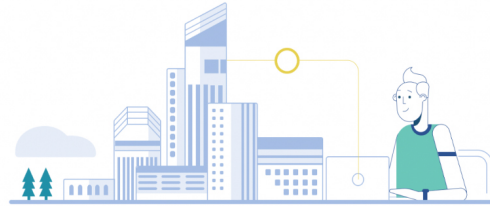
Are you starting a new Cisco DNA Center Cluster or joining an existing one?

Start A Cisco DNA  
Center Cluster

This appliance will be the primary  
node of a cluster.

Join A Cisco DNA  
Center Cluster

This appliance will be added as a  
node to the primary node of a cluster.



Next

- f) Click the **Start a Cisco DNA Center Cluster** radio button, then click **Next**.

Cisco DNA Center

Appliance Configuration

Welcome to Cisco DNA Center

Before you can use Cisco DNA Center, first complete the appropriate appliance configuration workflow. Which workflow matches your needs?

Install 

Configure a standalone node or cluster's primary node.

Use this quick, simplified wizard to set up the Enterprise, Management, and Internet interfaces on the same interface with default settings.

Advanced Install 

Configure a standalone node or any node in a cluster.

Use this wizard to access all of the available appliance configuration options.



Back

Start

- g) Click the **Install** radio button, then click **Start**.

The **Overview** slider opens. Click > to view a summary of the tasks that the wizard will help you complete.

✕

## Overview

Complete the basic tasks required to configure your appliance for use with Cisco DNA Center.



Start Workflow



- h) Click **Start Workflow** to start the wizard.

The **Appliance Interface Overview** screen opens, providing a description of the four interfaces that are available on your Cisco DNA Center appliance.

Cisco DNA Center
Install

## Appliance Interface Overview

In order for Cisco DNA Center to operate properly, you need to configure four interfaces on your appliance:

1. **Enterprise Network Interface:** Connects your appliance to the Enterprise network.
2. **Intracenter Link Interface:** Connects your appliance to your cluster.
3. **Management Network Interface:** (Optional) Accesses the Cisco DNA GUI from your Management network.
4. **Internet Access Interface:** (Optional) Accesses the internet.

In this workflow, the Intracenter Link Interface is predefined. The other three interfaces will be configured together on the Enterprise port.

Exit
Next

The wizard will help you configure the Enterprise and Cluster ports, which are required for Cisco DNA Center functionality. If the wizard fails to display either or both of these ports in the next screen, they may be non-functional or disabled. If you discover that they are non-functional, choose **Exit** to exit the wizard 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 2 Complete the Install configuration wizard:

a) Click **Next**.

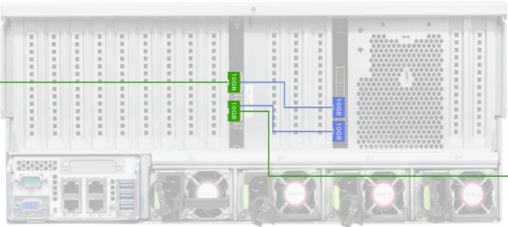
The **Configure The Enterprise Port** screen opens.

Cisco DNA Center
Install

### Configure the Enterprise Port

In this workflow, the Management Network and Internet Access Interfaces are on the same port as the Enterprise Network Interface. You can enter up to three DNS addresses. If your network resides behind a firewall, you must [allow access to these URLs](#) and [open these ports](#). If you are setting up a multinode cluster, the cluster's second and third nodes must reside in the same subnet as the primary node. [Download the Intracenter Link interface's information](#)

■ Connected    ■ Disconnected    ■ LACP-disabled



**Enterprise & Management Network & Internet Access Interface**

LACP Mode: Disabled

IP Address: 10.106.172.27

Netmask: 255.255.255.128

Default Gateway: 10.106.172.1

**Intracenter Link Interface**

Interface Name: cluster

LACP Mode: Disabled

IP Address: 169.254.6.64

Subnet Mask: 255.255.255.128

Exit
Next

The configuration wizard sets up the Enterprise, Management, and Internet Access interfaces on the Enterprise port. The wizard also prepopulates values for almost all of the listed parameters.

If your network resides behind a firewall, do the following:

- Click the **allow access to these URLs** link to view a popup window that lists the URLs that Cisco DNA Center must be able to access.
- Click the **open these ports** link to view a popup window that lists the network service ports that must be available for Cisco DNA Center to use.

b) Click **Next**.

The **DNS Configuration** screen opens.

c) In the **DNS** field, enter the IP address of the preferred DNS server. To enter additional DNS servers, click the **Add (+)** icon.

**Important** You can configure a maximum of three DNS servers. Problems can occur if you configure more than three DNS servers for an appliance.

d) Click **Next**.

The wizard validates the information you have entered, confirms that the port is up, and notifies you of any settings that need to be changed before you can proceed with the wizard. If the settings you have entered are valid and the port is up, the wizard's **Interface to Port Configuration** screen opens.



Cisco DNA Center Install

### Interface to Port Configuration

We are going to configure the following interfaces. Click **Configure** and wait for configuration to be done before proceeding to the next step.

**Configure**

Interface Name	enterprise
LACP Mode	Disabled
IP Address	10.106.172.27
Netmask	255.255.255.128
Default Gateway	10.106.172.1

Interface Name	cluster
LACP Mode	Disabled
IP Address	169.254.6.64
Subnet Mask	255.255.255.128

[Exit](#) [Back](#) [Next](#)

- e) Review the interface settings that have been set, then click **Configure**.
- f) After initial interface configuration has completed, click **Next** to proceed to the next wizard screen.

The **Configure Proxy Server Information** screen opens.

Cisco DNA Center Install

### Configure Proxy Server Information

Does your network use a proxy server to access the internet?

Yes  No

Proxy Server\*  
  
E.g. http://example.com

Port\*  
  
Enter port number between 0 to 65535.

Username

Password

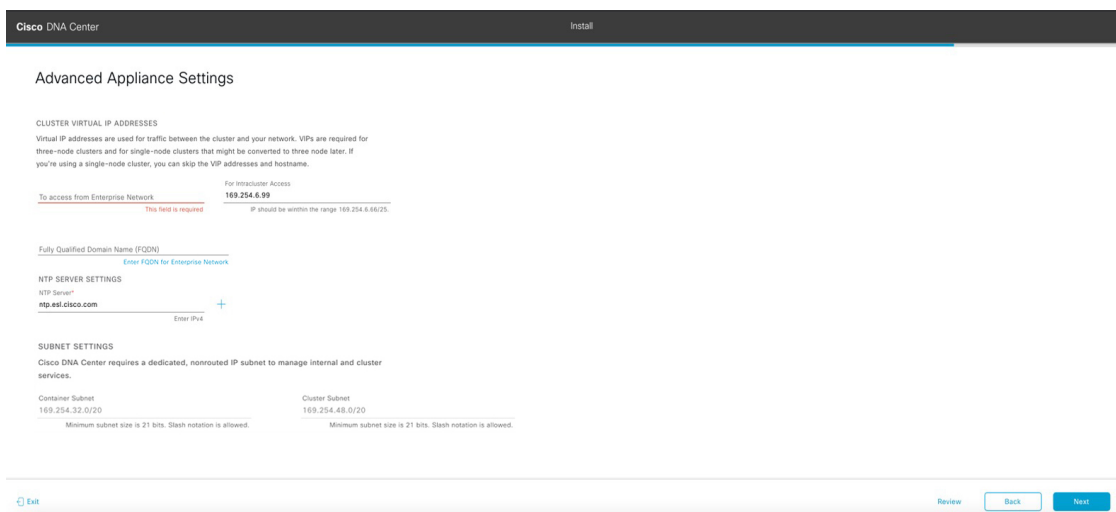
[Exit](#) [Review](#) [Back](#) [Next](#)

- g) Do one of the following, then click **Next**:
- If your network does *not* use a proxy server to access the internet, click the **No** radio button.
  - If your network does use a proxy server to access the internet, enter the values described in the following table:

**Table 47: Primary Node Entries for Proxy Server Settings**

Proxy Server field	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.
Port field	Enter the port your appliance used to access the network proxy.
Username field	Enter the user name used to access the network proxy. If no proxy login is required, leave this field blank.
Password field	Enter the password used to access the network proxy. If no proxy login is required, leave this field blank.

The wizard validates the information you have entered and notifies you of any settings that need to be changed before you can proceed with the wizard. If the settings you have entered are valid, the wizard's **Advanced Appliance Settings** screen opens.



h) Enter configuration values for your cluster, then click **Next**.

**Table 48: Primary Node Entries for Advanced Appliance Settings**

Cluster Virtual IP Addresses	
To access from Enterprise Network and For Intracluster Access fields	Enter the virtual IP address that will be used for traffic between the cluster and both the Enterprise and Intracluster interfaces on your appliance. This is required for single-node clusters that will be converted into a three-node cluster in the future. If you have a single-node cluster setup and don't plan to move to a three-node cluster setup, you can leave the fields in this section blank.  <b>Important</b> If you choose to configure a virtual IP address, you must enter one 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 <b>UP</b> state.

Fully Qualified Domain Name (FQDN) field	<p>Enter the fully qualified domain name (FQDN) for your cluster. Cisco DNA Center does the following with this hostname:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> </ul>
<b>NTP Server Settings</b>	
NTP Server field	<p>Enter at least one NTP server address or hostname. To enter additional NTP server addresses or hostnames, click the <b>Add (+)</b> icon.</p> <p>For a production deployment, Cisco recommends that you configure a minimum of three NTP servers.</p>
<b>Subnet Settings</b>	
Container Subnet field	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 you cannot enter another subnet.
Cluster Subnet field	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 you cannot enter another subnet.

The **Enter CLI Password** screen opens.

Cisco DNA Center Install

Enter CLI Password

CLI Password: Identifies the password for the CLI username maglev. This password ensures secure access to each appliance using the CLI command line. If required, you can assign a different CLI password for each maglev CLI username on each appliance in a cluster.

Username\*  
maglev

Password\*  
..... [SHOW](#)

[View Password Criteria](#)

Retype to Confirm\*  
..... [SHOW](#)

[Exit](#) [Review](#) [Back](#) [Next](#)

- i) Enter and confirm the password for the `maglev` user, then click **Next**.

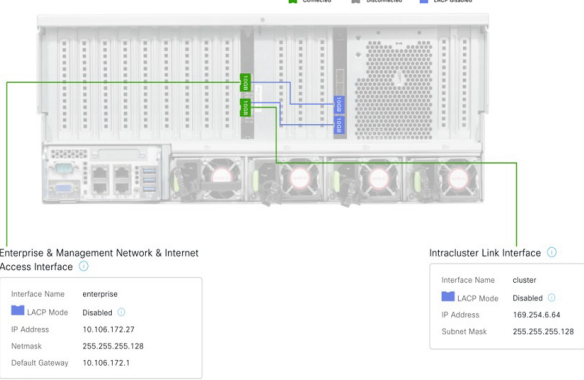
The wizard validates the information you have entered and notifies you of any settings that need to be changed before you can proceed with the wizard. If the settings you have entered are valid, the wizard's **Summary** screen opens.

Cisco DNA Center Install

### Summary

Please review the settings that you have entered. If you need to make any changes, click the appropriate Edit link and make the necessary updates. You can download the generated configuration in JSON format from [here](#). When you are happy with your settings, click Start Configuration.

Enterprise Port [Edit](#)



Enterprise & Management Network & Internet Access Interface	
Interface Name	enterprise
LACP Mode	Disabled
IP Address	10.106.172.27
Netmask	255.255.255.128
Default Gateway	10.106.172.1

Intracuster Link Interface	
Interface Name	cluster
LACP Mode	Disabled
IP Address	169.254.6.64
Subnet Mask	255.255.255.128

[Exit](#) [Start Configuration](#)

**Note** To download the appliance configuration as a JSON file, click the [here](#) link.

- j) Scroll to the bottom of the screen and review all of the settings that you have entered while completing the wizard. If necessary, click the appropriate **Edit** link to open the wizard screen in which you want to make updates.
- k) To complete the configuration of your Cisco DNA Center appliance, click **Start Configuration**.

The wizard screen continuously updates during the process, indicating the tasks that are currently being completed and their progress, as well as any errors that have occurred. To save a local copy of this information as a text file, click the **Download** link.

Cisco DNA Center
Install

## Appliance Configuration In Progress

It should take about 30 minutes to configure the appliance. **Do not press your browser's back button or refresh this page.** The page will update after configuration completes.

30%

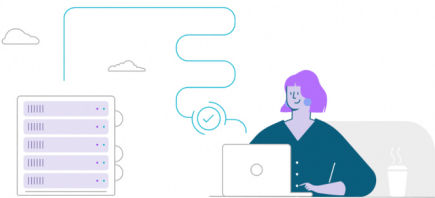
Initializing the cluster using kubeadm

Started: 04/09/2020 12:15:36

Download

```

                17:40:20 2021 GMT
                2021-12-03T05:37:06.616Z14 | kubelet.conf Apr 13 12:12:14 2020 GMT Apr 13 17:40:21 2021 GMT
                2021-12-03T05:37:06.616Z15 | admin.conf Apr 13 12:12:14 2020 GMT Apr 13 17:40:21 2021 GMT
                2021-12-03T05:37:06.616Z16 | scheduler.conf Apr 13 12:12:14 2020 GMT Apr 13 17:40:22 2021 GMT
                2021-12-03T05:37:06.616Z17 | controller-
                manager.conf Apr 13 12:12:14 2020 GMT Apr 13 17:40:22 2021 GMT
                2021-12-03T05:37:06.616Z18 | -----
                -----
            
```



**Step 3** After appliance configuration completes, click the copy icon in the **Cisco DNA Center - Admin Credential** area to copy the default admin superuser password.

Cisco DNA Center
Install

## Appliance Configuration Complete!

**Important:** Take note of the credentials displayed below. You can click the copy icon if you want to save them locally. You will use these credentials to log in to Cisco DNA Center for the first time. After logging in, you will be prompted to change the password.


CISCO DNA CENTER - ADMIN CREDENTIAL

Username     admin

password     maglev1@3

What's Next?

Open Cisco DNA Center



**Important** Cisco DNA Center automatically sets this password when you complete the Install configuration wizard. Ensure that you click the copy icon before you proceed. Otherwise, you will not be able to log in to Cisco DNA Center for the first time.

**Note** As a security measure, you'll be prompted to change this password after you log in. For more information, see [Complete the Quick Start Workflow, on page 229](#).

---

### What to do next

As you are deploying this appliance in standalone mode, continue by performing first-time setup: [First-Time Setup Workflow](#).

## Configure the Primary Node Using the Advanced Install Configuration Wizard

Perform the following steps to configure the first installed appliance as the primary node using the Advanced Install configuration wizard. You must always configure the first appliance as the primary node, whether it will operate standalone or as part of a cluster.



### Important

- The following second generation Cisco DNA Center appliances support configuration using this wizard:
  - 112-core appliance: Cisco part number DN2-HW-APL-XL
  - 112-core promotional appliance: Cisco part number DN2-HW-APL-XL-U
- You can only use this wizard to complete the initial configuration of a new Cisco DNA Center appliance. To reimage an appliance that's been configured previously, you will need to use the Maglev Configuration wizard (see [Configure the Appliance Using the Maglev Wizard, on page 81](#)).
- 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.
- 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.

---

If you are configuring the installed appliance as a secondary node for an existing cluster that already has a primary node, follow the steps in [Configure a Secondary Node Using the Advanced Install Configuration Wizard, on page 209](#) instead.

### Before you begin

Ensure that you:

- Installed the Cisco DNA Center software image onto your appliance, as described in [Reimage the Appliance, on page 74](#).



**Important** This is only applicable if you are going to configure a promotional appliance, because the Cisco DNA Center software image is not preinstalled on the 112-core promotional appliance (Cisco part number DN2-HW-APL-XL-U).

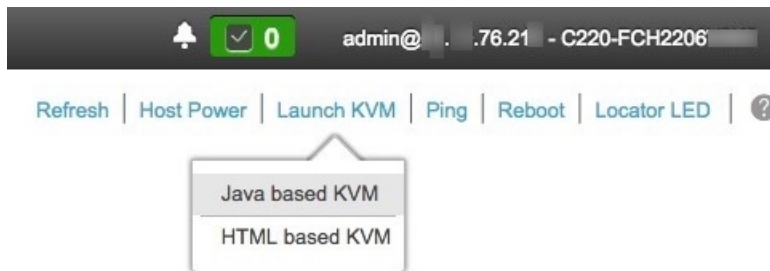
- Collected all of the information called for in [Required IP Addresses and Subnets, on page 29](#) and [Required Configuration Information](#).
- Installed the first appliance as described in [Appliance Installation Workflow](#).
- Configured Cisco IMC browser access on the primary node, as described in [Enable Browser Access to Cisco Integrated Management Controller](#).
- Checked that the primary node's ports and the switches it uses are properly configured, as described in [Execute Preconfiguration Checks](#).
- Are using a browser that is compatible with Cisco IMC and Cisco DNA Center. For a list of compatible browsers, see the [Release Notes](#) 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 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

Start the Advanced Install configuration wizard:

- Point your browser to the Cisco IMC IP address you set during the Cisco IMC GUI configuration you performed, then 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 blue link menu at the upper right, as shown below.



- From the blue link menu, choose **Launch KVM** and then select either **Java based KVM** or **HTML based KVM**. If you select the 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 the HTML-based KVM, it will launch the KVM console in a separate browser 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 Maglev Configuration Wizard prompts.

- 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**. Then switch to the KVM console to continue.
- In the KVM console: Choose **Power > Power Cycle System (cold boot)**.

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

After displaying reboot messages, the KVM console displays the **Static IP Configuration** screen.

```

STEP #None
-----
Welcome to the Maglev Configuration Wizard!

Please Enter Static IP Information for Enterprise Interface Configuration,
Static IP is configured as an alternative to DHCP for web UI Configuration.
- Click Configure after entering Information for configuring IP which will
be configured on Enterprise Interface
- Click Skip to move to config wizard

NOTE: Default Configuration mode is IPv4,
Please select IPv6 mode for Ipv6 Configuration

-----
STATIC IP CONFIGURATION

IPv6 mode
IP Address:
Netmask:
Default Gateway Address:
Static Routes:

Web installation:
https://10.106.172.47:9004/

-----
< cancel >      skip >>      configure >>

```

Note the URL listed in the **Web Installation** field.

d) Do one of the following:

- If you want a DHCP server to assign an IP address, subnet mask, and default gateway to your appliance's Enterprise interface, click **Skip**.
- If you want to assign your own IP address, subnet mask, and default gateway to your appliance's Enterprise interface, enter the information described in the following table and then click **Configure**.

IPv6 Mode check box	If you want to configure an IPv6 address, check this check box.
IP Address field	Enter the static IP address you want to use.
Netmask field	Enter the netmask for the IP address you specified in the previous field: <ul style="list-style-type: none"> <li>• If you entered an IPv4 address, you can enter either a netmask or CIDR address.</li> <li>• If you entered an IPv6 address, you can only enter a CIDR address.</li> </ul>



Default Gateway Address field	Specify the default gateway that will be used to route traffic.
Static Routes field	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 Management port only.

The KVM console displays the Maglev Configuration wizard welcome screen.

```
Welcome to the Maglev Configuration Wizard!

The wizard will walk you through the steps to configure this host. Select one of the options below to specify how you
would like to configure this host:

Start a Cisco DNA Center Cluster
Join a Cisco DNA Center Cluster

< exit >
```

- e) To bring up the **Appliance Configuration** screen, open the URL that was displayed in the **Static IP Configuration** screen.

Cisco DNA Center

Appliance Configuration

Welcome to Cisco DNA Center

Are you starting a new Cisco DNA Center Cluster or joining an existing one?

Start A Cisco DNA  
Center Cluster

This appliance will be the primary  
node of a cluster.

Join A Cisco DNA  
Center Cluster

This appliance will be added as a  
node to the primary node of a cluster.



Next

- f) Click the **Start a Cisco DNA Center Cluster** radio button, then click **Next**.

Cisco DNA Center Appliance Configuration

Welcome to Cisco DNA Center

Before you can use Cisco DNA Center, first complete the appropriate appliance configuration workflow. Which workflow matches your needs?

**Install**


Configure a standalone node or cluster's **primary node**.

Use this quick, simplified wizard to set up the Enterprise, Management, and Internet interfaces on the same interface with default settings.

**Advanced Install**

Configure a standalone node or **any node in a cluster**.

Use this wizard to access all of the available appliance configuration options.



- g) Click the **Advanced Install** radio button, then click **Start**.

The **Advanced Install Overview** slider opens. Click > to view a summary of the tasks that the wizard will help you complete.

### Advanced Install Overview

Prepare your appliance for use with Cisco DNA Center by configuring its interfaces and entering cluster and other required information.



- h) Click **Start Workflow** to start the wizard.

The **Appliance Interface Overview** screen opens, providing a description of the four appliance interfaces that you can configure.

The screenshot shows the Cisco DNA Center Advanced Install wizard. The title bar reads "Cisco DNA Center" and "Advanced Install". The main heading is "Appliance Interface Overview". Below the heading, a note states: "In order for Cisco DNA Center to operate properly, you need to configure four interfaces on your appliance:". A numbered list follows:

1. **Enterprise Network Interface:** Connects your appliance to the Enterprise network.
2. **Intracenter Link Interface:** Connects your appliance to your cluster.
3. **Management Network Interface:** (Optional) Accesses the Cisco DNA Center GUI from your Management network.
4. **Internet Access Interface:** (Optional) Accesses the internet.

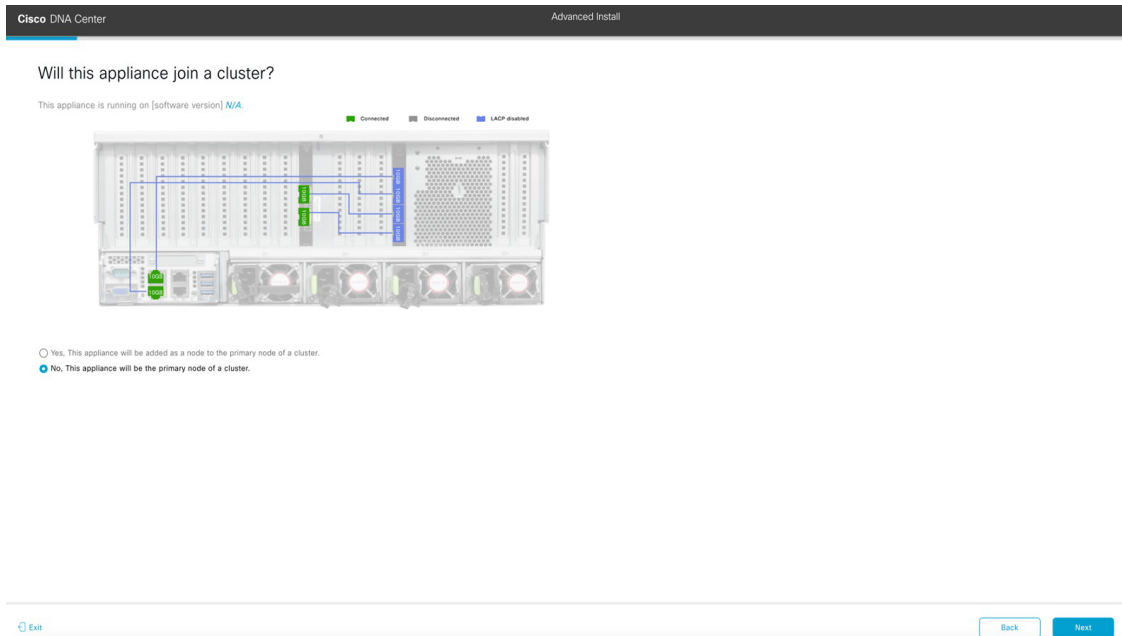
Below the list, a note explains: "In this workflow, the Enterprise Network Interface and the Intracenter Link Interface will each have their own dedicated port. You can choose to have either Management Network Interface and/or Internet Access Interface be on the same port as the Enterprise Network Interface or assign them to a separate designated port." At the bottom of the wizard window, there are "Exit" and "Next" buttons.

**Important** At a minimum, you must configure the Enterprise and Intracenter ports, as they are required for Cisco DNA Center functionality. If the wizard fails to display either or both of these ports during the course of configuration, they may be non-functional or disabled. If you discover that they are non-functional, choose **Exit** to exit the wizard 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).

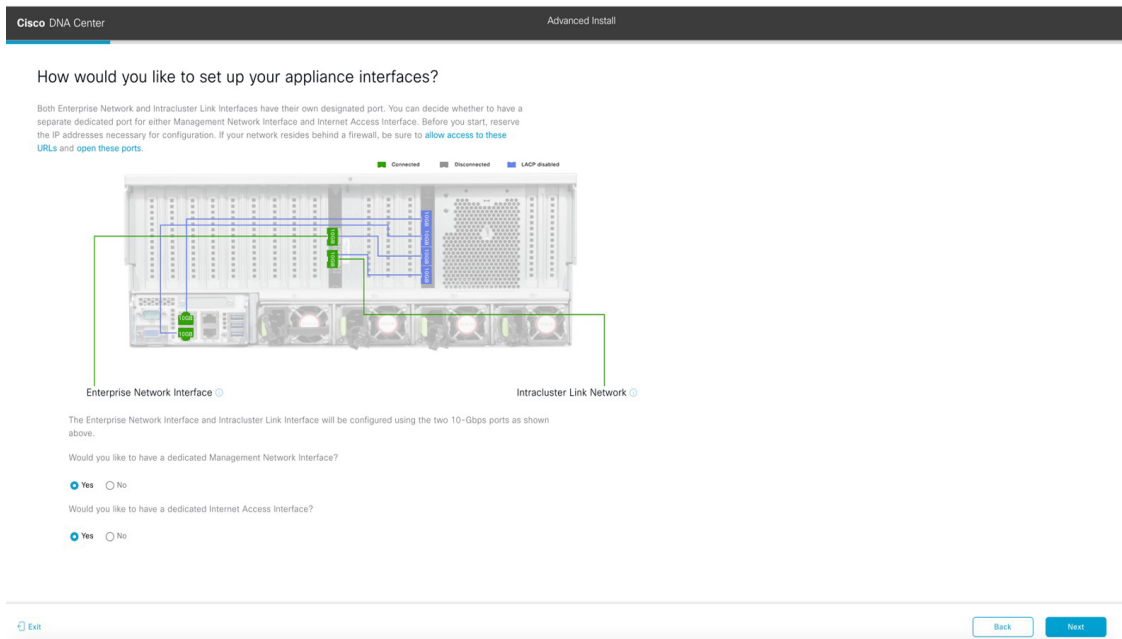
**Step 2** Complete the Advanced Install wizard:

a) Click **Next**.

The **Will this appliance join a cluster?** screen opens.



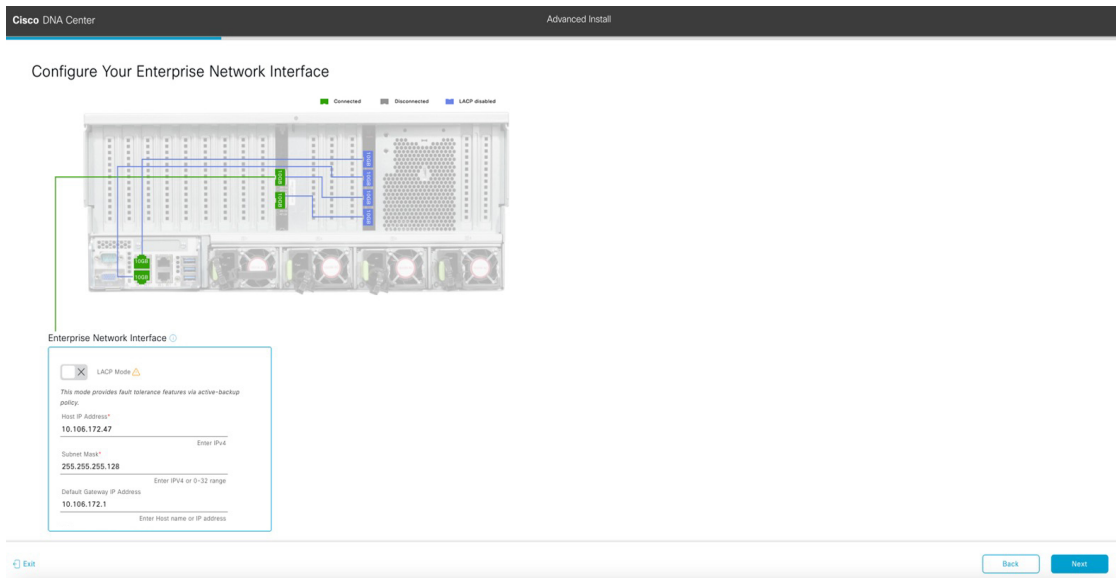
- b) Click the **No** radio button (as you are configuring your cluster's primary node), then click **Next**. The **How would you like to set up your appliance interfaces?** screen opens.



If your network resides behind a firewall, do the following:

- Click the **allow access to these URLs** link to view a popup window that lists the URLs that Cisco DNA Center must be able to access.
- Click the **open these ports** link to view a popup window that lists the network service ports that must be available for Cisco DNA Center to use.

- c) Indicate whether you want to configure dedicated Management and Internet Access interfaces, then click **Next**. The **Configure Your Enterprise Network Interface** screen opens.



- d) Enter configuration values for the Enterprise interface, then click **Next**.

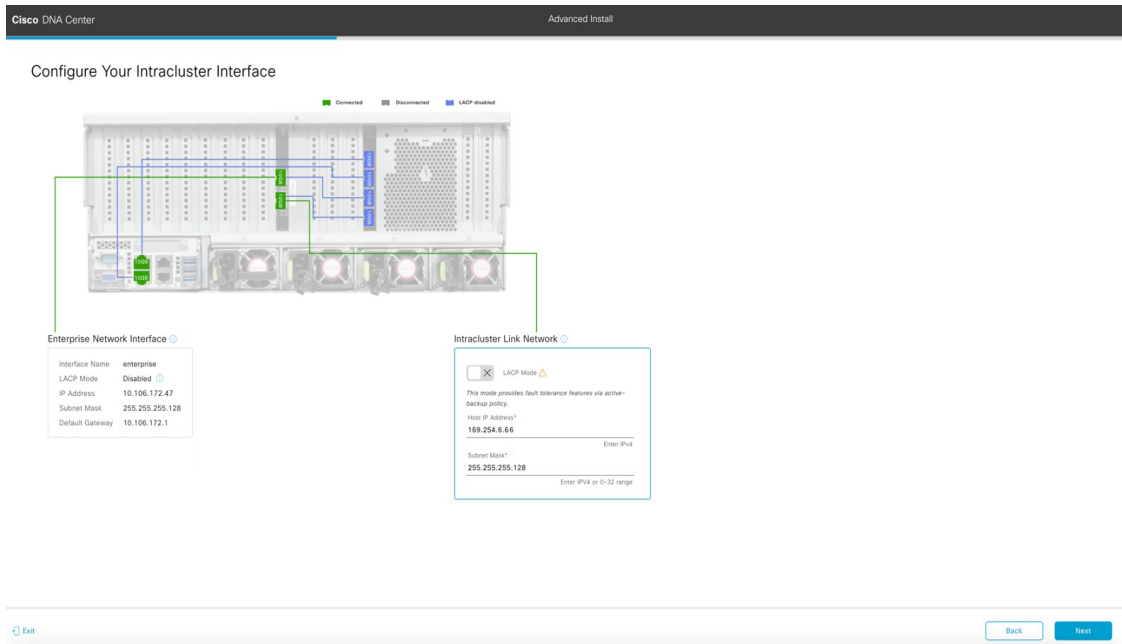
As explained in [Interface Cable Connections](#), this is a required interface used to link the appliance to the enterprise network. See [Required IP Addresses and Subnets, on page 29](#) and [Required Configuration Information](#) for a more detailed description of the values you need to enter.

**Table 49: Primary Node Entries for the Enterprise Interface**

LACP Mode slider	<p>Choose one of the following network interface controller (NIC) bonding modes for the Enterprise interface:</p> <ul style="list-style-type: none"> <li>• <b>Active-Backup mode:</b> This mode provides fault tolerance by aggregating two Ethernet interfaces into a single logical channel. When the interface that's currently active goes down, the other interface takes its place and becomes active.</li> <li>• <b>LACP mode:</b> This mode aggregates two Ethernet interfaces that share the same speed and duplex settings into a single logical channel. This provides load balancing and higher bandwidth.</li> </ul> <p>For more information about Cisco DNA Center's implementation of NIC bonding, see <a href="#">NIC Bonding Overview, on page 67</a>.</p>
Host IP Address field	Enter the IP address for the Enterprise port. This is required.
Subnet Mask field	Enter the netmask for the port's IP address. This is required.

<p>Default Gateway IP Address field</p>	<p>Enter a default gateway IP address to use for the port.</p> <p><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.</p> <p><b>Note</b> You designated this interface to use the default gateway assigned to it by a DHCP server. Complete the following steps to specify a different gateway:</p> <ol style="list-style-type: none"> <li>1. Delete the IP address that is currently listed in this field and then click <b>Exit</b>.  This will bring you back to the first wizard screen.</li> <li>2. Return to the Enterprise port's wizard screen and enter the gateway IP address you want to use.</li> </ol>
---	--

The wizard validates the information you have entered, confirms that the port is up, and notifies you of any settings that need to be changed before you can proceed with the wizard. If the settings you have entered are valid and the port is up, the wizard's **Configure Your Intracluster Interface** screen opens.



e) Enter configuration values for your Intracluster interface, then click **Next**.

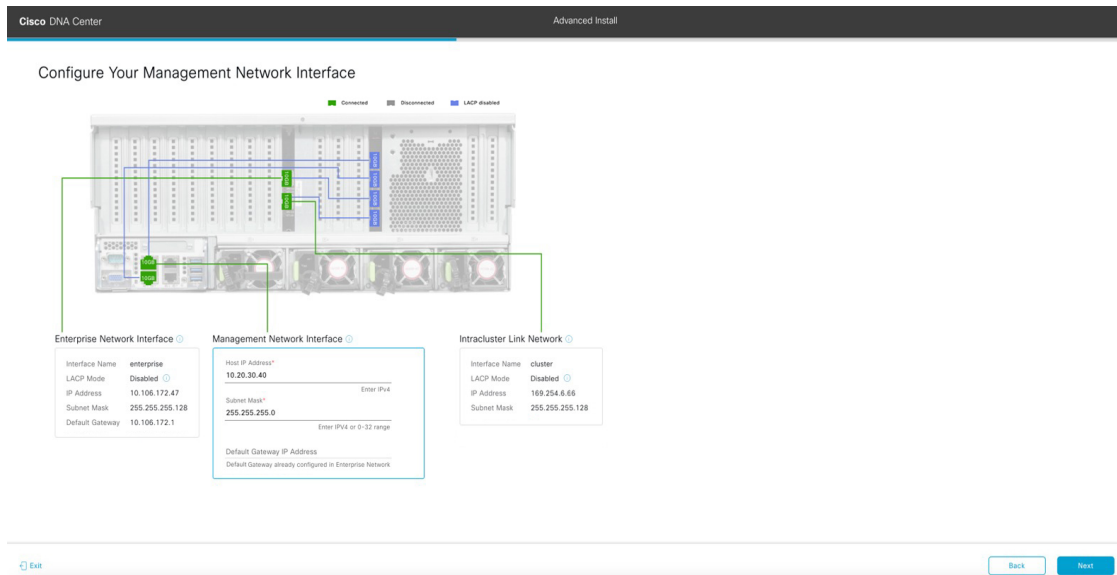
As explained in [Interface Cable Connections](#), this required port is used to link the appliance to your cluster. See [Required IP Addresses and Subnets](#), on page 29 and [Required Configuration Information](#) for a more detailed description of the values you need to enter.

- Note**
- If you opted to configure the Enterprise and Internet Access interfaces on the same port, complete this step and then proceed to Step 2f (which describes how to configure your Management interface).
  - If you opted to configure the Enterprise and Management interfaces on the same port, complete this step and then skip ahead to Step 2g (which describes how to configure your Internet Access interface).
  - If you opted to configure the Enterprise, Management, and Internet Access interfaces on the same port, complete this step and then skip ahead to Step 2h.

**Table 50: Primary Node Entries for the Intracluster Interface**

LACP Mode slider	<p>Choose one of the following NIC bonding modes for the Intracluster interface:</p> <ul style="list-style-type: none"> <li>• <b>Active-Backup mode:</b> This mode provides fault tolerance by aggregating two Ethernet interfaces into a single logical channel. When the interface that's currently active goes down, the other interface takes its place and becomes active.</li> <li>• <b>LACP mode:</b> This mode aggregates two Ethernet interfaces that share the same speed and duplex settings into a single logical channel. This provides load balancing and higher bandwidth.</li> </ul> <p>For more information about Cisco DNA Center's implementation of NIC bonding, see <a href="#">NIC Bonding Overview, on page 67</a>.</p>
Host IP Address field	Enter the IP address for the Cluster port. This is required. Note that you cannot change the address of the Cluster port later.
Subnet Mask field	Enter the netmask for the port's IP address. This is required.

The wizard validates the information you have entered, confirms that the port is up, and notifies you of any settings that need to be changed before you can proceed with the wizard. If the settings you have entered are valid and the port is up, the wizard's **Configure Your Management Network Interface** screen opens.





- f) (Optional) Enter configuration values for the Management port, then click **Next**.

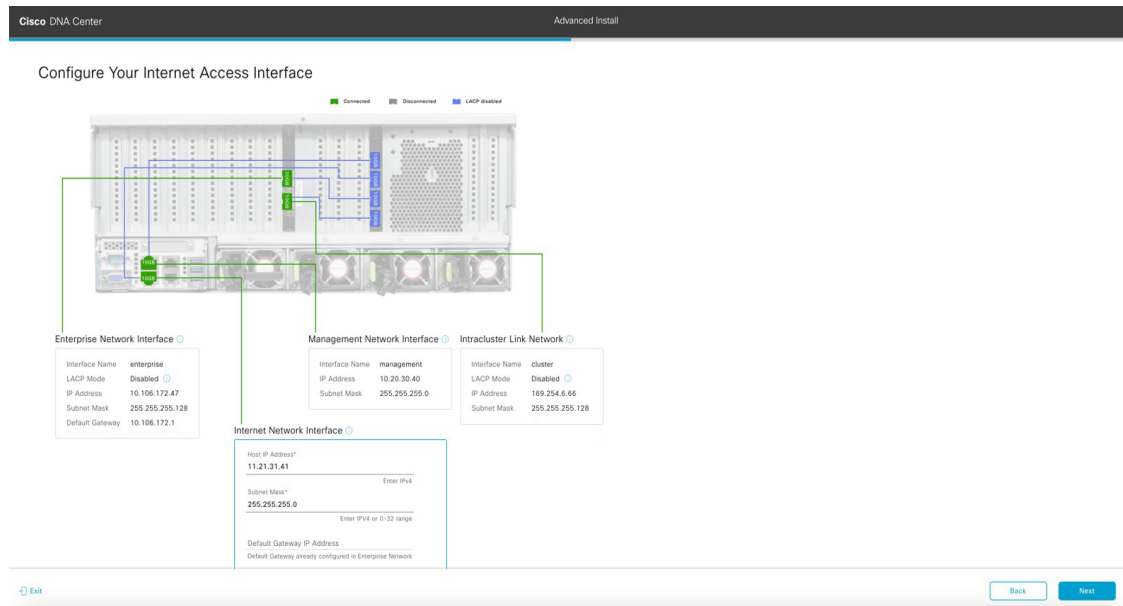
As explained in [Interface Cable Connections](#), this port is used to access the Cisco DNA Center GUI from your management network. If you chose to configure a dedicated Management interface, enter the information described in the following table. (See [Required IP Addresses and Subnets, on page 29](#) and [Required Configuration Information](#) for a more detailed description of the values you need to enter.)

**Note** If you opted to configure the Enterprise and Internet Access interfaces on the same port, complete this step and then skip ahead to Step 2h.

**Table 51: Primary Node Entries for the Management Port**

Host IP Address field	Enter the IP address for the Management port.
Subnet Mask field	Enter the netmask for the port's IP address.
Default Gateway IP Address field	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.

The wizard validates the information you have entered, confirms that the port is up, and notifies you of any settings that need to be changed before you can proceed with the wizard. If the settings you have entered are valid and the port is up, the wizard's **Configure Your Internet Access Interface** screen opens.



- g) (Optional) Enter configuration values for the Internet Access interface, then click **Next**.

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 Enterprise port. If you chose to configure a dedicated Internet Access interface, enter the information described in the following table. (See [Required IP Addresses and Subnets, on page 29](#) and [Required Configuration Information](#) for a more detailed description of the values you need to enter.)

Table 52: Primary Node Entries for the Internet Access Port

Host IP Address field	Enter the IP address for the Internet Access port.
Subnet Mask field	Enter the netmask for the port's IP address. This is required if you entered an IP address in the previous field.
Default Gateway IP Address field	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.

The wizard validates the information you have entered, confirms that the port is up, and notifies you of any settings that need to be changed before you can proceed with the wizard. If the settings you have entered are valid and the port is up, the wizard's **Interface to Port Configuration** screen opens.

- h) Review the settings that you have entered for the primary node's interfaces.  
If you need to make any changes, click the **Edit** link for the relevant interface.
- i) When you are happy with the interface settings, click **Configure**.
- j) After initial interface configuration has completed, click **Next** to proceed to the next wizard screen.  
The **DNS Configuration** screen opens.

Cisco DNA Center Advanced Install

### DNS Configuration

Enter the IP address of the preferred DNS server. To enter additional DNS servers, click the Add (+) icon. You can configure a maximum of three DNS servers. Problems can occur if you configure more than three DNS servers for an appliance.

DNS\*  +  
Enter an IPv4 address

Exit Review Back Next

- k) Enter the IP address of the preferred DNS server, then click **Next**. To enter additional DNS servers, click the **Add (+)** icon.

**Important**

- For each node in your cluster, configure a maximum of three DNS servers. Problems can occur if you configure more than three DNS servers for an appliance.
- For NTP, ensure port 123 (UDP) is open between Cisco DNA Center and your NTP server.

The **Configure Proxy Server Information** screen opens.

Cisco DNA Center Advanced Install

### Configure Proxy Server Information

Does your network use a proxy server to access the internet?

Yes  No

Proxy Server\*  
 E.g. http://example.com

Port\*  
  
Enter port number between 0 to 65535.

Username

Password

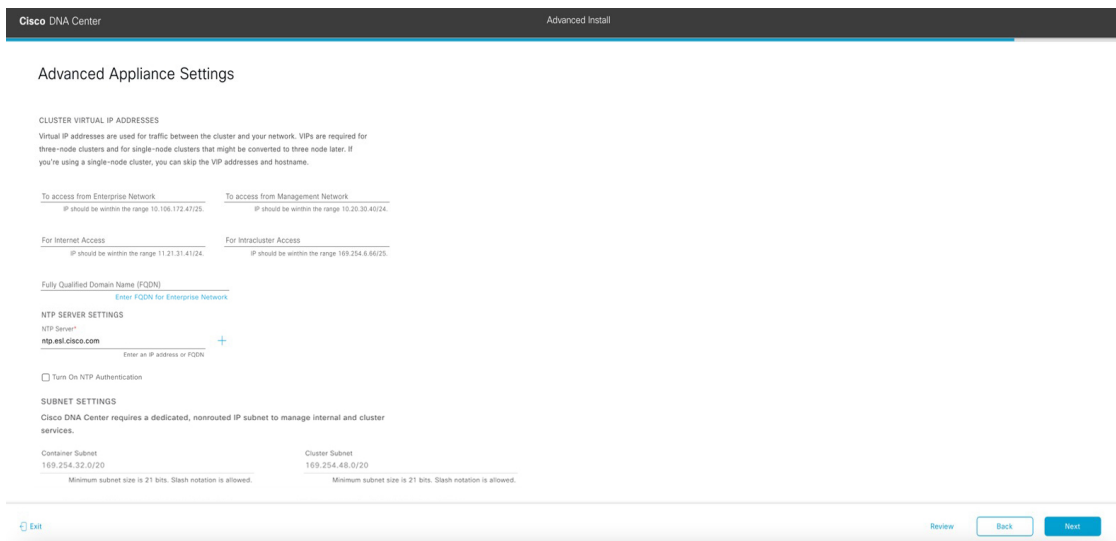
Exit Review Back Next

- l) Do one of the following and then click **Next**:
- If your network does *not* use a proxy server to access the internet, click the **No** radio button.
  - If your network does use a proxy server to access the internet, enter the values described in the following table:

**Table 53: Primary Node Entries for Proxy Server Settings**

Proxy Server field	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.
Port field	Enter the port your appliance used to access the network proxy.
Username field	Enter the user name used to access the network proxy. If no proxy login is required, leave this field blank.
Password field	Enter the password used to access the network proxy. If no proxy login is required, leave this field blank.

The wizard validates the information you have entered and notifies you of any settings that need to be changed before you can proceed with the wizard. If the settings you have entered are valid and the port is up, the wizard's **Advanced Appliance Settings** screen opens.



m) Enter configuration values for your cluster, then click **Next**.

**Table 54: Primary Node Entries for Advanced Appliance Settings**

<b>Cluster Virtual IP Addresses</b>
-------------------------------------

<p>To access from Enterprise Network, To access from Management Network, For Internet Access, and For Intracluster Access fields</p> <p><b>Note</b> If you configured the Management or Internet Access interface on the same port as the Enterprise interface, its corresponding field is not displayed in this section.</p>	<p>Enter the virtual IP address that will be used for traffic between the cluster and the interfaces that you have configured on your primary node. 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 don't plan to move to a three-node cluster setup, you can leave the fields in this section blank.</p> <p><b>Important</b> If you choose to configure a virtual IP address, you must enter one 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 <b>UP</b> state.</p>
<p>Fully Qualified Domain Name (FQDN) field</p>	<p>Enter the fully qualified domain name (FQDN) for your cluster. Cisco DNA Center does the following with this hostname:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• In the Subject Alternative Name (SAN) field of Cisco DNA Center certificates, it uses the FQDN to the define the Plug and Play server that should be used for device provisioning.</li> </ul>
<p><b>NTP Server Settings</b></p>	
<p>NTP Server field</p>	<p>Enter at least one NTP server address or hostname. To enter additional NTP server addresses or hostnames, click the <b>Add (+)</b> icon.</p> <p>For a production deployment, Cisco recommends that you configure a minimum of three NTP servers.</p>
<p>Turn On NTP Authentication check box</p>	<p>To enable the authentication of your NTP server before it's synchronized with Cisco DNA Center, check this check box and then enter the following information:</p> <ul style="list-style-type: none"> <li>• The NTP server's key ID. Valid values range between 1 and 4294967295 (2<sup>32</sup>-1). This value corresponds to the key ID that's defined in the NTP server's key file.</li> <li>• The SHA-1 key value associated with the NTP server's key ID. This 40-character hex string resides in the NTP server's key file.</li> </ul> <p><b>Note</b> Ensure that you enter a key ID and key value for each NTP server that you configured in the previous field.</p>
<p><b>Subnet Settings</b></p>	
<p>Container Subnet field</p>	<p>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.</p>

## Configure the Primary Node Using the Advanced Install Configuration Wizard

Cluster Subnet field

A dedicated, non-routed IP subnet that Cisco DNA Center uses to manage internal cluster services. By default, this is already set to **169.254.48.0/20**, and we recommend that you use this subnet.

The **Enter CLI Password** screen opens.

Cisco DNA Center Advanced Install

### Enter CLI Password

CLI Password: Identifies the password for the CLI username maglev. This password ensures secure access to each appliance using the CLI command line. If required, you can assign a different CLI password for each maglev CLI username on each appliance in a cluster

Username\*  
maglev

Password\*  
[masked] [SHOW](#)

[View Password Criteria](#)

Retype to Confirm\*  
[masked] [SHOW](#)

[Exit](#) [Review](#) [Back](#) [Next](#)

- n) Enter and confirm the password for the `maglev` user, then click **Next**.

The wizard validates the information you have entered and notifies you of any settings that need to be changed before you can proceed with the wizard. If the settings you have entered are valid, the wizard's **Summary** screen opens.

Cisco DNA Center Advanced Install

### Summary

Please review the settings that you have entered. If you need to make any changes, click the appropriate Edit link and make the necessary updates. You can download the generated configuration in JSON format from [here](#). When you are happy with your settings, click Start Configuration.

Ports Configuration Completed

Enterprise Network Interface

Interface Name	enterprise
LACP Mode	Disabled
IP Address	10.106.172.47
Subnet Mask	255.255.255.128
Default Gateway	10.106.172.1

Management Network Interface

Interface Name	management
IP Address	10.20.30.40
Subnet Mask	255.255.255.0

Intracluster Link Network

Interface Name	cluster
LACP Mode	Disabled
IP Address	169.254.6.66
Subnet Mask	255.255.255.128

Internet Network Interface

Interface Name	internet
IP Address	11.21.31.41
Subnet Mask	255.255.255.0

[Exit](#) [Start Configuration](#)

**Note** To download the appliance configuration as a JSON file, click the **here** link.

- o) Review all of the settings that you have entered while completing the wizard. If necessary, click the appropriate **Edit** link to open the wizard screen in which you want to make updates.
- p) To complete the configuration of your Cisco DNA Center appliance, click **Start Configuration**.

The wizard screen continuously updates during the process, indicating the tasks that are currently being completed and their progress, as well as any errors that have occurred. To save a local copy of this information as a text file, click the download icon.

The screenshot shows the 'Configuration' page of the Cisco DNA Center wizard. The main heading is 'Appliance Configuration In Progress'. Below this, there is a note: 'It should take about 90 minutes to complete the configuration of your appliance. As you wait, you can view a video that explains the next steps in the Cisco DNA Center setup process.' A progress bar indicates 'Initializing the cluster using kubeadm' at 30%. To the right, a terminal window shows the start time '04/09/2020 12:15:36' and a list of log entries for various components like 'credentialmanager.pem', 'kong.pem', 'kube-admin.pem', etc., with their respective timestamps.

### What to do next

When this task is complete:

- If you are deploying this appliance in standalone mode only, continue by performing 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 Using the Advanced Install Configuration Wizard, on page 209](#).

## Configure a Secondary Node Using the Advanced Install Configuration Wizard

Perform the following steps to configure the second and third appliances in the cluster using the Advanced Install configuration wizard.

**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.
- The following second generation Cisco DNA Center appliances support configuration using this wizard:
  - 112-core appliance: Cisco part number DN2-HW-APL-XL
  - 112-core promotional appliance: Cisco part number DN2-HW-APL-XL-U
- You can only use this wizard to complete the initial configuration of a new Cisco DNA Center appliance. To reimage an appliance that's been configured previously, you will need to use the Maglev Configuration wizard (see [Configure the Appliance Using the Maglev Wizard, on page 81](#)).
- 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.
- 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.

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:

- 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://172.29.131.224:443]
```

NAME	DISPLAY_NAME	DEPLOYED	AVAILABLE	STATUS	PROGRESS
access-control-application	Access Control Application	2.1.388.60364	-	DEPLOYED	
ai-network-analytics	AI Network Analytics	2.7.8.528	-	DEPLOYED	
app-hosting	Application Hosting	1.7.0.2108120753	-	DEPLOYED	
application-policy	Application Policy	2.1.388.170155	-	DEPLOYED	
application-registry	Application Registry	2.1.388.170155	-	DEPLOYED	
application-visibility-service	Application Visibility Service	2.1.388.170155	-	DEPLOYED	
assurance	Assurance - Base	2.2.3.337	-	DEPLOYED	
automation-core	NCP - Services	2.1.388.60364	-	DEPLOYED	
base-provision-core	Automation - Base	2.1.388.60364	-	DEPLOYED	
cloud-connectivity-contextual-content	Cloud Connectivity - Contextual Content	1.3.1.364	-	DEPLOYED	DEPLOYED
cloud-connectivity-data-hub	Cloud Connectivity - Data Hub	1.6.0.380	-	DEPLOYED	
cloud-connectivity-tethering	Cloud Connectivity - Tethering	2.1.1.43	-	DEPLOYED	
cloud-provision-core	Cloud Device Provisioning Application	2.1.388.60364	-	DEPLOYED	
command-runner	Command Runner	2.1.388.60364	-	DEPLOYED	
device-onboarding	Device Onboarding	2.1.388.60364	-	DEPLOYED	
disaster-recovery	Disaster Recovery	2.1.388.3600024	-	DEPLOYED	
dna-core-apps	Network Experience Platform - Core	2.1.388.60364	-	DEPLOYED	
dnac-platform	Cisco DNA Center Platform	1.6.1.126	-	DEPLOYED	
dnac-search	Cisco DNA Center Global Search	1.6.99.10	-	DEPLOYED	
endpoint-analytics	AI Endpoint Analytics	1.5.0.226	-	DEPLOYED	
group-based-policy-analytics	Group-Based Policy Analytics	2.2.3.55	-	DEPLOYED	
icap-automation	Automation - Intelligent Capture	2.1.388.60364	-	DEPLOYED	
image-management	Image Management	2.1.388.60364	-	DEPLOYED	
machine-reasoning	Machine Reasoning	2.1.388.210008	-	DEPLOYED	
ncp-system	NCP - Base	2.1.388.60364	-	DEPLOYED	
ndp-base-analytics	Network Data Platform - Base Analytics	1.6.1.686	-	DEPLOYED	
ndp-platform	Network Data Platform - Core	1.6.1.705	-	DEPLOYED	
ndp-ui	Network Data Platform - Manager	1.6.1.662	-	DEPLOYED	
network-visibility	Network Controller Platform	2.1.388.60364	-	DEPLOYED	
path-trace	Path Trace	2.1.388.60364	-	DEPLOYED	
platform-ui	Cisco DNA Center UI	1.6.3.155	-	DEPLOYED	
rbac-extensions	RBAC Extensions	2.1.388.190003	-	DEPLOYED	
rogue-management	Rogue and aWiPS	2.3.0.24	-	DEPLOYED	
sd-access	SD Access	2.1.388.60364	-	DEPLOYED	
sensor-assurance	Assurance - Sensor	2.2.3.317	-	DEPLOYED	
sensor-automation	Automation - Sensor	2.1.388.60364	-	DEPLOYED	
ssa	Stealthwatch Security Analytics	2.1.388.1090064	-	DEPLOYED	
system	System	1.6.551	-	DEPLOYED	
system-commons	System Commons	2.1.388.60364	-	DEPLOYED	
umbrella	Cisco Umbrella	2.1.388.590077	-	DEPLOYED	
wide-area-bonjour	Wide Area Bonjour	2.4.364.75035	-	DEPLOYED	

- 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, as doing so will result in unpredictable behavior.
- 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:

- Installed the Cisco DNA Center software image onto your appliance, as described in [Reimage the Appliance, on page 74](#).



#### Important

This is only applicable if you are going to configure a promotional appliance, because the Cisco DNA Center software image is not preinstalled on the 112-core promotional appliance (Cisco part number DN2-HW-APL-XL-U).

- Configured the first appliance in the cluster, following the steps in [Configure the Primary Node Using the Advanced Install Configuration Wizard, on page 192](#).
- Collected all of the information called for in [Required IP Addresses and Subnets, on page 29](#) 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 home page by clicking the **Help** icon (🔍) and choosing **About > Show 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 nodes as described in [Enable Browser Access to Cisco Integrated Management Controller](#).
  - Checked that both secondary nodes' ports and the switches they use are properly configured, as described in [Execute Preconfiguration Checks](#).
  - Are using a compatible browser. For a list of compatible browsers, see the [Release Notes](#) 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 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**

Start the Advanced Install configuration wizard:

- a) Point your browser to the Cisco IMC IP address you set during the Cisco IMC GUI configuration you performed, then 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 blue link menu at the upper right, as shown below.



- b) From the blue link menu, choose **Launch KVM** and then select either **Java based KVM** or **HTML based KVM**. If you select the 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 the HTML-based KVM, it will launch the KVM console in a separate browser 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 Maglev Configuration Wizard prompts.

- c) 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**. Then switch to the KVM console to continue.

- In the KVM console: Choose **Power > Power Cycle System (cold boot)**.

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

After displaying reboot messages, the KVM console displays the **Static IP Configuration** screen.

```

STEP #None
-----
Welcome to the Maglev Configuration Wizard!

Please Enter Static IP Information for Enterprise Interface Configuration,
Static IP is configured as an alternative to DHCP for web UI Configuration.
- Click Configure after entering Information for configuring IP which will
be configured on Enterprise Interface
- Click Skip to move to config wizard

NOTE: Default Configuration mode is IPv4,
Please select IPv6 mode for Ipv6 Configuration

-----
STATIC IP CONFIGURATION

IPv6 mode

IP Address:
Netmask:
Default Gateway Address:
Static Routes:

Web installation:
https://10.106.172.47:9004/

-----
< cancel >      skip >>      configure >>

```

Note the URL listed in the **Web Installation** field.

d) Do one of the following:

- If you want a DHCP server to assign an IP address, subnet mask, and default gateway to your appliance's Enterprise interface, click **Skip**.
- If you want to assign your own IP address, subnet mask, and default gateway to your appliance's Enterprise interface, enter the information described in the following table and then click **Configure**.

IPv6 Mode check box	If you want to configure an IPv6 address, check this check box.
IP Address field	Enter the static IP address you want to use.
Netmask field	Enter the netmask for the IP address you specified in the previous field: <ul style="list-style-type: none"> <li>• If you entered an IPv4 address, you can enter either a netmask or CIDR address.</li> <li>• If you entered an IPv6 address, you can only enter a CIDR address.</li> </ul>
Default Gateway Address field	Specify the default gateway that will be used to route traffic.

Static Routes field	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 Management port only.
---------------------	--

The KVM console displays the Maglev Configuration wizard welcome screen.

```

Welcome to the Maglev Configuration Wizard!

The wizard will walk you through the steps to configure this host. Select one of the options below to specify how you
would like to configure this host:

Start a Cisco DNA Center Cluster
Join a Cisco DNA Center Cluster

< exit >

```

- e) To bring up the **Appliance Configuration** screen, open the URL that was displayed in the **Static IP Configuration** screen.

Cisco DNA Center Appliance Configuration

Welcome to Cisco DNA Center


Are you starting a new Cisco DNA Center Cluster or joining an existing one?

Start A Cisco DNA Center Cluster

This appliance will be the primary node of a cluster.

Join A Cisco DNA Center Cluster

This appliance will be added as a node to the primary node of a cluster.



Next

- f) Click the **Join a Cisco DNA Center Cluster** radio button, then click **Next**.

Cisco DNA Center

Appliance Configuration

Welcome to Cisco DNA Center

Before you can use Cisco DNA Center, first complete the appropriate appliance configuration workflow.  
Which workflow matches your needs?

Advanced Install

Configure a standalone node or **any node in a cluster.**

Use this wizard to access all of the available appliance configuration options.



Back

Start

- g) Click the **Advanced Install** radio button, then click **Start**.

The **Advanced Install Overview** slider opens. Click > to view a summary of the tasks that the wizard will help you complete.

## Advanced Install Overview

Prepare your appliance for use with Cisco DNA Center by configuring its interfaces and entering cluster and other required information.



Start Workflow



- h) Click **Start Workflow** to start the wizard.

The **Appliance Interface Overview** screen opens, providing a description of the four appliance interfaces that you can configure.

Cisco DNA Center Advanced Install

---

### Appliance Interface Overview

In order for Cisco DNA Center to operate properly, you need to configure four interfaces on your appliance:

1. **Enterprise Network Interface:** Connects your appliance to the Enterprise network.
2. **Intracenter Link Interface:** Connects your appliance to your cluster.
3. **Management Network Interface:** (Optional) Accesses the Cisco DNA Center GUI from your Management network.
4. **Internet Access Interface:** (Optional) Accesses the Internet.

In this workflow, the Enterprise Network Interface and the Intracenter Link Interface will each have their own dedicated port. You can choose to have either Management Network Interface and/or Internet Access Interface be on the same port as the Enterprise Network Interface or assign them to a separate designated port.

---

[Exit](#) **Next**

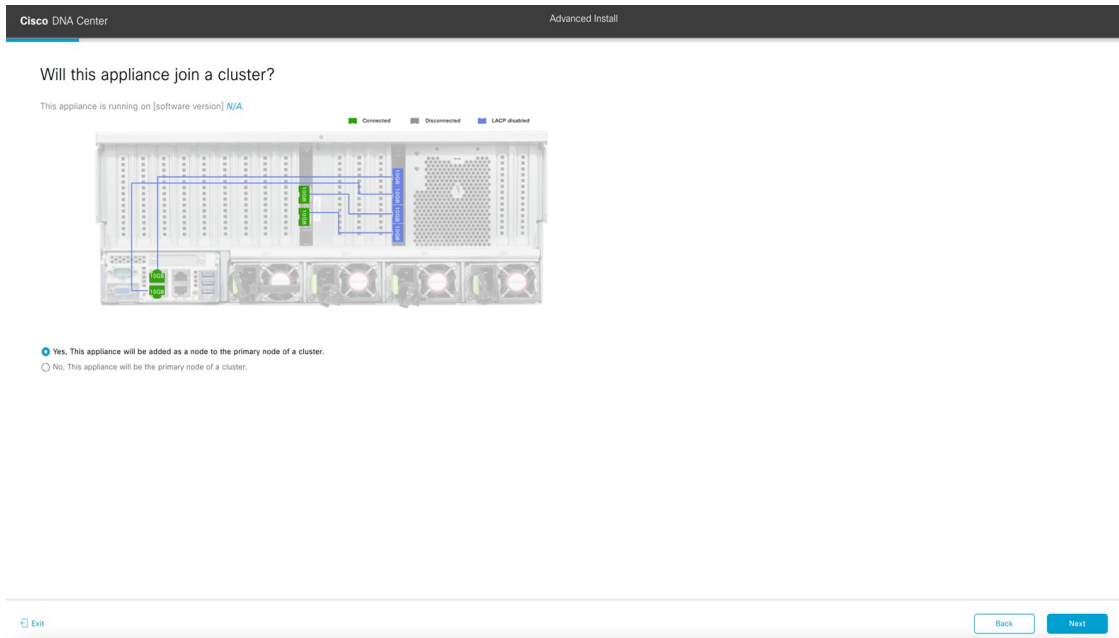
**Important** At a minimum, you must configure the interfaces on your appliance's Enterprise and Cluster ports, as they are required for Cisco DNA Center functionality. If the wizard fails to display either or both of these ports during the course of configuration, they may be non-functional or disabled. If you discover that they are non-functional, choose **Exit** to exit the wizard 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 2** Complete the Advanced Install configuration wizard:

a) Click **Next**.

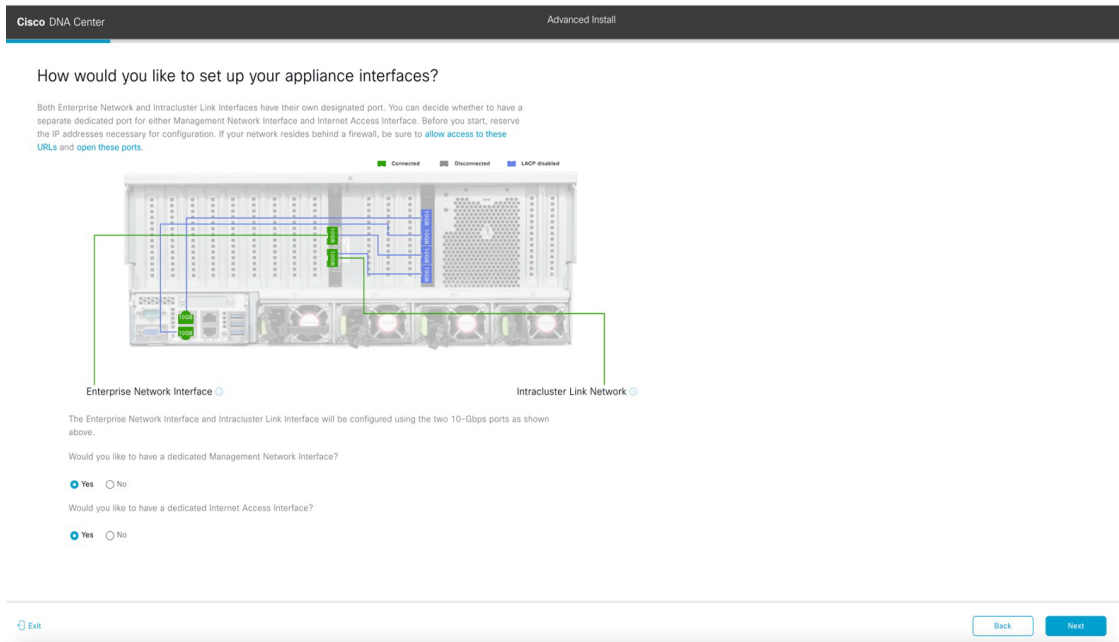
The **Will this appliance join a cluster?** screen opens.

## Configure a Secondary Node Using the Advanced Install Configuration Wizard



b) Click the **Yes** radio button, then click **Next**.

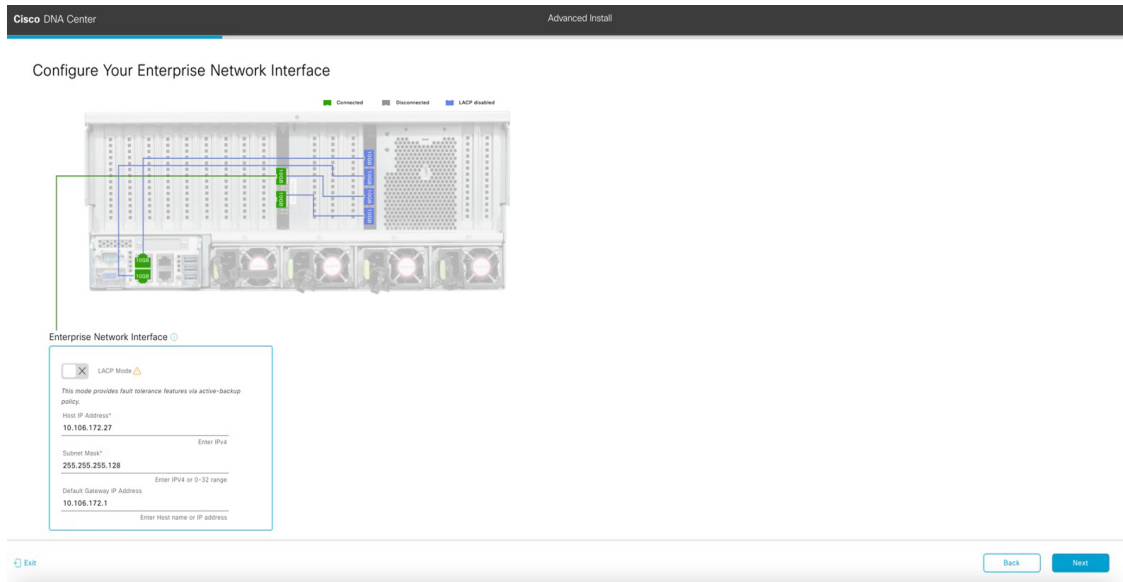
The **How would you like to set up your appliance interfaces?** screen opens.



c) Indicate whether you want to configure dedicated Management and Internet Access interfaces, then click **Next**.

The **Configure Your Enterprise Network Interface** screen opens.





d) Enter configuration values for the Enterprise interface, then click **Next**.

As explained in [Interface Cable Connections](#), this is a required interface used to link the appliance to the enterprise network. See [Required IP Addresses and Subnets, on page 29](#) and [Required Configuration Information](#) for a more detailed description of the values you need to enter.

**Table 55: Secondary Node Entries for the Enterprise Interface**

<p>LACP Mode slider</p>	<p>Choose one of the following network interface controller (NIC) bonding modes for the Enterprise interface:</p> <ul style="list-style-type: none"> <li>• <b>Active-Backup mode:</b> This mode provides fault tolerance by aggregating two Ethernet interfaces into a single logical channel. When the interface that's currently active goes down, the other interface takes its place and becomes active.</li> <li>• <b>LACP mode:</b> This mode aggregates two Ethernet interfaces that share the same speed and duplex settings into a single logical channel. This provides load balancing and higher bandwidth.</li> </ul> <p>For more information about Cisco DNA Center's implementation of NIC bonding, see <a href="#">NIC Bonding Overview, on page 67</a>.</p>
<p>Host IP Address field</p>	<p>Enter the IP address for the Enterprise port. This is required.</p>
<p>Subnet Mask field</p>	<p>Enter the netmask for the port's IP address. This is required.</p>

Default Gateway IP Address field	<p>Enter a default gateway IP address to use for the port.</p> <p><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.</p> <p><b>Note</b> You designated this interface to use the default gateway assigned to it by a DHCP server. Complete the following steps to specify a different gateway:</p> <ol style="list-style-type: none"> <li>1. Delete the IP address that is currently listed in this field and then click <b>Exit</b>. This will bring you back to the first wizard screen.</li> <li>2. Return to the Enterprise port's wizard screen and enter the gateway IP address you want to use.</li> </ol>
----------------------------------	---

The wizard validates the information you have entered, confirms that the port is up, and notifies you of any settings that need to be changed before you can proceed with the wizard. If the settings you have entered are valid and the port is up, the wizard's **Configure Your Intracluster Interface** screen opens.

- e) Enter configuration values for your Intracluster interface, then click **Next**.

As explained in [Interface Cable Connections](#), this required port is used to link the appliance to your cluster. See [Required IP Addresses and Subnets, on page 29](#) and [Required Configuration Information](#) for a more detailed description of the values you need to enter.

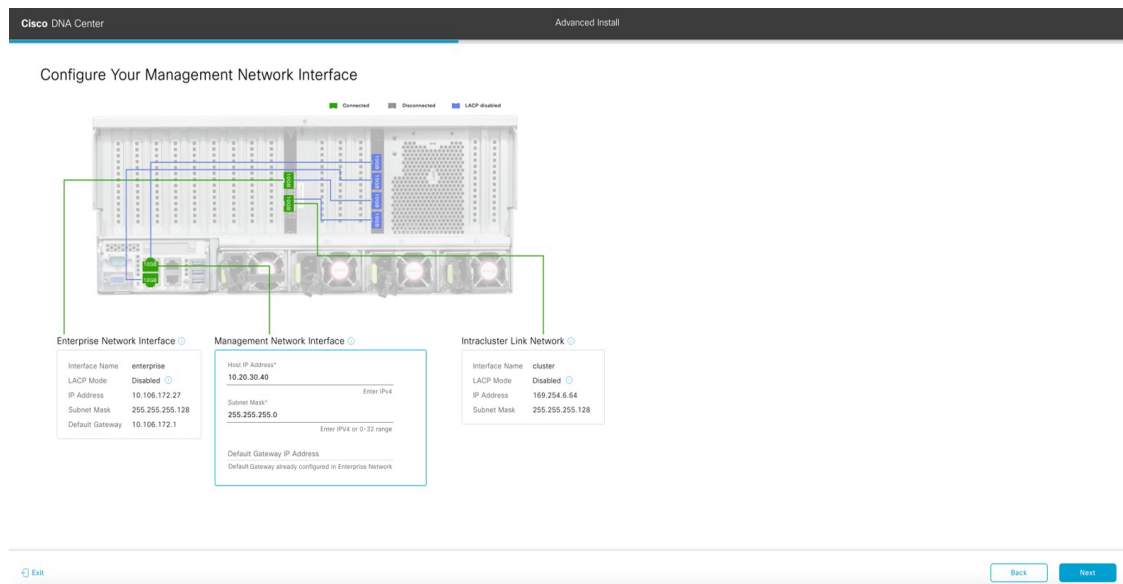
**Note**

- If you opted to configure the Enterprise and Internet Access interfaces on the same port, complete this step and then proceed to Step 2f (which describes how to configure your Management interface).
- If you opted to configure the Enterprise and Management interfaces on the same port, complete this step and then skip ahead to Step 2g (which describes how to configure your Internet Access interface).
- If you opted to configure the Enterprise, Management, and Internet Access interfaces on the same port, complete this step and then skip ahead to Step 2h.

**Table 56: Secondary Node Entries for the Intracluster Interface**

<p>LACP Mode slider</p>	<p>Choose one of the following NIC bonding modes for the Intracluster interface:</p> <ul style="list-style-type: none"> <li>• <b>Active-Backup mode:</b> This mode provides fault tolerance by aggregating two Ethernet interfaces into a single logical channel. When the interface that's currently active goes down, the other interface takes its place and becomes active.</li> <li>• <b>LACP mode:</b> This mode aggregates two Ethernet interfaces that share the same speed and duplex settings into a single logical channel. This provides load balancing and higher bandwidth.</li> </ul> <p>For more information about Cisco DNA Center's implementation of NIC bonding, see <a href="#">NIC Bonding Overview, on page 67</a>.</p>
<p>Host IP Address field</p>	<p>Enter the IP address for the Cluster port. This is required. Note that you cannot change the address of the Cluster port later.</p>
<p>Subnet Mask field</p>	<p>Enter the netmask for the port's IP address. This is required.</p>

The wizard validates the information you have entered, confirms that the port is up, and notifies you of any settings that need to be changed before you can proceed with the wizard. If the settings you have entered are valid and the port is up, the wizard's **Configure Your Management Network Interface** screen opens.



## Configure a Secondary Node Using the Advanced Install Configuration Wizard

- f) (Optional) Enter configuration values for the Management port, then click **Next**.

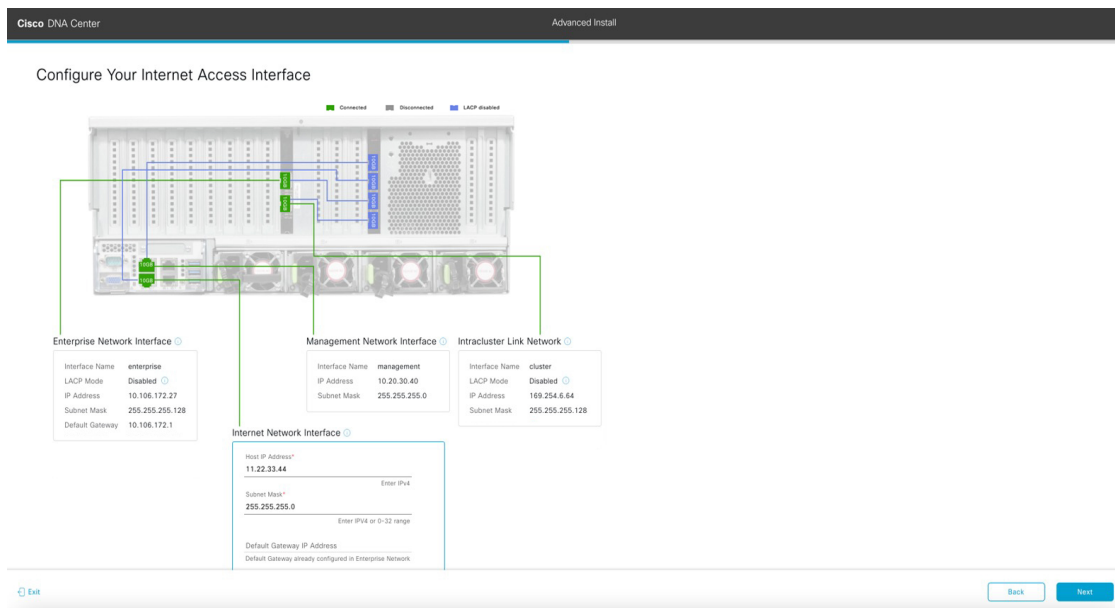
As explained in [Interface Cable Connections](#), this port is used to access the Cisco DNA Center GUI from your management network. If you chose to configure a dedicated Management interface, enter the information described in the following table. (See [Required IP Addresses and Subnets, on page 29](#) and [Required Configuration Information](#) for a more detailed description of the values you need to enter.)

**Note** If you opted to configure the Enterprise and Internet Access interfaces on the same port, complete this step and then skip ahead to Step 2h.

**Table 57: Secondary Node Entries for the Management Port**

Host IP Address field	Enter the IP address for the Management port.
Subnet Mask field	Enter the netmask for the port's IP address.
Default Gateway IP Address field	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.

The wizard validates the information you have entered, confirms that the port is up, and notifies you of any settings that need to be changed before you can proceed with the wizard. If the settings you have entered are valid and the port is up, the wizard's **Configure Your Internet Access Interface** screen opens.



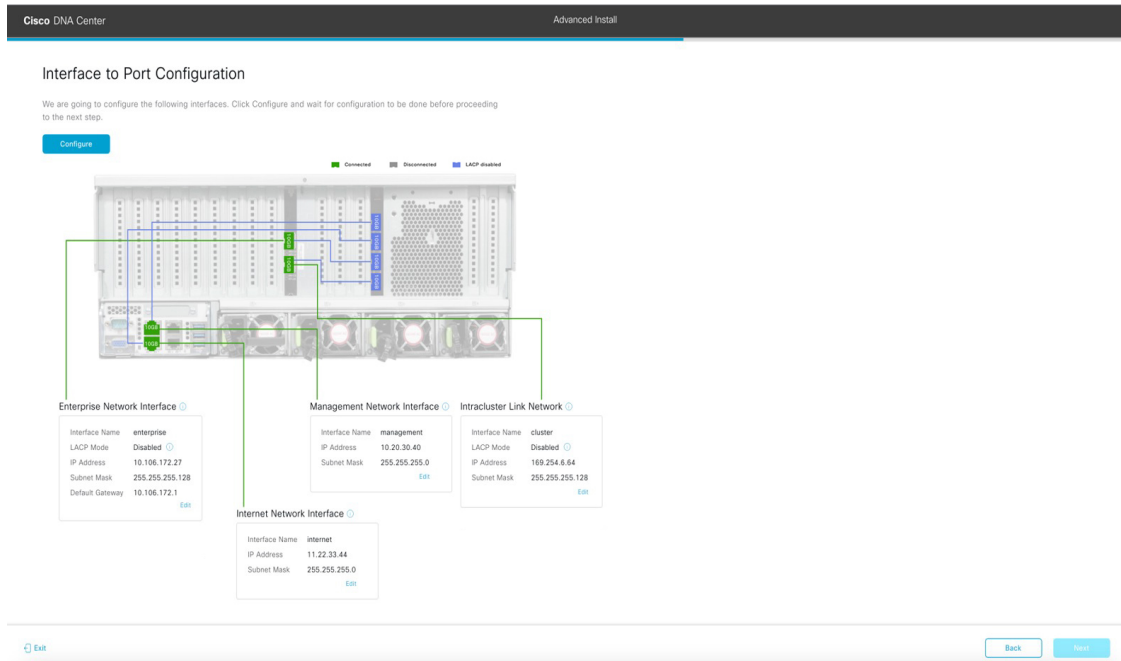
- g) (Optional) Enter configuration values for the Internet Access interface, then click **Next**.

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 Enterprise port. If you chose to configure a dedicated Internet Access interface, enter the information described in the following table. (See [Required IP Addresses and Subnets, on page 29](#) and [Required Configuration Information](#) for a more detailed description of the values you need to enter.)

**Table 58: Secondary Node Entries for the Internet Access Port**

Host IP Address field	Enter the IP address for the Internet Access port.
Subnet Mask field	Enter the netmask for the port's IP address. This is required if you entered an IP address in the previous field.
Default Gateway IP Address field	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.

The wizard validates the information you have entered, confirms that the port is up, and notifies you of any settings that need to be changed before you can proceed with the wizard. If the settings you have entered are valid and the port is up, the wizard's **Interface to Port Configuration** screen opens.



- h) Review the settings that you have entered for the secondary node's interfaces.

If you need to make any changes, click the **Edit** link for the relevant interface to return to its wizard screen.

- i) When you are happy with the interface settings, click **Configure**.  
j) After initial interface configuration has completed, click **Next** to proceed to the next wizard screen.

The **DNS Configuration** screen opens.

- k) Enter the IP address of the preferred DNS server, then click **Next**. To enter additional DNS servers, click the **Add (+)** icon.

**Important**

- For each node in your cluster, configure a maximum of three DNS servers. Problems can occur if you configure more than three DNS servers for an appliance.
- For NTP, ensure port 123 (UDP) is open between Cisco DNA Center and your NTP server.

The **Configure Proxy Server Information** screen opens.

- l) Do one of the following and then click **Next**:
- If your network does *not* use a proxy server to access the internet, click the **No** radio button.
  - If your network does use a proxy server to access the internet, enter the values described in the following table:

**Table 59: Secondary Node Entries for Proxy Server Settings**

Proxy Server field	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.
Port field	Enter the port your appliance used to access the network proxy.
Username field	Enter the user name used to access the network proxy. If no proxy login is required, leave this field blank.
Password field	Enter the password used to access the network proxy. If no proxy login is required, leave this field blank.

The wizard validates the information you have entered and notifies you of any settings that need to be changed before you can proceed with the wizard. If the settings you have entered are valid, the wizard's **Primary Node Details** screen opens.

Cisco DNA Center Advanced Install

### Primary Node Details

This appliance is getting added as a node for the multi-node setup with software version *N/A*. This information will be used when you need to log into the Maglev CLI.

Primary Node IP\*  
IP should be within Intra-Cluster's 169.254.5.66/25

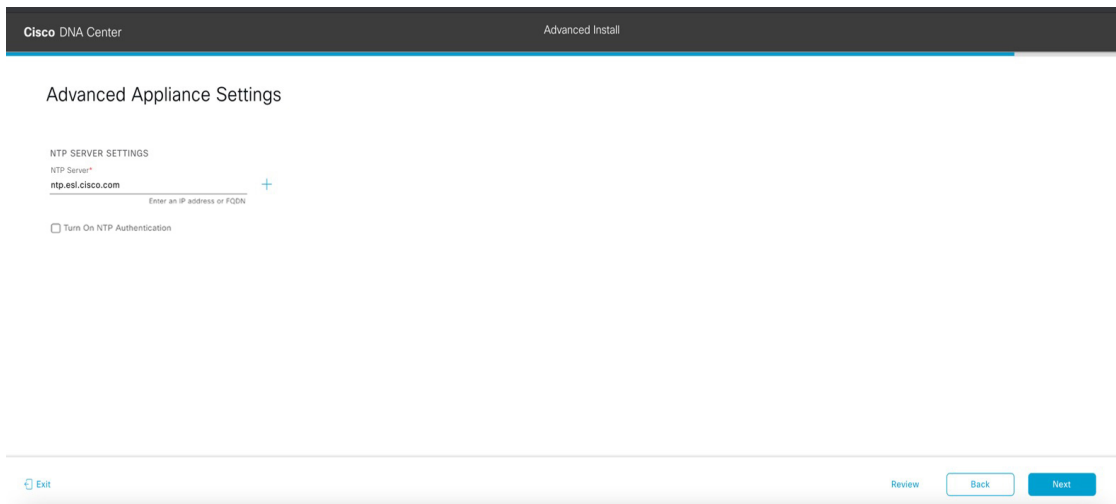
CLI Username  
 maglev

CLI Password\*  
 Enter CLI Password

Exit Review Back Next

- m) To establish a connection with your cluster's primary node, enter its IP address and password (by default, the username is already set to **maglev**) and then click **Next**.

The **Advanced Appliance Settings** screen opens.



n) Enter configuration values for your cluster, then click **Next**.

**Table 60: Secondary Node Entries for Advanced Appliance Settings**

NTP Server Settings	
NTP Server field	<p>Enter at least one NTP server address or hostname. To enter additional NTP server addresses or hostnames, click the <b>Add (+)</b> icon.</p> <p>For a production deployment, Cisco recommends that you configure a minimum of three NTP servers.</p>
Turn On NTP Authentication check box	<p>To enable the authentication of your NTP server before it's synchronized with Cisco DNA Center, check this check box and then enter the following information:</p> <ul style="list-style-type: none"> <li>• The NTP server's key ID. Valid values range between 1 and 4294967295 (2<sup>32</sup>-1). This value corresponds to the key ID that's defined in the NTP server's key file.</li> <li>• The SHA-1 key value associated with the NTP server's key ID. This 40-character hex string resides in the NTP server's key file.</li> </ul> <p><b>Note</b> Ensure that you enter a key ID and key value for each NTP server that you configured in the previous field.</p>

The **Enter CLI Password** screen opens.



Cisco DNA Center Advanced Install

### Enter CLI Password

CLI Password: Identifies the password for the CLI username maglev. This password ensures secure access to each appliance using the CLI command line. If required, you can assign a different CLI password for each maglev CLI username on each appliance in a cluster

Username\*  
maglev

Password\*  
..... [SHOW](#)

[View Password Criteria](#)

Retype to Confirm\*  
..... [SHOW](#)

[Review](#) [Back](#) [Next](#)

- o) Enter and confirm the password for the `maglev` user, then click **Next**.

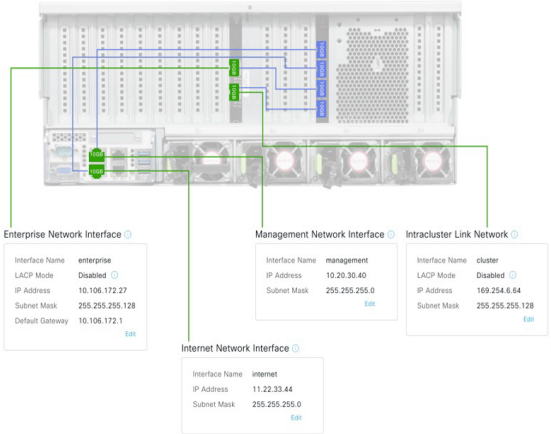
The wizard validates the information you have entered, confirms that the port is up, and notifies you of any settings that need to be changed before you can proceed with the wizard. If the settings you have entered are valid, the wizard's **Summary** screen opens.

Cisco DNA Center Advanced Install

### Summary

Please review the settings that you have entered. If you need to make any changes, click the appropriate **Edit** link and make the necessary updates. You can download the generated configuration in JSON format from [here](#). When you are happy with your settings, click **Start Configuration**.

Ports Configuration Completed



Interface Name	IP Address	Subnet Mask	LACP Mode
enterprise	10.106.172.27	255.255.255.128	Disabled
management	10.20.30.40	255.255.255.0	Disabled
cluster	169.254.6.64	255.255.255.128	Disabled
internet	11.22.33.44	255.255.255.0	Disabled

[Exit](#) [Start Configuration](#)

**Note** To download the appliance configuration as a JSON file, click the [here](#) link.

- p) Review all of the settings that you have entered while completing the wizard. If necessary, click the appropriate **Edit** link to open the wizard screen in which you want to make updates.
- q) To complete the configuration of your Cisco DNA Center appliance, click **Start Configuration**.

The configuration process takes roughly 90 minutes. The wizard screen continuously updates during the process, indicating the tasks that are currently being completed and their progress, as well as any errors that have occurred. To save a local copy of this information as a text file, click the download icon.

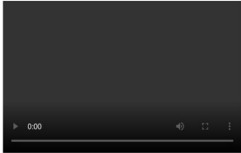
Cisco DNA Center
Configuration

### Appliance Configuration In Progress

It should take about 90 minutes to complete the configuration of your appliance. As you wait, you can view a video that explains the next steps in the Cisco DNA Center setup process.

Initializing the cluster using kubernetes 30%

ABOUT STARTING CISCO DNA CENTER



Started: 04/09/2020 12:15:36

-----

2021-05-05T16:56:59.32524 | -----

2021-05-05T16:56:59.32525 | credentialmanager.pem Apr 13 16:49:52 2020 GMT Apr 13 16:49:52 2021 GMT

2021-05-05T16:56:59.32526 | kong.pem Apr 13 16:49:51 2020 GMT Apr 13 16:49:51 2021 GMT

2021-05-05T16:56:59.32527 | kube-admin.pem Apr 13 16:49:50 2020 GMT Apr 13 16:49:50 2021 GMT

2021-05-05T16:56:59.32528 | kube-worker-1.pem Apr 13 16:49:52 2020 GMT Apr 13 16:49:52 2021 GMT

2021-05-05T16:56:59.32529 | maglev-registry.pem Apr 13 16:49:52 2020 GMT Apr 13 16:49:52 2021 GMT

2021-05-05T16:56:59.325210 | apiserver.crt Apr 13 12:12:14 2020 GMT Apr 13 17:40:20 2021 GMT

2021-05-05T16:56:59.325211 | apiserver-kubelet-client.crt Apr 13 12:12:14 2020 GMT Apr 13 17:40:20 2021 GMT

2021-05-05T16:56:59.325212 | front-proxy-ca.crt Apr 13 17:40:20 2020 GMT Apr 13 17:40:20 2020 GMT

2021-05-05T16:56:59.325213 | front-proxy-client.crt Apr 13 17:40:20 2020 GMT Apr 13 17:40:20 2021 GMT

2021-05-05T16:56:59.325214 | kubelet.conf Apr 13 12:12:14 2020 GMT Apr 13 17:40:21 2021 GMT

2021-05-05T16:56:59.325215 | admin.conf Apr 13 12:12:14 2020 GMT Apr 13 17:40:21 2021 GMT

2021-05-05T16:56:59.325216 | scheduler.conf Apr 13 12:12:14 2020 GMT Apr 13 17:40:22 2021 GMT

2021-05-05T16:56:59.325217 | controller-manager.conf Apr 13 12:12:14 2020 GMT Apr 13 17:40:22 2021 GMT

2021-05-05T16:56:59.325218 | -----

### What to do next

When this task is complete:

- If you have an additional appliance to deploy as the third and final node in the cluster, repeat this procedure.
- If you are finished adding nodes to the cluster, continue by performing 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 8

# Complete First-Time Setup

---

- [First-Time Setup Workflow](#), on page 229
- [Compatible Browsers](#), on page 229
- [Complete the Quick Start Workflow](#), on page 229
- [Integrate Cisco ISE with Cisco DNA Center](#), on page 235
- [Configure Authentication and Policy Servers](#), on page 241
- [Configure SNMP Properties](#), on page 244

## 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 253). 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 one of the following procedures:
  - [Configure the Primary Node Using the Maglev Wizard, on page 81](#)
  - [Configure the Primary Node Using the Advanced Install Configuration Wizard, on page 137](#) (44- or 56-core appliance)
  - [Configure the Primary Node Using the Advanced Install Configuration Wizard, on page 192](#) (112-core appliance)
- The information described in [Required First-Time Setup Information, on page 45](#).

---

**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** Do one of the following and then click **Log In**:

- If you completed the Maglev configuration wizard and chose the **Start using DNAC pre manufactured cluster** option, enter the admin's username (**admin**) and password (**maglev1@3**).
- If you completed the Maglev configuration wizard and chose the **Start configuration of DNAC in advanced mode** option, enter the admin's username (**admin**) and password that you set when you configured your Cisco DNA Center appliance.
- If you completed the Install configuration wizard, enter the admin's username (**admin**) and paste the password (**maglev1@3**) that you copied from the wizard's final screen.
- If you completed the Advanced Install configuration wizard, enter the admin's username (**admin**) and password that you set when you configured your Cisco DNA Center appliance.

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. The password you enter must be at least eight characters long.
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>	
<b>Note</b>	Cisco DNA Center does not support SNMPv2c credentials when FIPS mode is enabled. You'll need to enter SNMPv3 credentials instead. For more information regarding FIPS mode, see <a href="#">Configure the Primary Node Using the Maglev Wizard, on page 81</a> .
Name/Description	Name or description of the SNMPv2c read community string.
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	<p>Security level that SNMP messages require:</p> <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> <p><b>Note</b> When FIPS mode is enabled, Cisco DNA Center only supports <b>Authentication and Privacy</b> mode.</p>

Field	Description
Authentication Password	<p>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:</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>
Authentication Type	<p>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:</p> <ul style="list-style-type: none"> <li>• <b>SHA</b>: HMAC-SHA authentication.</li> <li>• <b>MD5</b>: HMAC-MD5 authentication.</li> </ul> <p><b>Note</b> Cisco DNA Center does not support this authentication type when FIPS mode is enabled.</p>
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>CISCOAES192</b>: 192-bit CBC mode AES for encryption.</li> <li>• <b>CISCOAES256</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>

Field	Description
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:

- Log in to the Cisco DNA Center GUI.
- Click the menu icon (☰) and choose **System > System 360**.
- In the Identity Services Engine (ISE) pane, verify that the status of all listed ISE servers is displayed as **Available** or **Configured**.
- In the Identity Services Engine (ISE) pane, click the **Update** link.
- 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:

- Log in to the Cisco ISE nodes that are shown as pxGrid servers in the **Identity Services Engine (ISE)** pane.
- 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 a 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 235.



---

**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 TACAS 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 9

# Troubleshoot the Deployment

---

- [Troubleshooting Tasks](#), on page 245
- [Log Out](#), on page 245
- [Reconfigure the Appliance Using the Configuration Wizard](#), on page 246
- [Power Cycle the Appliance](#), on page 247

## 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 CIMC 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 247.

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 CIMC 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
- NIC bonding enablement

### Before you begin

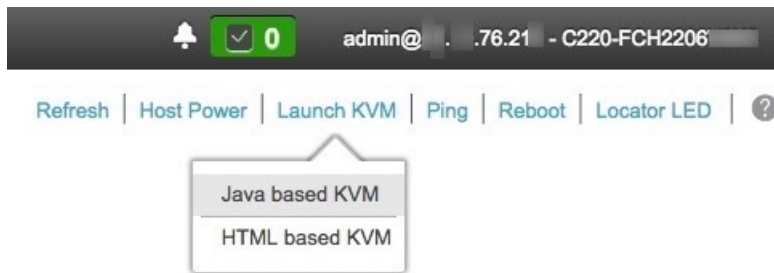
You will need the Linux user name (*maglev*) and password that are currently configured on the target appliance.

---

### 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 **HTML-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 Using the Maglev Wizard](#). 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.

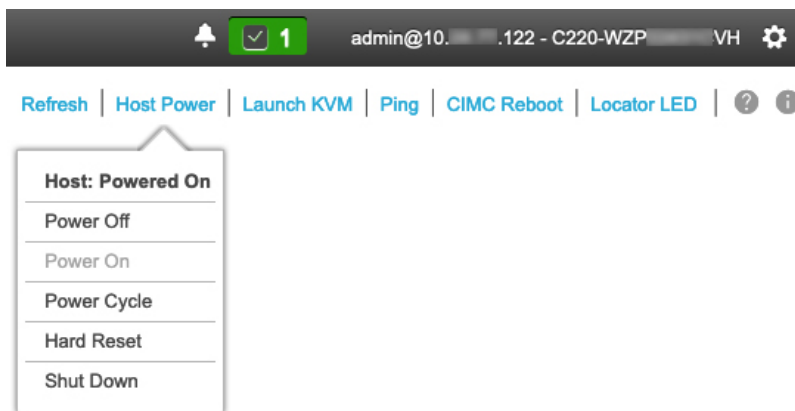


**Caution** Power cycling your appliance from the Cisco IMC GUI can result in the corruption or loss of data. Only do so if your appliance is completely unresponsive to SSH, the Cisco IMC console, or the physical console.

### 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 58](#)).

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 figures in [Front and Rear Panels, on page 5](#).

- 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 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 251](#)
  - [Existing HA Deployment of the Primary Node with Standard Interface Configurations, on page 252](#)
  - [Existing HA Deployment of Primary Node with Nonstandard Interface Configurations, on page 253](#)
  - [Activate HA, on page 253](#)
  - [Additional HA Deployment Considerations, on page 254](#)

## 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:

- If you are configuring an appliance using the Maglev Configuration wizard, see [Configure the Primary Node Using the Maglev Wizard, on page 81](#).
- If you are configuring an appliance using the browser-based configuration wizard, see the "Configure the Primary Node Using the Advanced Install Configuration Wizard" topic specific to your appliance:
  - [Configure the Primary Node Using the Advanced Install Configuration Wizard](#)

- [Configure the Primary Node Using the Advanced Install Configuration Wizard](#)

**Step 2** Configure the second and third appliances in the cluster:

- If you are configuring an appliance using the Maglev Configuration wizard, see [Configure a Secondary Node Using the Maglev Wizard, on page 103](#).
- If you are configuring an appliance using the browser-based configuration wizard, see the "Configure a Secondary Node Using the Advanced Install Configuration Wizard" topic specific to your appliance:
  - [Configure a Secondary Node Using the Advanced Install Configuration Wizard](#)
  - [Configure a Secondary Node Using the Advanced Install Configuration Wizard](#)

---

## 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 Cisco DNA Center 2.3.4.

For information about upgrading your current release of Cisco DNA Center, see [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:

- If you are configuring appliances using the Maglev Configuration wizard, see [Configure a Secondary Node Using the Maglev Wizard, on page 103](#).
- If you are configuring appliances using the browser-based configuration wizard, see the "Configure a Secondary Appliance Using the Advanced Install Configuration Wizard" topic specific to your appliance:
  - [Configure a Secondary Node Using the Advanced Install Configuration Wizard](#)
  - [Configure a Secondary Node Using the Advanced Install Configuration Wizard](#)

**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 Primary Node with Nonstandard Interface Configurations](#).

---

## Existing HA Deployment of 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 Cisco DNA Center 2.3.4.  
For information about upgrading your current release of Cisco DNA Center, see [Cisco DNA Center Upgrade Guide](#).
- Step 2** Create a backup of the remote repository.  
See the "Backup and Restore" chapter in the [Cisco Digital Network Architecture 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.
- If you are configuring appliances using the Maglev Configuration wizard, see [Configure a Secondary Node Using the Maglev Wizard, on page 103](#).
  - If you are configuring appliances using the browser-based configuration wizard, see the "Configure a Secondary Appliance Using the Advanced Install Configuration Wizard" topic specific to your appliance:
    - [Configure a Secondary Node Using the Advanced Install Configuration Wizard](#)
    - [Configure a Secondary Node Using the Advanced Install Configuration Wizard](#)
- 

## 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:
- From the Cisco DNA Center home page, choose **Network Telemetry** from the **Tools** area.  
The **Network Telemetry** window appears.
  - Click the **Site View** tab.
  - 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.