Cisco Catalyst Center Fourth-Generation Appliance Installation Guide, Release 3.3.x

Cisco Catalyst Center
Updated October 26, 2026

Abbreviated Cisco Trademarks

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)

Topics included

1 Review the Catalyst Center Appliance Features.....7
Appliance hardware specifications.....8
Medium Catalyst Center appliance.....8
Large Catalyst Center appliance.....10
Extra large Catalyst Center appliance.....12
Third and fourth-generation appliances differences.....14
Front and rear panels.....14
Physical specifications.....23
Environmental specifications.....23
Power supply specifications.....25

2 Plan the Deployment.....27
Planning workflow.....28
Catalyst Center and Cisco Software-Defined Access.....28
Interface cable connections.....28
Required IP addresses and subnets.....31
Required internet URLs and fully qualified domain names.....34
Provide secure access to the internet.....38
Communication ports.....38
HTTP port 80 exception list.....43
Disaster recovery ports.....44
Required ports and protocols for Cisco Software-Defined Access.....46
Required configuration information.....53
Required first-time setup information.....53
Password policy.....55
Password requirements.....56

3 Install the Appliance.....57
Appliance installation workflow.....58
Unpack and inspect the appliance.....58
Review the installation warnings and guidelines.....58
Statement 1071—Warning Definition.....60
Statement 1005—Circuit Breaker.....60
Statement 1074—Comply with Local and National Electrical Codes.....60
Statement 1017—Restricted Area.....61
Review the rack requirements.....61
Connect and power on the appliance.....62
Check the LEDs.....62

4 Prepare the Appliance for Configuration....65
Preparation for appliance configuration overview....66
Enable browser access to the Cisco Integrated Management Controller....66
Execute preconfiguration tasks....71
NIC bonding overview....74
Appliance support....76
Reimage the appliance....76
Verify the Catalyst Center image....77
Create a bootable USB flash drive....78
Delete and recreate the virtual drives on a Catalyst Center appliance....81
Install the Catalyst Center ISO image....82
Catalyst Center appliance configuration....83

5 Configure the Appliance Using the Maglev Wizard....85
Appliance configuration overview....86
IPv4 and IPv6 considerations....86
Password considerations....86
VLAN mode considerations....86
Configure the primary node using the Maglev wizard....87
FIPS mode support....109
Configure a secondary node using the Maglev wizard....110
Upgrade to the latest Catalyst Center release....128

6 Configure the Appliance Using the Browser-Based Wizard....129
Appliance configuration overview....130
Browser-based configuration wizards....130
Password considerations....131
VLAN mode considerations....131
Configure an appliance using the Install Configuration wizard....131
Configure the primary node using the Advanced Install configuration wizard....142
Configure a secondary node using the Advanced Install configuration wizard....158
Upgrade to the latest Catalyst Center release....175

7 Complete First-Time Setup....177
First-time setup workflow....178
Compatible browsers....178
Log in to Catalyst Center for the first time....178
Complete the Quick Start workflow....181
Device credential information....182
Catalyst Center setup methods....186
Complete the express setup....186
Complete the standard setup....188

Complete the expert setup....191
Integrate Cisco ISE with Catalyst Center....192
Group-Based Access Control: policy data migration and synchronization....195
Configure authentication and policy servers....198
Configure SNMP properties....202

8 Troubleshoot the Deployment....205
Troubleshooting tasks....206
Log out....206
Reconfigure the appliance using the Configuration wizard....206
Power cycle the appliance....207
Using SSH....208
Using the Cisco IMC GUI....208

Appendix A: Review High Availability Cluster Deployment Scenarios....211
New HA deployment....212
Existing HA deployment of the primary node with standard interface configurations....212
Existing HA deployment of primary node with nonstandard interface configurations....213
Activate HA....213
Additional HA deployment considerations....214
Telemetry....214
Wireless controller....214

1 Review the Catalyst Center Appliance Features

Topics:

- Appliance hardware specifications
- Front and rear panels
- Physical specifications
- Environmental specifications
- Power supply specifications

Appliance hardware specifications

Cisco provides Catalyst Center as a rack-mountable physical appliance with these hardware specifications.

Catalyst Center supports various hardware appliance sizes.

Medium Catalyst Center appliance

Lists the hardware specifications for the fourth-generation medium Catalyst Center appliance.

This table provides the hardware specifications for the fourth-generation medium Catalyst Center appliance.

Table 1: Medium Catalyst Center appliance hardware specifications

Feature	Description
Cisco part number	Standard appliance: DN4-HW-APL
Chassis	One rack-unit (1RU) Cisco Unified Computing System (UCS) C225 M8 chassis
Number of cores	32
Processors	One AMD EPYC™ 9355P processor
Memory	256 GB total (eight 32 GB DDR5 DIMMs)
Storage/disk management (RAID)	Cisco Trimode M1 24G RAID Controller with 4GB FBWC: Standard appliance: • 2 x 960 GB SSD, RAID 1 (slots 1 and 2)–`BOOT` virtual drive: **960 GB** • 2 x 1.9 TB SSD, RAID 1 (slots 3 and 4)–`SHARED` virtual drive: **1.9 TB** • 6 x 1.9 TB SSD, RAID 10 (slots 5 through 10)–`ANALYTICS` virtual drive: **5.7 TB**

Feature	Description
Network and management I/O	Supported connectors: • Standard appliance: Two Ethernet ports (1/10/25-Gbps) on the Intel E810-XXVDA2 network adapter • Standard appliance: Four Ethernet ports (1/10/25-Gbps) on the Intel E810-XXVDA4L network adapter **Note** These ports are active only when NIC bonding is enabled on the appliance. For more information, refer to NIC bonding overview on page 74. • One 1-Gb Ethernet dedicated management port (RJ-45 connector) • Two 1-Gb/10-Gb BASE-T Ethernet LAN ports (RJ-45 connectors) The dual LAN ports support 10 Gbps, 1 Gbps, 100 Mbps, or 10 Mbps. They autonegotiate to the correct link speed based on the link partner capability. These connectors are available but not typically used in the day-to-day operation of Catalyst Center: • One RS-232 serial port (RJ-45 connector) • One VGA video connector port (DB-15 connector) • Two USB 3.0 ports • One front-panel keyboard/video/mouse (KVM) connector for use with the KVM breakout cable. The breakout cable provides two USB 2.0 connectors, one VGA DB15 video connector, and one serial port (RS232) RJ45 connector.
Power	Two 2300 W AC power supplies, for 1 + 1 redundancy
Cooling	Eight hot-swappable fan modules for front-to-rear cooling
Video	The Cisco Integrated Management Controller (Cisco IMC) provides video using the Matrox G200e video/graphics controller: • Integrated 2D graphics core with hardware acceleration • Embedded DDR memory interface supports up to 512 MB of addressable memory (8 MB is allocated by default to video memory) • Supports display resolutions up to 1920 x 1200 16bpp @ 60Hz • High-speed integrated 24-bit RAMDAC • Single lane PCI-Express host interface running at Gen 2 speed
ACPI	The advanced configuration and power interface (ACPI) 4.0 standard is supported.
Integrated management processor	Baseboard Management Controller (BMC) running Cisco IMC firmware. Depending on the Cisco IMC settings, you can access Cisco IMC through the 1-Gb dedicated management port or a Cisco virtual interface card (VIC).

Large Catalyst Center appliance

Lists the hardware specifications for the fourth-generation large Catalyst Center appliance.

This table summarizes the hardware specifications for the fourth-generation large Catalyst Center appliance.

Table 2: Large Catalyst Center appliance hardware specifications

Feature	Description
Cisco part number	Standard appliance: DN4-HW-APL-L
Chassis	1RU Cisco UCS C225 M8 chassis
Number of cores	48
Processors	One AMD EPYC™ 9455P processor
Memory	384 GB total (twelve 32 GB DDR5 DIMMs)
Storage/disk management (RAID)	Cisco Trimode M1 24G RAID Controller with 4GB FBWC: Standard appliance: • 2 x 960 GB SSD, RAID 1 (slots 1 and 2)–`BOOT` virtual drive: **960 GB** • 2 x 3.8 TB SSD, RAID 1 (slots 3 and 4)–`SHARED` virtual drive: **3.8 TB** • 6 x 3.8 TB SSD, RAID 10 (slots 5 through 10)–`ANALYTICS` VD: **11.4 TB**–`ANALYTICS` virtual drive: **11.4 TB**

Feature	Description
Network and management I/O	Supported connectors: • Standard appliance: Two Ethernet ports (1/10/25-Gbps) on the Intel E810-XXVDA2 network adapter • Standard appliance: Four Ethernet ports (1/10/25-Gbps) on the Intel E810-XXVDA4L network adapter **Note** These ports are active only when NIC bonding is enabled on the appliance. For more information, refer to NIC bonding overview on page 74. • One 1-Gb Ethernet dedicated management port (RJ-45 connector) • Two 1-Gb/10-Gb BASE-T Ethernet LAN ports (RJ-45 connectors) The dual LAN ports support 10 Gbps, 1 Gbps, 100 Mbps, or 10 Mbps. They autonegotiate to the correct link speed based on the link partner capability. These connectors are available but not typically used in the day-to-day operation of Catalyst Center: • One RS-232 serial port (RJ-45 connector) • One VGA video connector port (DB-15 connector) • Two USB 3.0 ports • One front-panel keyboard/video/mouse (KVM) connector for use with the KVM breakout cable. The breakout cable provides two USB 2.0 connectors, one VGA DB15 video connector, and one serial port (RS232) RJ45 connector.
Power	Two 2300 W AC power supplies, for 1 + 1 redundancy
Cooling	Eight hot-swappable fan modules for front-to-rear cooling
Video	The Cisco IMC provides video using the Matrox G200e video/graphics controller: • Integrated 2D graphics core with hardware acceleration • Embedded DDR memory interface supports up to 512 MB of addressable memory (8 MB is allocated by default to video memory) • Supports display resolutions up to 1920 x 1200 16bpp @ 60Hz • High-speed integrated 24-bit RAMDAC • Single lane PCI-Express host interface running at Gen 2 speed
ACPI	The ACPI 4.0 standard is supported.
Integrated management processor	BMC running Cisco IMC firmware. Depending on the Cisco IMC settings, you can access Cisco IMC through the 1-Gb dedicated management port or a Cisco VIC.

Extra large Catalyst Center appliance

Lists the hardware specifications for the fourth-generation extra large Catalyst Center appliance.

This table provides the hardware specifications for the fourth-generation extra large Catalyst Center appliance.

Table 3: Extra large Catalyst Center appliance hardware specifications

Feature	Description
Cisco part number	Standard appliance: DN4-HW-APL-XL
Chassis	1RU Cisco UCS C225 M8 chassis
Number of cores	72
Processors	One AMD EPYC™ 9565P processor
Memory	768 GB total (twelve 64 GB DDR5 DIMMs)
Storage/disk management (RAID)	Cisco Trimode M1 24G RAID Controller with 4GB FBWC: Standard appliance: • 2 x 960 GB SSD, RAID 1 (slots 1 and 2)–`BOOT` virtual drive: **960 GB** • 2 x 3.8 TB SSD, RAID 1 (slots 3 and 4)–`SHARED` virtual drive: **3.8 TB** • 6 x 7.6 TB SSD, RAID 10 (slots 5 through 10)–`ANALYTICS` virtual drive: **22.8 TB**

Feature	Description
Network and management I/O	Supported connectors: • Standard appliance: Two Ethernet ports (1/10/25-Gbps) on the Intel E810-XXVDA2 network adapter • Standard appliance: Four Ethernet ports (1/10/25-Gbps) on the Intel E810-XXVDA4L network adapter **Note** These ports are active only when NIC bonding is enabled on the appliance. For more information, refer to NIC bonding overview on page 74. • One Ethernet port (1-Gbps) dedicated management (RJ-45 connector) • Two Ethernet LAN ports (1-Gbps/10-Gbps BASE-T) (RJ-45 connectors) The dual LAN ports support 10 Gbps, 1 Gbps, 100 Mbps, or 10 Mbps. They autonegotiate to the correct link speed based on the link partner capability. These connectors are available but not typically used in the day-to-day operation of Catalyst Center: • One RS-232 serial port (RJ-45 connector) • One VGA video connector port (DB-15 connector) • Two USB 3.0 ports • One front-panel keyboard/video/mouse (KVM) connector for use with the KVM breakout cable. The breakout cable provides two USB 2.0 connectors, one VGA DB15 video connector, and one serial port (RS232) RJ45 connector.
Power	Two 2300 W AC power supplies, for 1 + 1 redundancy
Cooling	Eight hot-swappable fan modules for front-to-rear cooling
Video	The Cisco IMC provides video using the Matrox G200e video/graphics controller: • Integrated 2D graphics core with hardware acceleration • Embedded DDR memory interface supports up to 512 MB of addressable memory (8 MB is allocated by default to video memory) • Supports display resolutions up to 1920 x 1200 16bpp @ 60Hz • High-speed integrated 24-bit RAMDAC • Single lane PCI-Express host interface running at Gen 2 speed
ACPI	The ACPI 4.0 standard is supported.
Integrated management processor	BMC running Cisco IMC firmware. Depending on the Cisco IMC settings, you can access Cisco IMC through the 1-Gb dedicated management port or a Cisco VIC.

Third and fourth-generation appliances differences

Describes the key differences between third-generation and fourth-generation Cisco appliances.

A third and fourth-generation appliance is a Cisco hardware platform generation that

- introduces new processor architectures and memory technologies,
- standardizes the chassis design across models, and
- updates storage profiles, impacting deployment and feature support.

Key hardware and configuration differences by appliance generation

Use this information when planning a new installation or replacing an appliance in an existing deployment.

Fourth-generation appliances retain the medium, large, and extra-large deployment profiles used by third-generation appliances. Although some fourth-generation models have fewer physical processor cores, the corresponding deployment profile and supported scale remain the basis for selecting a replacement appliance.

The table provides the significant points of differences between third and fourth-generation appliances.

Table 4: Third and fourth-generation Cisco appliances comparison

Deployment profile	Third-generation appliance	Fourth-generation appliance	Important difference
Medium	**DN3-HW-APL**; 32 cores; 256 GB DDR4; 1 RU; 10 drives	**DN4-HW-APL**; 32 cores; 256 GB DDR5; 1 RU; 10 drives	New processor architecture, DDR5 memory, and storage controller.
Large	**DN3-HW-APL-L**; 56 cores; 384 GB DDR4; 1 RU; 10 drives	**DN4-HW-APL-L**; 48 cores; 384 GB DDR5; 1 RU; 10 drives	Reduced physical core count with the same large appliance profile and memory.
Extra-large	**DN3-HW-APL-XL**; 80 cores; 768 GB DDR4; 2 RU; 12 drives	**DN4-HW-APL-XL**; 72 cores; 768 GB DDR5; 1 RU; 10 drives	Reduced rack space and drive count, with higher-capacity analytics drives

Front and rear panels

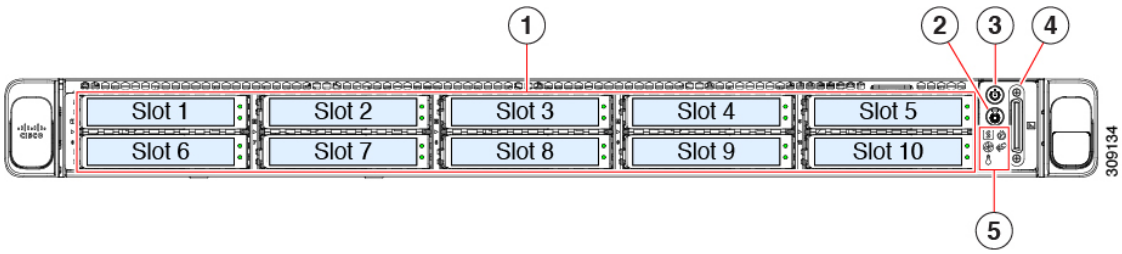
Information about the Catalyst Center appliance front and rear panels.

The following figures and tables describe the front and rear panels of the Catalyst 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: Catalyst Center appliance front panel



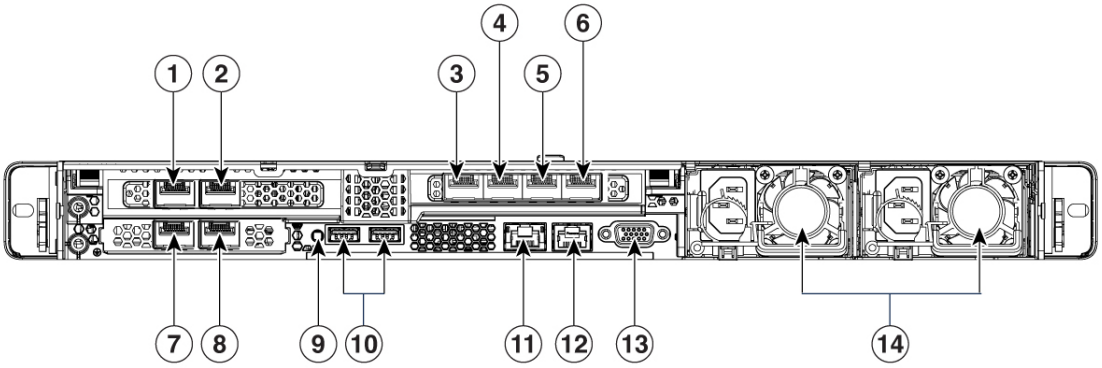
Callout number	Description
1	The appliance includes 10 drives. 32-core standard appliance: • 2 x 960 GB SSD, RAID 1 (slots 1 and 2) • 2 x 1.9 TB SAS, RAID 1 (slots 3 and 4) • 6 x 1.9 TB SSD, RAID 10 (slots 5 through 10) 32-core encrypted appliance: • 2 x 960 GB SED, RAID 1 (slots 1 and 2) • 2 x 3.8 TB SED, RAID 1 (slots 3 and 4) • 6 x 1.9 TB SED, RAID 10 (slots 5 through 10) 48-core standard appliance: • 2 x 960 GB SSD, RAID 1 (slots 1 and 2) • 2 x 3.8 TB SAS, RAID 1 (slots 3 and 4) • 6 x 3.8 TB SSD, RAID 10 (slots 5 through 10) 48-core encrypted appliance: • 2 x 960 GB SED, RAID 1 (slots 1 and 2) • 2 x 3.8 TB SED, RAID 1 (slots 3 and 4) • 6 x 3.8 TB SED, RAID 10 (slots 5 through 10) 72-core standard appliance: • 2 x 960 GB SSD, RAID 1 (slots 1 and 2) • 2 x 3.8 TB SAS, RAID 1 (slots 3 and 4) • 6 x 7.6 TB SSD, RAID 10 (slots 5 through 10) 72-core encrypted appliance: • 2 x 960 GB SED, RAID 1 (slots 1 and 2) • 2 x 3.8 TB SED, RAID 1 (slots 3 and 4) • 6 x 7.6 TB SED, RAID 10 (slots 5 through 10) Each installed drive includes two LEDs: a fault LED on the left and an activity LED on the right. When the drive fault LED indicates: • Off: The drive is operating properly. • Amber: The drive has failed. • Amber, blinking: The drive is rebuilding. When the drive activity LED indicates: • Off: There is no drive in the sled (no access, no fault). • Green: The drive is ready. • Green, blinking: The drive is reading or writing data.
2	Unit identification ( ): • Off: The unit identification function is not in use. • Blue, blinking: The unit identification function is activated.

Callout number	Description
3	Power button (): • Off: There is no AC power to the server. • Amber: The server is in standby power mode. Power is supplied only to the Cisco IMC and some motherboard functions. • Green: The server is in main power mode. Power is supplied to all server components.
4	KVM connector (used with KVM cable that provides one DB-15 VGA, one DB-9 serial, and two USB 2.0 connectors)

Callout number	Description

5	System LED cluster:
	• System health ( ):
	  • Green: The server is running in normal operating condition.
	  • Green, blinking: The server is performing system initialization and memory check.
	  • Amber, steady: The server is in a degraded operational state (minor fault).
	  • Amber, 2 blinks: There is a major fault with the system board.
	  • Amber, 3 blinks: There is a major fault with the memory DIMMs.
	  • Amber, 4 blinks: There is a major fault with the CPUs.
	• Power supply status ( ):
	  • Green: All power supplies are operating normally.
	  • Amber, steady: One or more power supplies are in a degraded operational state.
	  • Amber, blinking: One or more power supplies are in a critical fault state.
	• Fan status ( ):
	  • Green: All fan modules are operating properly.
	  • Amber, blinking: One or more fan modules breached the non-recoverable threshold.
	• Network link activity ( ):
	  • Off: The Ethernet LOM port link is idle.
	  • Green: One or more Ethernet LOM ports are link-active, but there is no activity.
	  • Green, blinking: One or more Ethernet LOM ports are link-active, with activity.
	• Temperature status ( ):
	  • Green: The server is operating at normal temperature.
	  • Amber, steady: One or more temperature sensors breached the critical threshold.
	  • Amber, blinking: One or more temperature sensors breached the non-recoverable threshold.

Figure 2: Catalyst Center appliance rear panel


1
2
3
4
5
6
7
8
9
10
11
12
13
14

Callout number	Description
1, 4	10-Gbps Enterprise Port (Network Adapter 1): In the Maglev Configuration wizard, this port appears as Network Adapter 1. Connect this port to a switch that provides access to your Enterprise network. • The primary instance (callout 1) is the left port on the Intel E810-XXVDA2 network adapter, in the appliance's PCIe riser 1. • The secondary instance (callout 4) is the second port on the Intel E810-XXVDA4 network adapter, in the appliance's PCIe riser 3. This port has a link status (ACT) LED and a link speed (LINK) LED. When the link status LED indicates: • Off: Link is active, but there is no traffic present. • Green, blinking: Traffic is present on the active link. When the speed LED indicates: • Off: No link is present. • Amber: Link speed is 10 Gbps or less. **Note** Although capable of operating at lower speeds, this port is intended to operate at 10 Gbps only.
2, 3	

Callout number	Description
5,8	10-Gbps Intracluster Port (Network Adapter 2): In the Maglev Configuration wizard, this port is called Network Adapter 2. Connect this port to a switch that provides access to the other nodes in the cluster. • The primary instance (callout 2) is the right port on the Intel E810-XXVDA2 network adapter, in the appliance's PCIe riser 1. • The secondary instance (callout 3) is the first port on the Intel E810-XXVDA4 network adapter, in the appliance's PCIe riser 3. This port has a link status (ACT) LED and a link speed (LINK) LED. When the link status LED indicates: • Off: Link is active, but there is no traffic present. • Green, blinking: Traffic is present on the active link. When the speed LED indicates: • Off: No link is present. • Amber: Link speed is 10 Gbps or less. **Note** Although capable of operating at lower speeds, this port is intended to operate at 10 Gbps only.

Callout number	Description

6,7	1-Gbps/10-Gbps Internet Port (Network Adapter 4): This Ethernet port can support 1 Gbps and 10 Gbps, depending on the link partner. It is identified as Network Adapter 4 in the Maglev Configuration wizard. This port is optional. Use it to connect to the internet if you cannot use the 10-Gbps enterprise port. Connect the port to the internet or to a proxy server that connects to the internet.
	• The primary instance (callout 8) is the right port on the Intel E810-XXVDA2 network adapter, in the appliance's Modular LAN-on-motherboard (mLOM) card bay.
	• The secondary instance (callout 5) is the third port on the Intel E810-XXVDA4 network adapter, located in the appliance's PCIe riser 3.
	This port has a link status (ACT) LED and a link speed (LINK) LED.
	• When the link status LED indicates:
	  • Off: Link is active, but there is no traffic present.
	  • Green, blinking: Traffic is present on the active link.
	• When the speed LED indicates:
	  • Off: No link is present.
	  • Amber: Link speed is 10 Gbps or less.
	Note
	Although capable of operating at lower speeds, this port is intended to operate at 10 Gbps only.

Callout number	Description
	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. • The primary instance (callout 7) is the left port on the Intel E810-XXVDA2 network adapter, in the appliance's mLOM card bay. • The secondary instance (callout 6) is the fourth port on the Intel E810-XXVDA4 network adapter, in the appliance's PCIe riser 3. This port has a link status (ACT) LED and a link speed (LINK) LED. When the link status LED indicates: • Off: Link is active, but there is no traffic present. • Green, blinking: Traffic is present on the active link. When the speed LED indicates: • Off: No link is present. • Amber: Link speed is 10 Gbps or less. **Note** Although capable of operating at lower speeds, this port is intended to operate at 10 Gbps only.
9	System identification button/LED
10	USB 3.0 ports (two)
11	1-Gbps Cisco IMC Port: This is the embedded port to the left of the COM port. The port receives an IP address when you enable browser access to the appliance's Cisco IMC GUI (see Enable browser access to the Cisco Integrated Management Controller on page 66). 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. This port has a link status LED and a link speed LED. When the link status LED indicates: • Off: No link is present. • Green, blinking: Traffic is present on the active link. • Green: Link is active, but there is no traffic present. When the speed LED indicates: • Off: Link speed is 10 Mbps or less. • Green: Link speed is 1 Gbps. • Amber: Link speed is 100 Mbps.
12	COM port (RJ-45 connector)

Callout number	Description
13	VGA video port (DB-15 connector)
14	Power supplies (two, providing 1+1 redundancy)

Note

If NIC bonding has been enabled on your Catalyst Center appliance, two instances of the Enterprise, Intracluster, Management, and Internet port are available to configure and use. Refer to NIC bonding overview on page 74.

Physical specifications

Lists the physical specifications for the fourth-generation Catalyst Center appliance.

This table lists the physical specifications for the fourth-generation Catalyst Center appliance.

Description	Specification
Height	1.7 in. (43.2 mm)
Width	16.9 in. (429.0 mm)
Depth (length)	Server only: 30 in. (762 mm) Server with slide rail: 31.5 in (800.1 mm)
Weight	• Maximum, fully configured with rail kit: 42.43 lb (19.30 kg) • Minimum with 1 HDD, 1 CPU, 1DIMM, and 1 1600 W PSU, no rail kit: 22.32 lb (10.13 kg)

Environmental specifications

Environmental specifications for fourth-generation Catalyst Center appliances.

Refer to this table for the environmental specifications for fourth-generation Catalyst Center appliances.

Table 5: Catalyst Center appliance environmental specifications

Description	Specification

Temperature, operating	• 10° C to 35° C (50° F to 95° F) with no direct sunlight • Derate the maximum temperature by 1° C per every 300 meters of altitude above sea level.
Temperature, non-operating (when the server is stored or transported)	• Below -40° C or above 65° C (below -40° F or above 149° F) • Maximum rate of change (operating and non-operating) 20° C/hr (36° F/hr)
Extended operating temperature	• 5° C to 40° C (41° F to 104° F) with no direct sunlight • Maximum allowable operating temperature derated: 1° C/125 m (1° F/228 ft) above 950 m (3117 ft) • System performance may be impacted when operating in the extended operating temperature range. • Operation above 40° C is limited to less than 1% of annual operating hours. • Hardware configuration limits apply to extended operating temperature range.
Humidity (RH), operating	8 to 90% and 24° C (75o F) maximum dew-point temperature, non-condensing environment
Humidity (RH), non-operating (when the server is stored or transported)	Below 5% or above 95% and 33o C (91o F) maximum dew-point temperature, non-condensing environment
Altitude, operating	0 to 10,000 feet
Altitude, non-operating (when the server is stored or transported)	0 to 40,000 feet
Sound power level: • Measure A-weighted per ISO7779 LwAd (Bels) • Operation at 73° F (23° C)	5.8

Note

Although the ASHRAE guidelines define multiple classes with different operating ranges, the *recommended* temperature and humidity operating range is the same for each class. The *recommended* temperature range is 64.4° F to 80.6° F (18° C to 27° C).

For general information, see the Cisco Unified Computing System Site Planning Guide: Data Center Power and Cooling.

Sound pressure level:	43

- Measure A-weighted per ISO7779 LpAm (dBA)
- Operation at 73° F (23° C)

Power supply specifications

Information about the power specifications for the appliance.

The specifications for the power supplies provided with the Catalyst Center appliance are listed in these topics. The fourth-generation appliance ships with two 2300 W power supplies (Cisco part number UCSC-PSU1-2300W).

Note

- For specific power information for the exact configuration of your appliance, use the Cisco UCS Power Calculator: http://ucspowercalc.cisco.com.
- For the 80PLUS platinum certification documented in these topics, you can find test results at https://www.clearesult.com/80plus/.

Table 6: AC power supply specifications

Description	Specification
AC Input Voltage	Nominal range: 100–230 VAC (Range: 90–264 VAC)
AC Input Frequency	Nominal range: 50 to 60Hz (Range: 47–63 Hz)
Maximum AC Input current	13 A at 100 VAC
Maximum input volt-amperes	2515 VA at 208 VAC
Maximum inrush current	30 A at 35° C
Maximum hold-up time	80 ms at 1600 W
Maximum output power per PSU	2300W at 220-240V input and limited to 1200W when operating at low-line input voltage, 110-127V
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 C20

2 Plan the Deployment

Topics:

- Planning workflow
- Catalyst Center and Cisco Software-Defined Access
- Interface cable connections
- Required IP addresses and subnets
- Required internet URLs and fully qualified domain names
- Provide secure access to the internet
- Communication ports
- HTTP port 80 exception list
- Disaster recovery ports
- Required ports and protocols for Cisco Software-Defined Access
- Required configuration information
- Required first-time setup information
- Password policy
- Password requirements

Planning workflow

Information about the planning and information gathering needed to conduct proper appliance installation and configuration.

Complete these planning and information-gathering tasks before installing, configuring, and setting up your Catalyst Center appliance. After you finish these tasks, install your appliance in the data center.

1. Review the recommended cabling and switching requirements for standalone and cluster installations. See Interface cable connections on page 28.
2. Gather IP addresses, subnets, and other IP traffic information to apply during appliance configuration. See Required IP addresses and subnets on page 31.
3. Prepare a solution that provides the required access to web-based resources. See Required internet URLs and fully qualified domain names on page 34 and Provide secure access to the internet on page 38.
4. Reconfigure the firewalls and security policies for Catalyst Center traffic. See Communication ports on page 38. If you are using Catalyst Center to manage a Cisco Software-Defined Access (SD-Access) network, see also Required ports and protocols for Cisco Software-Defined Access.
5. Gather the additional information that is used during appliance configuration and first-time setup. See Required configuration information on page 53 and Required first-time setup information on page 53.

Catalyst Center and Cisco Software-Defined Access

Briefly describes Cisco Software-Defined Access and Catalyst Center.

You can use Catalyst 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, so that you can automate tasks such as configuration, provisioning, and troubleshooting. The Cisco SD-Access solution accelerates network adaptation to business needs, improves issue resolution, and minimizes security-breach impacts.

This guide provides an overview of the Cisco SD-Access solution. If you plan to implement a Cisco SD-Access fabric with Catalyst Center, you can find more information and guidance in these resources

- For more information about how Catalyst Center leverages Cisco SD-Access to automate solutions that are not possible with typical networking approaches and techniques, see the *Cisco Software-Defined Access Solution Design Guide*.
- For guidance in using Cisco SD-Access access segmentation to enhance network security, see the *SD-Access Segmentation Design Guide*.
- For more information about Catalyst Center and the Cisco SD-Access solution working together with other Cisco and third-party products, see the Design Zone.

Interface cable connections

Explains the required and optional interface cable connections and provides cabling guidance.

Connect the ports on the appliance to a switch that provides these types of network access. You must configure the Enterprise port and Intracluster port interfaces at a minimum, because they are essential for Catalyst Center functionality.

When NIC bonding is enabled on a fourth-generation appliance, a secondary instance of the Enterprise port, Intracluster port, Management port, and Internet port resides on the Intel E810-XXVDA2 2X25/10 GBE SFP PCIE NIC. Connect these ports to a switch that's different from the one that you will connect to the primary instance of these ports (see NIC bonding overview on page 74).

Note

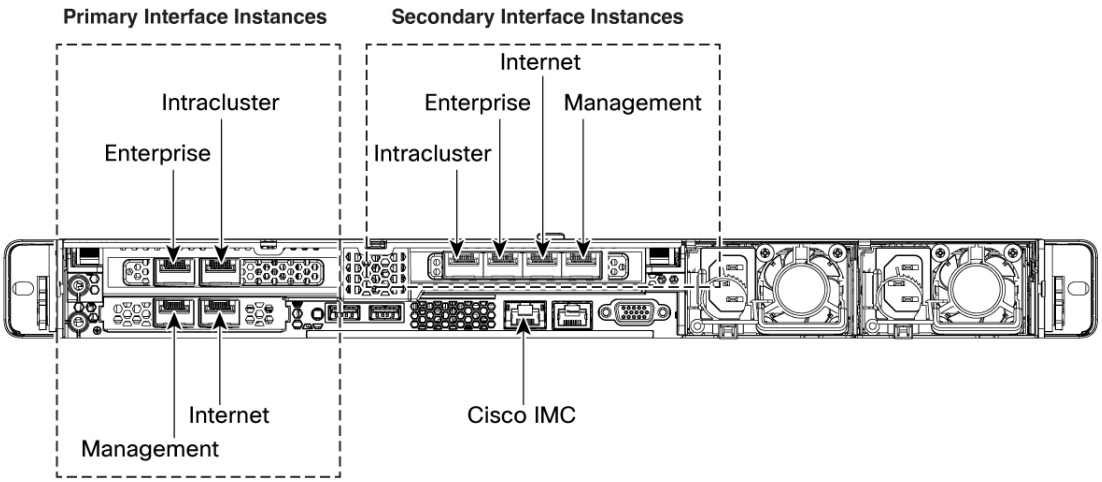
- During appliance configuration, the Maglev Configuration wizard prevents you from continuing until you assign the **Cluster Link** option to an interface. For both single-node and three-node deployments, assign the Intracluster port as the Cluster Link.
- You cannot change the interface marked as the Cluster Link after configuration completes. To change it, you must reimage the appliance. (For a description of the tasks you need to complete in order to reimage your Catalyst Center appliance, see Reimage the appliance on page 76.) Set up the Cluster Port with an IP address to support the expansion to a three-node cluster. Connect the cluster link interface to a switch port, and ensure it is in the UP state.
- To build multiple clusters, you must use a separate IP scheme for each cluster to prevent cross-cluster interaction and corruption.

- **(Required) 10-Gbps Enterprise port (network adapter 1)**: The purpose of this port is to enable Catalyst 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: This is the left port on the Intel E810-XXVDA2 network adapter, in the appliance's PCIe riser 1.
  - Secondary instance: This is the second port on the Intel E810-XXVDA4 network adapter, in the appliance's PCIe riser 3.
- **(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: This is the right port on the Intel E810-XXVDA2 network adapter, in the appliance's PCIe riser 1.
  - Secondary instance: This is the first port on the Intel E810-XXVDA4 network adapter, in the appliance's PCIe riser 3.
- **(Optional) 1-Gbps/10-Gbps Management port (network adapter 3)**: This port provides access to the Catalyst Center GUI so you can 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: This is the left port on the Intel E810-XXVDA2 network adapter, in the appliance's mLOM card bay.
  - Secondary instance: This is the fourth port on the Intel E810-XXVDA4 network adapter, in the appliance's PCIe riser 3.
- **(Optional) 1-Gbps/10-Gbps Internet port (network adapter 4)**: This port is optional. Use it only if you cannot connect the appliance to the Internet (including to your Internet proxy server) using the 10-Gbps Enterprise Port (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: This is the right port on the Intel E810-XXVDA2 network adapter, in the appliance's Modular LAN-on-motherboard (mLOM) card bay.
  - Secondary instance: This is the third port on the Intel E810-XXVDA4 network adapter, located in the appliance's PCIe riser 3.

- **(Optional, but strongly recommended) 1-Gbps Cisco IMC port**: This port, located to the left of the COM port on a fourth-generation Catalyst Center appliance, provides browser access to the 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.

This figure shows the recommended connections for a single-node Catalyst Center cluster, as well as the label that's assigned to each interface:

Figure 3: Recommended cabling for the Catalyst Center appliance



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 Catalyst Center cluster are the same as those for a single-node cluster and use the same ports. Do this when you cable a three-node cluster:

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

For more details on each of the ports, see the rear panel diagram and accompanying descriptions for your chassis in Front and rear panels on page 14.

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.

Supported media types for cabling the 10 Gbps enterprise and cluster ports include:

- SFP-10G-SR-S (Short range, MMF)

- SFP-10G-LR (Long range, SMF)
- SFP-H10GB-CU1M (Twinax cable, passive, 1 meter (3.28 feet))
- SFP-H10GB-CU3M (Twinax cable, passive, 3 meters (9.84 feet))
- SFP-H10GB-CU5M (Twinax cable, passive, 5 meters (16.4 feet))
- SFP-H10GB-ACU7M (Twinax cable, active, 7 meters (23 feet))

Required IP addresses and subnets

Explains the required appliance port (NIC) addresses, IP addresses, and subnets for a single-node or three-node cluster.

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 these 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 additional IP addresses and dedicated IP subnets, which are prompted for and applied during the configuration of the appliance, including:

- **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, because they are required for Catalyst 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

- 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 as if you were configuring for a three-node cluster.
- If the intracluster link for a single-node cluster fails, the VIP addresses associated with the Management and Enterprise interfaces also fail. When this happens:
  - Catalyst Center is unusable until the intracluster link is restored.
  - The Software Image Management [SWIM] and Cisco Identity Services Engine [ISE] integration becomes non-operational.
  - Cisco Catalyst Assurance data 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 Catalyst Center, see the *Cisco Catalyst Center Security Best Practices Guide*.
- **DNS server IP addresses**: The IP addresses for your network's preferred Domain Name System (DNS) servers. Specify up to three DNS server IP addresses as a space-separated list during configuration. Make sure the DNS servers have an entry for localhost that resolves to `127.0.0.1`; otherwise, network validation will fail.

Caution

Problems can occur if you specify more than three servers for an appliance.

- **(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* through which the traffic will be routed 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, like 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, Catalyst Center configures a link-local subnet (**169.254.32.0/20**) for this parameter. We recommend that you use this subnet. If you decide to enter another subnet, ensure that it does not conflict or overlap with any other subnet used by Catalyst 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 these 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 Catalyst Center appliance is completed, you *cannot* assign a different subnet without first reimaging the appliance (see Reimage the appliance on page 76).

- **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, Catalyst Center configures a link-local subnet (**169.254.48.0/20**) for this parameter, and we recommend that you use this subnet. If you decide to enter another subnet, ensure that it does not conflict with or overlap any other subnet used by Catalyst 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 these 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, 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 Catalyst Center appliance is completed, you *cannot* assign a different subnet without first reimaging the appliance (see Reimage the appliance on page 76).
- 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 Catalyst Center internal services require a dedicated set of IP addresses. This is a Catalyst Center microservice architecture requirement. To accommodate this requirement, you must allocate two dedicated subnets for each Catalyst Center system.

The appliance requires this amount of address space to maintain system performance. It uses internal routing and tunneling technologies for east-west (internode) communications. Using overlapping address spaces forces the appliance to run Virtual Routing and Forwarding (VRF) FIBs internally. This process creates multiple encapsulation and decapsulation steps for packets going between services. These steps cause high internal latency and result in cascading impacts at higher layers.

The Kubernetes-based service containerization architecture of Catalyst Center is another reason. Each appliance uses the IP addresses in this space for each Kubernetes K8 node. Multiple nodes can make up a single service. Currently, Catalyst 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 intentionally large to ensure that Cisco can add new services and features without running out of IP addresses. This also avoids requiring the reallocation of contiguous address spaces when upgrading 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 Catalyst 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

Lists the internet addresses Catalyst Center must be able to access.

You must provide secure access to the required URLs and Fully Qualified Domain Names (FQDNs) for the appliance to function.

This 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.

Caution

If you do not provide access to the listed URLs and FQDNs, the associated features will not work as intended.

Note

- The appliance interface configured to route internet-bound traffic serves as the source for all communications.
- Since the destination domain names may change without notice, it is recommended to specify them using wildcards.

For more information about internet proxy access requirements, refer to Provide secure access to the internet.

Table 7: Required URLs and FQDN access

In order to...	...Catalyst Center must access these URLs and FQDNs
Download updates for system software and application packages.	Recommended: https://*.ciscoconnectdna.com/* [1] To avoid wildcards, specify these URLs instead. • https://www.ciscoconnectdna.com • https://catalogsvc-cdn.ciscoconnectdna.com • https://catalogsvc-reg.ciscoconnectdna.com • https://catalogsvc-reg-cdn.ciscoconnectdna.com • https://catalogsvc-cm.ciscoconnectdna.com • https://app-cdn.ciscoconnectdna.com
Submit user feedback to the product team.	https://dnacenter.uservoice.com
Smart Account and SWIM software downloads.	• https://apx.cisco.com • https://cloudsso.cisco.com/as/token.oauth2 • https://*.cisco.com/* • https://download-ssc.cisco.com/
Authenticate with the cloud domain.	https://dnaservices.cisco.com

[1] Cisco owns and maintains ciscoconnectdna.com and its subdomains. The Cisco Connect DNA infrastructure meets Cisco Security and Trust guidelines. It is tested for security on a continuous basis. This infrastructure is robust, with built-in load balancing and automation capabilities. A cloud operations team monitors and maintains the infrastructure to ensure continuous availability.

In order to...	...Catalyst Center must access these URLs and FQDNs
Integrate with ThousandEyes.	• app.thousandeyes.com This URL uses AWS and might map to *.awsglobalaccelerator.com. Other services that might use AWS could also map to the AWS domain. • api.thousandeyes.com
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.	https://api-cx.cisco.com
Integrate with Webex.	• http://analytics.webexapis.com • https://webexapis.com
Connectivity with Cisco Catalyst Cloud and apps hosted there (e.g. AppX MS Teams Integration, Talos integration).	*.cisco.com:443 Otherwise, specific FQDNs are: • neoffers.cisco.com • neoffers-de.cisco.com • neoffers-sg.cisco.com • dnaservices.cisco.com
Integrate with Cisco Meraki.	Recommended: *.meraki.com:443 Customers who want to avoid wildcards can specify these URLs instead: • dashboard.meraki.com:443 • api.meraki.com:443
Check SSL/TLS certificate revocation status using OCSP/CRL.	• http://validation.identrust.com • http://commercial.ocsp.identrust.com **Note** These URLs must be reachable both directly and through the proxy server configured for Catalyst Center.
Allow Cisco authorized specialists to collect troubleshooting data when Catalyst Center Remote Support functionality is enabled.	wss://prod.radkit-cloud.cisco.com:443

In order to...	...Catalyst Center must access these URLs and FQDNs
Integrate with cisco.com and Cisco Smart Licensing.	*.cisco.com:443 To avoid wildcards, specify these URLs instead: • software.cisco.com • commerce.cisco.com • id.cisco.com • cloudsso.cisco.com • cloudsso1.cisco.com • cloudsso2.cisco.com • apiconsole.cisco.com • api.cisco.com • apx.cisco.com • smartreceiver.cisco.com • sso.cisco.com • apmx-prod1-vip.cisco.com • apmx-prod2-vip.cisco.com • tools.cisco.com • tools1.cisco.com • tools2.cisco.com
Connect to the Network-Based Application Recognition (NBAR) cloud.	prod.sdavc-cloud-api.com:443
Enable the Rogue Management application to detect rogue vendor names.	https://standards-oui.ieee.org/
Render accurate information in site and location maps.	• www.mapbox.com • *.tiles.mapbox.com/* :443. For a proxy, the destination is *.tiles.mapbox.com/* **Note** • These URLs are required by the browser to render maps. • Browsers must support WebGL (https://webglreport.com/?v=1).
For Cisco AI Network Analytics data collection, configure your network or HTTP proxy to allow outbound HTTPS (TCP 443) access to the cloud hosts.	• https://api.use1.prd.kairos.ciscolabs.com (US East Region) • https://api.euc1.prd.kairos.ciscolabs.com (EU Central Region)

In order to...	...Catalyst Center must access these URLs and FQDNs
Access a menu of interactive help flows that let you complete specific tasks from the GUI.	https://ec.walkme.com
Access the licensing service.	https://swapi.cisco.com
Integrate with Cisco Spaces.	• https://ciscospaces.io • https://ciscospaces.eu • https://ciscospaces.sg

Provide secure access to the internet

Recommends use of an HTTPS proxy server to access remote URLs securely.

By default, your appliance connects to the internet to download software updates, licenses, device software, map information, and user feedback. Maintain an internet connection for these configuration tasks.

Note

The appliance interface that's configured to route internet-bound traffic acts as the source for all communications.

Use an HTTPS proxy server to access remote URLs securely. Also use an HTTPS proxy server so your appliance can access the URLs in the Required internet URLs and fully qualified domain names list. During appliance installation, you are prompted to enter the proxy server's URL, port number, and login credentials if needed.

Your appliance currently supports communication with proxy servers over HTTP only. Place the HTTPS proxy server anywhere within your network. The proxy server communicates with the internet using HTTPS, while the appliance uses HTTP to communicate with the proxy. Specify the proxy's HTTP port when configuring the appliance.

To change the proxy setting after configuration, use the GUI.

Communication ports

Information about securing the Catalyst Center deployment by efficiently managing the ports.

Use the table to learn which ports Catalyst Center uses, which services communicate over them, and the reasons for their use. The Recommended Action column explains if you can restrict network traffic to known IP addresses or ranges, block connections without affecting Catalyst Center functionality, or if you must keep the port open.

Important

- Outbound communications from Catalyst Center use the routable interface IP address of the node hosting a service. For multinode clusters, include each node's interface IP and VIP address in the proxy and firewall rules.
- Security recommendations:
  - Deploy a firewall between Catalyst Center and the management or enterprise network to secure your Catalyst Center deployment using a layered approach.

- Open the ports to specific IP addresses or ranges.

Some destination ports in Catalyst Center are duplicated. Review the relevant section to learn how and why to use each network service. Limit source or destination IP addresses or ranges in the firewall rules. If a service is not used in your Catalyst Center deployment, keep the port closed.

Table 8: Communication ports used by Catalyst Center

Port	Service name	Purpose	Recommended action
Administering or configuring Catalyst Center			
TCP 443	UI, REST, HTTPS	GUI, REST, HTTPS management port.	Keep the port open.
TCP 2222	Catalyst Center shell	Connect to the Catalyst Center shell.	Keep the port open. Restrict the known IP address to be the source.
TCP 9004	Web UI installation	Serves the GUI-based installation page (required only if you decide to install Catalyst Center using the web-based option).	Keep the port open until you complete the node installation.
TCP 9005	Web UI installation API service	Serves the API for the web-based installation (connected by the browser client from port 9004; no external agent requires access).	Keep the port open until the cluster formation is complete.
Administering or configuring Cisco IMC			
TCP 22	Catalyst Center shell	Connects to the Catalyst Center shell.	Keep the port open. Configure the known IP address as the source.
UDP and TCP 53	DNS	Used to resolve a DNS name to an IP address.	Keep the port open if DNS names are used instead of IP addresses for other services, such as an NTP DNS name.
UDP and TCP 389	LDAP	Cisco IMC user management LDAP.	Optional if external user authentication via LDAP is needed.
TCP 443	UI, REST, HTTPS	Web UI, REST, HTTPS management port.	Keep the port open.
UDP and TCP 636	LDAPS	Cisco IMC user management via LDAP over SSL.	Optional if external user authentication via LDAPS is needed.
TCP 2068	HTTPS	Remote KVM console redirect port.	Keep the port open until you complete the node installation.
UDP 123	NTP	Synchronize the time with an NTP server.	Keep the port open.
UDP 161	SNMP polling/config	SNMP server polling and configurations.	Optional for SNMP server polling and configurations.

Port	Service name	Purpose	Recommended action
UDP 162	SNMP traps	Send SNMP traps to an external SNMP server.	Optional for a SNMP server collector.
UDP 514	Syslog	View faults and logs on an external server.	Optional for sending message logs to an external server.
Catalyst Center outbound to device and other systems			
–	ICMP	Catalyst Center uses ICMP messages to discover network devices and troubleshoot network connectivity issues.	Enable ICMP.
TCP 22	SSH	Catalyst Center uses SSH to connect to network devices so that it can: • read the device configuration for discovery and • make the configuration changes. Catalyst Center also uses SSH (port 22) for automation backup to the remote sync (rsync) storage server.	SSH must be open between Catalyst Center and the managed network.
TCP 23	Telnet	Avoid using Telnet. Use SSH for secure communication. **Note** Although Telnet is discouraged, Catalyst Center can use Telnet to connect to devices in order to read the device configuration for discovery, and make configuration changes.	If you must use Telnet for device management, understand that Telnet does not provide security mechanisms such as encryption. Use SSH for secure management.
TCP 49	TACACS+	Needed only if you are using external authentication such as Cisco ISE with a TACACS+ server.	Open the port only if you use external authentication with a TACACS+ server.
TCP 80	HTTP	Catalyst Center uses HTTP for trust pool updates.	To access Cisco-supported trust pools, configure your network to allow outgoing traffic from the appliance to this URL: http://www.cisco.com/security/pki/

Port	Service name	Purpose	Recommended action
TCP 80	OCSP/CRL	Catalyst Center verifies SSL/TLS certificate revocation status using OCSP/CRL.	Ensure these URLs are reachable directly and through the proxy server configured for Catalyst Center. If they are not reachable, Catalyst Center skips certificate revocation checks when connecting to cisco.com. http://validation.identrust.com http://commercial.ocsp.identrust.com
UDP 53	DNS	Catalyst Center uses DNS to resolve hostnames.	Keep the port open for DNS hostname resolution.
TCP and UDP 111, 20048, and 32767	NFS	Used for Assurance backups.	Keep the port open.
UDP 123	NTP	Catalyst Center uses NTP to synchronize the time from the source that you specify.	Keep the port open for time synchronization.
UDP 161	SNMP	Catalyst Center uses SNMP to discover network devices; to read device inventory details, including device type; and for telemetry data purposes, including CPU and RAM.	Keep the port open for network device management and discovery.
TCP 443	HTTPS	Catalyst Center uses HTTPS for cloud-tethered upgrades.	Keep the port open for cloud tethering, telemetry, and software upgrades. Keep the port open for Cisco ISE.
TCP 830	NETCONF	Catalyst Center uses NETCONF for device inventory, discovery, and configuration.	Keep the port open for network device management and discovery of devices that support NETCONF.
UDP 1645 or 1812	RADIUS	Needed only if you are using external authentication with a RADIUS server.	Keep the port open only if an external RADIUS server is used to authenticate user login to Catalyst Center.
TCP 5222, 8910	Cisco ISE	Catalyst Center uses Cisco ISE XMP for PxGrid.	Keep the port open for Cisco ISE.
TCP 9060	Cisco ISE	Catalyst Center uses Cisco ISE ERS API traffic.	Keep the port open for Cisco ISE.
Device to Catalyst Center			
–	ICMP	Devices use ICMP messages to communicate network connectivity issues.	Enable ICMP to allow device communication.

Port	Service name	Purpose	Recommended action
TCP 22, 80, 443	HTTPS, SFTP, HTTP	Software image download from Catalyst Center through HTTPS:443, SFTP:22, HTTP:80. Certificate download from Catalyst Center through HTTPS:443, HTTP:80 (Cisco 9800 Wireless Controller, PnP), Sensor/Telemetry. JWT (auth token) fetch from Catalyst Center through HTTPS:443 (any Access Point using the Cisco Catalyst Assurance Intelligent Capture feature). **Note** Block port 80 if you don't use Plug and Play (PnP), Software Image Management (SWIM), Embedded Event Management (EEM), device enrollment, or Cisco 9800 Wireless Controller.	Ensure that firewall rules limit the source IP address for hosts or network devices granted access on these ports. For more information on HTTP 80 usage, see the "HTTP Port 80 Exception List" topic in the *Cisco Catalyst Center Security Best Practices Guide*.
UDP 67	BOOTP	Used to initiate communication between a network device and Catalyst Center.	Keep the port open.
UDP 123	NTP	Devices use NTP for time synchronization.	Keep the port open to allow devices to synchronize the time.
UDP 162	SNMP	Catalyst Center receives SNMP network telemetry from devices.	Keep the port open for data analytics based on SNMP.
UDP 514	Syslog	Catalyst Center receives syslog messages from devices.	Keep the port open for data analytics based on syslog.
2049	NFS	Used for Assurance backups.	Keep the port open.
UDP 6007	NetFlow	Catalyst Center receives NetFlow network telemetry from devices.	Keep the port open for data analytics based on NetFlow.
TCP 9991	Wide Area Bonjour Service	Catalyst Center receives multicast Domain Name System (mDNS) traffic from the Service Discovery Gateway (SDG) agents using the Bonjour Control Protocol.	Keep the port open on Catalyst Center if the Bonjour application is installed.
UDP 21730	Application Visibility Service	Application Visibility Service CBAR device communication.	Keep the port open when CBAR is enabled on a network device.

Port	Service name	Purpose	Recommended action
TCP 25103	Cisco 9800 Wireless Controller and Cisco Catalyst 9000 switches with streaming telemetry enabled	Used for telemetry.	Keep the port open for telemetry connections between Catalyst Center and Catalyst 9000 devices.
TCP 32626	Intelligent Capture (gRPC) collector	Used to establish a gRPC channel for receiving AP/client statistics and packet capture data related to the Cisco Catalyst Assurance Intelligent Capture feature.	Keep the port open if you are using the Cisco Catalyst Assurance Intelligent Capture (gRPC) feature.

HTTP port 80 exception list

List of HTTP port 80 exceptions.

Table 9: List of HTTP port 80 exceptions

Area	Why HTTP port 80 is needed	Applicable Catalyst Center/device version	How security is accomplished despite the lack of E2E encryption
SCEP	RFC 8894 - Simple Certificate Enrollment Protocol	All Catalyst Center and device versions.	SCEP uses shared secret and PKCS12 encrypted CSR/certificate exchange.
Plug and Play	PnP Hello runs over HTTP but switches to HTTPS when the device downloads ios.p7b. The device establishes HTTPS with Catalyst Center by anchoring trust on the ios.7b trusted bundle.	All Catalyst Center and device versions.	Ios.p7b is protected with an encrypted hash signed by Cisco Manufacturing CA.
Telemetry Certificate Download	The certificate is downloaded using HTTP.	All Catalyst Center and device versions.	Certificates downloaded are encrypted in PKCS12.
SWIM	You can import images from the remote server (HTTP) to the Catalyst Center image repository.	All Catalyst Center versions.	Images imported through HTTP are verified for integrity by checking the hash of the file.

Disaster recovery ports

Information about securing the disaster recovery setup.

If you are using disaster recovery in your production environment, use the firewall and security policies that secure your disaster recovery setup. Open the ports given in the table to ensure that Catalyst Center has the access it requires to set up disaster recovery across your network's data centers.

> **Note**
>
> For three-node clusters, ensure that you allow the source Enterprise IP address of each node.

Table 10: Catalyst Center disaster recovery ports

Source port	Source	Destination port	Destination	Description
Any	Catalyst Center Enterprise IP/VIP	TCP 443	Catalyst Center Enterprise VIP	REST API Access
Any	Catalyst Center Enterprise IP/VIP	UDP 500	Catalyst Center Enterprise VIP	IPSec tunnel
Any	Catalyst Center Enterprise IP/VIP	TCP 873	Catalyst Center Enterprise VIP	Replication of GlusterFS data through rsync
Any	Catalyst Center Enterprise IP/VIP	UDP 4500	Catalyst Center Enterprise VIP	IPSec tunnel
Any	Catalyst Center Enterprise IP/VIP	TCP 8300	Catalyst Center Enterprise VIP	Consul RPC communication
Any	Catalyst Center Enterprise IP/VIP	TCP 8301	Catalyst Center Enterprise VIP	Consul SERF LAN port
Any	Catalyst Center Enterprise IP/VIP	UDP 8301	Catalyst Center Enterprise VIP	Consul SERF LAN port
Any	Catalyst Center Enterprise IP/VIP	TCP 8302	Catalyst Center Enterprise VIP	Consul SERF WAN port[2]
Any	Catalyst Center Enterprise IP/VIP	UDP 8302	Catalyst Center Enterprise VIP	Consul SERF WAN port[1]
Any	Catalyst Center Enterprise IP/VIP	TCP 8443	Catalyst Center Enterprise VIP	HA proxy API access [3]
Any	Catalyst Center Enterprise IP/VIP	UDP 500	Witness IP	IPSec tunnel

[2] This requirement will be removed in a future Catalyst Center release.
[3] This requirement will be added in a future Catalyst Center release.

Source port	Source	Destination port	Destination	Description
Any	Catalyst Center Enterprise IP/VIP	TCP 2222	Witness IP	TCP ping for witness reachability
Any	Catalyst Center Enterprise IP/VIP	UDP 4500	Witness IP	IPSec tunnel
Any	Catalyst Center Enterprise IP/VIP	TCP 8300	Witness IP	Consul RPC communication
Any	Catalyst Center Enterprise IP/VIP	TCP 8301	Witness IP	Consul SERF LAN port
Any	Catalyst Center Enterprise IP/VIP	UDP 8301	Witness IP	Consul SERF LAN port
Any	Catalyst Center Enterprise IP/VIP	TCP 8302	Witness IP	Consul SERF WAN port[1]
Any	Catalyst Center Enterprise IP/VIP	UDP 8302	Witness IP	Consul SERF WAN port[1]
Any	Catalyst Center Enterprise IP/VIP	TCP 8443	Witness IP	HA proxy API access [2]
Any	Catalyst Center Enterprise/ Management VIP	TCP 179	Neighbor router	BGP session with neighbor router **Note** Open this port if BGP is configured to advertise the disaster recovery VIP.
Any	Witness IP	UDP 53	DNS Server	From witness to DNS server
Any	Witness IP	UDP 123	NTP Server	From witness to NTP server
Any	Witness IP	TCP 443	Catalyst Center Enterprise VIP	Access APIs during disaster recovery registration
Any	Witness IP	UDP 500	Catalyst Center Enterprise VIP	IPSec tunnel
Any	Witness IP	UDP 4500	Catalyst Center Enterprise VIP	IPSec tunnel
Any	Witness IP	TCP 8300	Catalyst Center Enterprise VIP	Consul RPC communication
Any	Witness IP	TCP 8301	Catalyst Center Enterprise VIP	Consul SERF LAN port
Any	Witness IP	UDP 8301	Catalyst Center Enterprise VIP	Consul SERF LAN port

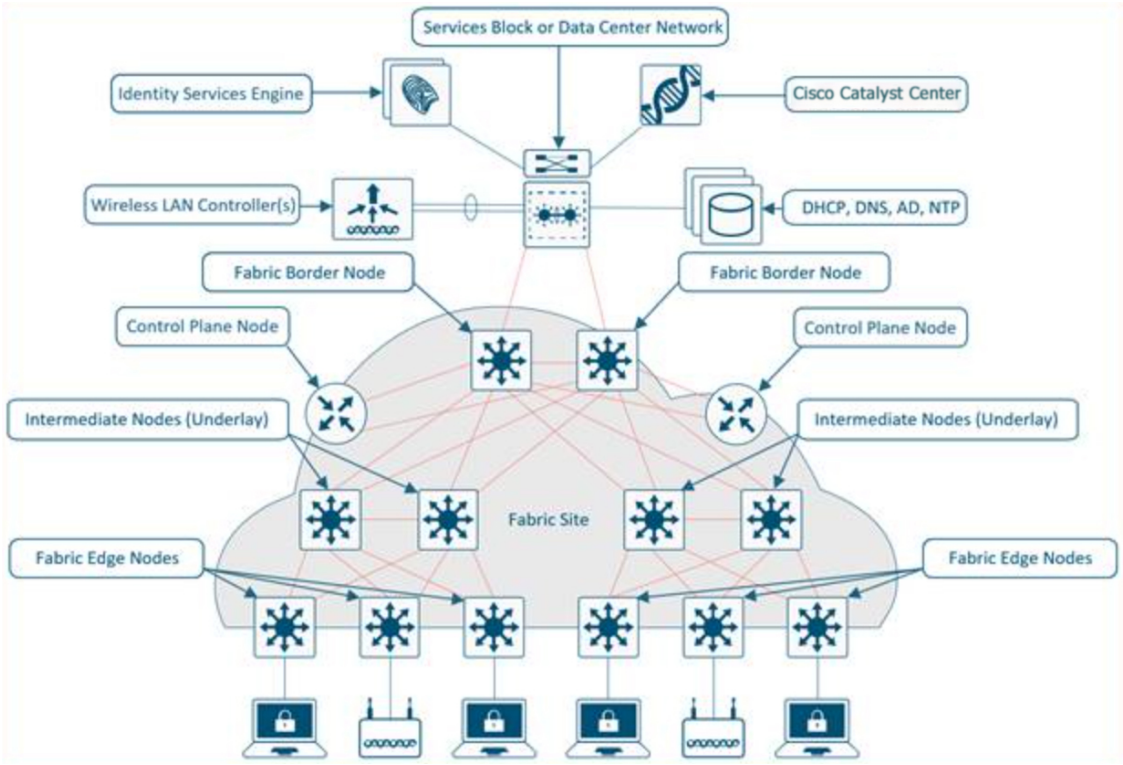
Source port	Source	Destination port	Destination	Description
Any	Witness IP	TCP 8302	Catalyst Center Enterprise VIP	Consul SERF WAN port[1]
Any	Witness IP	UDP 8302	Catalyst Center Enterprise VIP	Consul SERF WAN port[1]
Any	Witness IP	TCP 8443	Catalyst Center Enterprise VIP	HA proxy API access [2]

Required ports and protocols for Cisco Software-Defined Access

Explains extra ports, protocols, and network traffic required with the Cisco SD-Access infrastructure.

This topic describes the ports, protocols, and types of traffic involved in a typical Cisco SD-Access fabric deployment, similar to what is shown in the figure.

Figure 4: Cisco SD-Access fabric infrastructure



If you have implemented Cisco SD-Access in your network, use this table to plan your firewall and security policies for your Cisco SD-Access infrastructure. This setup also allows Catalyst Center to automate your network management.

Note

The appliance interface configured to route internet-bound traffic serves as the source for all communications.

Table 11: Catalyst Center traffic

Source port[4]	Source	Destination port	Destination	Description
Any	Catalyst Center	UDP 53	DNS server	From Catalyst Center to DNS server
Any	Catalyst Center	TCP 22	Fabric underlay	From Catalyst Center to fabric switches' loopbacks for SSH
Any	Catalyst Center	TCP 23	Fabric underlay	From Catalyst Center to fabric switches' loopbacks for TELNET
Any	Catalyst Center	UDP 161	Fabric underlay	From Catalyst Center to fabric switches' loopbacks for SNMP device discovery
ICMP	Catalyst Center	ICMP	Fabric underlay	From Catalyst Center to fabric switches' loopbacks for SNMP device discovery
Any	Catalyst Center	TCP 443	Fabric underlay	Hosts applications for switches and for NFVIS
Any	Catalyst Center	UDP 6007	Switches and routers	From Catalyst Center to switches and routers for NetFlow
Any	Catalyst Center	TCP 830	Fabric underlay	From Catalyst Center to fabric switches for Netconf (Cisco SD-Access embedded wireless)
UDP 123	Catalyst Center	UDP 123	Fabric underlay	From Catalyst Center to fabric switches for the initial period during LAN automation
Any	Catalyst Center	UDP 123	NTP server	From Catalyst Center to NTP server
Any	Catalyst Center	TCP 22, UDP 161	Cisco Wireless Controller	From Catalyst Center to Cisco wireless controller
ICMP	Catalyst Center	ICMP	Cisco Wireless Controller	From Catalyst Center to Cisco Wireless Controller
Any	AP	TCP 32626	Catalyst Center	Used for receiving traffic statistics and packet capture data used by the Cisco Catalyst Assurance Intelligent Capture (gRPC) feature.

[4] Cluster, PKI, SFTP server, and proxy port traffic are not included in this table.

Table 12: Internet connectivity traffic

Source port	Source	Destination port	Destination	Description
Any	Catalyst Center	TCP 443	registry.ciscoconnectdna.com	Download Catalyst Center package updates
Any	Catalyst Center	TCP 443	www.ciscoconnectdna.com	Download Catalyst Center package updates
Any	Catalyst Center	TCP 443	registry-cdn.ciscoconnectdna.com	Download Catalyst Center package updates
Any	Catalyst Center	TCP 443	cdn.ciscoconnectdna.com	Download Catalyst Center package updates
Any	Catalyst Center	TCP 443	software.cisco.com	Download device software
Any	Catalyst Center	TCP 443	cloudsso.cisco.com	Validate Cisco.com and Smart Account credentials
Any	Catalyst Center	TCP 443	cloudsso1.cisco.com	Validate Cisco.com and Smart Account credentials
Any	Catalyst Center	TCP 443	cloudsso2.cisco.com	Validate Cisco.com and Smart Account credentials
Any	Catalyst Center	TCP 443	apiconsole.cisco.com	CSSM Smart Licensing API
Any	Catalyst Center	TCP 443	sso.cisco.com	Cisco.com credentials and Smart Licensing
Any	Catalyst Center	TCP 443	api.cisco.com	Cisco.com credentials and Smart Licensing
Any	Catalyst Center	TCP 443	apx.cisco.com	Cisco.com credentials and Smart Licensing
Any	Catalyst Center	TCP 443	dashboard.meraki.com	Meraki integration
Any	Catalyst Center	TCP 443	api.meraki.com	Meraki integration
Any	Catalyst Center	TCP 443	n63.meraki.com	Meraki integration
Any	Catalyst Center	TCP 443	dnacenter.uservoice.com	User feedback submission
Any	Catalyst Center Admin Client	TCP 443	*.mapbox.com/:443	Render maps in the browser (for access through proxy, the destination is *.mapbox.com/*)
Any	Catalyst Center	TCP 443	www.mapbox.com	Maps and Cisco Wireless Controller country code identification

Table 13: Cisco Software-Defined Access fabric underlay traffic

Source port[5]	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.

[5] Border routing protocol, SPAN, profiling, and telemetry traffic are not included in this table.

Any	Fabric underlay	TCP 80	Catalyst Center	From fabric switch and router loopback IPs to Catalyst Center for PnP
Any	Fabric underlay	TCP 443	Catalyst Center	From fabric switch and router loopback IPs to Catalyst Center for image upgrade
Any	Fabric underlay	UDP 162	Catalyst Center	From fabric switch and router loopback IPs to Catalyst Center for SNMP Traps
Any	Fabric underlay	UDP 514	Catalyst Center	From fabric switches and routers to Cisco Catalyst Assurance
Any	Fabric underlay	UDP 6007	Catalyst Center	From fabric switches and routers to Catalyst Center for NetFlow
Any	Fabric underlay	UDP 123	Catalyst Center	From fabric switches to Catalyst Center; used when doing LAN automation
ICMP	Fabric underlay	ICMP	Catalyst Center	From fabric switch and router loopbacks to Catalyst Center for SNMP: device discovery
UDP 161	Fabric underlay	Any	Catalyst Center	From fabric switch and router loopbacks to Catalyst 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, control plane	Any	Fabric routers, switches, and Cisco Wireless Controller	• LISP control-plane communications • From control-plane loopback IP to Cisco wireless controller for fabric-enabled wireless
TCP and UDP 4342	Fabric underlay, control plane	TCP and UDP 4342	Fabric routers, switches, and Cisco Wireless Controller	• LISP-encapsulated control messages • From control-plane loopback IP toCisco Wireless Controller for fabric-enabled wireless
Any	Fabric underlay	UDP 4789	Fabric Routers and Switches	Fabric-encapsulated data packets (VXLAN-GPO)
Any	Fabric underlay	UDP 1645/1646/1812/1813	Cisco ISE	From fabric switch and router loopback IPs to Cisco ISE for RADIUS
ICMP	Fabric underlay	ICMP	Cisco ISE	From fabric switches and routers to Cisco ISE for troubleshooting
UDP 1700/3799	Fabric underlay	Any	Cisco ISE	From fabric switches to Cisco 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	Fabric routers, switches, and Cisco Wireless Controller	• LISP-encapsulated control messages • From Control plane loopback IP to Cisco wireless controller for fabric-enabled wireless

UDP and TCP 4342/4343	Control plane	Any	Fabric routers, switches, and Cisco Wireless Controller	• LISP-encapsulated control messages • From Control plane loopback IP toCisco Wireless Controller for fabric-enabled wireless

Table 14: 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	• TCP 443 (Cisco AireOSwireless controllers) • TCP 25103 (Cisco 9800 wireless controllers and Cisco Catalyst 9000 switches with streaming telemetry enabled)	Catalyst Center	From Cisco Wireless Controller to Catalyst 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	Catalyst Center	From Cisco Wireless Controller to Catalyst Center for device discovery
UDP 161	Cisco Wireless Controller	Any	Catalyst Center	From Cisco Wireless Controller to Catalyst Center for SNMP
Any	Cisco Wireless Controller	UDP 162	Catalyst Center	From Cisco Wireless Controller to Catalyst 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	Catalyst Center	From wireless controllers to Catalyst Center for NetFlow network telemetry
ICMP	Cisco Wireless Controller	ICMP	Catalyst 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	Cisco ISE	From Cisco Wireless Controller to Cisco ISE for Guest SSID web authorization
Any	Cisco Wireless Controller	UDP 1645,1812	Cisco ISE	From Cisco Wireless Controller to Cisco ISE for RADIUS authentication
Any	Cisco Wireless Controller	UDP 1646, 1813	Cisco ISE	From Cisco Wireless Controller to Cisco ISE for RADIUS accounting
Any	Cisco Wireless Controller	UDP 1700, 3799	Cisco ISE	From Cisco Wireless Controller to Cisco ISE for RADIUS CoA
ICMP	Cisco Wireless Controller	ICMP	Cisco ISE	From Cisco Wireless Controller to Cisco ISE ICMP for troubleshooting
Any	Cisco Wireless Controller	UDP 123	NTP server	From Cisco Wireless Controller to NTP server

Table 15: 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 16: Cisco ISE traffic

Source port[6]	Source	Destination port	Destination	Description
Any	Cisco ISE	TCP 64999	Border	From Cisco ISE to border node for SGT Exchange Protocol (SXP)
Any	Cisco ISE	UDP 514	Catalyst Center	From Cisco ISE to syslog server (Catalyst Center)
UDP 1645/1646/1812/1813	Cisco ISE	Any	Fabric underlay	From Cisco ISE to fabric switches and routers for RADIUS and authorization

[6] Note: High availability and profiling traffic are not included in this table.

Any	Cisco ISE	UDP 1700/3799	Fabric underlay,Cisco Wireless Controller	From Cisco ISE to fabric switch and router loopback IP addresses for RADIUS Change of Authorization (CoA). UDP port 3799 must also be open from Cisco ISE to the wireless controller for CoA.
ICMP	Cisco ISE	ICMP	Fabric underlay	From Cisco ISE to fabric switches for troubleshooting
Any	Cisco ISE	UDP 123	NTP server	From Cisco ISE to NTP server
UDP 1812/1645/1813/1646	Cisco ISE	Any	Cisco Wireless Controller	From Cisco ISE to Cisco Wireless Controller for RADIUS
ICMP	Cisco ISE	ICMP	Cisco Wireless Controller	From Cisco ISE to Cisco Wireless Controller for troubleshooting

Table 17: 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 18: NTP server traffic

Source port	Source	Destination port	Destination	Description
UDP 123	NTP server	Any	Cisco ISE	From NTP server to Cisco ISE
UDP 123	NTP server	Any	Catalyst Center	From NTP server to Catalyst 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 19: 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

Explains the required information that you must enter during the configuration of the appliance.

During appliance configuration, you must enter this information, in addition to the items listed in Required IP addresses and subnets on page 31:

- **Linux username**: This is `maglev`. Use this username on all appliances in a cluster, including the primary and secondary nodes. You cannot change the username.
- **Linux password**: Identifies the password for the Linux user named `maglev`. This password ensures secure access to each appliance using the Linux command line. If needed, you can assign a different password for the `maglev` user on each appliance in the cluster.

  Ensure that the password you configure complies with the Password requirements on page 56.

  The Linux password is encrypted and hashed in the Catalyst 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 Catalyst Center in a cluster. This is the password for the superuser account `admin`, which you use to log in to Catalyst Center for the first time (see Log in to Catalyst Center for the first time on page 178). You are prompted to change this password when you log in for the first time.

  Ensure that the password you configure complies with the Password requirements on page 56.
- **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 the Cisco Integrated Management Controller on page 66).

  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 on page 28).

Required first-time setup information

Explains the information that you must provide during the first-time setup of Catalyst Center.

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

- **New admin superuser password**: You will be prompted to enter a new password for the Catalyst Center admin super user. Resetting the super user password enhances operational security. This is especially important if, for example, the enterprise staff member who installed and configured the Catalyst Center appliance is not a Catalyst 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 Catalyst 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 Catalyst Center in order to get updates to the Catalyst Center software, manage device licenses, and retrieve other downloadable content.
- **Catalyst Center users**: User names, passwords, and privilege settings for the new Catalyst Center users you will be creating. Always use one of the new user accounts for normal Catalyst Center operations. Use the admin super user account only for reconfiguring Catalyst Center and for operations that require super user privileges.

Important

Ensure that the passwords you configure for Catalyst Center users and the admin super user comply with the Password requirements on page 56.

Use this information to complete additional setup tasks, which can be done after your first login:

- **Catalyst Center server IP address 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 Catalyst Center, as explained in Integrate Cisco ISE With Catalyst Center.

  When you install or upgrade to the latest release of Catalyst Center, the system checks whether 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 Catalyst Center.

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

  Catalyst Center data present in the previous version is preserved when you upgrade. The data migration operation merges data from Catalyst Center and Cisco ISE. If a conflict occurs during migration, the system uses data from Cisco ISE.

  If Catalyst Center becomes unavailable, and it is imperative to manage policies before Catalyst Center becomes available again, 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 Catalyst Center is available again, you must disable the Read-Only override on Cisco ISE, and re-synchronize the policy data on Catalyst Center Group Based Access Control Settings page.

> ⚠ **Caution**
>
> Use this option only when necessary. Changes made directly in Cisco ISE do not transfer to Catalyst Center.

- **Authorization and policy server information:** If you are using Cisco ISE as your authentication and policy server, you need the same information listed in the previous bullet, plus:
  - ISE CLI user name
  - CLI password
  - server FQDN
  - subscriber name (such as *cc*)
  - ISE SSH key (optional)
  - protocol choice (RADIUS or TACACS)
  - authentication port
  - accounting port
  - 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 Catalyst Center with your chosen authentication and policy server, as explained in Configure authentication and policy servers on page 198.
- **SNMP retry and timeout values**: This is required to set up device polling and monitoring, as explained in Configure SNMP properties on page 202.

Password policy

Describes the password policy in Catalyst Center.

After you have deployed Catalyst Center, review these password policy requirements.

Fresh Catalyst Center deployments

This section describes password policies for new deployments.

- The default password for the maglev user and admin superuser is **P@ssword9**.

  You are prompted to change the password for the admin superuser after you log in to the Catalyst Center GUI for the first time.
- When you change any user's password or configure a new user, ensure their password complies with the new requirements.

Catalyst Center upgrades

This section explains password behavior during system upgrades.

- Role-Based Access Control (RBAC) users configured in an earlier release of Catalyst Center can continue using their current password to log in to Catalyst Center 2.3.7.9 and later.

  For example, you upgraded an appliance from release 2.3.7.6 to 2.3.7.11. You backed up the data from the appliance. Later, you restored the backup file onto another appliance with Catalyst Center 2.3.7.11 installed. Existing RBAC users can log in using their current password.

- When you change any user's password or configure a new RBAC user, ensure their password complies with the new requirements.

Refer to Password requirements on page 56 to learn the criteria your new password must meet.

Password requirements

Describes password requirements for Catalyst Center.

Any user password you configure in Catalyst Center 2.3.7.11 or later must meet these requirements:

- Is at least nine characters in length.
- Includes characters from at least three of these categories:
  - Uppercase letters (A through Z)
  - Lowercase letters (a through z)
  - Numbers (0 through 9)
  - Special characters (such as !, $, and #)
- Does not contain more than four consecutive characters on an English QWERTY keyboard.

  For example, `59Asdfpj!` is not a valid password because it contains the characters `a`, `s`, `d`, and `f` in succession.
- Does not contain two or more consecutive characters from the associated username.
- Does not contain a complete word from any language.
- Does not contain a phrase based on personal information.

Note

You can reuse a previous password only after you use 24 different passwords.

3 Install the Appliance

Topics:

- Appliance installation workflow
- Unpack and inspect the appliance
- Review the installation warnings and guidelines
- Review the rack requirements
- Connect and power on the appliance
- Check the LEDs

Appliance installation workflow

Introduction to the Catalyst Center appliance installation workflow.

To physically install your Catalyst Center appliance, complete the tasks described in this chapter for each appliance you want to install. Install all appliances before configuring the primary node.

After you complete all of the tasks, continue with the steps in Preparation for appliance configuration overview on page 66.

Unpack and inspect the appliance

Describes what to check when unpacking your Catalyst Center appliance package.

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

Procedure

1. Remove the appliance from its cardboard container. Save all packaging material in case you need to ship the appliance in the future.
2. Compare your shipment with the equipment list provided by your customer service representative. Confirm that you received all items.
3. Check for any damage. Immediately report any missing items or damage to your customer service representative. Have this information ready:
   - Invoice number of the shipper as shown on the packing slip
   - Model number and serial number of the damaged unit
   - Description of damage
   - Effect of damage on the installation

Review the installation warnings and guidelines

Warnings, cautions, and guidelines to follow when physically installing an appliance.

These guidelines apply when installing an appliance:

- Plan your site configuration and prepare your site before installing the appliance. For information about recommended site planning and preparation tasks, see the *Cisco UCS Site Preparation Guide*.
- Ensure that there is adequate space around the appliance for servicing and airflow. Air enters through the front of the appliance and exits through the back.
- Ensure that the site's air conditioning meets the thermal requirements listed in Environmental specifications on page 23.

- Ensure that the cabinet or rack meets the requirements in Review the rack requirements on page 61.
- Ensure that the site's power meets the requirements in Power supply specifications on page 25. If available, use a UPS to protect against power failures.
- Carefully review the cautions and warnings.

Caution

To ensure proper airflow, rack the appliances using rail kits. Stacking units without rail kits blocks the air vents on top of the appliances. This results in overheating, increased fan speeds, and greater power consumption. Mount your appliances on rail kits during installation to ensure the required minimum spacing between units. No additional spacing is required when units are mounted using rail kits.

Caution

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

Statement 1071—Warning Definition

Warning

IMPORTANT SAFETY INSTRUCTIONS

Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Read the installation instructions before using, installing, or connecting the system to the power source. Use the statement number at the beginning of each warning statement to locate its translation in the translated safety warnings for this device.

SAVE THESE INSTRUCTIONS



Statement 1005—Circuit Breaker

Warning

This product relies on the building's installation for short-circuit (overcurrent) protection. To reduce the risk of electric shock or fire, ensure that the protective device is rated at no more than:

250 V, 15 A.

Statement 1074—Comply with Local and National Electrical Codes

> **Warning**
>
> To reduce risk of electric shock or fire, installation of the equipment must comply with local and national electrical codes.

Statement 1017—Restricted Area

> **Warning**
>
> This unit is intended for installation in restricted access areas. Only skilled, instructed, or qualified personnel can access a restricted access area.

Review the rack requirements

Provides rack requirement information.

Ensure your rack meets these requirements:

- Use a standard 19 in. (48.3 cm) wide, four-post EIA rack with mounting posts that conform to English universal hole spacing, as specified in Section 1 of ANSI/EIA-310-D-1992.
- Use the Cisco-supplied slide rails. The rack-post holes can be one of these types: square 0.38 in. (9.6 mm), round 0.28 in. (7.1 mm), size 12-24 UNC, or size 10-32 UNC.
- Provide at least one rack unit (RU), or 1.75 in. (44.45 mm), of vertical rack space for every 32-core or 48-core or 72-core appliance server.

Supported Cisco slide rail kits

The server supports these rail kit options:

- Part UCSC-RAIL-D is a ball bearing slide rail kit.
- Part UCSC-CMA-C220-D is a reversible cable management arm for the ball bearing slide rail kit used with 32-core and 48-core appliances.

Rack installation tools required

You do not need tools to install the slide rails sold by Cisco Systems for this server.

Slide rail and cable management arm dimensions

The slide rails for this server have an adjustment range of 24 in. (610 mm) to 36 in. (914 mm).

The optional cable management arm adds additional length requirements:

- For the 32-core, 48-core, and 72-core appliances, the distance from the rear of the server to the rear of the cable management arm is 7.6 in. (193 mm).
- For the 32-core, 48-core, and 72-core appliances, the total length of the server including the cable management arm is 37.6 in. (955 mm).

Connect and power on the appliance

Describes how to power on the appliance and check that it's functional.

Describes how to power on the appliance and check that it's functional.

Procedure

1. Attach a supplied power cord to each power supply in the appliance. Connect the power cords to a grounded AC power outlet. Refer to Power supply specifications on page 25.

   Note

   You can use either one or both of the power supplies that come with the appliance. One power supply is mandatory; one more can be added for 1 + 1 redundancy.

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

   The Power Status LED displays the power status of the appliance:

   - Green: All power supplies are operating normally.
   - Amber, steady: One or more power supplies are in a degraded operational state.
   - Amber, blinking: One or more power supplies are in a critical fault state.

   For more information about these and other appliance LEDs, refer to Front and rear panels on page 14.

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.

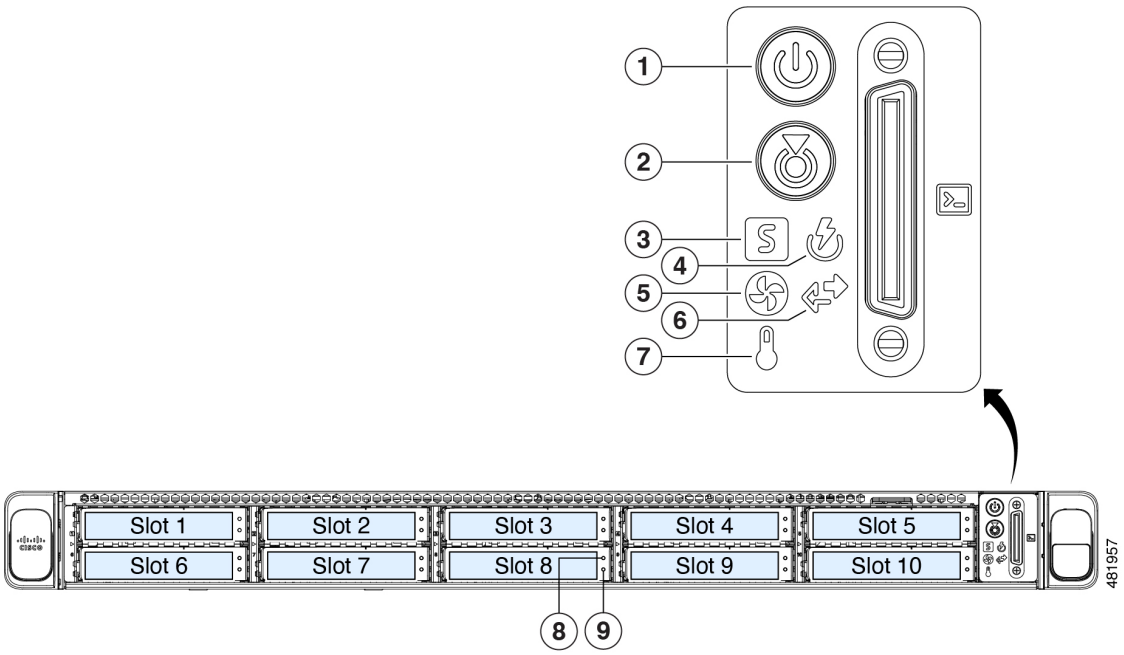
Check the LEDs

Describes what the LEDs on a Catalyst Center appliance indicate.

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.

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

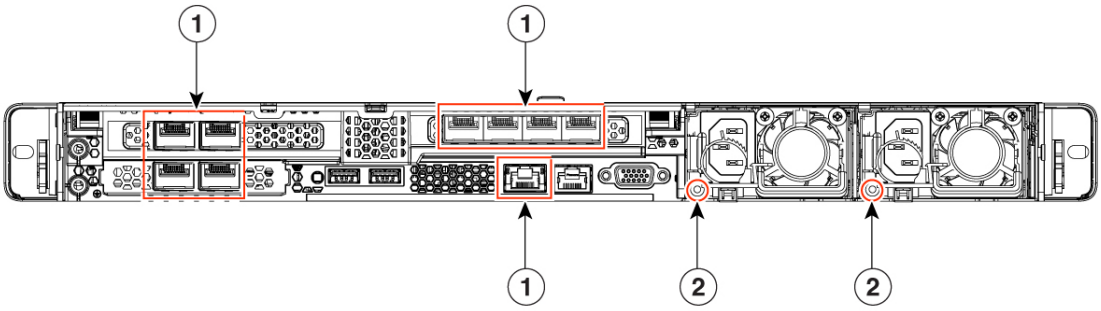
Figure 5: Catalyst Center appliance front panel LEDs



This table describes the how the front panel LED indicators should appear.

LED	Status indicator
1	Power status: Green
2	Unit identification: Off
3	System status: Green
4	Power supply status: Green
5	Fan status: Green
6	Network link activity: Off
7	Temperature status: Green
8	Drive fault LED: Off
9	Drive activity LED: Green

Figure 6: Catalyst Center appliance rear panel LEDs



This table describes the how the rear panel LED indicators should appear.

LED	Status indicator
1	After initial power-on, 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 or browser-based configuration wizard, the link status and link speed LEDs for all **cabled** ports should be green. The LED for all **uncabled** ports should remain off.
2	AC power supply status LEDs: Green

4 Prepare the Appliance for Configuration

Topics:

- Preparation for appliance configuration overview
- Enable browser access to the Cisco Integrated Management Controller
- Execute preconfiguration tasks
- NIC bonding overview
- Reimage the appliance
- Catalyst Center appliance configuration

Explains how to prepare the Catalyst Center appliance for configuration, including enabling browser access to the Cisco Integrated Management Controller (IMC), executing preconfiguration tasks, and optionally reinstalling the Catalyst Center software if needed before proceeding to appliance configuration.

Preparation for appliance configuration overview

Provides an overview of the appliance configuration process.

Before you can successfully configure your Catalyst Center appliance, first complete these tasks:

1. Enable browser access to Cisco IMC for the appliance (refer to Enable browser access to the Cisco Integrated Management Controller on page 66).
2. Check and adjust important hardware and switch settings using Cisco IMC to Execute preconfiguration tasks on page 71.
3. Reinstall the preinstalled Catalyst Center software in certain situations. For example, reinstall before you change the current cluster link configuration. If you need to reinstall the software, complete the tasks in Reimage the appliance on page 76.

> **Note**
>
> If you do not need to reimage your appliance, go to Appliance configuration overview on page 86.

Enable browser access to the Cisco Integrated Management Controller

Describes how to use the Cisco IMC configuration utility to configure a Catalyst Center appliance's Cisco IMC port.

After installing the appliance, use the Cisco IMC configuration utility to assign an IP address and gateway to the appliance CIMC port. You can access the Cisco IMC GUI to configure the appliance.

After you complete the Cisco IMC setup, log in to Cisco IMC and run the tasks listed in Execute preconfiguration tasks on page 71 to ensure correct configuration.

Note

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

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**.
3. In the **Modify User Details** dialog box, check the **Change Password** check box.
4. Enter and confirm the new password, and then click **Save**.

Procedure

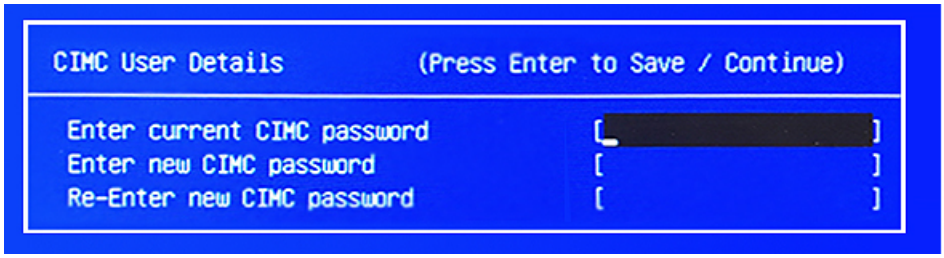
1. Access the appliance console by attaching either of these options:
   - A KVM cable to the KVM connector on the appliance front panel.
   - A keyboard and monitor to the USB and VGA ports on the appliance rear panel.
2. Make sure that the appliance power cord is plugged in and the power is on.
3. Press the **Power** button on the front panel to boot the appliance.

   The Cisco IMC configuration utility boot screen opens.



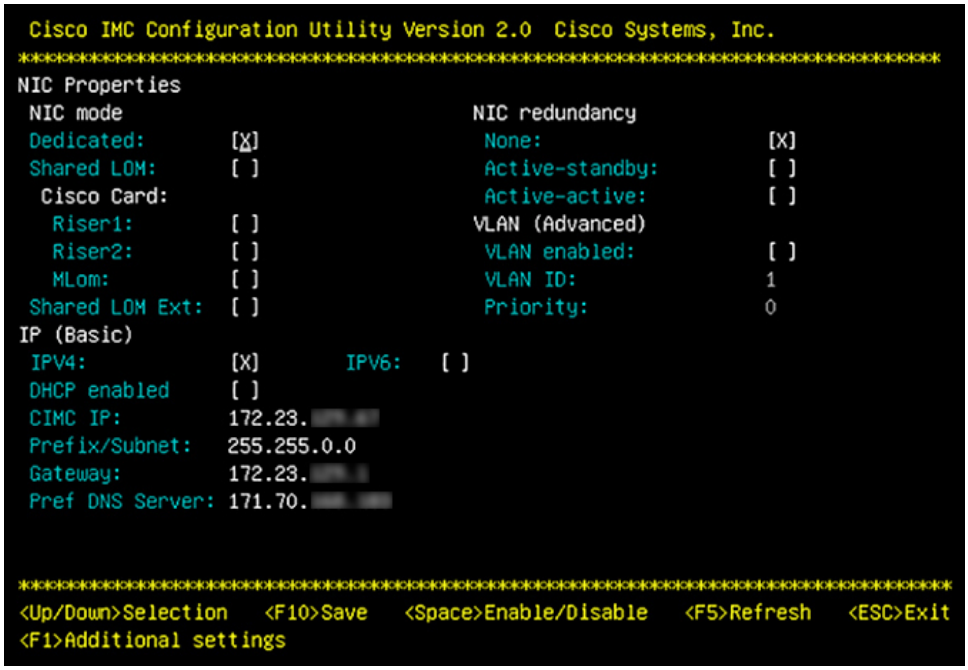
4. Press **F8** to perform the Cisco IMC configuration.

   The CIMC configuration utility displays the **CIMC User Details** screen, as shown.



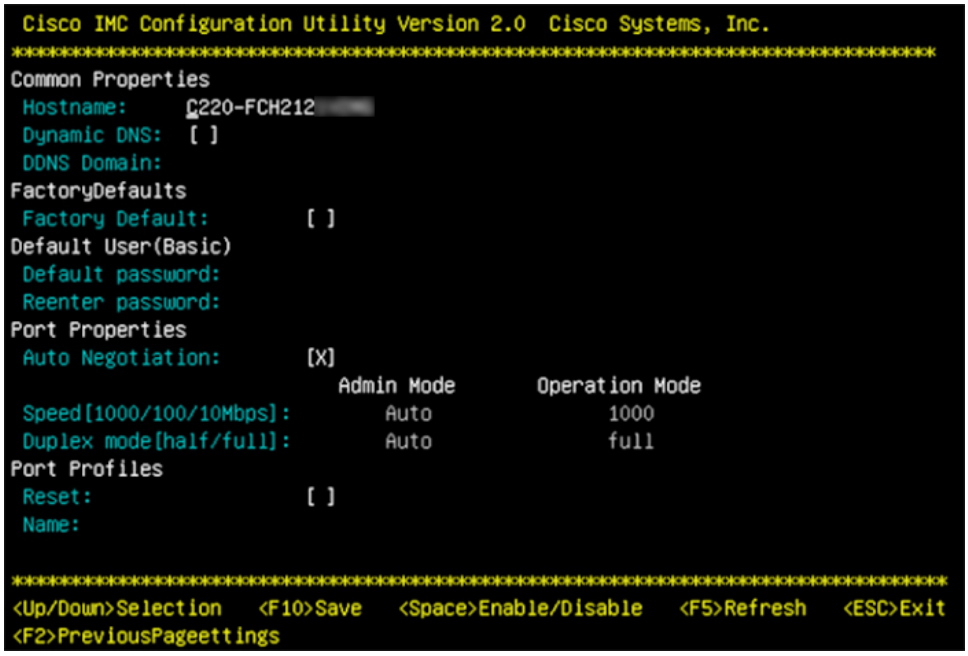
5. Enter the default CIMC user password (the default on a new appliance is *password*) in the **Enter current CIMC Password** field.
6. Enter and confirm the new CIMC user password in the **Enter new CIMC password** and **Re-Enter new CIMC password** fields.

   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.



7. Perform these 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**.
8. Press **F1** to specify **Additional settings**.

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



9. Perform these 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.
10. Press **F10** to save the settings.
11. Press **Escape** to exit and reboot the appliance.
12. After the settings are saved and the appliance finishes rebooting, open a browser on a client machine that can access the appliance subnet, and enter this URL:

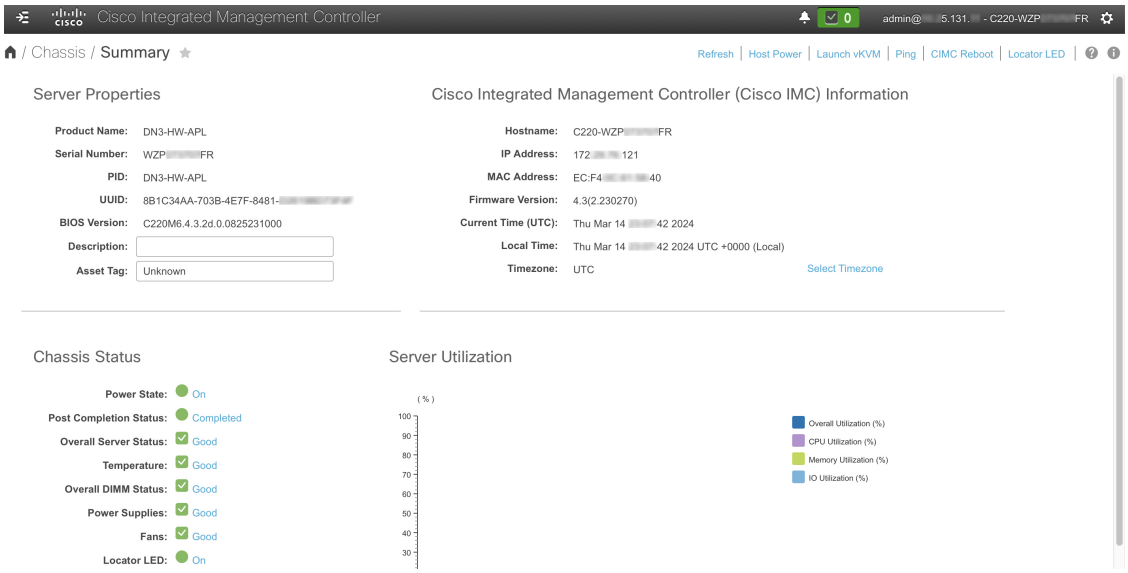
    `https://`***`CIMC_ip_address`***, where ***`CIMC_ip_address`*** is the Cisco IMC port IP address that you entered in Step 7.

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



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

    If your login is successful, a **Cisco Integrated Management Controller Chassis Summary** window appears in your browser.



14. Confirm that this version of Cisco IMC is supported by the Catalyst Center release you're going to install:
    a) View the version listed in the **Firmware Version** field.
    b) Refer to the release notes for the Catalyst Center release you are installing. The “Supported Firmware” section indicates the Cisco IMC version that your Catalyst Center release supports.
    c) Do one of these tasks:
        - If the right Cisco IMC version is installed, you can stop here.
        - If you need to update your Cisco IMC version, refer to the *Cisco Host Upgrade Utility User Guide* for instructions.

Execute preconfiguration tasks

Describes the tasks you need to complete to ensure the proper configuration and deployment of the Catalyst Center appliance.

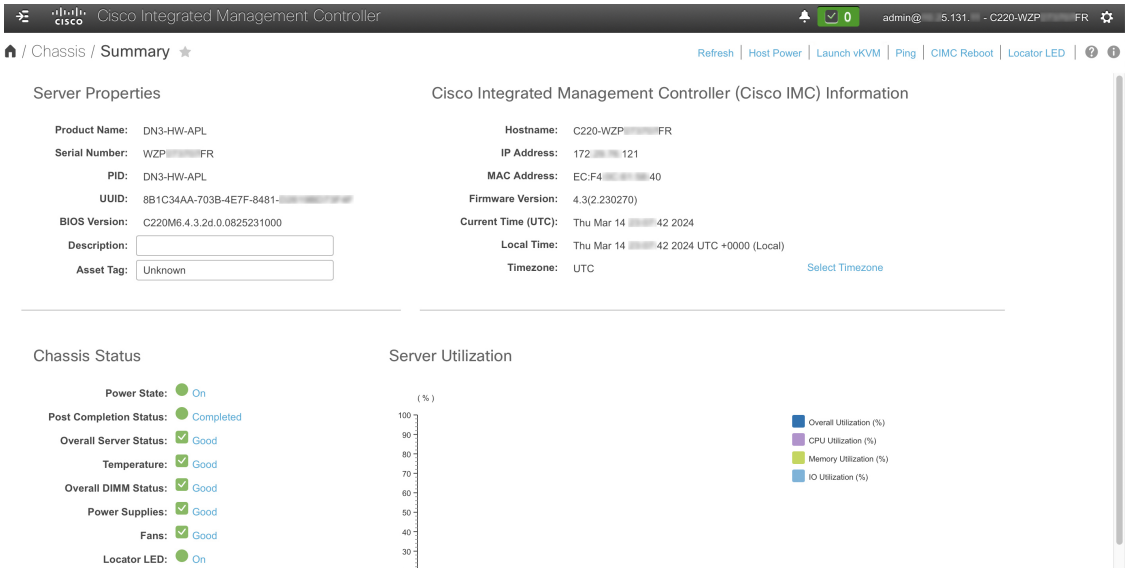
First install the appliance and set up access to the Cisco IMC GUI. Refer to Appliance installation workflow on page 58 and Enable browser access to the Cisco Integrated Management Controller on page 66. Then use Cisco IMC to complete the preconfiguration tasks to ensure correct configuration and deployment.

1. Synchronize the appliance hardware with the Network Time Protocol (NTP) servers that manage your network. Use the same NTP servers whose hostnames or IPs you collected while planning your implementation, as explained in Required IP addresses and subnets on page 31. This synchronization is critical for keeping your Catalyst Center data synchronized properly across the network.
2. Reconfigure the switches connected to the 10 Gbps appliance ports to support higher throughput settings.

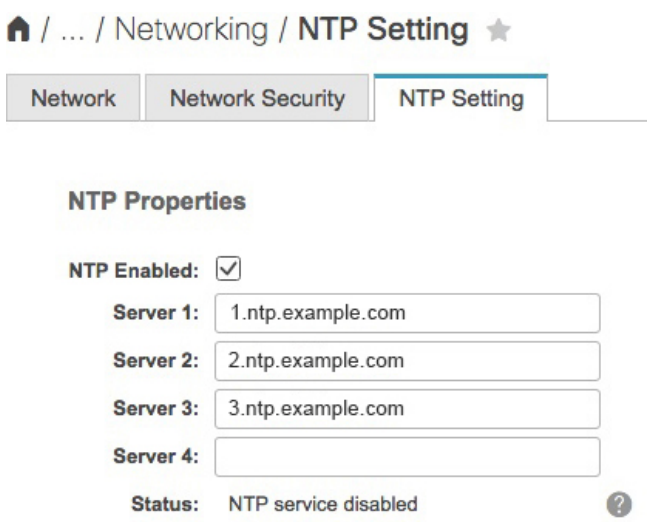
Procedure

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 the Cisco Integrated Management Controller on page 66.

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



2. Synchronize the appliance's hardware with the Network Time Protocol (NTP) servers you use to manage your network accordingly:
   a) From the top-left corner of the Cisco IMC GUI, click the **Toggle Navigation** icon ( ).
   b) From the Cisco IMC menu, choose **Admin** > **Networking**. Select the **NTP Setting** tab.
   c) Make sure that the **NTP Enabled** check box is checked, then enter up to four NTP server host names or addresses in the numbered **Server** fields, as shown.



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

> **Note**
>
> - Fourth-generation Catalyst Center appliances do not use a virtual interface card (VIC). High throughput is already enabled by default on the network interface card (NIC) installed in your fourth-generation appliance, so you do not need to configure the NIC in Cisco IMC.
> - You cannot use NTP authentication in Cisco IMC.

3. Reconfigure your switches to match the high-throughput settings on the appliance accordingly:
   a) Using a Secure Shell (SSH) client, log in to the switch to be configured and enter EXEC mode at the switch prompt.
   b) Configure the switch port.

   On a Cisco Catalyst switch, enter these 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 these 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**
>
> - These commands are examples only.
> - The switch port on Catalyst Center fourth-generation appliances must be set to access mode for proper operation. Trunk mode is not supported.

c) Run the show interface tengigabitethernet *portID* command. 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:

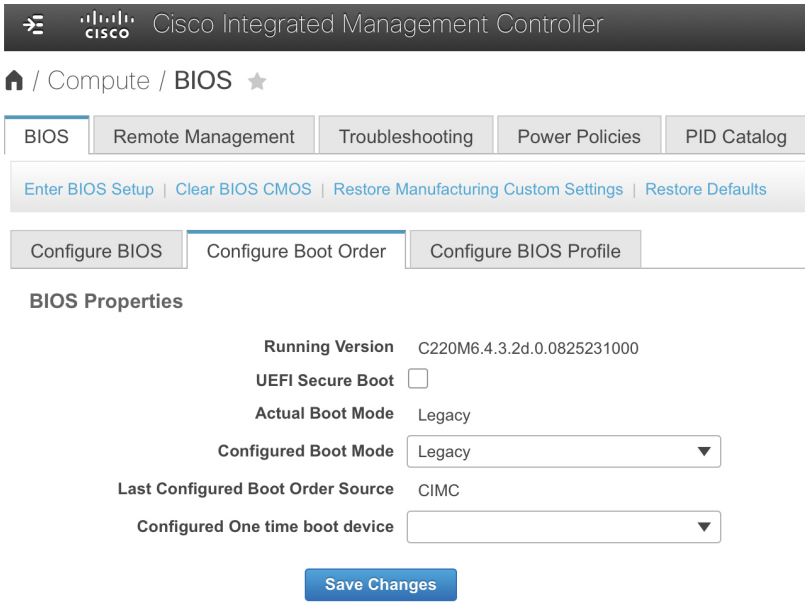
```
MySwitch#show mac address-table interface tengigabitethernet 1/1/3
          Mac Address Table
-------------------------------------------
Vlan     Mac Address       Type      Ports
----     -----------       ----      -----
99       XXXe.3161.1000    DYNAMIC   Te1/1/3
Total Mac Addresses for this criterion: 1

MySwitch#
```

4. In the **Configured Boot Mode** drop-down list, verify that **UEFI** is displayed.

Note

Fourth-generation Catalyst Center appliances operate only in UEFI mode. Legacy boot mode is not supported.



To access the **Configure Boot Order** tab:

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

Caution

Do not change the appliance from **UEFI** boot mode. Fourth-generation Catalyst Center appliances do not support **Legacy** boot mode.

What to do next

After completing this task, do one of these tasks:

- If you need to reinstall Catalyst Center software before you configure your appliance, refer to Reimage the appliance on page 76.
- If you are ready to configure your appliance, continue to Appliance configuration overview on page 86.

NIC bonding overview

Provides an overview of the network interface controller bonding feature.

On any given Catalyst Center appliance, you can configure the Enterprise, Intracluster, Management, and Internet interfaces. If you enable network interface controller (NIC) bonding on an appliance, each of the interfaces has two instances. The primary instance (located on either your appliance's motherboard or Intel E810-XXVDA2 network adapter) is connected to one switch. The secondary instance (located on your appliance's Intel E810-XXVDA4 network adapter) is connected to a different switch. NIC bonding consolidates the two instances of each interface into a single logical interface. It appears as a single device with one MAC address. Enabling this feature provides benefits that depend on the bonding mode you select when configuring your appliance's interfaces. Benefits include:

> **Note**
>
> Both single-node and three-node Catalyst 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 Catalyst 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, Catalyst Center automatically sets the throughput to 1-Gbps.

- **LACP mode**: When selected, the two interfaces that Catalyst 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, these items must first be in place:
  - Ensure the Linux utility tool supports the base drivers that are used to retrieve the speed and duplex mode of each interface.
  - Ensure the switch that is connected to the Enterprise port supports dynamic interface aggregation.
  - Ensure that after you enable LACP on the switch:
    - The LACP mode is set to **active**. This setting 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
  - The LACP rate is set to **fast**. This setting 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.
- You can only enable LACP mode on your appliance's Intracluster interface during the initial configuration of your appliance.

Before you use NIC bonding in your production environment, do these tasks:

- Confirm that your appliance supports this feature. Refer to Appliance support on page 76.
- Determine where the secondary ports are located on your appliance's rear panel. Refer to Front and rear panels on page 14.
- View the recommended appliance-switch cabling. Refer to Interface cable connections on page 28.

Appliance support

Indicates the fourth-generation Catalyst Center appliances that support NIC bonding.

All fourth-generation Catalyst Center appliances support NIC bonding:

- Medium appliance:
  - Standard: DN4-HW-APL
- Large appliance:
  - Standard: DN4-HW-APL-L
- Extra large appliance:
  - Standard: DN4-HW-APL-XL

Reimage the appliance

Describes the steps that need to be completed to reimage a Catalyst Center appliance.

You might need to reimage your Catalyst Center appliance after some situations like recovering from a backup or changing your cluster link configuration. Complete this procedure to reimage your appliance.

Procedure

1. Download the Catalyst Center ISO image. Verify that it is a genuine Cisco image.

   Refer to Verify the Catalyst Center image on page 77.

2. Create a bootable USB drive that contains the Catalyst Center ISO image.

   Refer to Create a bootable USB flash drive on page 78.

3. Delete and recreate the virtual drives on your Catalyst Center appliance: Delete and recreate the virtual drives on a Catalyst Center appliance.
4. Reinstall Catalyst Center onto your appliance.

   Refer to Install the Catalyst Center ISO image on page 82.

Verify the Catalyst Center image

Describes how to verify that the Catalyst Center image you downloaded is a genuine Cisco image.

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

Before you begin

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

Procedure

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

   Depending on your operating system, enter one of these commands:

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

   On Microsoft Windows, use the certutil tool because it does not include a built-in checksum utility:

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

   For example:

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

   On Windows, you can also use the Windows PowerShell to generate the digest. For example:

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

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

6. Verify that the image is genuine and from Cisco by verifying its signature:

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

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

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

7. After confirming that you have downloaded a Cisco image, create a bootable USB drive that contains the Catalyst Center image. See Create a bootable USB flash drive on page 78.

Create a bootable USB flash drive

Introduction to the section that describes how to create a bootable USB flash drive for installation of the Catalyst Center ISO image.

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

Before you begin:

- Download and verify your copy of the Catalyst Center ISO image. Refer to Verify the Catalyst Center image on page 77.
- Confirm that the USB flash drive you are using meets these requirements:
  - USB 3.0 or later
  - 64 GB minimum
  - Unencrypted

> **Note**
>
> Use only Etcher, the Linux CLI, or the Mac CLI to burn the Catalyst Center ISO image.
>
> Use a USB drive only for temporary maintenance tasks, such as reimaging or recovery. Remove the USB drive immediately after the task is completed; do not leave the USB drive connected permanently.

Using Etcher

Describes how to create a bootable USB drive using the Etcher utility.

Procedure

1. Download and install Etcher (version 1.3.1 or later). You can use this free and open-source utility to create a bootable USB drive on your laptop or desktop.

   You can download Etcher for Linux, macOS, or Windows at https://www.balena.io/etcher/.

> **Note**
>
> Use Etcher only on Windows 10 or later to avoid compatibility issues.

2. From the machine on which you installed Etcher, connect a USB drive and then start Etcher.
3. In the top-right corner of the window, click ⚙ and verify that these Etcher settings are set:
   - Auto-unmount on success
   - Validate write on success
4. Click **Back** to return to the main Etcher window.
5. Click **Select Image**.
6. Navigate to the Catalyst Center ISO image you downloaded previously. Select it, and then click **Open**.

   You should see the name of the USB drive you connected under the drive icon (). If it is not:

   a. Click **Select drive**.

   b. Click the radio button for the correct USB drive, and then click **Continue**.
7. Click **Flash!** to copy the ISO image to the USB drive.

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

Using the Linux CLI

Describes how to create a bootable USB drive using the Linux CLI.

Procedure

---

1. Verify that your USB flash drive is recognized by your machine:
   a) Insert a flash drive into the USB port of your machine.
   b) Open a Linux shell and run this command: **lsblk**

      The command lists the disk partitions that are configured on your machine, as shown in this 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 is listed. This partition indicates the presence of a USB flash drive.

2. Burn the Catalyst 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 status=progress && sync**

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

Using the Mac CLI

Describes how to create a bootable USB drive using the Mac CLI.

Procedure

---

1. Determine the disk partition associated with your USB flash drive:
   a) Open a Terminal window and run this command: **diskutil list**

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

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

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

2. Unmount the flash drive partition: **diskutil unmountDisk** *flash-drive-partition*

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

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

   Continuing our example, assume that you are working with a Catalyst Center ISO image named `CC-SW-1.330.iso`. You would run this command, which creates a macOS disk image named `CC-1.330.dmg`: **hdiutil convert -format UDRW -o CC-1.330 CC-SW-1.330.iso**

   > **Note**
   >
   > Do not put the ISO image in a Box partition.

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 this command: **sudo dd if=CC-1.330.dmg of=/dev/disk2 bs=1m status=progress**

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

Delete and recreate the virtual drives on a Catalyst Center appliance

Describes how to delete and recreate the BOOT, SHARED, and ANALYTICS virtual drives before you reimage a fourth-generation Catalyst Center appliance.

Complete this procedure tto delete and recreate the virtual drives on your Catalyst Center appliance.

Before you begin

- Back up any appliance data that you need to retain.
- Obtain the Cisco IMC IP address and login credentials.
- Identify whether the appliance is medium, large, or extra-large.
- Ensure that the hard disk remains first in the configured boot order.

Note

- Deleting a virtual drive permanently deletes all data stored on that drive. Complete this procedure only when you are preparing to reimage the appliance.
- Fourth-generation appliances do not support virtual-drive reinitialization.
- Fourth-generation Catalyst Center appliances use UEFI boot mode. Do not configure or initialize any virtual drive or mark them as a bootable drive.

Procedure

1. Log in to the appliance's Cisco IMC by using the Cisco IMC IP address, user ID, and password.
2. Choose **Storage** > **Controllers**, and select the storage controller that manages the appliance drives.
3. Choose **Virtual Drive Info**.
4. Delete the existing virtual drives:
   a. Select the **BOOT** virtual drive and choose **Delete**.
   b. Confirm the deletion when prompted.
   c. Repeat these actions for the **SHARED** and **ANALYTICS** virtual drives.
5. Choose **Physical Drive Info**, and then choose **Actions** > **Create Virtual Drive**.
6. Select **MRAID**, and then select **From Unused Physical Drives**.
7. Create the **BOOT** virtual drive using this configuration, and then save it:

Table 20: Configuration settings

Setting	Value
Name	BOOT
RAID level	RAID 1
Physical drives	Drives 1 and 2

Setting	Value
Drives per span	2
Span depth	1
Strip size	65536
Read-ahead policy	NoReadAhead
Write-cache policy	WriteThrough
Boot drive	False

8. Repeat Step 5 through Step 7 to create the remaining virtual drives. Use these settings:

Table 21: Settings

Virtual drive	RAID level	Physical drives	Drives per span	Span depth	Boot drive
SHARED	RAID 1	Drives 3 and 4	2	1	False
ANALYTICS	RAID 10	Drives 5 through 10	2	3	False

Use a strip size of **65536**, the **NoReadAhead** read-ahead policy, and the **WriteThrough** write-cache policy for both virtual drives.

9. Return to **Virtual Drive Info** and verify that:
   - The **BOOT**, **SHARED**, and **ANALYTICS** virtual drives are listed.
   - The status of each virtual drive is **Optimal**.
   - **Boot Drive(s)** displays **False** for each virtual drive.

> **Note**
>
> Do not initialize the virtual drives or mark them as bootable. Fourth-Generation appliances use UEFI boot entries.

Install the Catalyst Center ISO image

Describes how to install the Catalyst Center ISO image from a bootable USB drive onto an appliance.

Complete this procedure to install the Catalyst Center ISO image onto your appliance.

Before you begin

Create the bootable USB drive from which you will install the Catalyst Center ISO image. See Create a bootable USB flash drive on page 78.

Procedure

1. Connect the bootable USB drive with the Catalyst Center ISO image to the appliance.
2. Log in to Cisco IMC and start a KVM session.
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.
4. In the window that appears, click **Yes** to acknowledge that you are about to execute a server control action.
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.
6. Select your USB drive and then press **Enter**.

   Note

   Select the **UEFI** entry for the USB drive, and then press **Enter**, if the boot menu displays multiple entries.

   Mount the drive as a removable disk.
7. In the **GNU GRUB** bootloader window, select **Catalyst Center Installer** and then press **Enter**.

   Note

   The bootloader automatically boots the Catalyst Center Installer instead if you do not make a selection within 30 seconds.

   The installer reboots and opens the wizard's welcome screen. Continue to Step 4 using the appropriate procedure according to whether you will configure a primary or secondary cluster node:
   - Configure the primary node using the Maglev wizard on page 87
   - Configure a secondary node using the Maglev wizard on page 110

Catalyst Center appliance configuration

Provides a pointer to the steps you need to complete after reimaging your Catalyst Center appliance.

When the installation of the Catalyst Center ISO image completes, the installer reboots and opens the Maglev Configuration wizard's welcome screen. To finish the reimaging of your appliance, complete the steps described in Configure the Appliance Using the Maglev Wizard on page 85.

5 Configure the Appliance Using the Maglev Wizard

Topics:

- Appliance configuration overview
- IPv4 and IPv6 considerations
- Password considerations
- VLAN mode considerations
- Configure the primary node using the Maglev wizard
- Configure a secondary node using the Maglev wizard
- Upgrade to the latest Catalyst Center release

Appliance configuration overview

Provides information about configuring appliances based on the deployment mode.

You can deploy the appliance in your network in one of these 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 select Standalone mode for your initial deployment, you can add more appliances later to form a cluster. When configuring the standalone host, ensure that you set it 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 select Cluster mode for your initial deployment, be sure to finish configuring the primary node before configuring the secondary nodes.

To continue, complete these tasks:

1. Configure the primary node in your cluster. See Configure the primary node using the Maglev wizard on page 87.
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 110.

IPv4 and IPv6 considerations

Indicates things to keep in mind regarding IPv4 and IPv6 addressing.

Understand these points about Catalyst Center and IPv4/IPv6 addressing:

- Catalyst Center does not support dual stack addressing, which is the simultaneous use of both IPv4 and IPv6 addressing.
- To switch from one addressing scheme to the other, you must Reimage the appliance.
- You cannot restore a backup file from an appliance that uses IPv4 to an appliance that uses IPv6, or vice versa.
- If your appliance uses IPv6 addressing, see the "IPv6 Limitations" section in the *Release Notes for Cisco Catalyst Center* for a description of the features that are not supported.

Password considerations

Provides pointers to the password policies and requirements for Catalyst Center.

Refer to these topics for a description of Catalyst Center's implementation of passwords.

- Password policy on page 55
- Password requirements on page 56

VLAN mode considerations

You can't use disaster recovery when VLAN mode is enabled for Catalyst Center.

Consider these details about VLAN mode:

- For a description of VLAN mode, refer to Configure the primary node using the Maglev wizard.

- VLAN mode:
  - Can only be enabled when you configure a Catalyst Center appliance using the Maglev Configuration wizard.
  - Cannot be enabled using any of the browser-based configuration wizards.
  - Cannot be disabled without reimaging the appliance.
- Disaster recovery is not supported by Catalyst Center deployments that have VLAN mode enabled.

Configure the primary node using the Maglev wizard

You can set up the first appliance in a cluster using the Maglev Configuration wizard.

Do 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 110 instead.

Important

- Verify that all of the IP addresses you enter while completing this procedure are valid addresses with valid netmasks. Also verify that the addresses and their corresponding subnets do not overlap. Service communication issues can result if they do.
- Before configuring the appliances in a three-node cluster, log out of those appliances. If you remain logged in, the Quick Start workflow—which you use to discover network devices and enable telemetry—does not start after you configure your cluster's appliances and log in to Catalyst Center for the first time.

Before you begin

Ensure that you have done these prerequisites:

- Collected all of the information specified in Required IP addresses and subnets on page 31 and Required configuration information on page 53.
- Installed the first appliance, as described in Appliance installation workflow on page 58.
- Configured Cisco IMC browser access on the primary node, as described in Enable browser access to the Cisco Integrated Management Controller on page 66.
- Checked that the ports of the primary node appliance, and the switches they use, are properly configured, as described in Execute preconfiguration tasks on page 71.
- Confirmed that you are using a compatible browser. For a list of compatible browsers, see the Release Notes document for the release of Catalyst Center you are installing.
- Enabled ICMP on the firewall between Catalyst Center and both the default gateway and the DNS server you specify in this procedure. The Maglev Configuration wizard uses ping to verify the gateway and DNS server you specify.

> **Caution**
>
> If ICMP is not enabled and a firewall is in place, the ping may be blocked, which will prevent you from completing the wizard.

Procedure

1. Point your browser to the Cisco IMC IP address you set during the Cisco IMC GUI configuration you did, and log in to the Cisco IMC GUI as the Cisco IMC user (refer to Enable browser access to the Cisco Integrated Management Controller on page 66).

   After you log in, the appliance displays the **Cisco Integrated Management Controller Chassis Summary** window with a hyperlinked menu at the top.

2. From the hyperlinked menu, select **Launch KVM** and then select **HTML-based KVM**.

   The KVM console opens in a separate window or tab automatically. Use it to monitor the progress of the configuration and respond to the Maglev Configuration wizard prompts.

3. With the KVM displayed, reboot the appliance by making one of these 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)**.

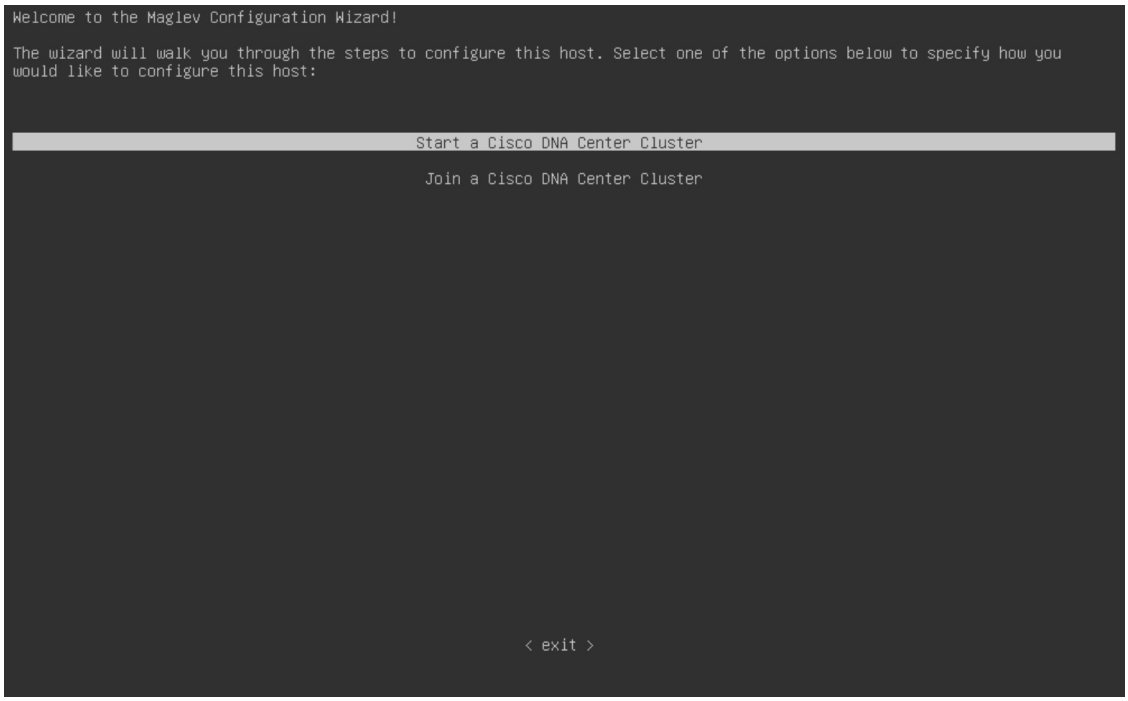
   If you are asked to confirm your choice to reboot the appliance, click **OK**.

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



4. Click **Skip**.

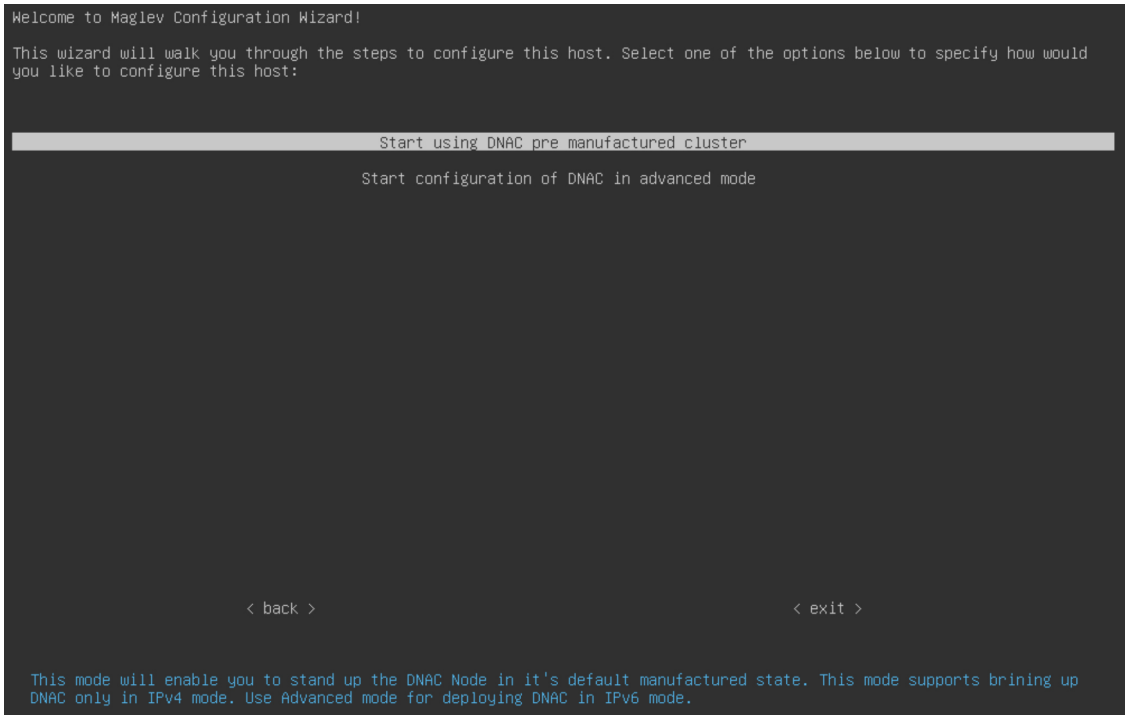
   The KVM console displays the Maglev Configuration wizard welcome screen.



> **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.

5. Click **Start a Catalyst Center Cluster** to begin configuring the primary node.

   The screen updates.



6. Select one of these options:

   - **Start using DNAC pre manufactured cluster**: Select 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: **P@ssword9**

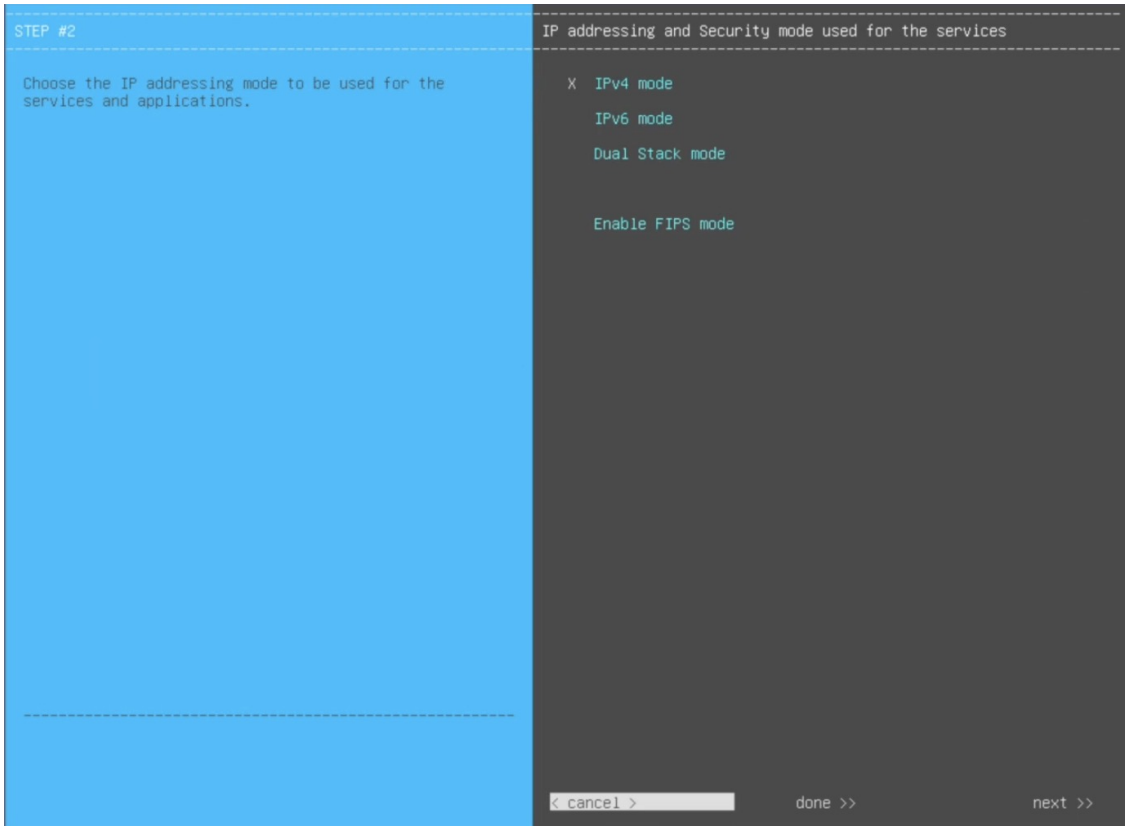
     You will *not* be able to change any of these settings, so select this option only if you want to use them.

     Important

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

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

   The screen updates.



7. Do these steps, then click **next>>** to continue:
   a) Specify whether the applications and services running on your Catalyst Center appliance will use IPv4 or IPv6 addressing.
   b) Optional: Check the **Enable FIPS Mode** check box to enable FIPS mode on your Catalyst Center appliance.

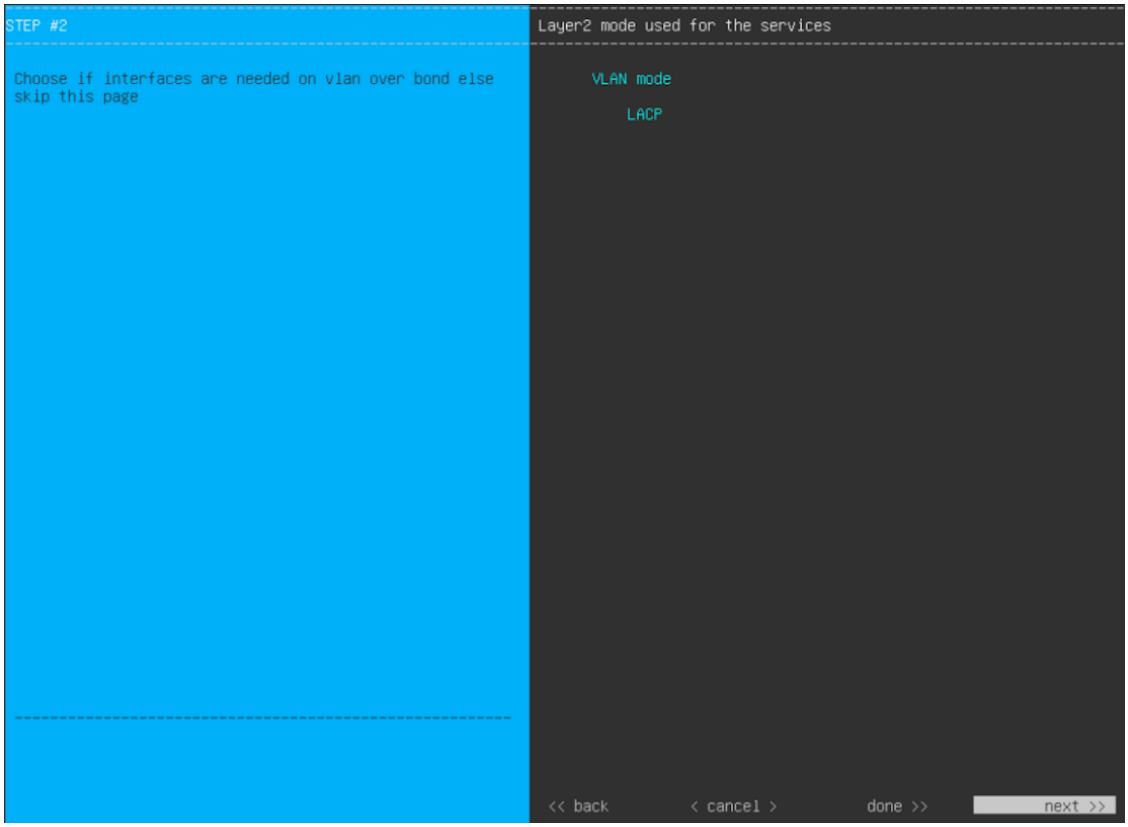
      Refer to FIPS mode support on page 109 for things to keep in mind when enabling FIPS mode on an appliance.

   Important

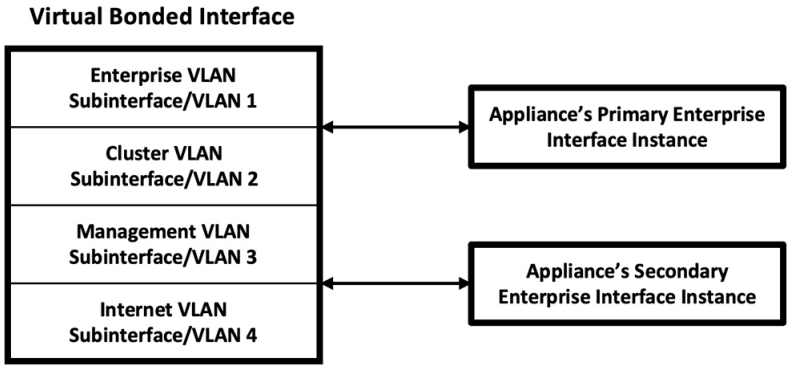
   In the next wizard screen, you can enable the **VLAN mode** feature, which creates a single bonded interface that connects to your network using both the primary and secondary instance of your appliance's Enterprise interface. This feature is not commonly used. Enable it only if your Catalyst Center deployment requires it.

   - If this is the case, complete the next step.
   - Otherwise, click **next>>** in the next wizard screen without making any selections. You can enable the NIC bonding functionality that was described previously in this guide in the wizard's Enterprise and Intracluster interface configuration screens.

8. (Optional) Follow the onscreen instructions to enable Layer 2 port channel mode (with VLAN tagging) for the appliance. After making your selections, click **next>>** to continue.



a) Select 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 this figure). By default, this interface operates in Active-Backup mode (which enables HA).



b) If you want this interface to operate in LACP mode instead (which enables load balancing and higher bandwidth), you must also select 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

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 this order:

a. (Required) 10 Gbps Enterprise port–network adapter #1

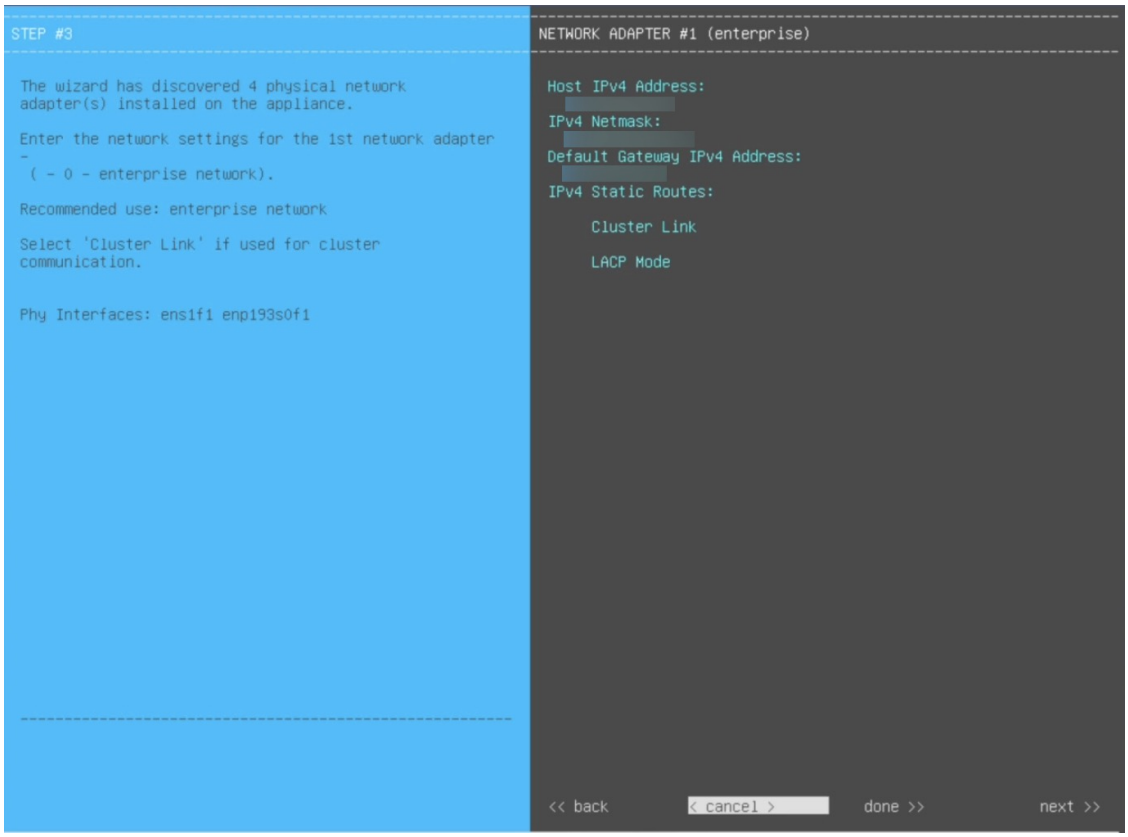
b. (Required) 10 Gbps Cluster port–network adapter #2

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 Catalyst Center functionality. If you discover that they are nonfunctional, select **cancel** to exit the configuration wizard immediately. Be sure that you have completed all of the steps provided in Execute preconfiguration tasks on page 71 before resuming the configuration or contacting the Cisco Technical Assistance Center.

9. The wizard first presents the 10 Gbps Enterprise port as **NETWORK ADAPTER #1**. As explained in Interface cable connections on page 28, 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 (refer to Required IP addresses and subnets on page 31 and Required configuration information on page 53 for the values to enter).



This table lists the configuration values for **NETWORK ADAPTER #1** to enter.

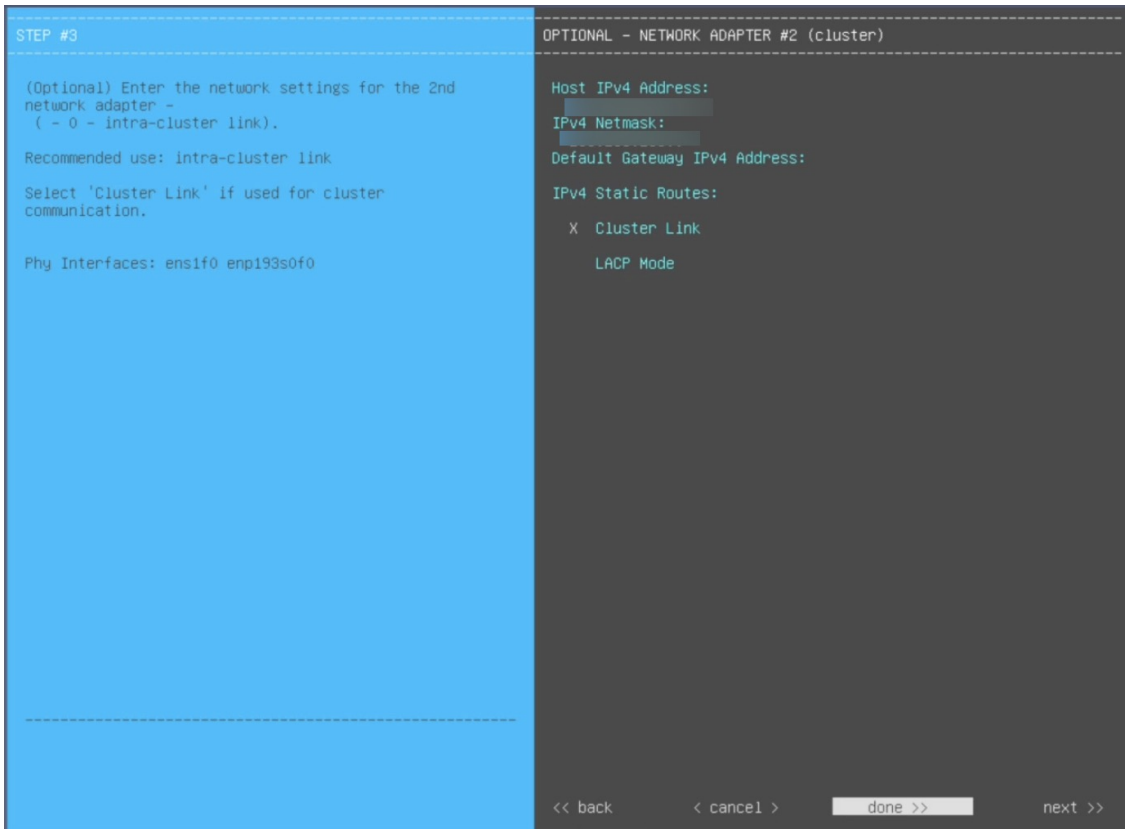
Table 22: Primary node entries for network adapter #1: 10 Gbps Enterprise port

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 these tasks: • If you selected IPv4 addressing, enter the netmask for the port's IP address. This is required. • If you selected IPv6 addressing, enter the prefix length (in bits). Valid values range from 10 through 127.

Default Gateway IPv4/IPv6 Address field	Enter a default gateway IP address to use for the port. **Important** 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. **Important** 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 this format, separated by spaces: *<network>/<netmask>/<gateway>*. This is usually required on the Catalyst 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	Do one of these tasks: • Leave this field blank and the port will operate in **Active-Backup** 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. • Check the check box to enable **LACP** 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. For more information about Catalyst Center's implementation of NIC bonding, refer to NIC bonding overview on page 74. **Note** This field is displayed if you didn't select any of the options in the previous step.

After you finish entering the configuration values, click **next>>** to continue. 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.

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 on page 28, 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 (refer to Required IP addresses and subnets on page 31 and Required configuration information on page 53 for the values to enter).



This table lists the configuration values for **NETWORK ADAPTER #2** to enter.

Table 23: Primary 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. You cannot change the address of the Cluster port later. **Note** If you selected the **Start using DNAC pre manufactured cluster** option previously, **169.254.6.66** will already be set in this field and you will not be able to enter a different address.
IPv4 Netmask/IPv6 Prefix Length field	Do one of these tasks: • If you selected IPv4 addressing, enter the netmask for the port's IP address. This is required. **Note** If you selected the **Start using DNAC pre manufactured cluster** option previously, **255.255.255.128** will already be set in this field and you will not be able to enter a different netmask. • If you selected IPv6 addressing, enter the prefix length (in bits). Valid values range from 10 through 127.
Default Gateway IPv4/IPv6 address field	Enter a default gateway IP address to use for the port. **Important** 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. **Important** 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 this format, separated by spaces: <*network*>/<*netmask*>/<*gateway*>. This is usually required on the Management port only.

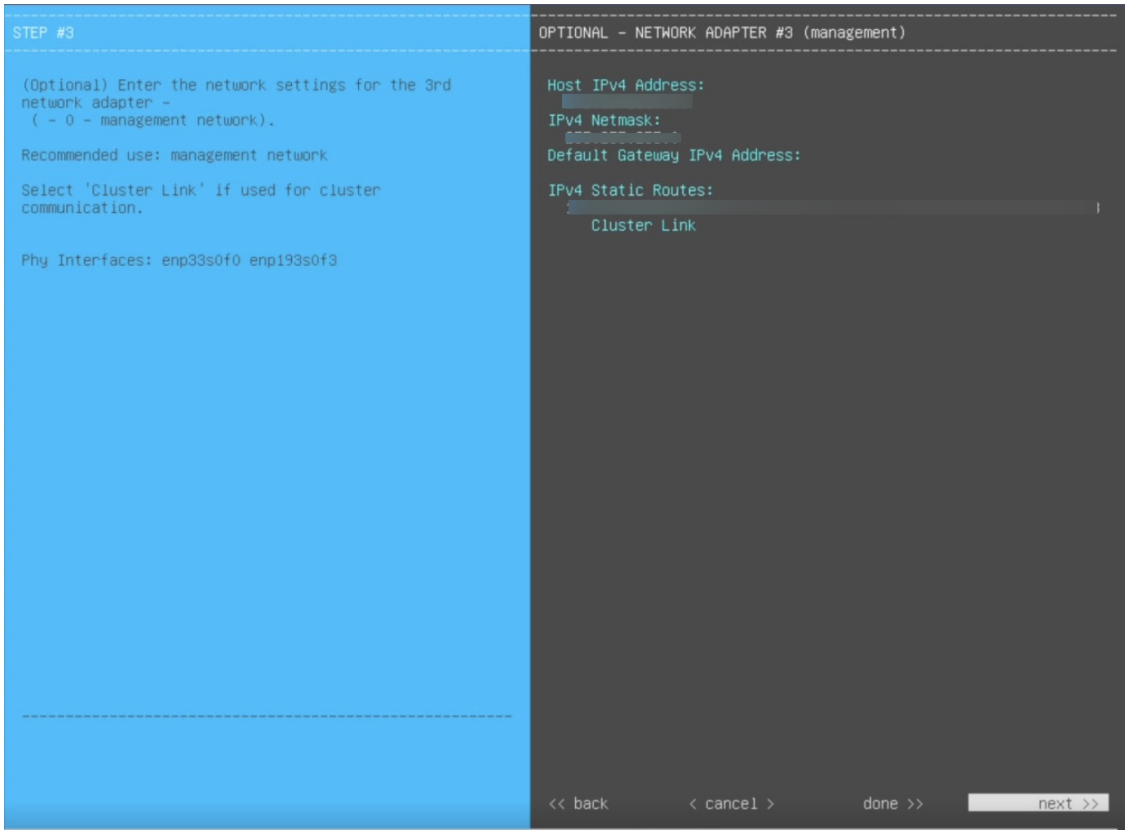
Cluster Link field	Check the check box to set this port as the link to a Catalyst Center cluster. This is required on the Cluster port only.
LACP Mode field	Do one of these tasks: • Leave this field blank and the port will operate in **Active-Backup** mode. This mode provides fault tolerance by aggregating 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. • Check the check box to enable **LACP** 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. For more information about Catalyst Center's implementation of NIC bonding, refer to NIC bonding overview on page 74.

Note

- This field is displayed if you didn't select any of the options in Step 8.
- You can only enable LACP mode on your appliance's Intracluster interface during the initial configuration of your appliance.

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

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 on page 28, this port is used to access the Catalyst Center GUI from your management network. Apply the host IP address, netmask, and other values that are appropriate for this purpose (refer to Required IP addresses and subnets on page 31 and Required configuration information on page 53 for the values to enter).



This table lists the configuration values for **NETWORK ADAPTER #3** to enter.

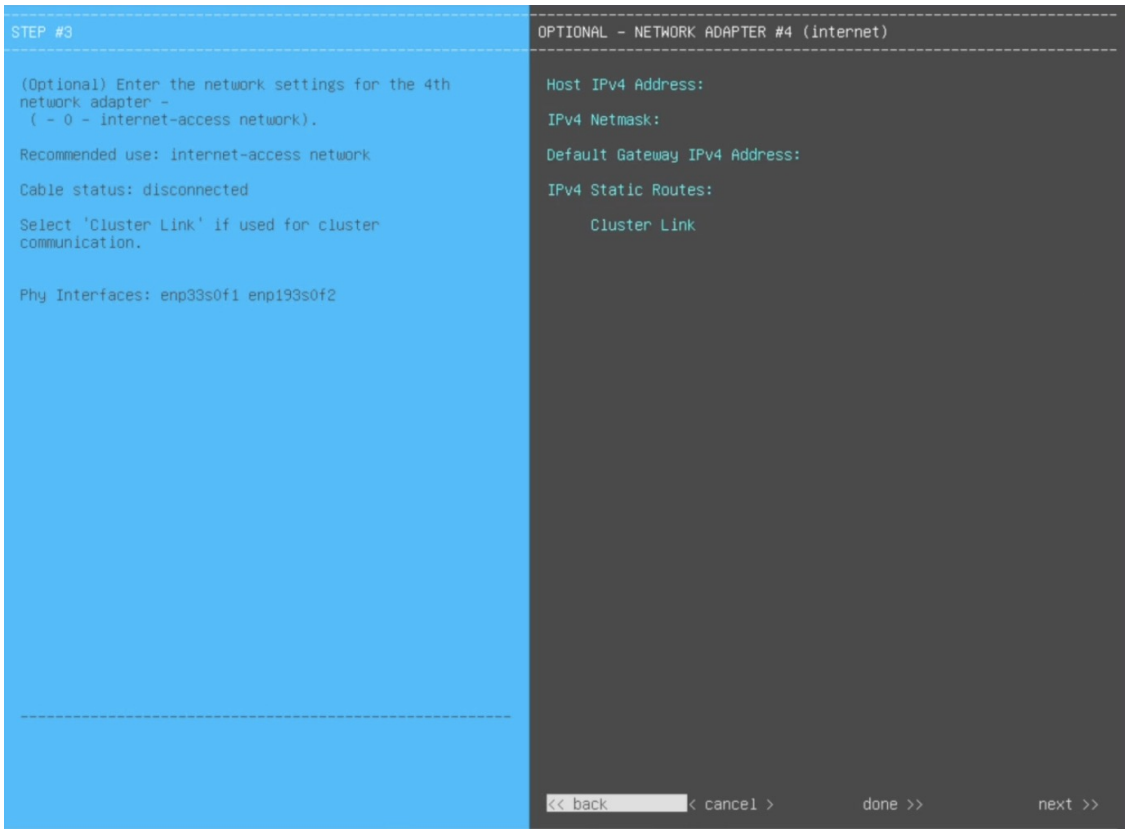
After you provide the necessary information, click **next>>** to continue. Correct validation errors, if any, as you did in previous screens. The wizard validates and applies your network adapter configurations.

Table 24: 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 Catalyst Center GUI from your management network; otherwise, you can leave it blank.
IPv4 Netmask/IPv6 Prefix Length field	Do one of these tasks if you entered an IP address: • If you selected IPv4 addressing, enter the netmask for the port's IP address. This is required. • If you selected IPv6 addressing, enter the prefix length (in bits). Valid values range from 10 through 127.
Default Gateway IPv4/IPv6 address field	Enter a default gateway IP address to use for the port. **Important** 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. **Important** • For NTP, ensure port 123 (UDP) is open between Catalyst Center and your NTP server. • 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 this format, separated by spaces: *<network>/<netmask>/<gateway>*.
Cluster Link field	Leave this field blank. It is required on the Cluster port only.

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 on page 28, 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 (refer to Required IP addresses and subnets on page 31 and Required configuration information on page 53 for the values to enter).



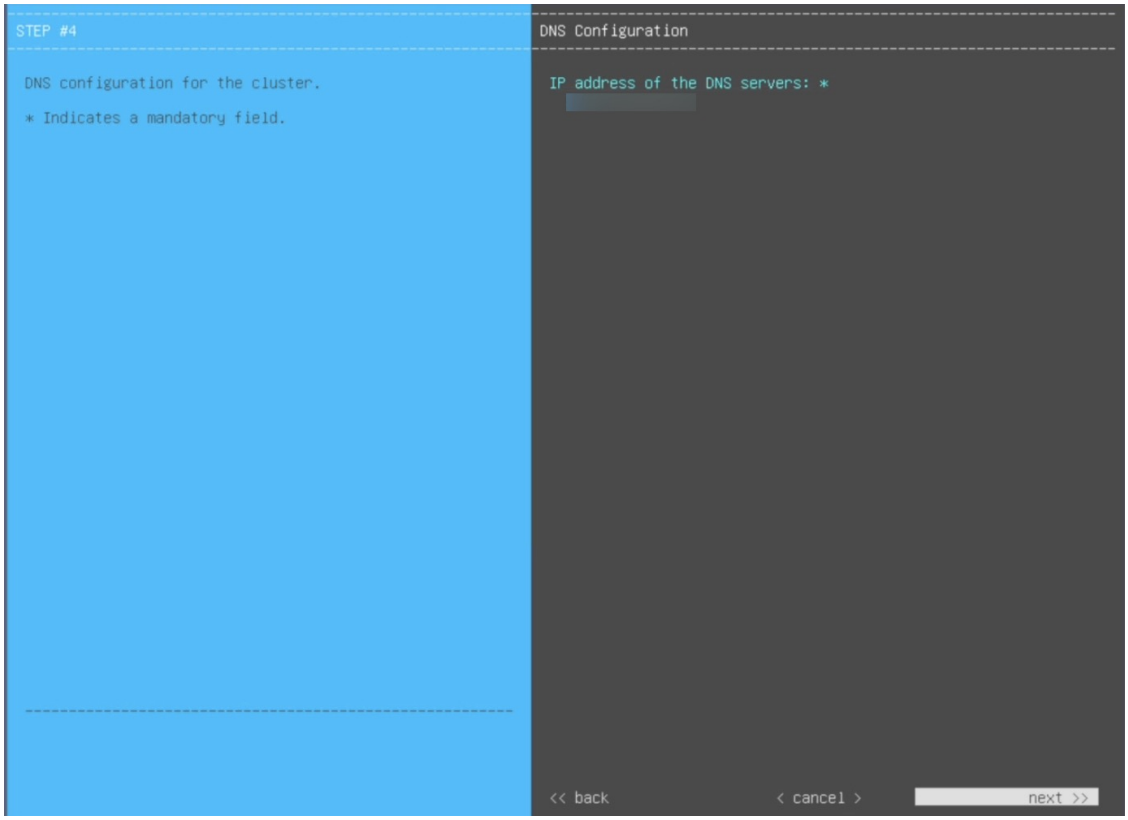
This table lists the configuration values for **NETWORK ADAPTER #4** to enter.

Table 25: 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 these tasks if you entered an IP address: • If you selected IPv4 addressing, enter the netmask for the port's IP address. This is required. • If you selected IPv6 addressing, enter the prefix length (in bits). Valid values range from 10 through 127.
Default Gateway IPv4/IPv6 address field	Enter a default gateway IP address to use for the Internet port. **Important** 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. **Important** 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 this format, separated by spaces: <*network*>/<*netmask*>/<*gateway*>. 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 continue. Correct validation errors, if any, as you did in previous screens. The wizard validates and applies your network adapter configurations.

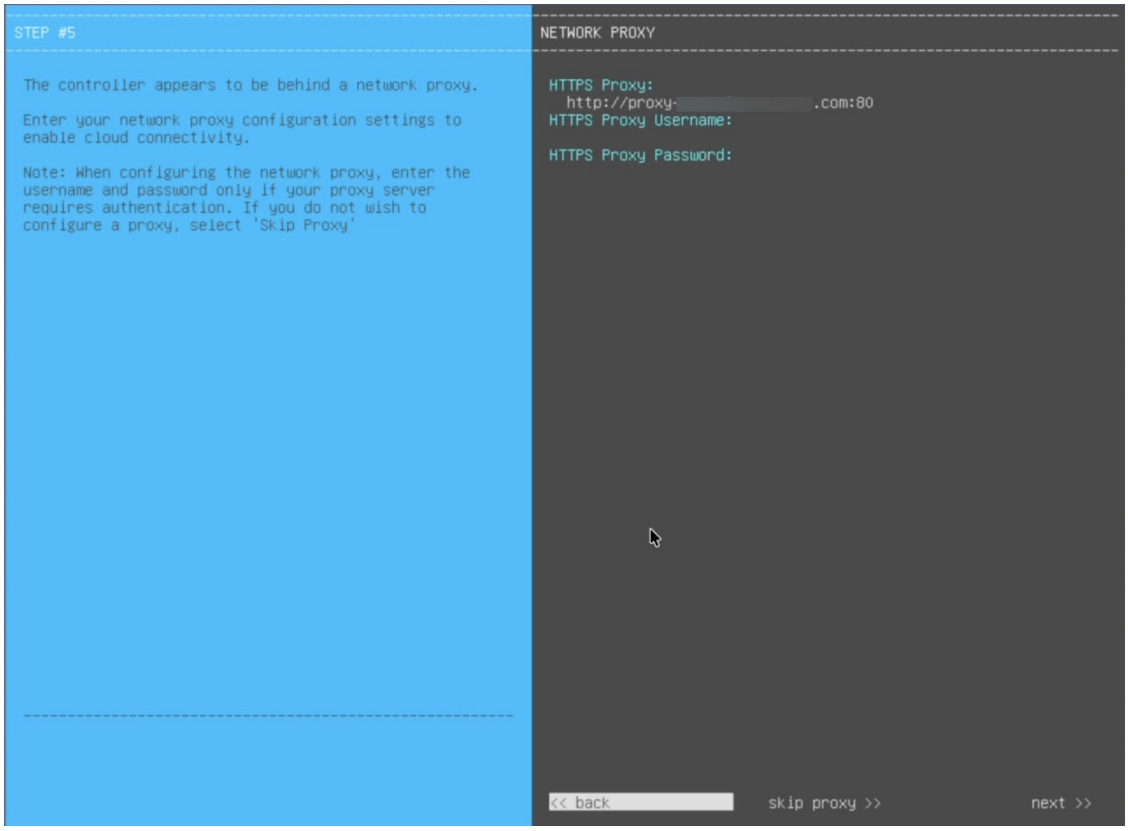
13. After the network adapter configuration is complete, the wizard prompts you to enter the IP address of the **DNS** server that you are using, as shown.



Note

If you plan to enable dual-stack mode for your Catalyst Center appliance, ensure that your DNS server supports both IPv4 and IPv6.

14. After DNS server configuration is complete, the wizard prompts you to enter configuration values for the **NETWORK PROXY** that you are using, as shown.



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

Table 26: Primary node entries for network proxy

HTTPS Proxy field	Enter the URL or host name of an HTTPS network proxy used to access the Internet. **Note** • Connection from Catalyst Center to the HTTPS proxy is supported only through HTTP in this release. • 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/
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 continue. Correct validation errors, if any, as you did in previous screens.

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



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 continue to the next step.

Important

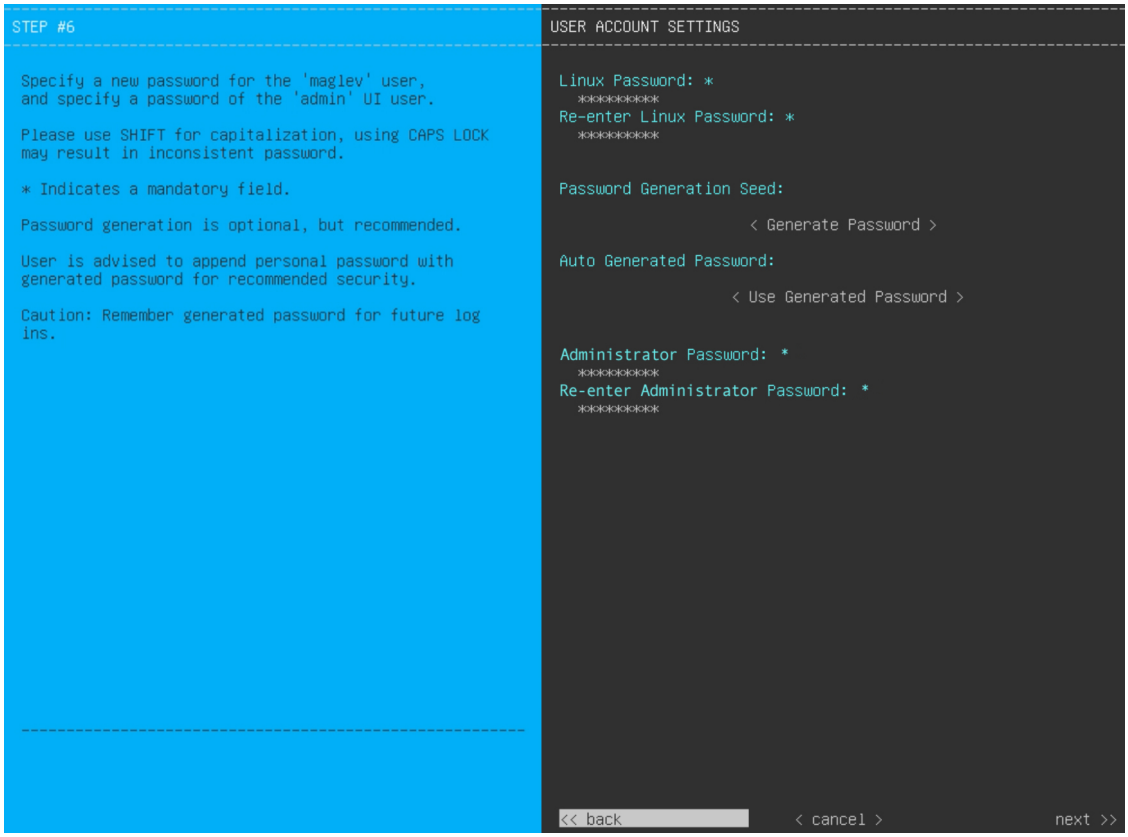
You must enter one virtual IP address for each configured network interface. You will not be able to complete the wizard unless you do so. These addresses are tied to the cluster link's status, which must be in the **UP** state.

You can also specify a fully qualified domain name (FQDN) for your cluster. Catalyst Center uses this domain name to do these tasks:

- 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 Catalyst Center manages.
- In the Subject Alternative Name (SAN) field of Catalyst Center certificates, the FQDN defines the Plug and Play server used for device provisioning.

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

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



This table lists the configuration values for **USER ACCOUNT SETTINGS** to enter.

Table 27: Primary node entries for user account settings

Linux Password field	Enter a Linux password for the maglev user that complies with the Password requirements on page 56.
Re-enter Linux Password field	Confirm the Linux password by entering it a second time.
Password Generation Seed field	To generate a Linux password automatically, enter a seed phrase in this field and then press <**Generate Password**>.
Auto Generated Password field	(Optional) The generated password includes the seed phrase. You may use this password or edit the auto-generated password. Press <**Use Generated Password**> to save the password.

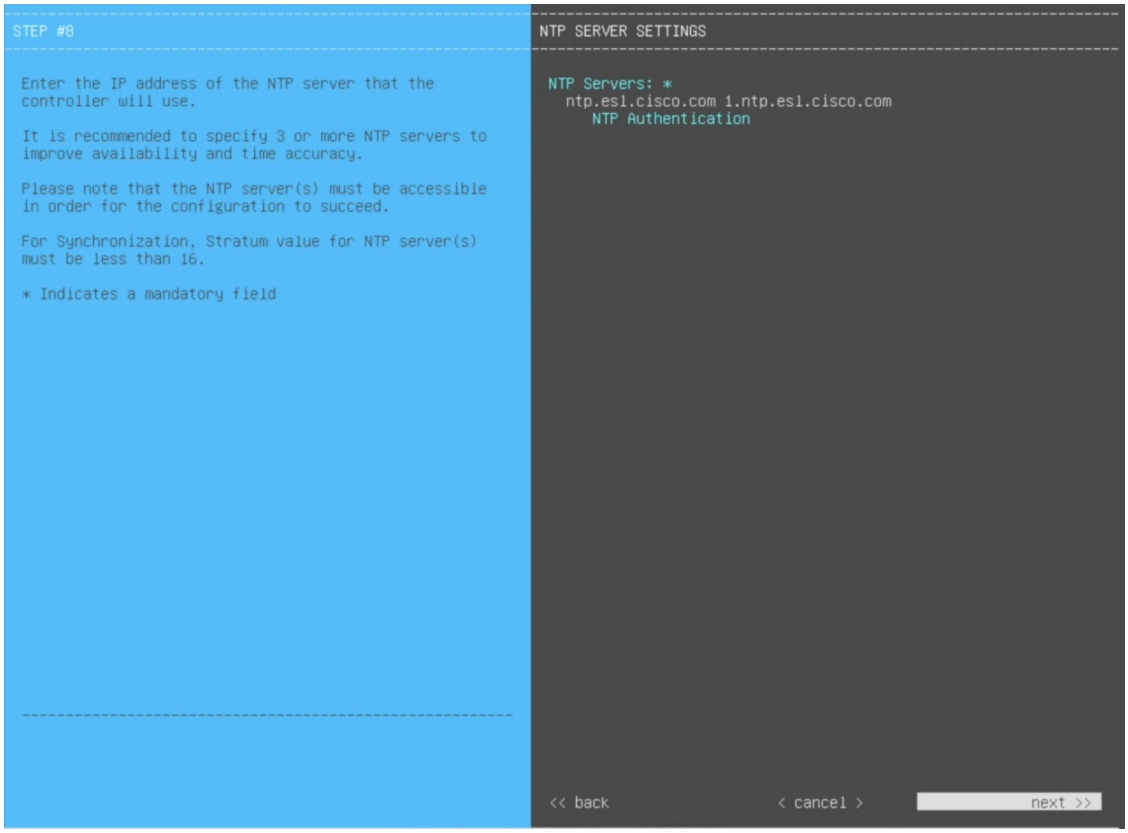
Administrator Password field	Enter a password for the default admin superuser, used to log in to Catalyst Center for the first time. Ensure that this password complies with the Password requirements on page 56.

> **Note**
>
> If you select the **Start using DNAC pre manufactured cluster** option previously, the default password (**P@ssword9**) has already been set for the appliance and cannot be changed in the configuration wizard. As a result, this and the next field are not displayed in this screen.

Re-enter Administrator Password field	Confirm the administrator password by entering it a second time.

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

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



This table lists the configuration values for **NTP SERVER SETTINGS** to enter.

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	To enable the authentication of your NTP server before it's synchronized with Catalyst Center, check this check box and then enter this information: • The NTP server's key ID. Valid values range between 1 and 4294967295 (2^32-1). This value corresponds to the key ID that's defined in the NTP server's key file. • 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.

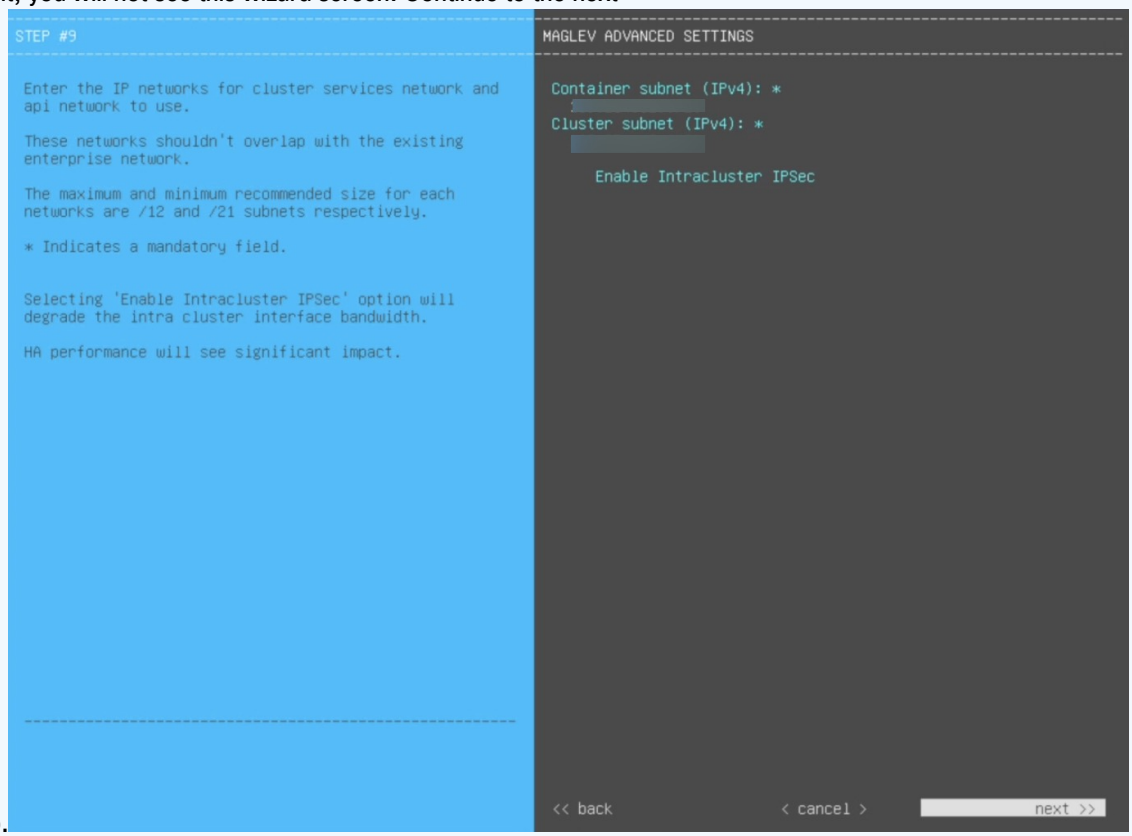
> **Note**
>
> Ensure that you enter a key ID and key value for each NTP server that you configured in the previous field.

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

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

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 this wizard screen. Continue to the next step.



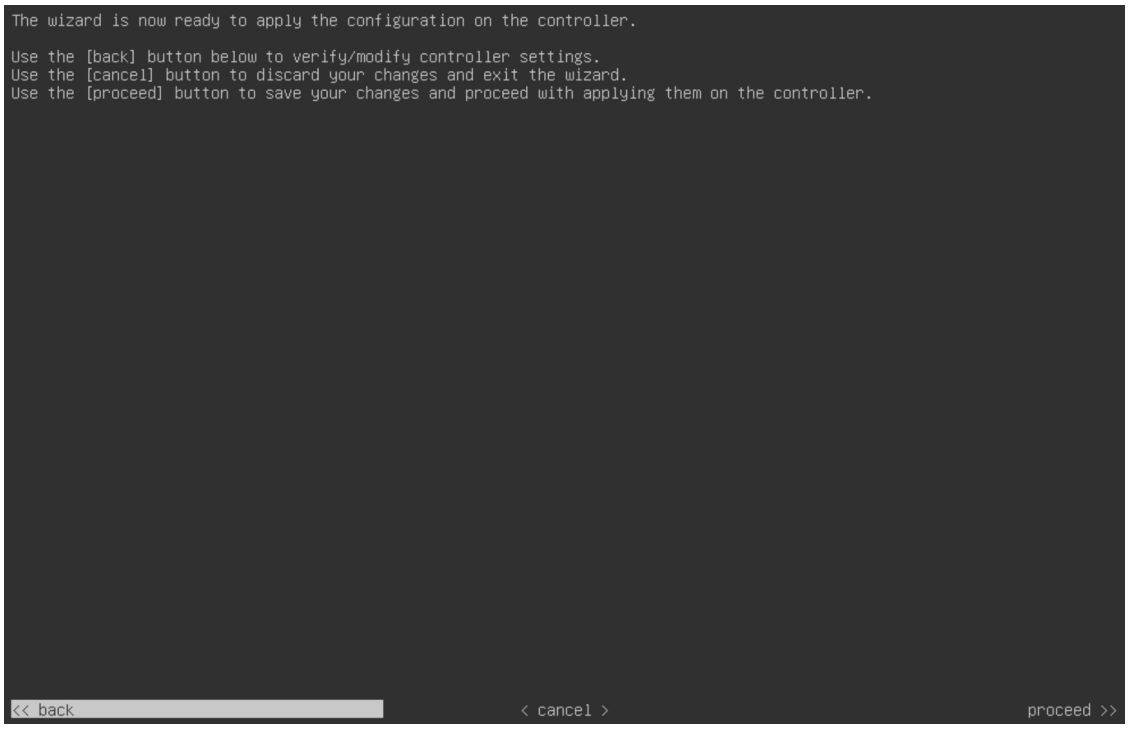
This table lists the configuration values for **MAGLEV ADVANCED SETTINGS** to enter.

Table 28: Primary node entries for Maglev advanced settings

Container Subnet field	A dedicated, non-routed IP subnet that Catalyst Center uses to manage internal services. By default, this is already set to **169.254.32.0/20**, and we recommend that you use this subnet. If you decide to enter another subnet, ensure that it does not conflict with or overlap any other subnet used by the Catalyst Center internal network or an external network. For more information, see the Container Subnet description in Required IP addresses and subnets on page 31.
Cluster Subnet field	A dedicated, non-routed IP subnet that Catalyst 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. If you decide to enter another subnet, ensure that it does not conflict with or overlap any other subnet used by the Catalyst Center internal network or an external network. For more information, see the Cluster Subnet description in Required IP addresses and subnets on page 31.
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 continue. Correct validation errors, if any, as you did in previous screens.

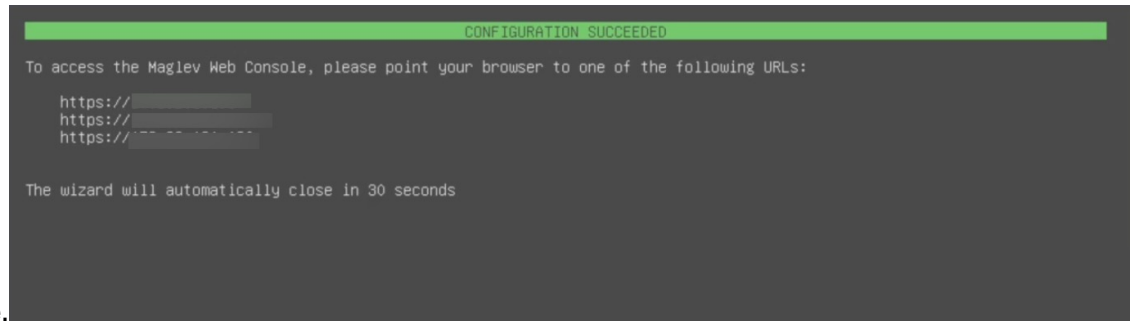
19. After you have entered the Maglev advanced settings, a final message appears, stating that the wizard is ready to apply the configuration (as shown).



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 using the KVM console.

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



What to do next

- If you are deploying this appliance in standalone mode only, do the first-time setup: First-time setup workflow on page 178.
- 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 110.

FIPS mode support

Indicates points to keep in mind when FIPS mode is enabled on an appliance.

Catalyst 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. Understand these 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 Catalyst 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.
- In the **USER ACCOUNT SETTINGS** screen, you will need to enter a password for the default admin superuser that complies with the Password requirements on page 56.
- When FIPS mode is enabled on an appliance, you cannot enable external authentication.
- A backup can only be restored on a Catalyst Center cluster that has the same FIPS mode setting configured as the source cluster. Backup and restore operations involving clusters with different FIPS mode settings will fail (since Catalyst Center will label backups as incompatible).
- If you selected the **Start using DNAC pre manufactured cluster** option while completing the Maglev Configuration wizard, the **IP addressing and Security mode used for the services** screen does not appear. You cannot enable FIPS mode in this scenario.
- Catalyst 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, which erases all existing data. You can then reconfigure the appliance with FIPS mode disabled. See Reimage the appliance for more information.
- When FIPS mode is enabled, you can enable KeyWrap only if Catalyst Center and Cisco ISE have not been integrated. See Configure authentication and policy servers on page 198 for more information.
- After configuring your appliance, do these steps 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 Catalyst Center GUI or CLI.
- When FIPS mode is enabled, some of the functions related to Endpoint Analytics are unavailable in the Catalyst 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

You can add additional appliances to a cluster using the Maglev Configuration wizard.

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

Important

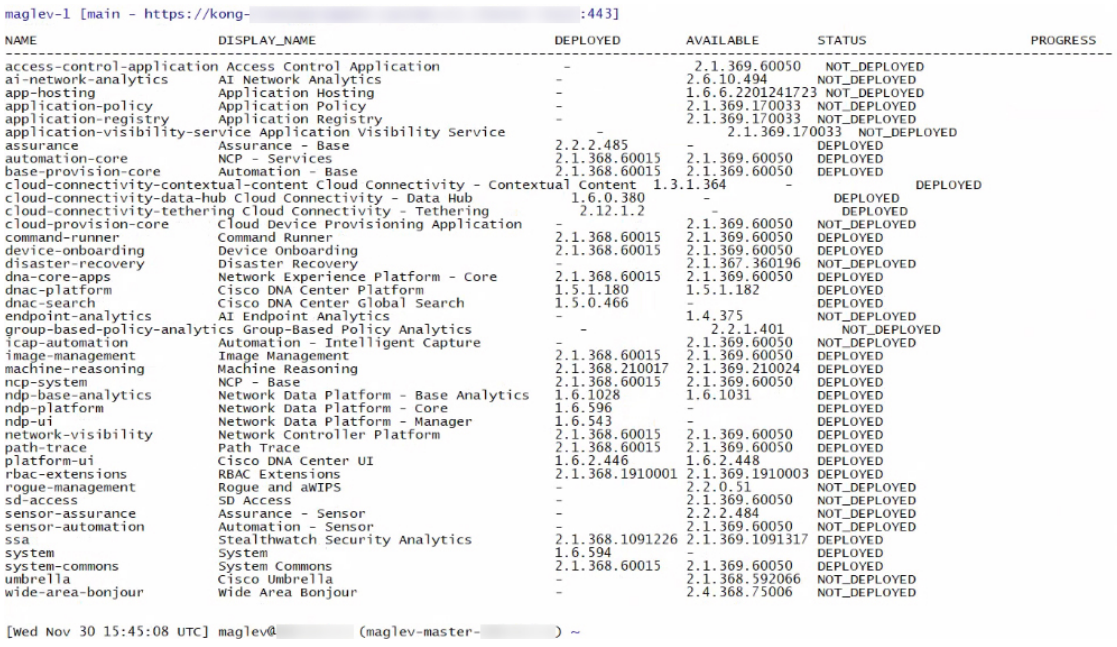
- In order to build a three-node cluster, the same version of the **System** package must be installed on your three Catalyst Center appliances. Otherwise, unexpected behavior and possible downtime can occur.
- Before you configure the appliances in a three-node cluster, ensure that you have logged out 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 Catalyst Center for the first time.
- Ensure that all of the IP addresses you enter while completing this procedure are valid addresses with valid 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 physical IP address of the cluster link of the first host in the cluster.

If you are replacing a node in an HA-enabled cluster, use the physical IP address of the cluster link of either of the remaining nodes.

When joining secondary nodes to a cluster, understand:

- 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 Catalyst 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`.



```
maglev-1 [main - https://kong-                                    :443]

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

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

- 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 according to the steps in Configure the primary node using the Maglev wizard on page 87.
- Collected all of the information specified in Required IP addresses and subnets on page 31 and Required configuration information on page 53.
- Installed the second and third appliances, as described in Appliance installation workflow on page 58.
- Have done these steps:
  1. Ran the **maglev package status** command on the first appliance.

     You can also access this information from the Catalyst 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 the Cisco Integrated Management Controller on page 66.
- Checked that both the secondary appliances' ports and the switches they use are properly configured (as described in Execute preconfiguration tasks on page 71).
- Confirmed that you are using a compatible browser. For a list of compatible browsers, see the Release Notes document for the version of Catalyst Center you are installing.
- Enabled ICMP on the firewall between Catalyst Center and both the default gateway and the DNS server you specify in this procedure. The Maglev Configuration wizard uses ping to verify the gateway and DNS server you specify.

> **Caution**
>
> 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.

Procedure

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 (refer to Enable browser access to the Cisco Integrated Management Controller on page 66).

   After successful login, the appliance displays the **Cisco Integrated Management Controller Chassis Summary** window, with a hyperlinked menu at the top of the window.
2. From the hyperlinked menu, select **Launch KVM** and then select **HTML based KVM**.

   The KVM console opens in a separate window or tab automatically. Use it to monitor the progress of the configuration and respond to the Maglev Configuration wizard prompts.
3. With the KVM displayed, reboot the appliance by selecting one of these 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.



4. Click **Skip**.

   The KVM console displays the Maglev Configuration wizard welcome screen.

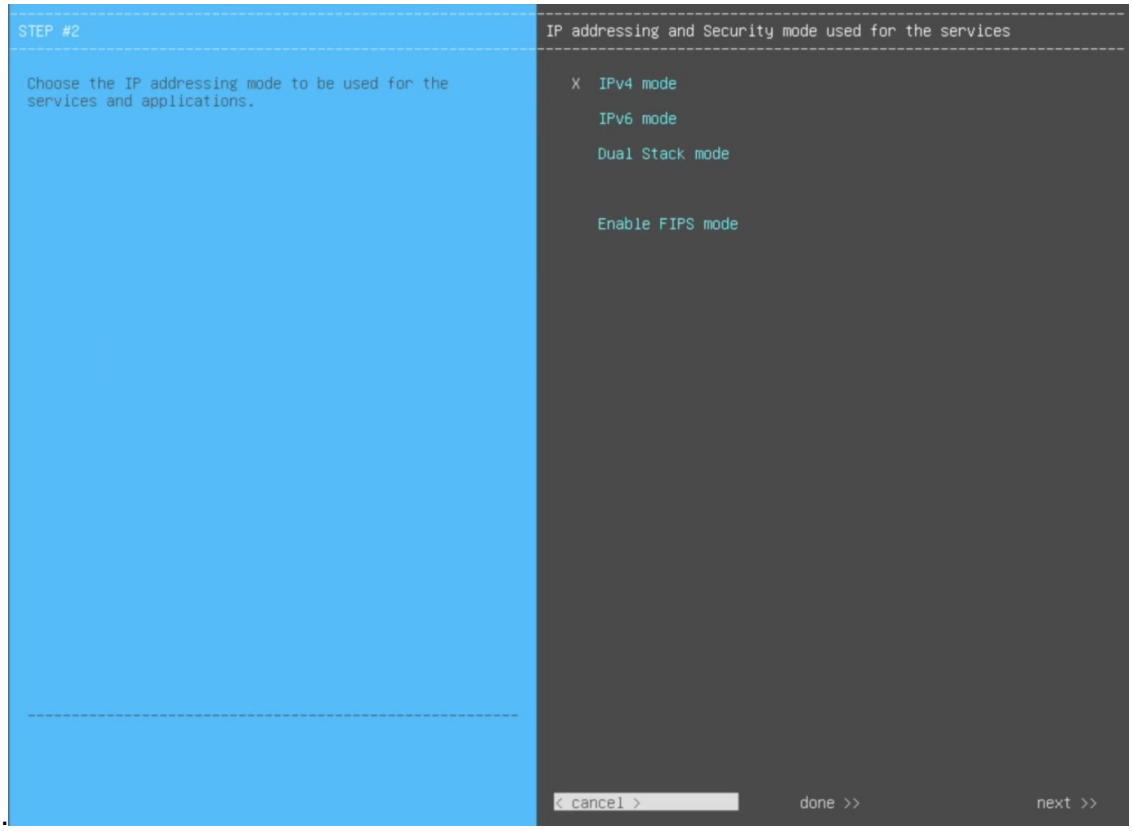


Note

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.

5. Click **Join a Catalyst Center Cluster** to begin configuring the secondary node.

The screen updates.



6. Do these steps, then click **next>>** to continue:
   a) Specify whether the applications and services running on your Catalyst Center appliance will use IPv4 or IPv6 addressing.
   b) Optional: Check the **Enable FIPS Mode** check box to enable FIPS mode on your Catalyst Center appliance.

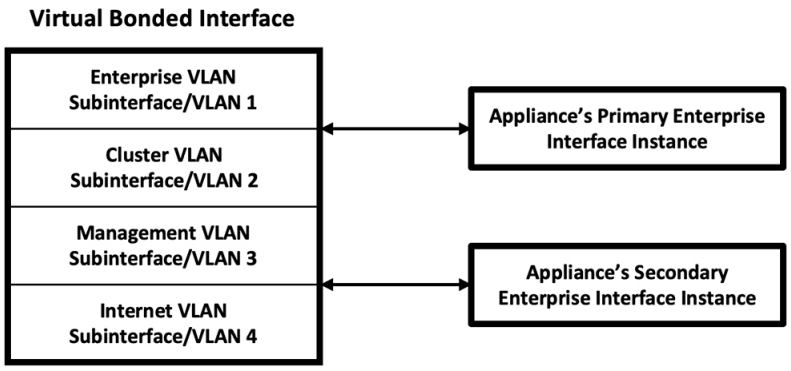
      Refer to FIPS mode support on page 109 for things to keep in mind when enabling FIPS mode on an appliance.

   Important

   In the next wizard screen, you can enable the **VLAN mode** feature, which creates a single bonded interface that connects to your network using both the primary and secondary instance of your appliance's Enterprise interface. This feature is not commonly used, so only enable it if you know it's required by your Catalyst Center deployment.

   - If this is the case, complete the next step.
   - Otherwise, click **next>>** in the next wizard screen without making any selections. You can enable the NIC bonding functionality that was described previously in this guide in the wizard's Enterprise and Intracluster interface configuration screens.

7. (Optional) Do these steps to enable Layer 2 port channel mode (with VLAN tagging) for the appliance. After making your selections, click **next>>** to continue.
   a) Select 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 this figure). By default, this interface operates in Active-Backup mode (which enables HA).



b) If you want this interface to operate in LACP mode instead (which enables load balancing and higher bandwidth), you must also select 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

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 this order:

a. (Required) 10-Gbps Enterprise port–network adapter #1

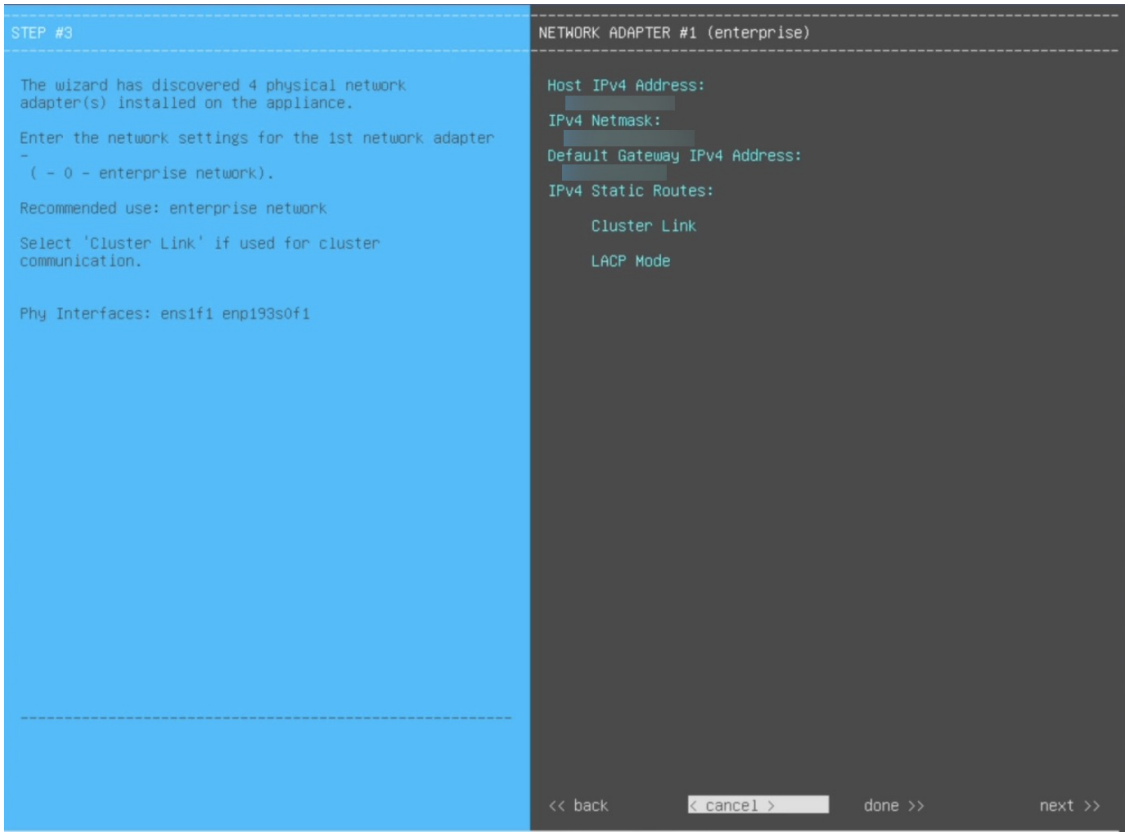
b. (Required) 10-Gbps Cluster port–network adapter #2

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 Catalyst Center functionality. If you discover that they are nonfunctional, select **cancel** to exit the configuration wizard immediately. Be sure that you have completed all of the steps provided in Execute preconfiguration tasks on page 71 before resuming the configuration or contacting the Cisco Technical Assistance Center.

8. The wizard first presents the 10-Gbps Enterprise port as **NETWORK ADAPTER #1**. As explained in Interface cable connections on page 28, 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 (refer to Required IP addresses and subnets on page 31 and Required configuration information on page 53 for the values to enter).



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

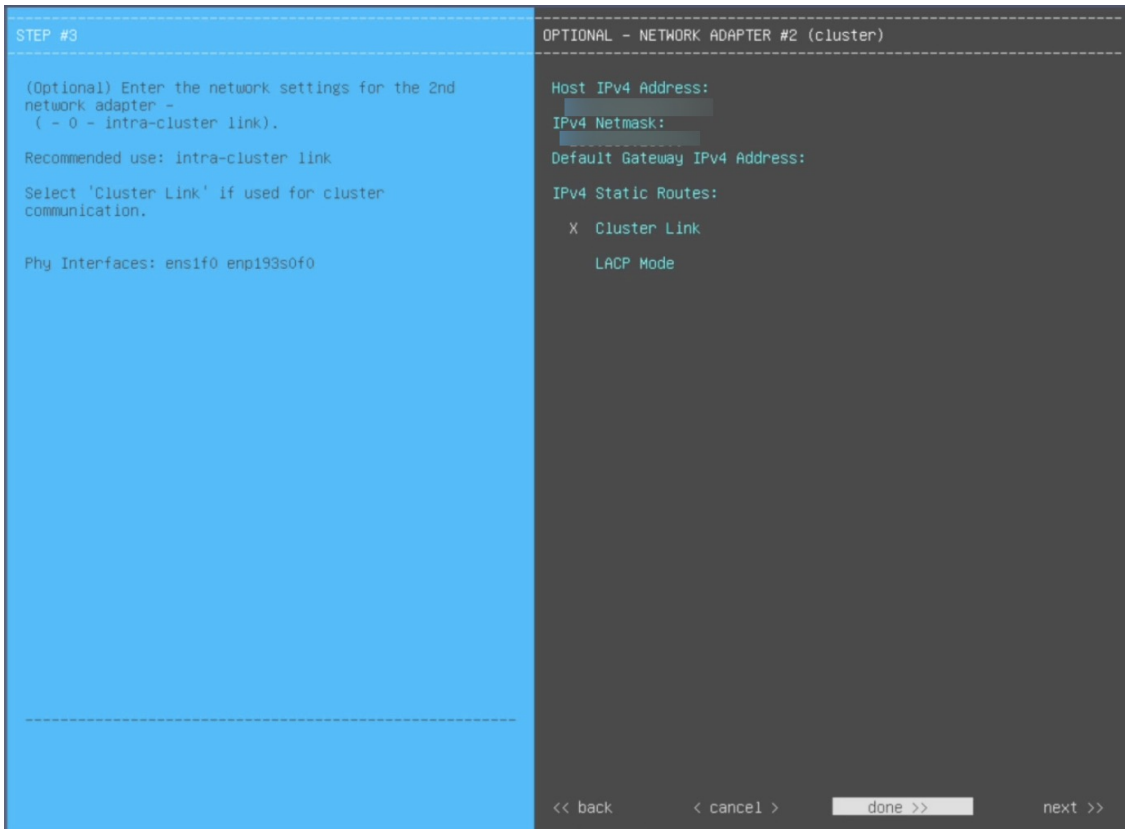
Table 29: Secondary node entries for network adapter #1: 10 Gbps Enterprise port

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 these tasks if you entered an IP address: • If you selected IPv4 addressing, enter the netmask for the port's IP address. This is required. • If you selected IPv6 addressing, enter the prefix length (in bits). Valid values range from 10 through 127.
Default Gateway IPv4/IPv6 address field	Enter a default gateway IP address to use for the port. **Important** 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. **Important** 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 this format, separated by spaces: *<network>/<netmask>/<gateway>*. This is usually required on the Catalyst 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. **Note** This field is displayed only if you set the Layer 2 LACP port channel 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 these tasks: • Leave this field blank and the port will operate in **Active-Backup** 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. • Check the check box to enable **LACP** 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. For more information about Catalyst Center's implementation of NIC bonding, refer to NIC bonding overview on page 74. **Note** This field is displayed if you didn't select any of the options in the previous step.

After you finish entering the configuration values, click **next>>** to continue. 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.

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 on page 28, 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 (refer to Required IP addresses and subnets on page 31 and Required configuration information on page 53 for the values to enter).



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

Table 30: Secondary node entries for network adapter #2: 10 Gbps Cluster port

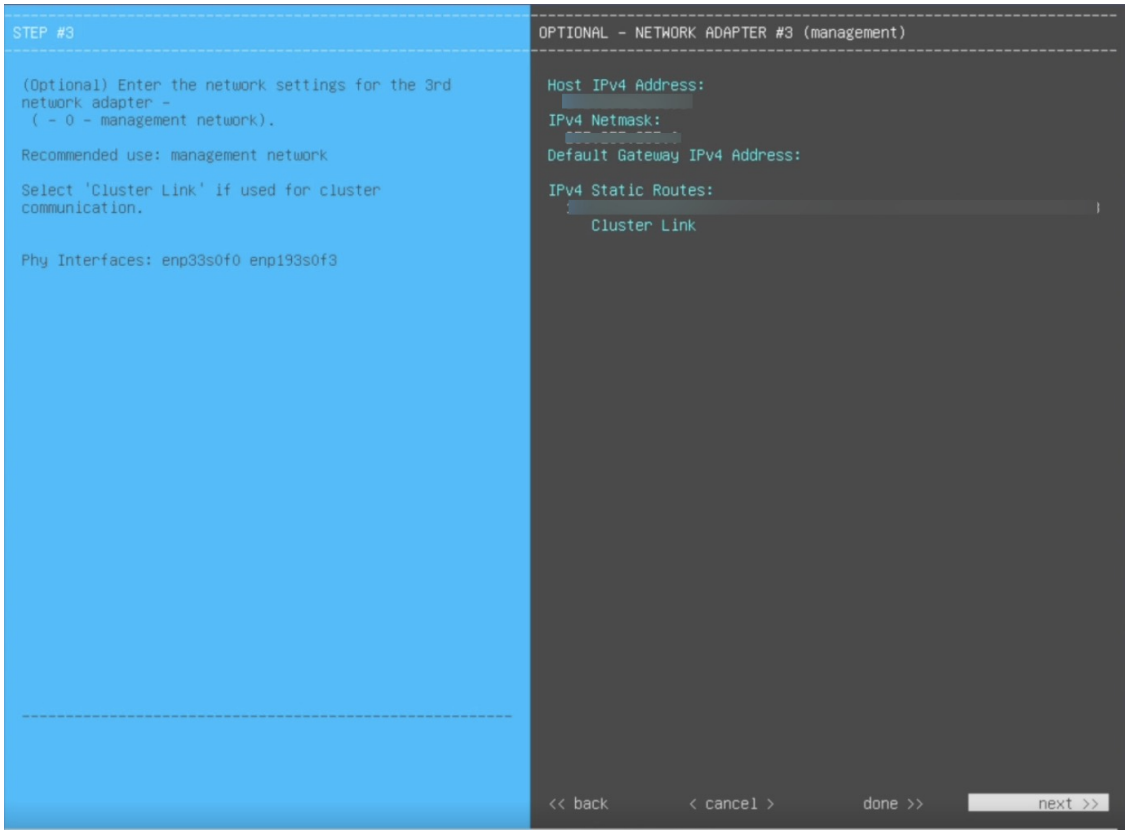
Host IPv4/IPv6 address field	Enter the IP address for the Cluster port. This is required. **Note** You cannot change the address of the Cluster port later.
IPv4 Netmask/IPv6 Prefix Length field	Do one of these tasks if you entered an IP address: • If you selected IPv4 addressing, enter the netmask for the port's IP address. This is required. • If you selected IPv6 addressing, enter the prefix length (in bits). Valid values range from 10 through 127.

Default Gateway IPv4/IPv6 address field	Enter a default gateway IP address to use for the port. **Important** 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. **Important** 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 this format, separated by spaces: *<network>/<netmask>/<gateway>*. 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. **Note** This field is displayed only if you set the Layer 2 LACP port channel 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 Catalyst Center cluster. This is required on the Cluster port only.

LACP Mode field	Do one of these tasks: • Leave this field blank and the port will operate in **Active-Backup** 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. • Check the check box to enable **LACP** 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. For more information about Catalyst Center's implementation of NIC bonding, refer to NIC bonding overview on page 74. **Note** • This field is displayed if you didn't select any of the options in Step 7. • You can only enable LACP mode on your appliance's Intracluster interface during the initial configuration of your appliance.

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

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 on page 28, this port is used to access the Catalyst Center GUI from your management network. Apply the host IP address, netmask, and other values that are appropriate for this purpose (refer to Required IP addresses and subnets on page 31 and Required configuration information on page 53 for the values to enter).



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

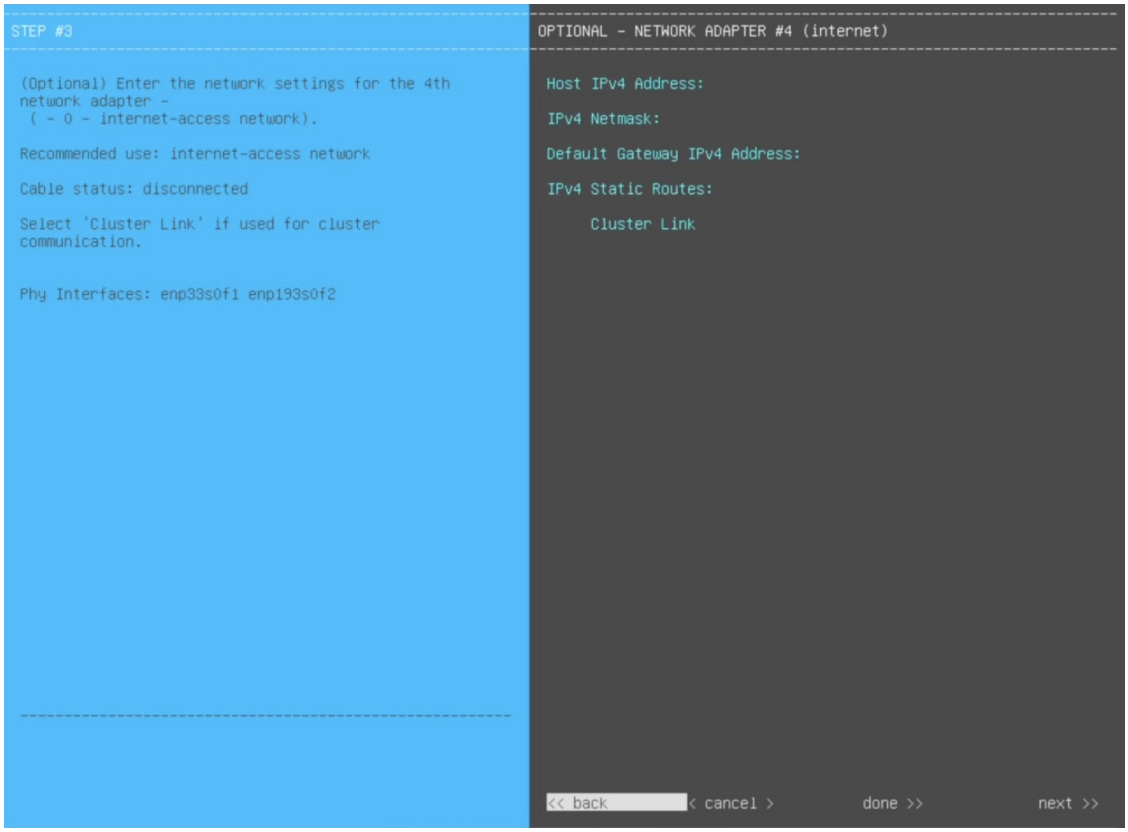
Table 31: Secondary node entries for network adapter #3: 1 Gbps/10 Gbps Management port

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 Catalyst Center GUI from your management network; otherwise, you can leave it blank.
IPv4 Netmask/IPv6 Prefix Length field	Do one of these tasks: • If you selected IPv4 addressing, enter the netmask for the port's IP address. This is required. • If you selected IPv6 addressing, enter the prefix length (in bits). Valid values range from 10 through 127.
Default Gateway IPv4/IPv6 address field	Enter a default gateway IP address to use for the port. **Important** 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. **Important** • For NTP, ensure port 123 (UDP) is open between Catalyst Center and your NTP server. • 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 this 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 continue. Correct validation errors, if any, as you did in previous screens. The wizard validates and applies your network adapter configurations.

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 on page 28, 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 (refer to Required IP addresses and subnets on page 31 and Required configuration information on page 53 for the values to enter).



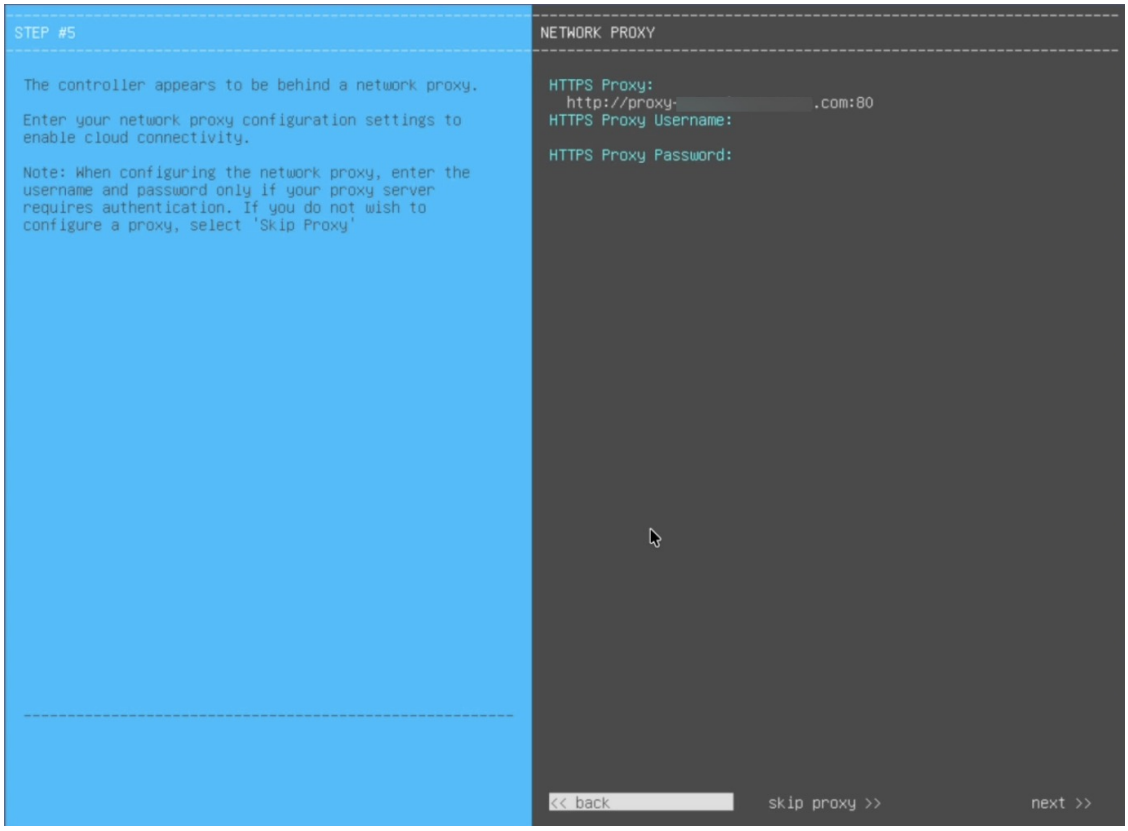
Enter the configuration values for **NETWORK ADAPTER #4**, as shown in this table.

Table 32: 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 these tasks: • If you selected IPv4 addressing, enter the netmask for the port's IP address. This is required. • If you selected IPv6 addressing, enter the prefix length (in bits). Valid values range from 10 through 127.
Default Gateway IPv4/IPv6 address field	Enter a default gateway IP address to use for the Internet port. **Important** 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. **Important** 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 this format, separated by spaces: <*network*>/<*netmask*>/<*gateway*>. 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 continue. Correct validation errors, if any, as you did in previous screens. The wizard validates and applies your network adapter configurations.

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.



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

Table 33: Secondary node entries for network proxy

HTTPS Proxy field	Enter the URL or host name of an HTTPS network proxy used to access the Internet. **Note** • Connection from Catalyst Center to the HTTPS proxy is supported only through HTTP in this release. • 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/
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 continue. Correct validation errors, if any, as you did in previous screens.

13. After the 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).



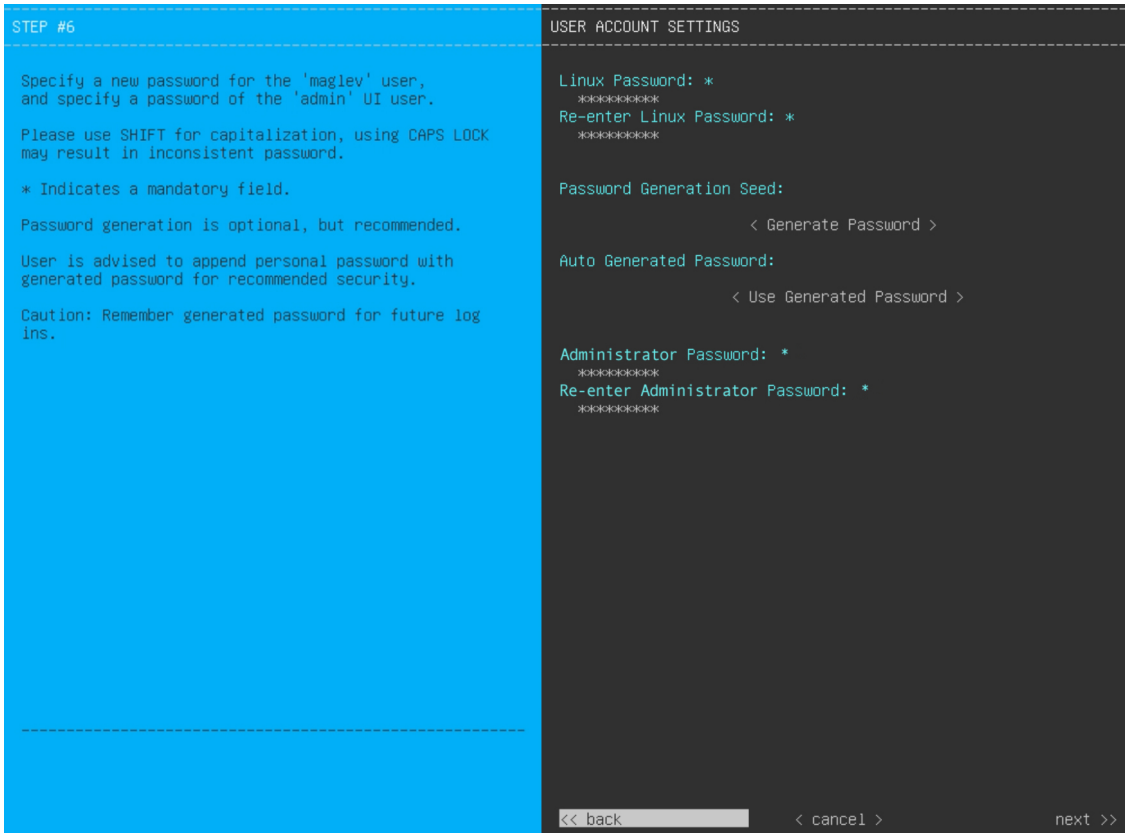
Enter the values for **MAGLEV CLUSTER DETAILS**, as shown in this table.

Table 34: 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 **maglev**.
Password field	Enter the Linux password you configured on the primary node.

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

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



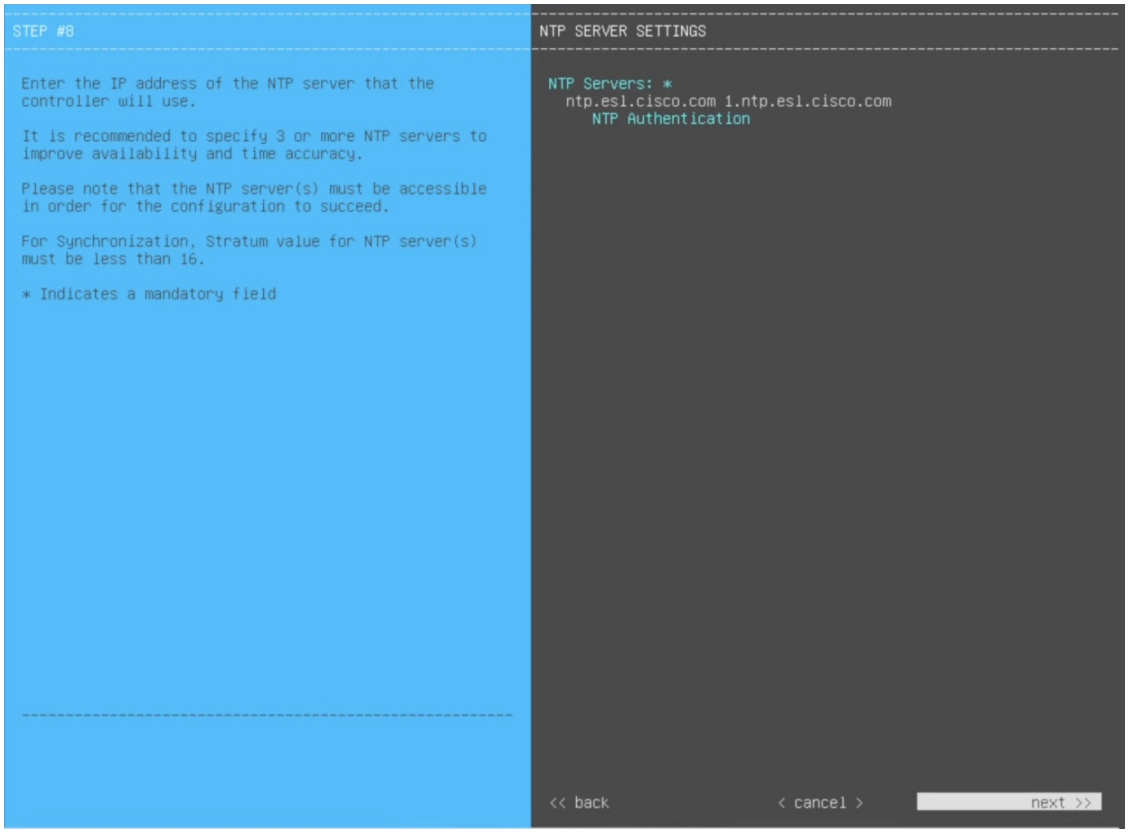
Enter the values for **USER ACCOUNT SETTINGS**, as shown in this table.

Table 35: Secondary node entries for user account settings

Linux Password field	Enter a Linux password for the maglev user that complies with the Password requirements on page 56.
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 <**Generate Password**> 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 <**Use Generated Password**> to save the password.
Administrator Password field	Enter a password for the default admin superuser, used to log in to Catalyst Center for the first time. Ensure that this password complies with the Password requirements on page 56.
Re-enter Administrator Password field	Confirm the administrator password by entering it a second time.

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

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 this table.

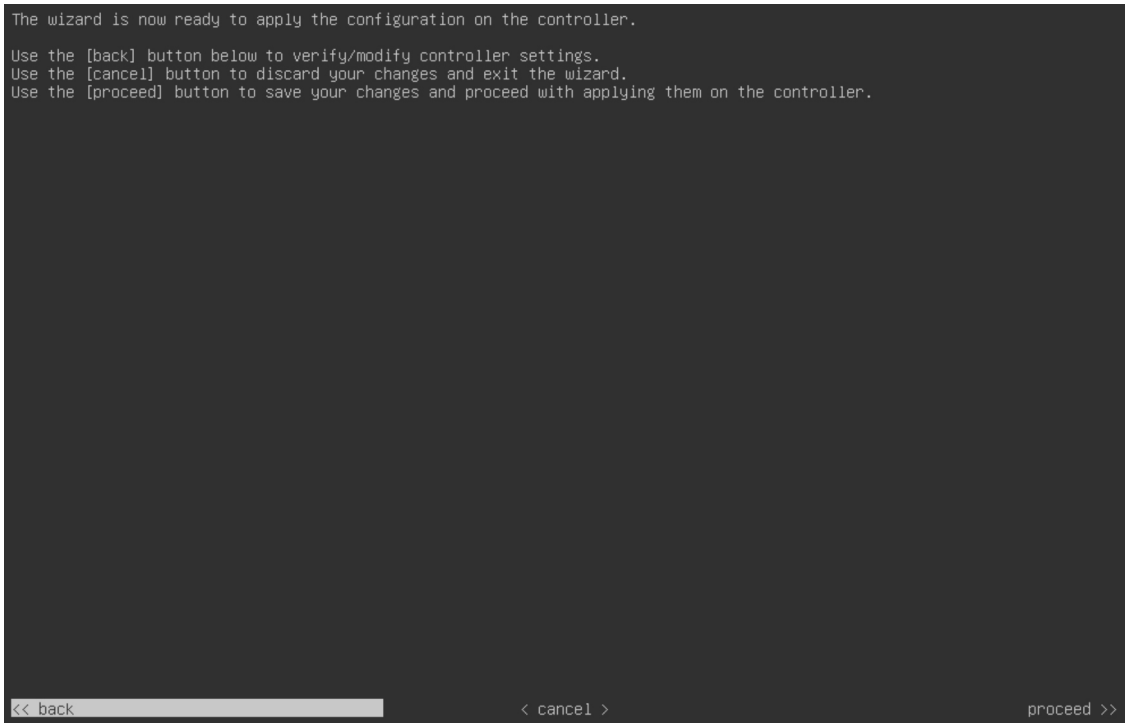
NTP Servers field	Enter one or more NTP server addresses or hostnames, separated by spaces. At least one NTP address or hostname is required. For a production deployment, we recommend that you configure a minimum of three NTP servers.
NTP Authentication check box	To enable the authentication of your NTP server before it's synchronized with Catalyst Center, check this check box and then enter this information: • The NTP server's key ID. Valid values range between 1 and 4294967295 (2^32-1). This value corresponds to the key ID that's defined in the NTP server's key file. • 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.

Note

Ensure that you enter a key ID and key value for each NTP server that you configured in the previous field.

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

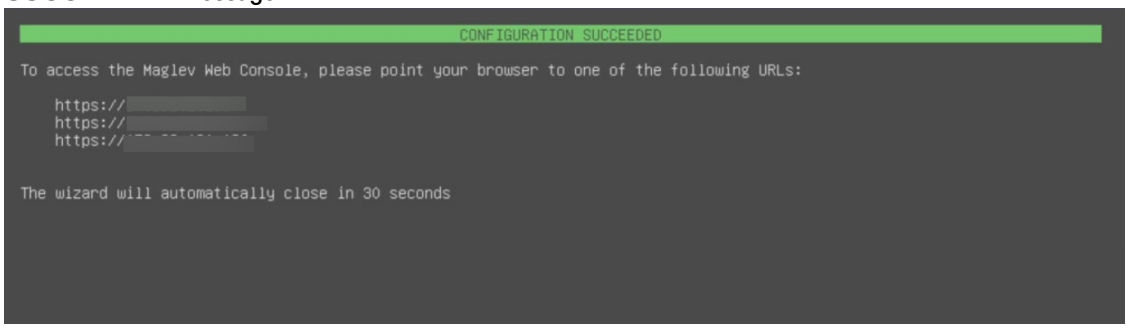
16. When you are finished entering the NTP server settings, a final message appears, stating that the wizard is ready to apply the configuration (as shown).



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

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

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



What to do next

- If you have an additional appliance to deploy as the third and final node in the cluster, repeat this procedure.
- If you have finished adding hosts to the cluster, do the first-time setup: First-time setup workflow on page 178.

Upgrade to the latest Catalyst Center release

You can upgrade to the latest Catalyst Center release.

For information about upgrading your current release of Catalyst Center, see the *Cisco Catalyst Center Upgrade Guide*.

6 Configure the Appliance Using the Browser-Based Wizard

Topics:

- Appliance configuration overview
- Password considerations
- VLAN mode considerations
- Configure an appliance using the Install Configuration wizard
- Configure the primary node using the Advanced Install configuration wizard
- Configure a secondary node using the Advanced Install configuration wizard
- Upgrade to the latest Catalyst Center release

Appliance configuration overview

Provides information about configuring appliances based on the deployment mode.

You can deploy the appliance in your network in one of these 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 select the Standalone mode for your initial deployment, it will be your primary node.

  Note

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

To continue, configure the primary node in your cluster. 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

Information to help you determine if you should use the Install Configuration wizard or Advanced Install Configuration wizard to configure your appliance.

Catalyst Center offers two browser-based wizards that you can use to configure your appliance. Read the descriptions to decide which wizard to complete.

Important

These wizards are available for use if you are configuring a new appliance that came with the latest release of Catalyst Center already installed. If you upgraded from an earlier version and want to use these wizards, contact Cisco TAC for support.

Install configuration wizard

This wizard streamlines the appliance configuration process by setting default values for the Enterprise, Management, and Internet Access interfaces as well as the Intracluster interface. All the interfaces reside on the appliance's Enterprise port. Use this wizard if you agree to use the default interface settings and want to activate your appliance quickly.

Note

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 to specify interface settings that differ from the default or to configure the second or third node in your cluster..

Browser-based wizard prerequisites

Describes the configuration of the appliance's enterprise interface using browser-based wizards.

To properly configure your appliance using either of the browser-based wizards, complete these tasks:

- Designate the enterprise interface on your appliance to use the IP address, subnet mask, and default gateway assigned by a DHCP server. The wizard does not allow changes to the assigned IP address or subnet mask, but allows you to change the default gateway. The assumption in this chapter is that the enterprise interface was selected for this purpose.
- Ensure that the IP address assigned by the DHCP server is reachable by the machine from which you will complete the wizard.
- Verify that both the enterprise and intracluster interfaces are connected and in the **UP** state.

Alternatively, specify your own IP address, subnet mask, and default gateway for the enterprise interface of your appliance by completing the Static IP Address Settings page.

Password considerations

Provides pointers to the password policies and requirements for Catalyst Center.

Refer to these topics for a description of Catalyst Center's implementation of passwords.

- Password policy on page 55
- Password requirements on page 56

VLAN mode considerations

You can't use disaster recovery when VLAN mode is enabled for Catalyst Center.

Consider these details about VLAN mode:

- For a description of VLAN mode, refer to Configure the primary node using the Maglev wizard.
- VLAN mode:
  - Can only be enabled when you configure a Catalyst Center appliance using the Maglev Configuration wizard.
  - Cannot be enabled using any of the browser-based configuration wizards.
  - Cannot be disabled without reimaging the appliance.
- Disaster recovery is not supported by Catalyst Center deployments that have VLAN mode enabled.

Configure an appliance using the Install Configuration wizard

You can configure a primary node in a three-node cluster or a standalone node and simplify the process by using the Install Configuration wizard.

Do 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. These fourth-generation Catalyst Center appliances support configuration using this wizard:

- Medium appliance:
  - Standard: DN4-HW-APL
- Large appliance:
  - Standard: DN4-HW-APL-L
- Extra large appliance:
  - Standard: DN4-HW-APL-XL

Important

- You can only use this wizard to complete the initial configuration of a new Catalyst Center appliance. To reimage an appliance that's been configured previously, you will need to use the Maglev Configuration wizard.
- You cannot use this wizard to configure the second or third appliance in a three-node cluster. Also, you cannot use this wizard to enable LACP mode on your appliance's Enterprise and Intracluster interfaces.
- Log out of any appliances in a three-node cluster before configuring them. 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 Catalyst 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:

- Collected all of the information called for in Required IP addresses and subnets on page 31 and Required configuration information on page 53.
- Installed the appliance.
- Configured Cisco IMC browser access on this appliance, as described in Enable browser access to the Cisco Integrated Management Controller on page 66.
- Checked that the appliance's ports and the switches it uses are properly configured, as described in Execute preconfiguration tasks on page 71.
- Are using a browser that is compatible with Cisco IMC and Catalyst Center. For a list of compatible browsers, see the Release Notes for the version of Catalyst Center that you are installing.
- Enabled ICMP on the firewall between Catalyst Center and the DNS servers you will specify in the procedure. This wizard uses Ping to verify the DNS server you specify. This ping can be blocked if there is a firewall between Catalyst 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.

Procedure

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 (refer to Enable browser access to the Cisco Integrated Management Controller on page 66).

After successful login, the appliance displays the **Cisco Integrated Management Controller Chassis Summary** window, with a blue link menu at the upper right.

b) From the blue link menu, select **Launch KVM** and then select **HTML based KVM**.

The KVM console opens in a separate browser window or tab automatically. Use it 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 these 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 the reboot messages, the KVM console displays the **Static IP Configuration** window.



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

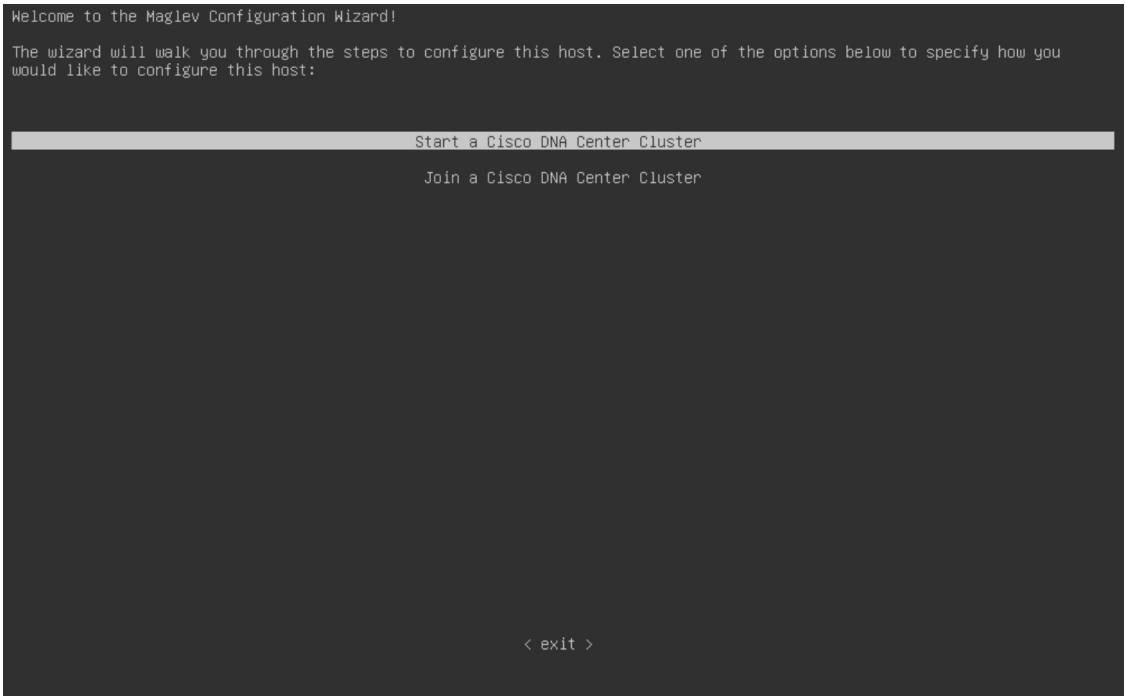
d) Do one of these tasks:

- 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 table and then click **Configure**.

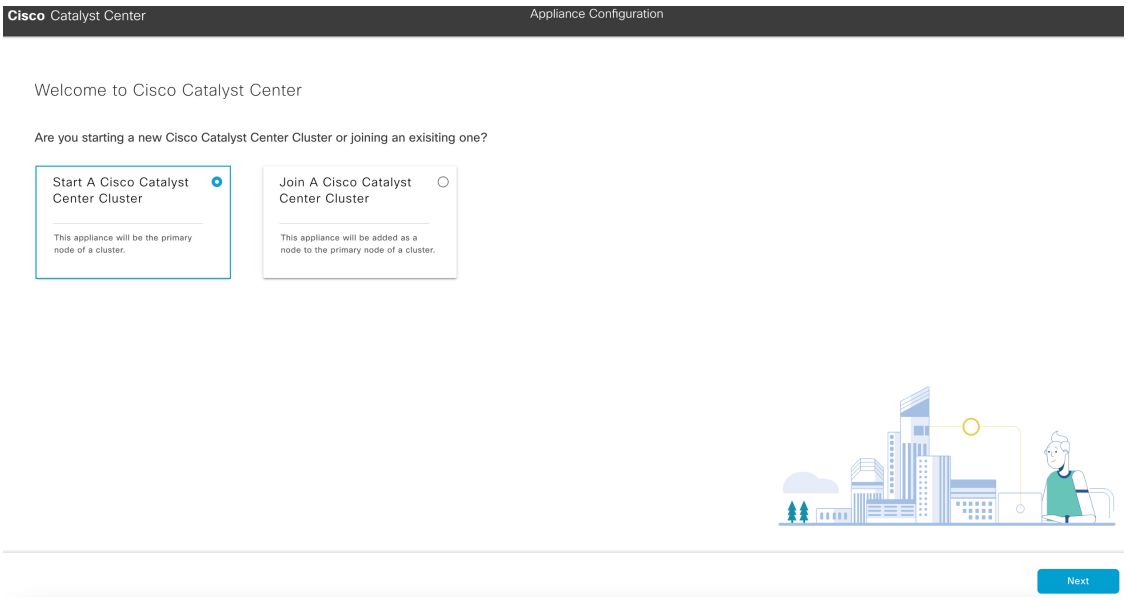
> **Note**
>
> You only need to specify an IP address, subnet mask, and default gateway for your appliance's Enterprise interface.

IPv6 Mode check box	If you want to configure an IPv6 address, check this check box.
IP Address field	Enter the static IP address that you want to use.
Netmask field	Enter the netmask for the IP address you specified in the previous field: • If you entered an IPv4 address, you can enter either a netmask or CIDR address. • If you entered an IPv6 address, you can only enter a CIDR address.
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 this format, separated by spaces: *<network>/<netmask>/<gateway>*. This is usually required on the Management port only.

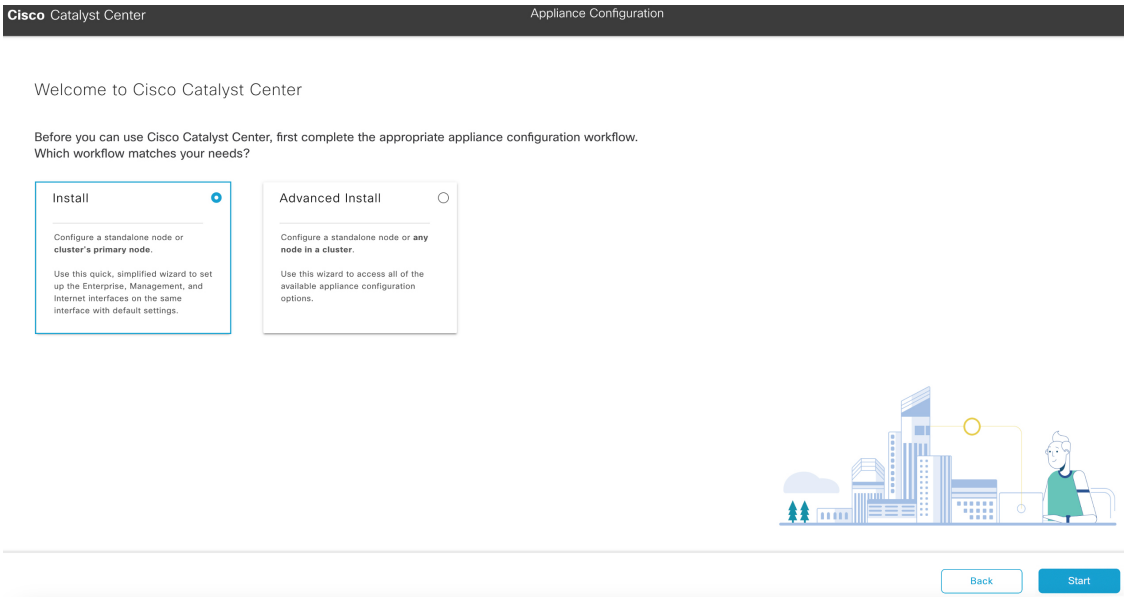
The KVM console displays the Maglev Configuration wizard welcome page.



e) To bring up the **Appliance Configuration** window, open the URL that displays in the **Static IP Configuration** window.

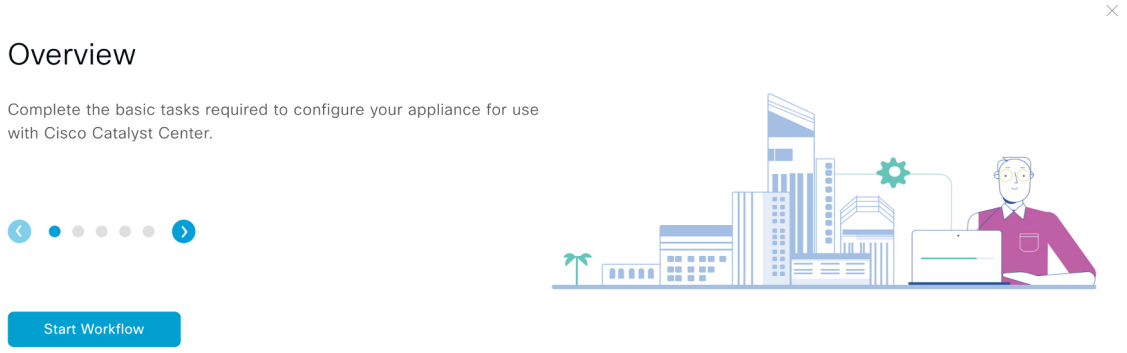


f) Click the **Start a Cisco Catalyst Center Cluster** radio button, then click **Next**.



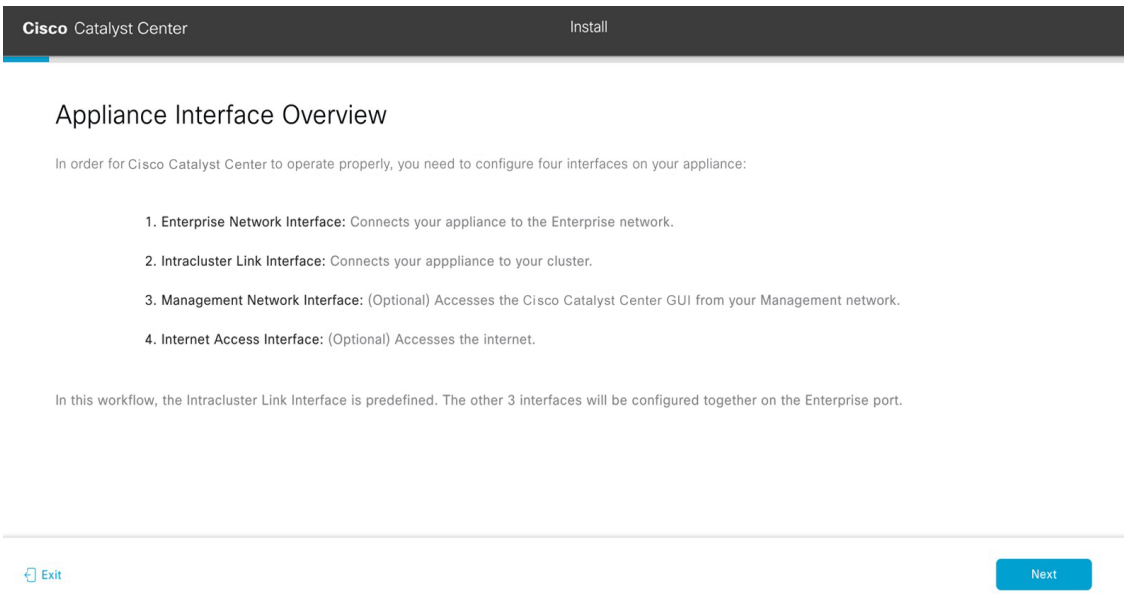
g) Click the **Install** radio button, then click **Start**.

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



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

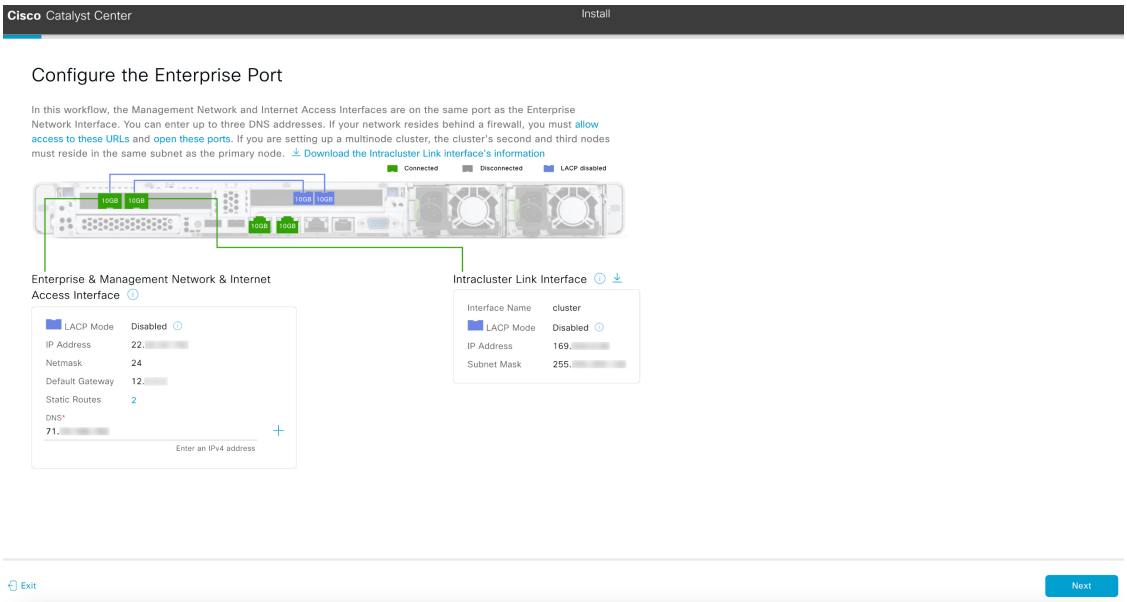
The **Appliance Interface Overview** window opens, providing a description of the four interfaces that are available on your Catalyst Center appliance:



The wizard will help you configure the Enterprise and Intracluster ports, which are required for Catalyst Center functionality. If the wizard fails to display either or both of these ports in the next page, they may be non-functional or disabled. If you discover that they are non-functional, click **Exit** to exit the wizard immediately. Be sure you have completed all of the steps provided in Execute preconfiguration tasks on page 71 before resuming configuration or contacting the Cisco Technical Assistance Center (TAC).

2. Complete the Install configuration wizard:
   a) Click **Next**.

   The **Configure The Enterprise Port** page opens.



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 these tasks:

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

b) In the **DNS** field, enter the IP address of the preferred DNS server.

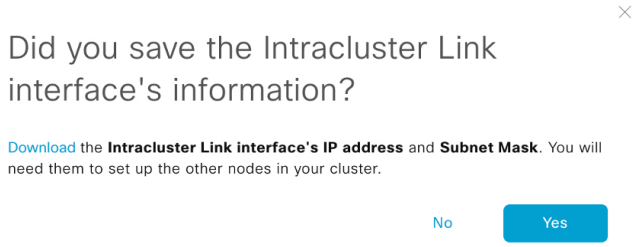
To enter additional DNS servers, click the **Add** (**+**) icon.

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 Catalyst Center and your NTP server.

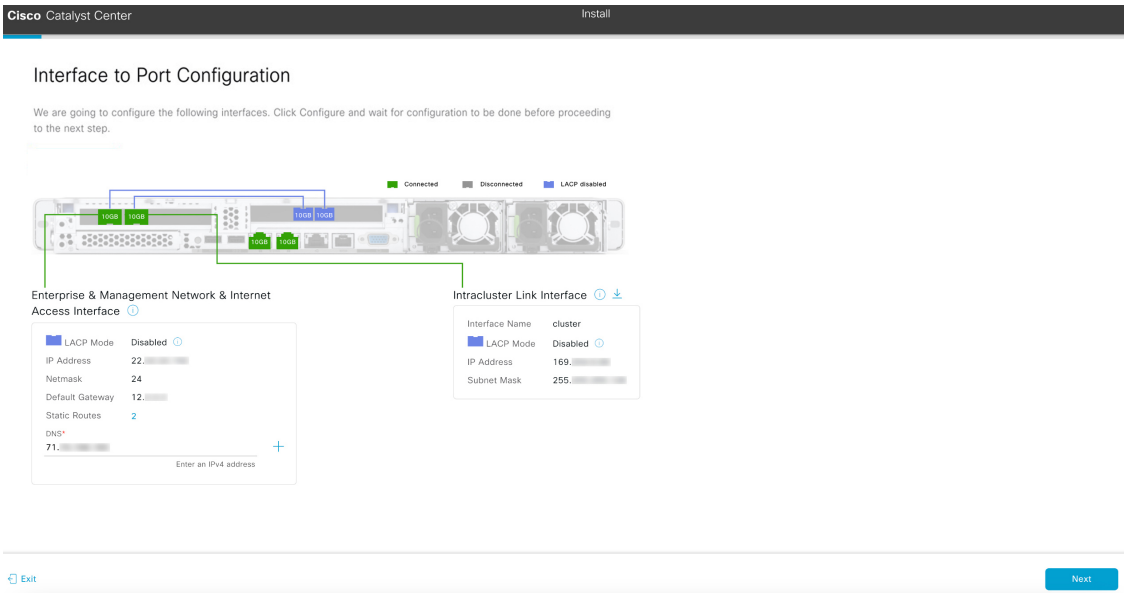
c) Click **Next**.

d) When prompted, click **Yes** to copy the Intracluster interface's IP address and subnet mask.



You'll need this information when you configure your cluster's secondary nodes.

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 continue with the wizard. If the settings you have entered are valid and the port is up, the wizard's **Interface to Port Configuration** page opens.

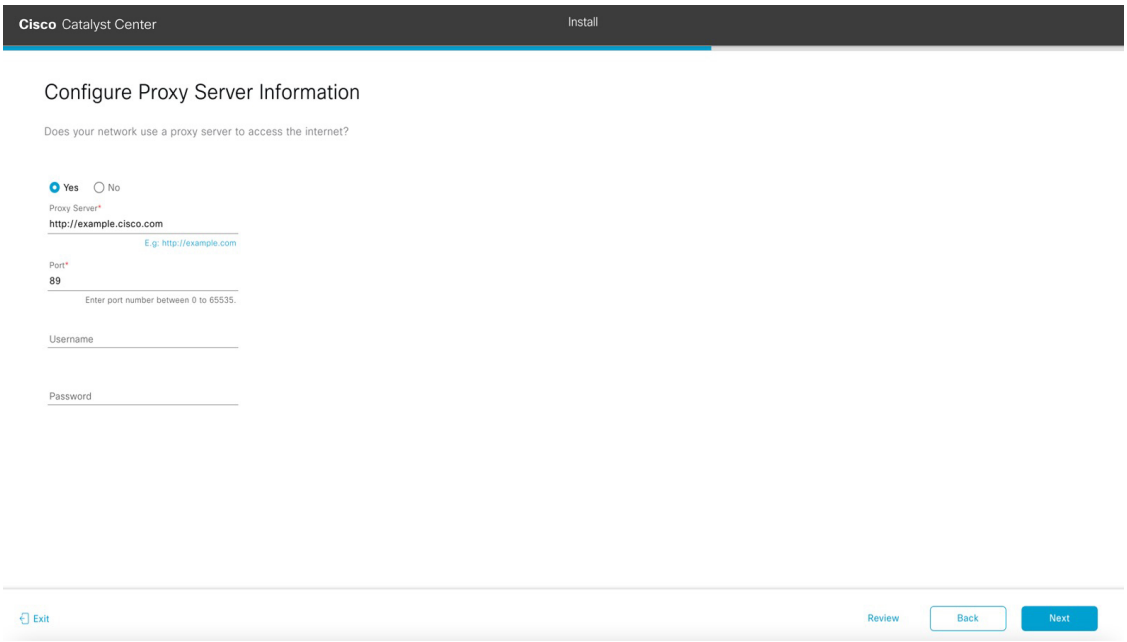


e) Click **Next**.

f) Review the interface settings that have been set, then click **Configure**.

g) After initial interface configuration has completed, click **Next** to continue to the next wizard page.

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



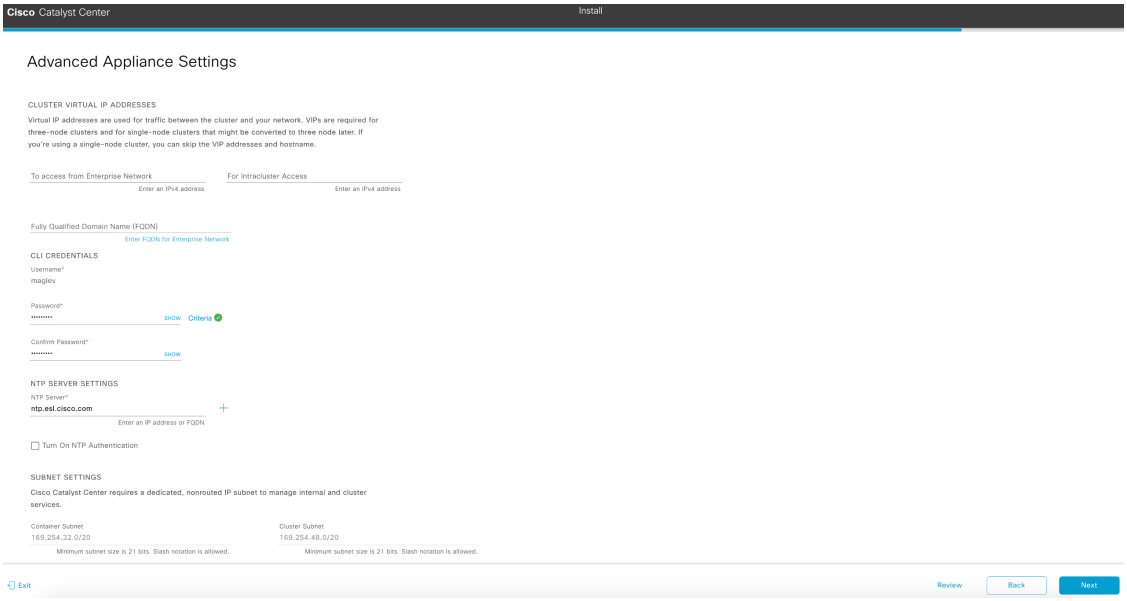
h) Do one of these tasks, then click **Next**:

- 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 this table:

Table 36: 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. **Note** Connection from Catalyst Center to the HTTPS proxy is supported only via HTTP in this release.
Port field	Enter the port that your appliance used to access the network proxy.
Username field	Enter the username 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 that you entered and notifies you of any settings that need to be changed before you can continue with the wizard. If the settings you have entered are valid, the wizard's **Advanced Appliance Settings** page opens.



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

Table 37: 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. **Important** If you decide 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 **UP** state.
Fully Qualified Domain Name (FQDN) field	Enter the fully qualified domain name (FQDN) for your cluster. Catalyst Center does these tasks with this hostname: • 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 Catalyst Center manages. • In the Subject Alternative Name (SAN) field of Catalyst Center certificates, it uses the FQDN to the define the Plug and Play server that should be used for device provisioning.

CLI credentials

Enter and confirm the password for the `maglev` user.

Important

Ensure that this password complies with the Password requirements on page 56.

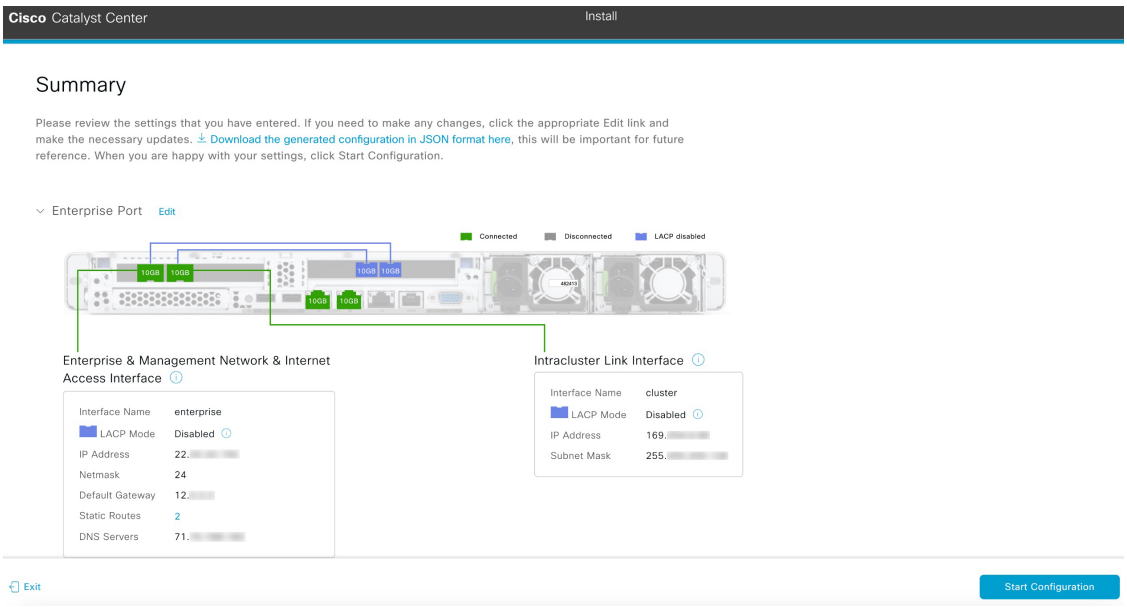
NTP server settings

NTP Server field	Enter at least one NTP server address or hostname. To enter additional NTP server addresses or hostnames, click the **Add** (**+**) icon. For a production deployment, Cisco recommends that you configure a minimum of three NTP servers.
Turn On NTP Authentication check box	To enable the authentication of your NTP server before it's synchronized with Catalyst Center, check this check box and then enter this information: • The NTP server's key ID. Valid values range between 1 and 4294967295 (2^32-1). This value corresponds to the key ID that's defined in the NTP server's key file. • 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. **Note** Ensure that you enter a key ID and key value for each NTP server that you configured in the previous field.

Subnet settings

Container Subnet field	A dedicated, non-routed IP subnet that Catalyst Center uses to manage internal services. By default, this is already set to **169.254.32.0/20**, and we recommend that you use this subnet.
Cluster Subnet field	A dedicated, non-routed IP subnet that Catalyst 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 wizard validates the information you have entered and notifies you of any settings that need to be changed before you can continue with the wizard. If the settings you entered are valid, the wizard's **Summary** page opens.

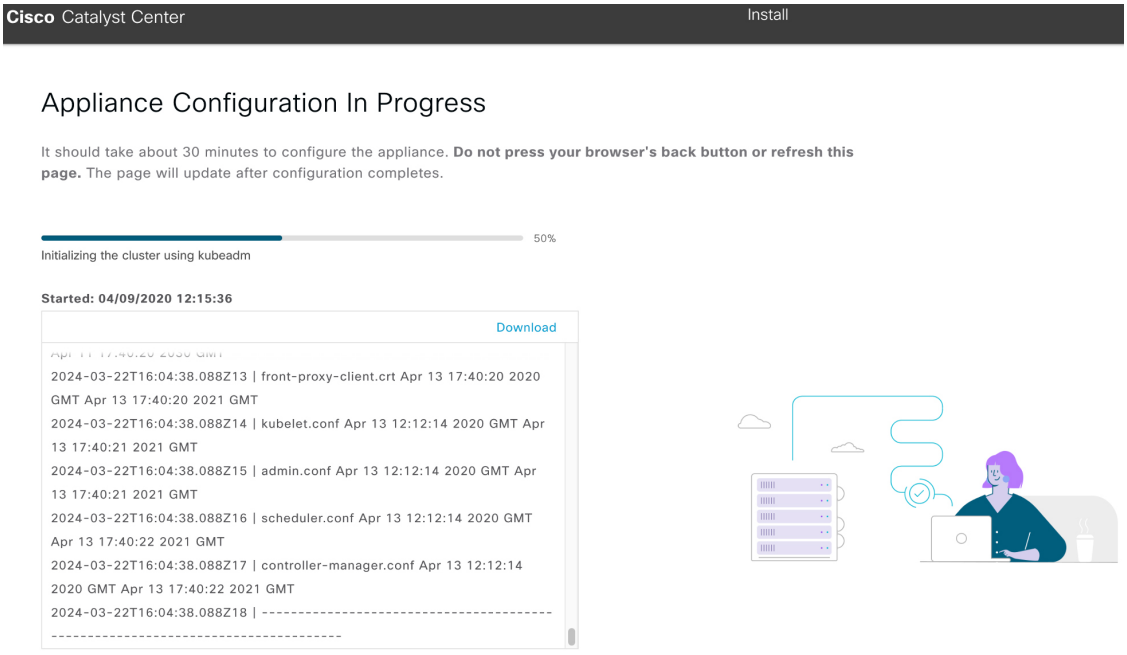


j) Scroll to the bottom of the page and review all of the settings that you have entered while completing the wizard. If necessary, click the **Edit** link to open the wizard page in which you can make updates.

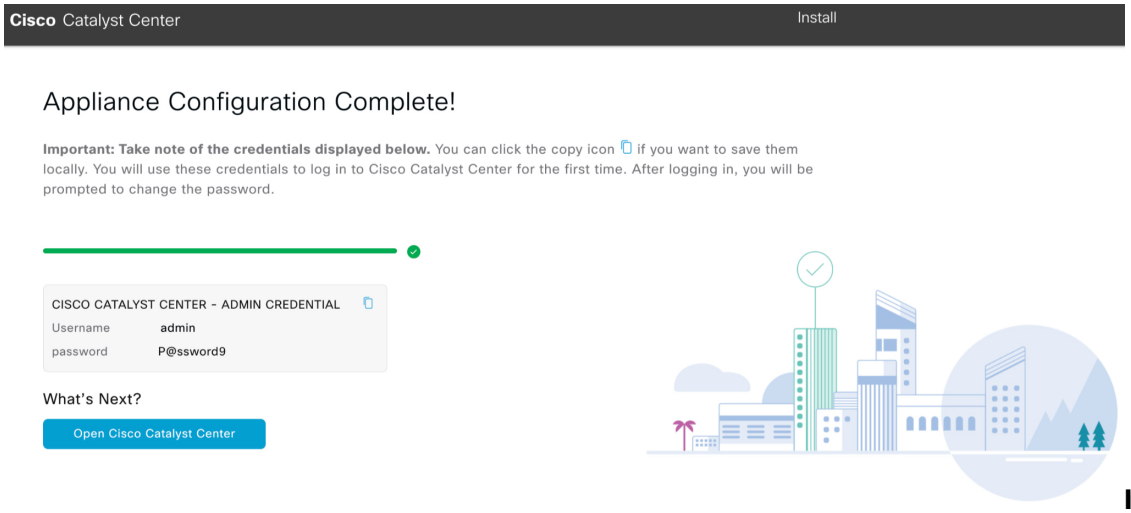
> **Note**
>
> To download the appliance configuration as a JSON file, click the relevant link.

k) To complete the configuration of your Catalyst Center appliance, click **Start Configuration**.

The wizard page 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.



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



Important

Catalyst Center automatically sets this password to **P@ssword9** when you complete the Install configuration wizard. Use this password to log in to Catalyst 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 Log in to Catalyst Center for the first time on page 178.

What to do next

As you are deploying this appliance in standalone mode, continue by doing the first-time setup: First-time setup workflow on page 178.

Configure the primary node using the Advanced Install configuration wizard

You can set up the first appliance in a cluster using the Advanced Install configuration wizard.

Whether standalone or part of a cluster, always configure the first appliance as the primary node.

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" instead instead.

To configure the first installed appliance as the primary node using the Advanced Install configuration wizard:

Important

- These fourth-generation Catalyst Center appliances support configuration using this wizard:

  - Medium appliance:
    - Standard: DN4-HW-APL
  - Large appliance:
    - Standard: DN4-HW-APL-L
  - Extra large appliance:
    - Standard: DN4-HW-APL-XL

- You can only use this wizard to complete the initial configuration of a new Catalyst Center appliance. To reimage an appliance that was configured previously, you must use the Maglev Configuration wizard.
- 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 discovers your network's devices and enables telemetry) will not start after you have configured your cluster's appliances and log in to Catalyst Center for the first time.
- Ensure that the IP addresses you enter while completing this procedure are valid addresses with valid netmasks. Also make sure that the addresses and their corresponding subnets do not overlap. Service communication issues can result when they do.

Before you begin

Ensure that you:

- Collected the information called for in Required IP addresses and subnets on page 31 and Required configuration information on page 53.
- Installed the first appliance, as described in Appliance installation workflow on page 58.
- Configured Cisco IMC browser access on the primary node, as described in Enable browser access to the Cisco Integrated Management Controller on page 66.
- Checked that the primary node's ports and the switches it uses are properly configured, as described in Execute preconfiguration tasks on page 71.
- Use a browser that is compatible with Cisco IMC and Catalyst Center. For a list of compatible browsers, see the Release Notes for the version of Catalyst Center you are installing.
- Enabled ICMP on the firewall between Catalyst Center and both the default gateway and the DNS server you specify in the provided 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.

Procedure

1. Start the Advanced Install configuration wizard:
   a) Point your browser to the Cisco IMC IP address that you set during the Cisco IMC GUI configuration you performed, then log in to the Cisco IMC GUI as the Cisco IMC user (refer to Enable browser access to the Cisco Integrated Management Controller on page 66).

      After successful login, the appliance displays the **Cisco Integrated Management Controller Chassis Summary** window, with a blue link menu at the upper right.

   b) In the blue link menu, select **Launch KVM** and then select **HTML based KVM**.

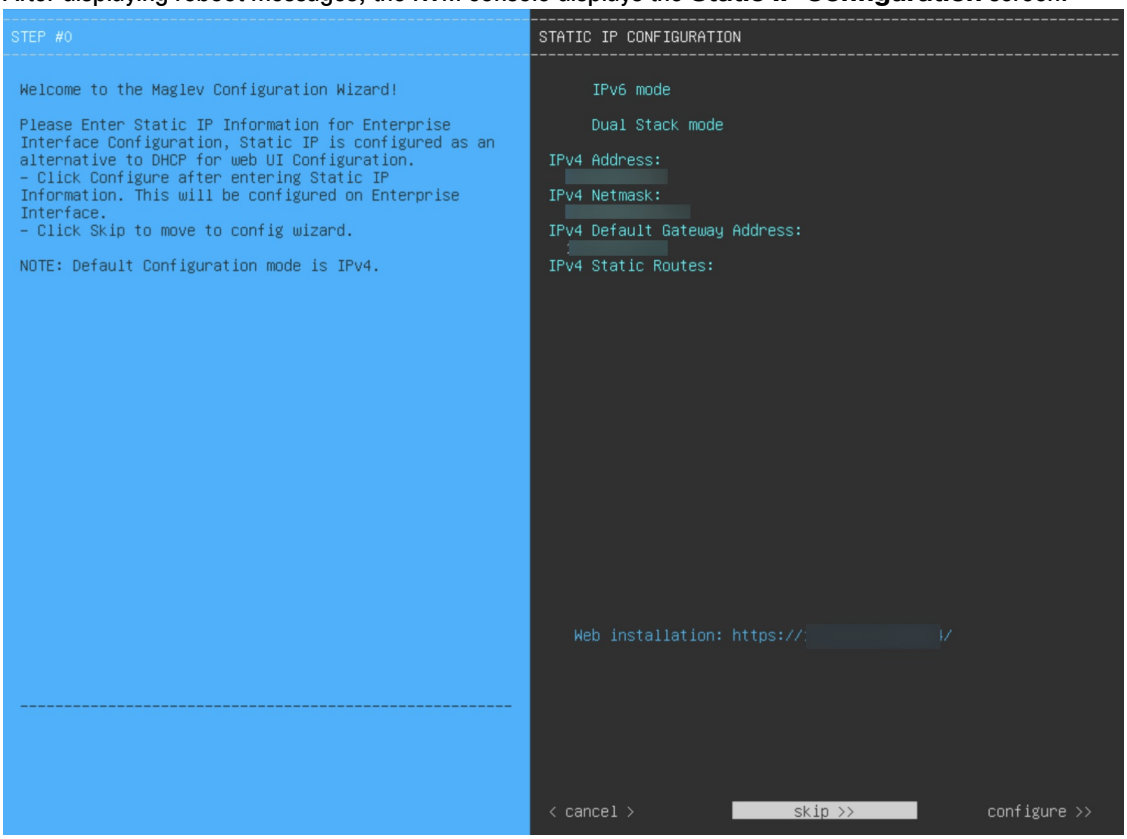
The KVM console opens in a separate browser window or tab automatically. Use it to monitor the progress of the configuration and respond to Maglev Configuration Wizard prompts.

c) With the KVM displayed, reboot the appliance by making one of these 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.



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

d) Do one of these tasks:

- 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 that this table describes and then click **Configure**.

> **Note**
>
> Only specify an IP address, subnet mask, and default gateway for your appliance's Enterprise interface.

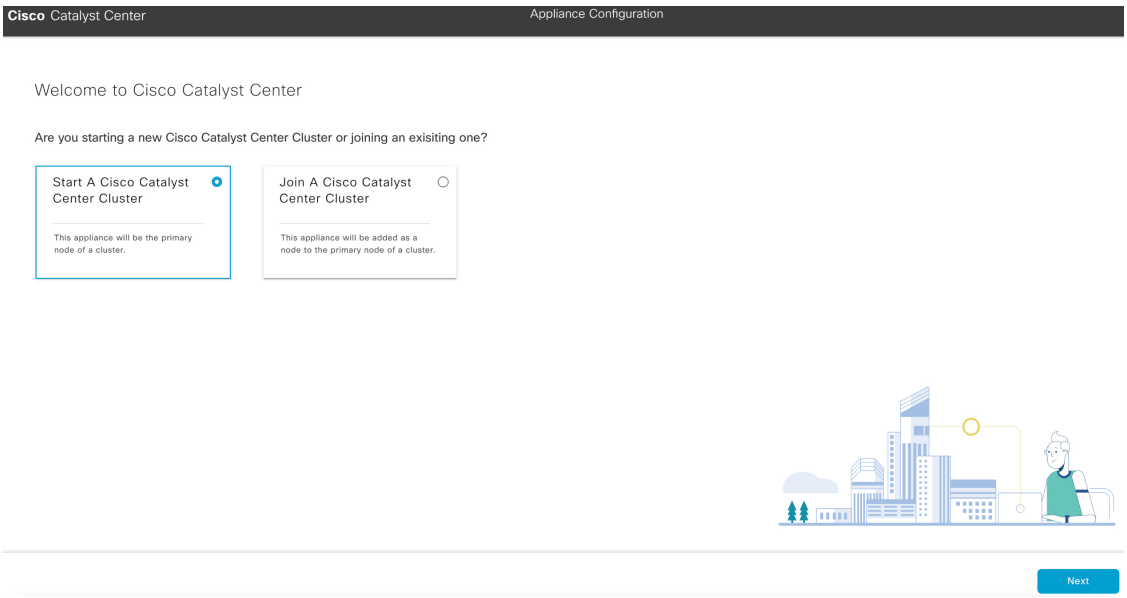
IPv6 Mode check box	If you want to configure an IPv6 address, check this check box.

IP Address field	Enter the static IP address that you want to use.
Netmask field	Enter the netmask for the IP address you specified in the previous field: • If you entered an IPv4 address, you can enter either a netmask or CIDR address. • If you entered an IPv6 address, you can only enter a CIDR address.
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 this format, separated by spaces: <*network*>/<*netmask*>/<*gateway*>. This is usually required on the Management port only.

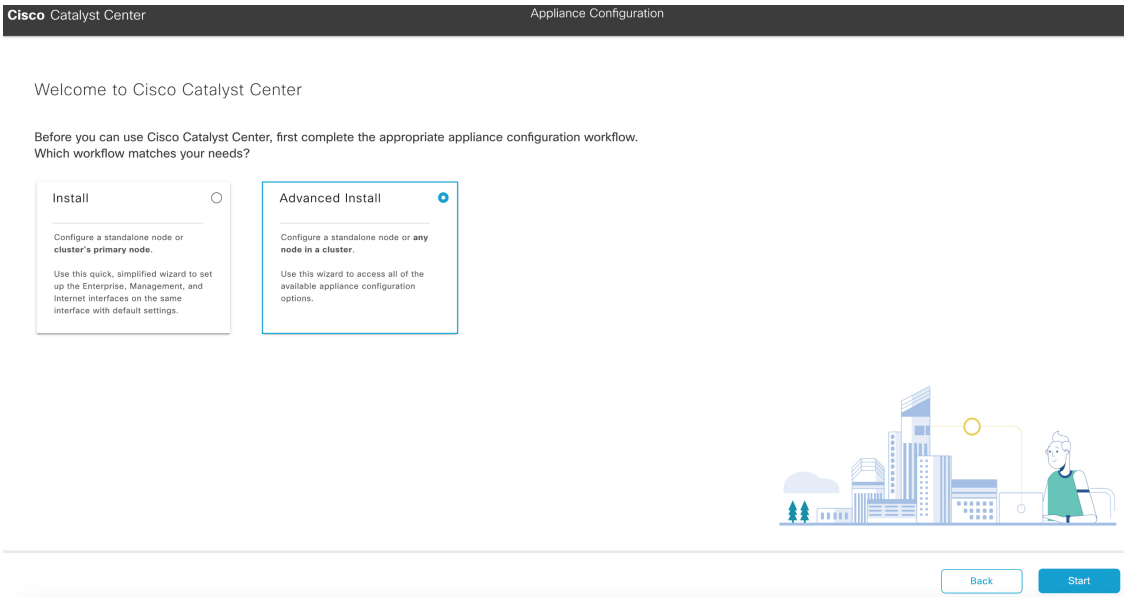
The KVM console displays the Maglev Configuration wizard welcome screen.



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

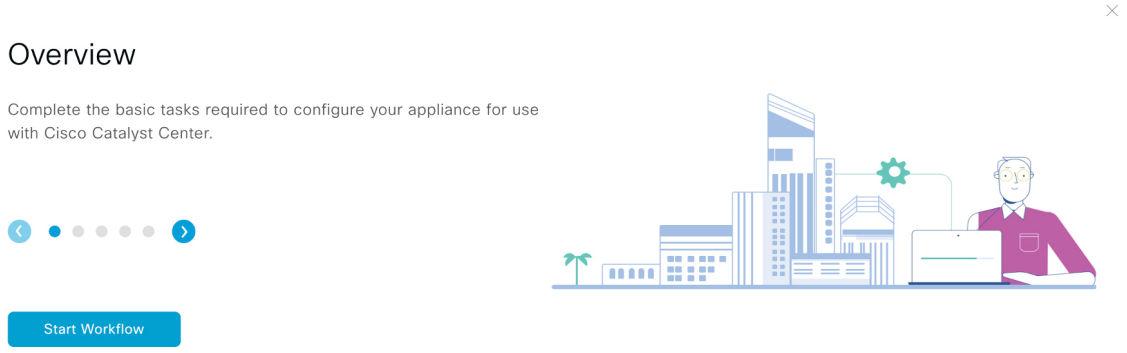


f) Click the **Start a Cisco Catalyst Center Cluster** radio button, then click **Next**.



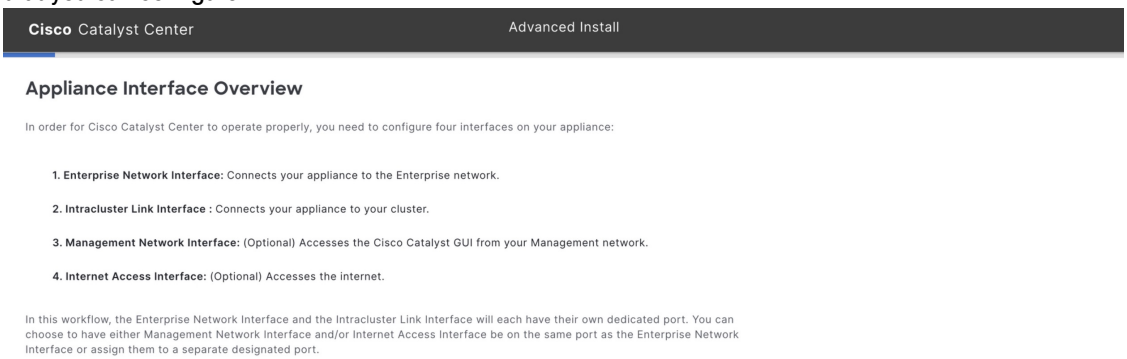
g) Click the **Advanced Install** radio button, then click **Start**.

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



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.

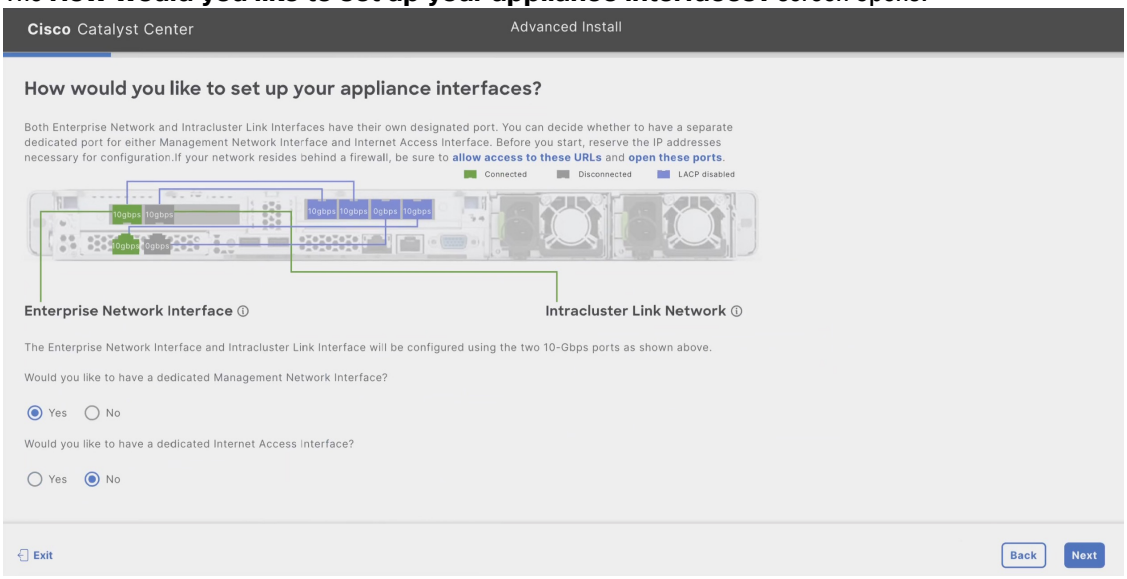


Important

At a minimum, configure the interfaces on your appliance's Enterprise and Cluster ports, as they are required for Catalyst Center functionality. If the wizard fails to display either or both of these ports during configuration, they may be nonfunctional or disabled. If you discover that they are nonfunctional, click **Exit** to exit the wizard immediately. Be sure you have completed the steps that are provided in Execute preconfiguration tasks on page 71 before resuming configuration or contacting the Cisco Technical Assistance Center (TAC).

2. Complete the Advanced Install configuration wizard:
   a) Click **Next**.

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

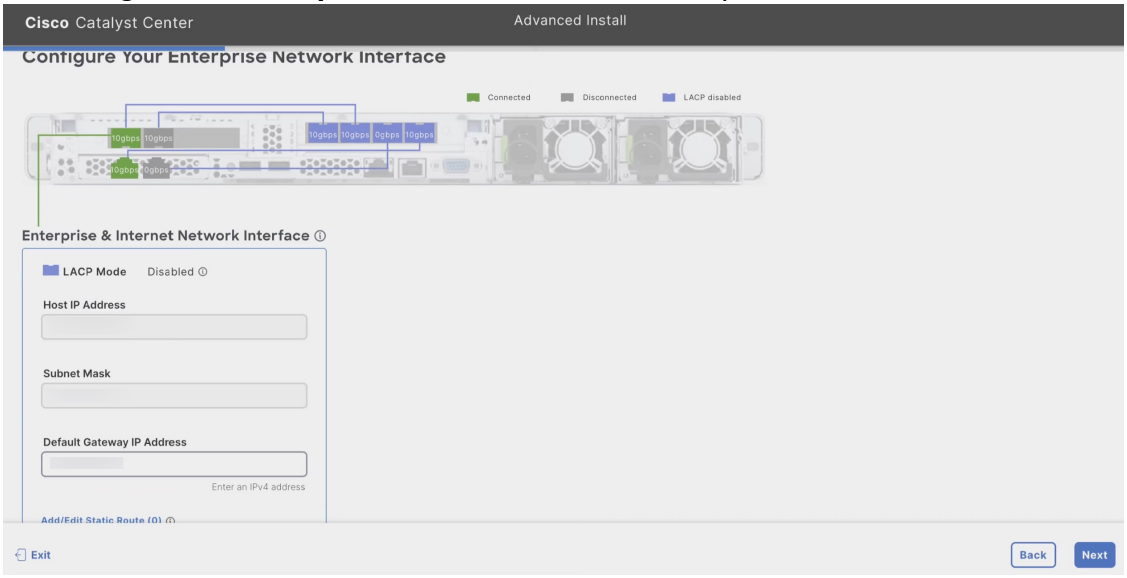


If your network resides behind a firewall, do these tasks:

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

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

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



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

As explained in Interface cable connections on page 28, this is a required interface that is used to link the appliance to the enterprise network. Refer to Required IP addresses and subnets on page 31 and Required configuration information on page 53 for a more detailed description of the values that you must enter.

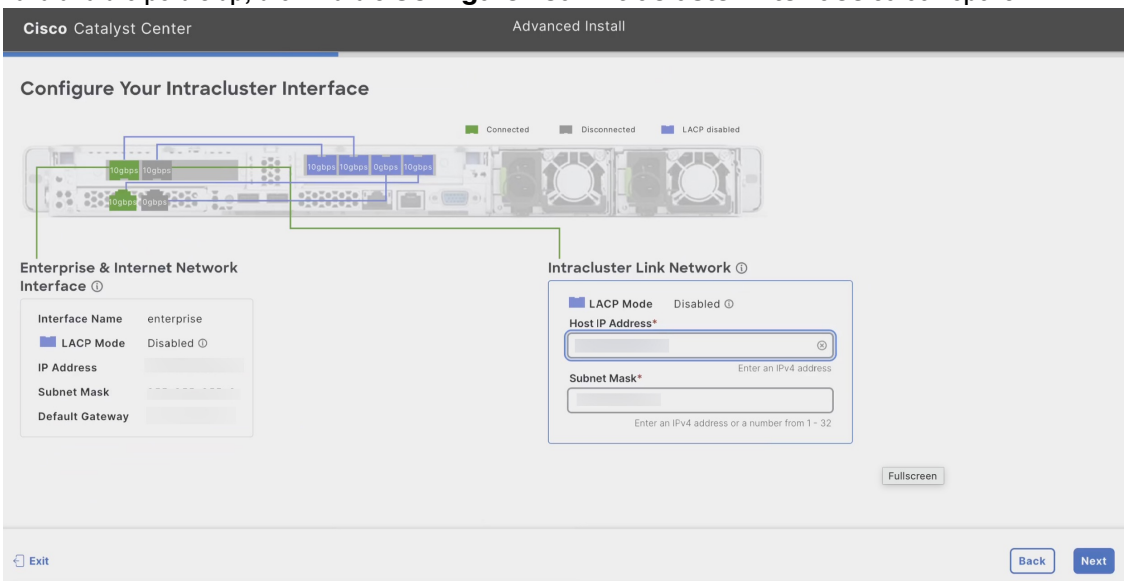
Table 38: Primary node entries for the Enterprise interface

LACP Mode slider	Select one of these network interface controller (NIC) bonding modes for the Enterprise interface: • **Active-Backup 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. • **LACP mode**: 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. For more information about Catalyst Center's implementation of NIC bonding, refer to NIC bonding overview on page 74.
Host IP Address field	Enter the IP address for the Enterprise interface. This is required.
Subnet Mask field	Enter the netmask for the interface's IP address. This is required.

Default Gateway IP Address field	Enter a default gateway IP address to use for the interface. **Important** Default Gateway: Enter an IP address for at least one interface. Failure to do so prevents completion of the configuration wizard. **Note** You designated this interface to use the default gateway assigned to it by a DHCP server. Complete these steps to specify a different gateway: 1. Delete the IP address that is currently listed in this field and then click **Exit**. This will bring you back to the first wizard screen. 2. Return to the Enterprise port's wizard screen and enter the gateway IP address you want to use.
DNS field	Enter the IP address of the preferred DNS server. 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 Catalyst Center and your NTP server.

The wizard validates the information that you have entered, confirms that the port is up, and notifies you of any settings that must be changed before you can continue with the wizard. If the settings that you have entered are

valid and the port is up, the wizard's **Configure Your Intracluster Interface** screen opens.



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

As explained in Interface cable connections on page 28, this required port is used to link the appliance to your cluster. Refer to Required IP addresses and subnets on page 31 and Required configuration information on page 53 for a more detailed description of the values you must enter.

Note

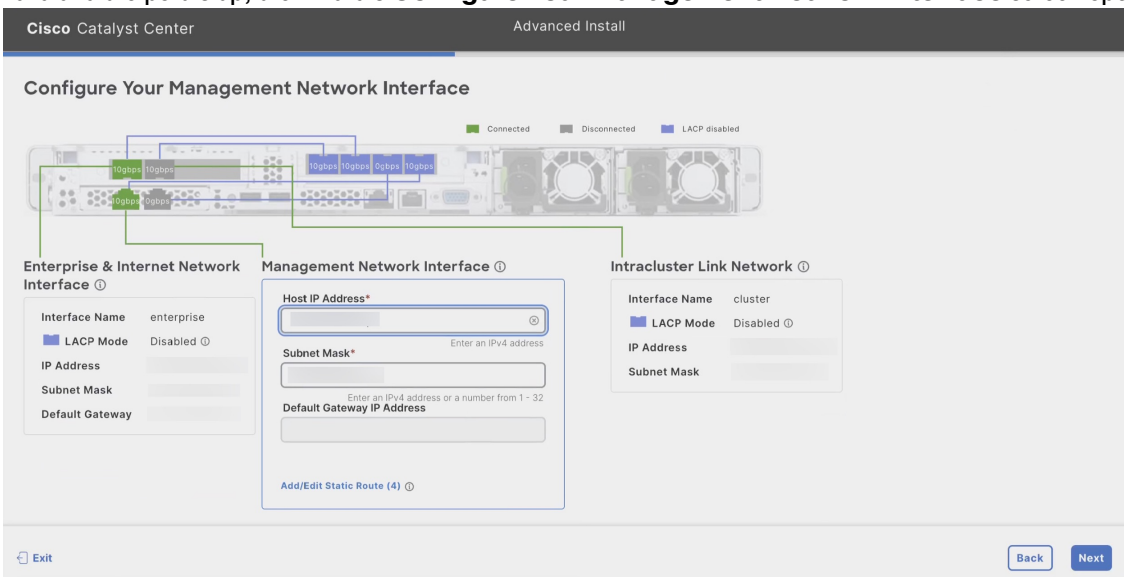
- If you opted to configure the Enterprise and Internet Access interfaces on the same port, complete this step and then continue to Step 2e (which describes how to configure your Management interface).
- If you opted to configure the Enterprise and Management interfaces on the same port, complete this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

Table 39: Primary node entries for the Intracluster interface

LACP Mode slider	Select one of these NIC bonding modes for the Intracluster interface: • **Active-Backup 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. • **LACP mode**: 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. **Important** If you want to enable LACP mode on your appliance's Intracluster interface, do so now. You won't be able to after you complete this wizard. For more information about Catalyst Center's implementation of NIC bonding, see NIC bonding overview on page 74.
Host IP Address field	Enter the IP address for the Intracluster interface. This is required. **Note** You cannot change the address of the Intracluster interface later.
Subnet Mask field	Enter the netmask for the interface's IP address. This is required.

The wizard validates the information that you have entered, confirms that the port is up, and notifies you of any settings that must be changed before you can continue with the wizard. If the settings that you have entered are

valid and the port is up, the wizard's **Configure Your Management Network Interface** screen opens.



e) (Optional) Enter the configuration values for the Management interface, then click **Next**.

As explained in Interface cable connections on page 28, this port is used to access the Catalyst Center GUI from your management network. If you chose to configure a dedicated Management interface, enter the information described in this table. (Refer to Required IP addresses and subnets on page 31 and Required configuration information on page 53 for a more detailed description of the values you must 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 2g.

Table 40: Primary node entries for the Management interface

Host IP Address field	Enter the IP address for the Management interface.
Subnet Mask field	Enter the netmask for the interface's IP address.
Default Gateway IP Address field	Enter a default gateway IP address to use for the interface. **Important** 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.

DNS field	Enter the IP address of the preferred DNS server. 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 Catalyst Center and your NTP server.

The wizard validates the information that you have entered, confirms that the port is up, and notifies you of any settings that must be changed before you can continue with the wizard. If the settings that you have entered are valid and the port is up, the wizard's **Configure Your Internet Access Interface** screen opens, provided you have selected a dedicated **Internet Access Interface** during setting up your appliance interface.

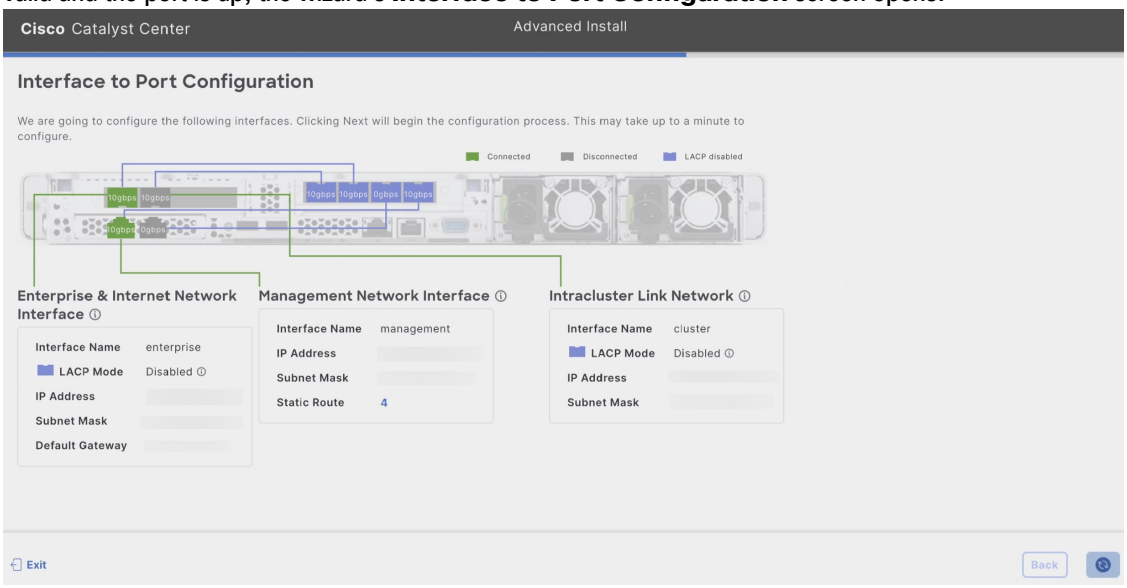
f) (Optional) Enter the configuration values for the Internet Access interface, then click **Next**.

As explained in Interface cable connections on page 28, 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 this table. (Refer to Required IP addresses and subnets on page 31 and Required configuration information on page 53 for a more detailed description of the values you must enter.)

Table 41: Primary node entries for the Internet Access interface

Host IP Address field	Enter the IP address for the Internet Access interface.
Subnet Mask field	Enter the netmask for the interface'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 interface. **Important** 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.
DNS field	Enter the IP address of the preferred DNS server. 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 Catalyst Center and your NTP server.

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

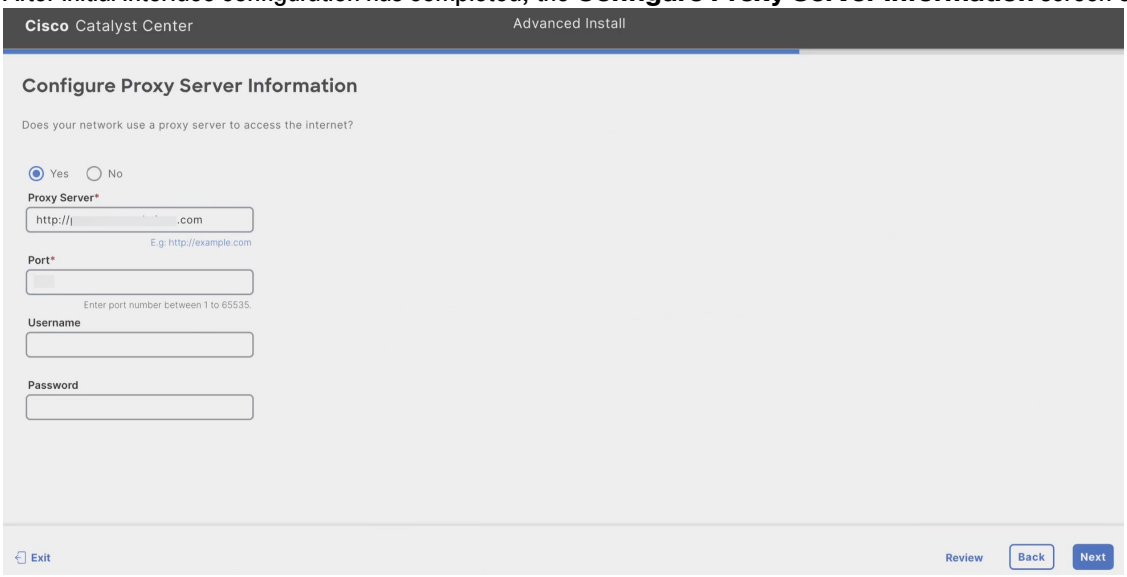


g) Review the settings that you have entered for the primary node's interfaces.

If you must make any changes, click the **Edit** link for the relevant interface.

h) When you are happy with the interface settings, click **Next**.

After initial interface configuration has completed, the **Configure Proxy Server Information** screen opens.



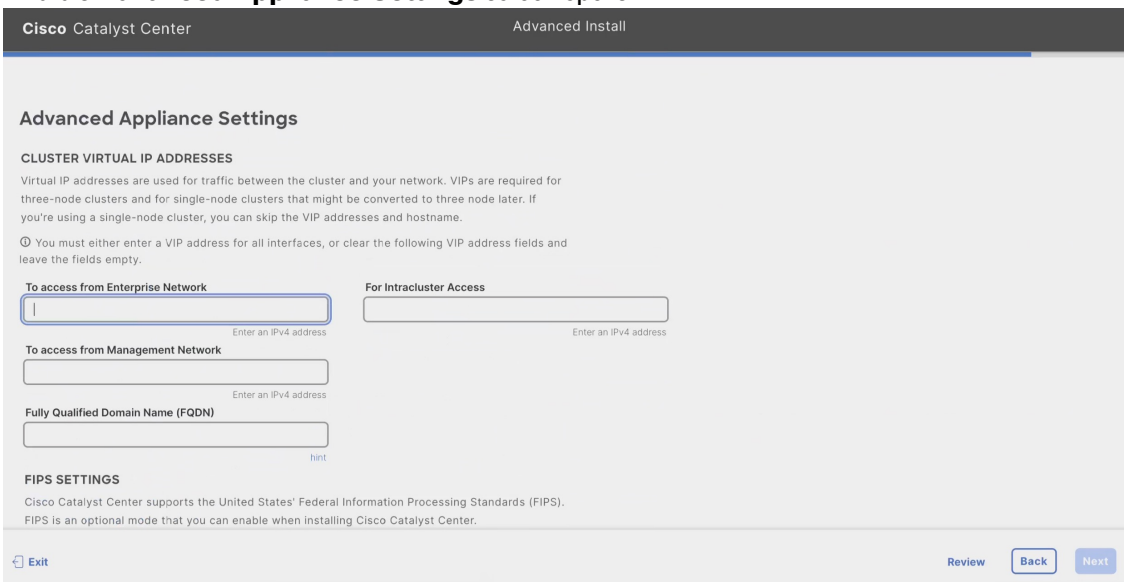
i) Do one of these tasks and then click **Next**:

- 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 this table:

Table 42: 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. **Note** Connection from Catalyst 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 that you have entered and notifies you of any settings that must be changed before you can continue with the wizard. If the settings that you have entered are valid and the port is up, the wizard's **Advanced Appliance Settings** screen opens.



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

Table 43: Primary node entries for advanced appliance settings

Cluster virtual IP addresses

To access from Enterprise Network, For Intracluster Access, To access from Management Network, and For Internet Access fields	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. **Important** If you decide 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 **UP** state.

Note

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.

Fully Qualified Domain Name (FQDN) field	Enter the fully qualified domain name (FQDN) for your cluster. Catalyst Center does these tasks with this hostname: • 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 Catalyst Center manages. • In the Subject Alternative Name (SAN) field of Catalyst Center certificates, it uses the FQDN to the define the Plug and Play server that should be used for device provisioning.

CLI credentials

Enter and confirm the password for the `maglev` user.

Important

Ensure that this password complies with the Password requirements on page 56.

Cisco Catalyst Center admin credentials

Enter a password for the default admin superuser, used to log in to Catalyst Center for the first time.

Important

Ensure that this password complies with the Password requirements on page 56.

NTP server settings

NTP Server field	Enter at least one NTP server address or hostname. To enter additional NTP server addresses or hostnames, click the **Add** (**+**) icon. For a production deployment, Cisco recommends that you configure a minimum of three NTP servers.

Turn On NTP Authentication check box	To enable the authentication of your NTP server before it's synchronized with Catalyst Center, check this check box and then enter this information: • The NTP server's key ID. Valid values range between 1 and 4294967295 (2^32-1). This value corresponds to the key ID that's defined in the NTP server's key file. • 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.

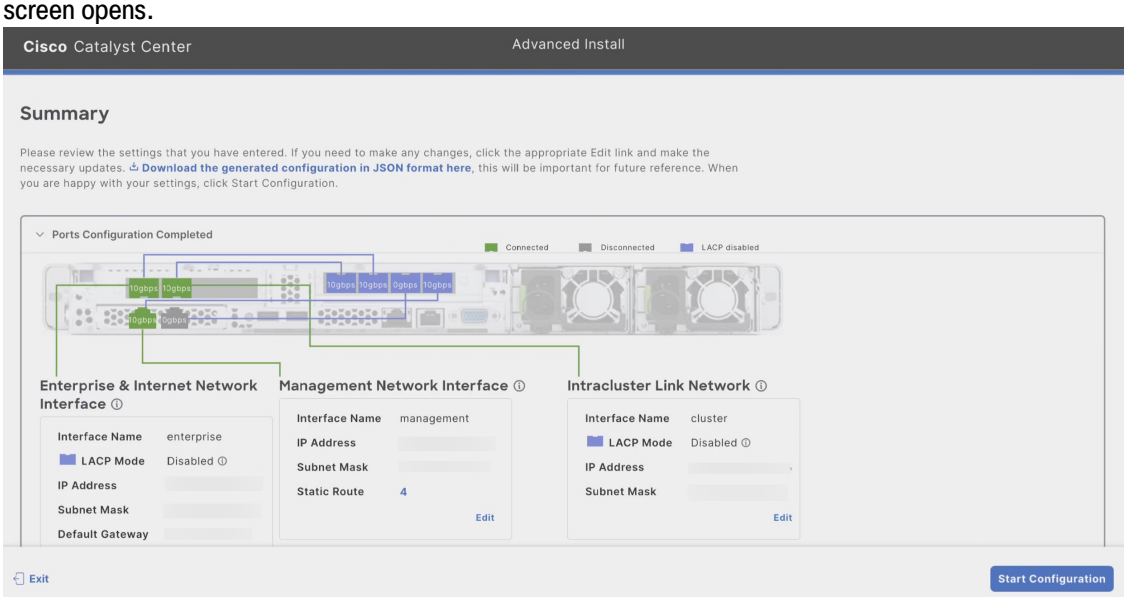
Note

Ensure that you enter a key ID and key value for each NTP server that you configured in the previous field.

Subnet settings

Container Subnet field	A dedicated, non-routed IP subnet that Catalyst Center uses to manage internal services. By default, this is already set to **169.254.32.0/20**, and we recommend that you use this subnet.
Cluster Subnet field	A dedicated, non-routed IP subnet that Catalyst 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 wizard validates the information that you have entered. It also notifies you of any settings that require changes before you can continue with the wizard. If the settings that you have entered are valid, the wizard's **Summary** screen opens.

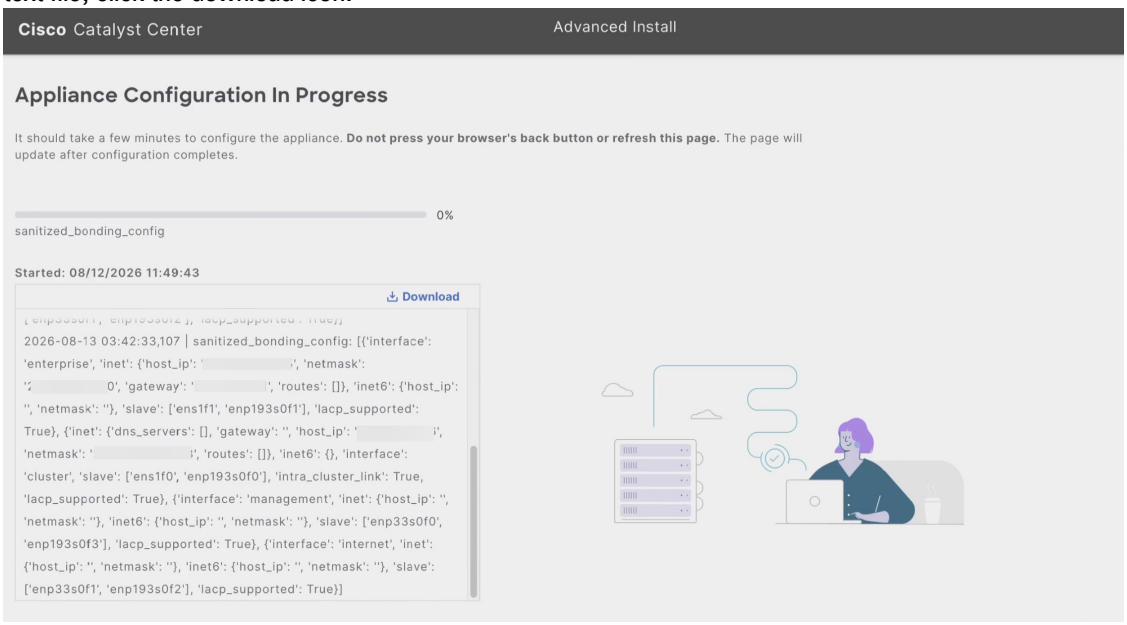


> **Note**
>
> To download the appliance configuration as a JSON file, click the **here** link.

k) Review 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.

l) To complete the configuration of your Catalyst Center appliance, click **Start Configuration**.

The wizard screen continuously updates during the process. It indicates the tasks that Catalyst Center is completing and their progress. It also indicates any errors that have occurred. To save a local copy of this information as a text file, click the download icon.



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 on page 178.
- 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

You can add additional nodes to a cluster using the Advanced Install configuration wizard.

Do these 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 Catalyst Center appliances. Otherwise, unexpected behavior and possible downtime can occur.
- These fourth-generation Catalyst Center appliances support configuration using the Advanced Install configuration wizard:
  - Medium appliance:
    - Standard: DN4-HW-APL
  - Large appliance:
    - Standard: DN4-HW-APL-L
  - Extra large appliance:
    - Standard: DN4-HW-APL-XL
- You can only use this wizard to complete the initial configuration of a new Catalyst Center appliance. To reimage an appliance that's been configured previously, you will need to use the Maglev Configuration wizard.
- 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 Catalyst Center for the first time.
- Enter valid IP addresses and netmasks during this procedure. Also make sure that the addresses and their corresponding subnets do not overlap. Service communication issues can result if they do.

Specify the first appliance in the cluster as the primary node when joining each new secondary node. Consider this information when joining secondary nodes to a cluster:

- Ensure all installed packages are deployed on the primary node before adding a new node to the cluster. You can check this by using Secure Shell to log in to the primary node's Catalyst 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`.

```
maglev-1 [main - https://kong-                                :443]

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

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

- 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 it results 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:

- Configured the first appliance in the cluster.
- Collected all of the information called for in Required IP addresses and subnets on page 31 and Required configuration information on page 53.
- Installed the second and third appliances, as described in Appliance installation workflow on page 58.
- Have completed these tasks:
  1. Ran the **maglev package status** command on the first appliance.

     You can also access this information from the Catalyst 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 the Cisco Integrated Management Controller on page 66.
- Checked that both secondary nodes' ports and the switches they use are properly configured, as described in Execute preconfiguration tasks on page 71.
- Are using a compatible browser. For a list of compatible browsers, refer to the Release Notes for the version of Catalyst Center you are installing.
- Enabled ICMP on the firewall between Catalyst Center and both the default gateway and the DNS server you specify in this topic 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.

Procedure

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 (refer to Enable browser access to the Cisco Integrated Management Controller on page 66).

      After successful login, the appliance displays the **Cisco Integrated Management Controller Chassis Summary** window, with a blue link menu at the upper right.

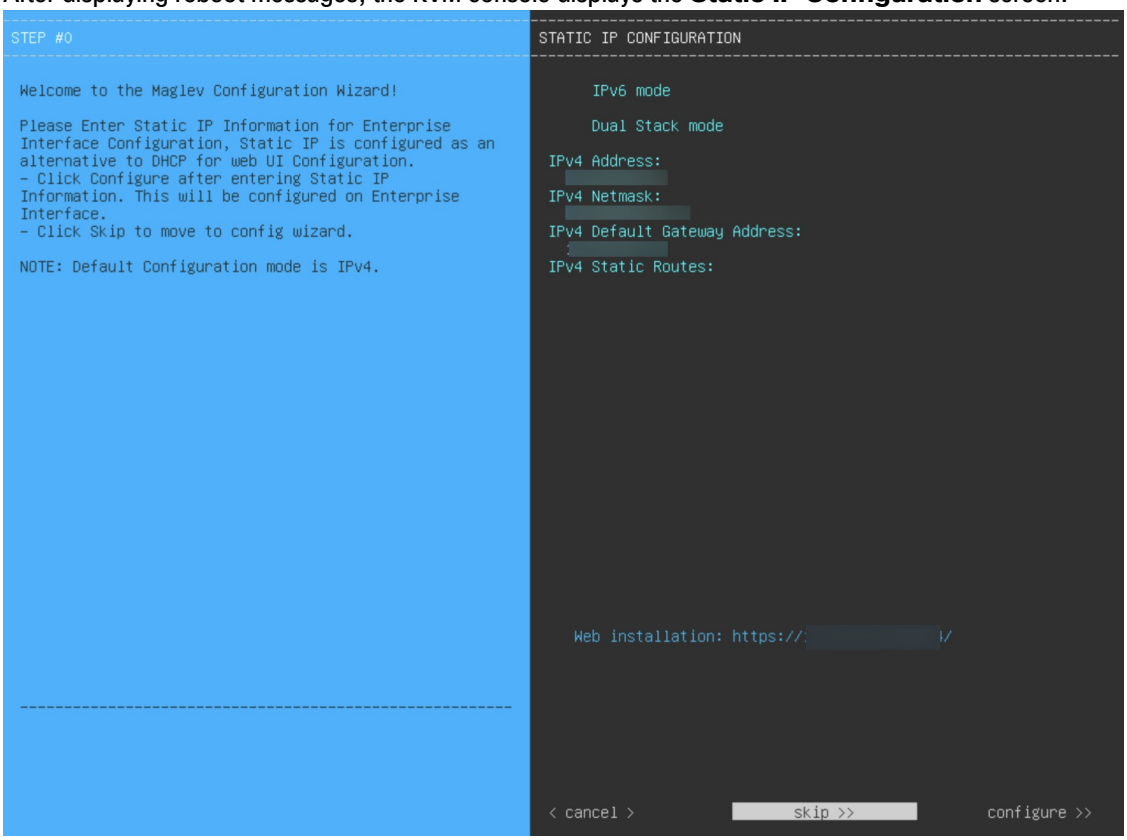
   b) From the blue link menu, select **Launch KVM** and then select **HTML based KVM**.

      The KVM console opens in a separate browser window or tab automatically. Use it 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 these 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.



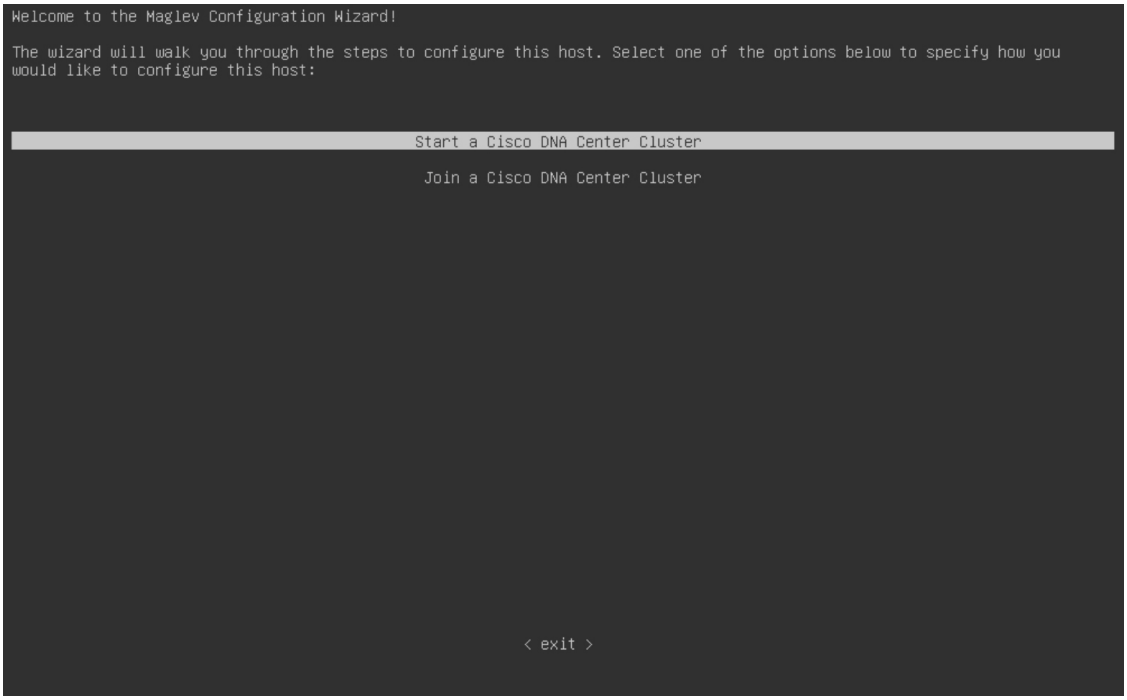
Remember the URL listed in the **Web Installation** field.

d) Do one of these tasks:

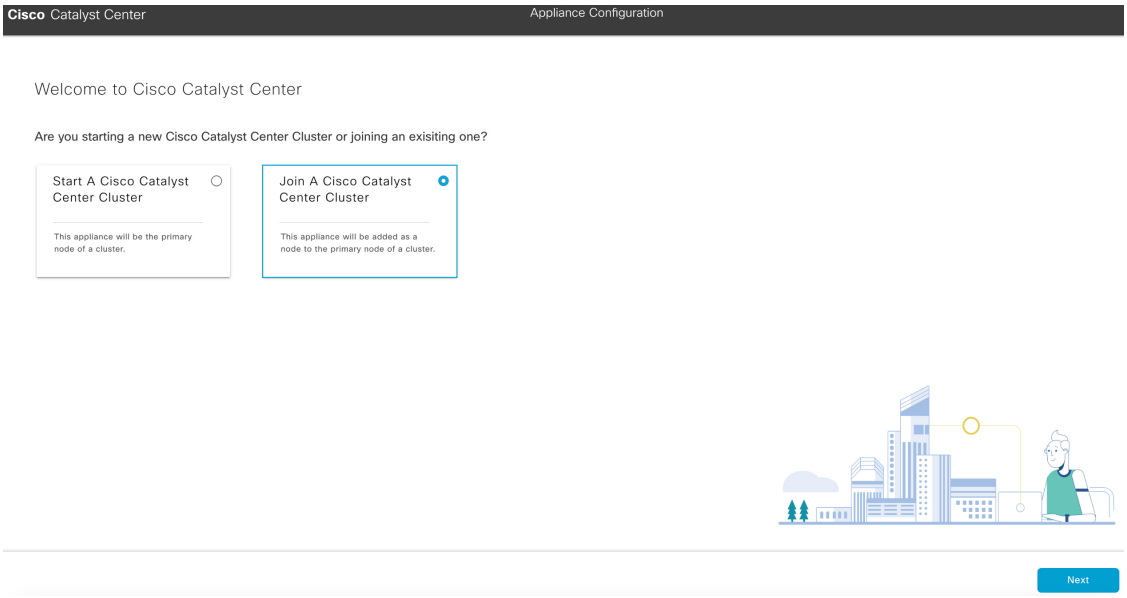
- If you want a DHCP server to assign an IP address, subnet mask, and default gateway to your appliance's Enterprise interface, click **Skip**.
- If you want to assign your own IP address, subnet mask, and default gateway to your appliance's Enterprise interface, enter the information described in this 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: • If you entered an IPv4 address, you can enter either a netmask or CIDR address. • If you entered an IPv6 address, you can only enter a CIDR address.
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 this format, separated by spaces: <*network*>/<*netmask*>/<*gateway*>. This is usually required on the Management port only.

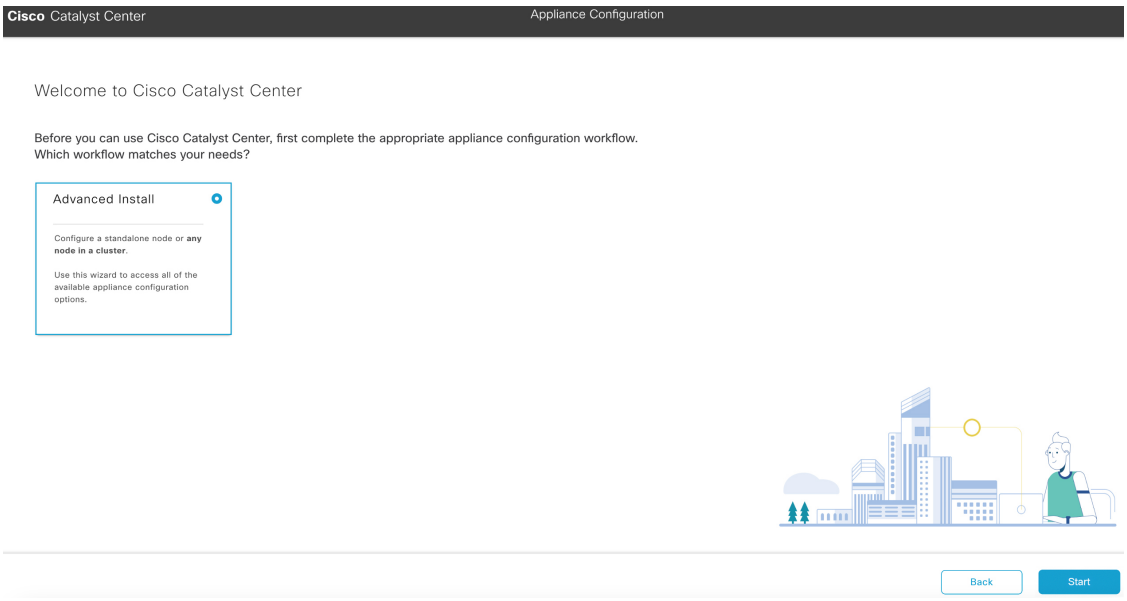
The KVM console displays the Maglev Configuration wizard welcome screen.



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

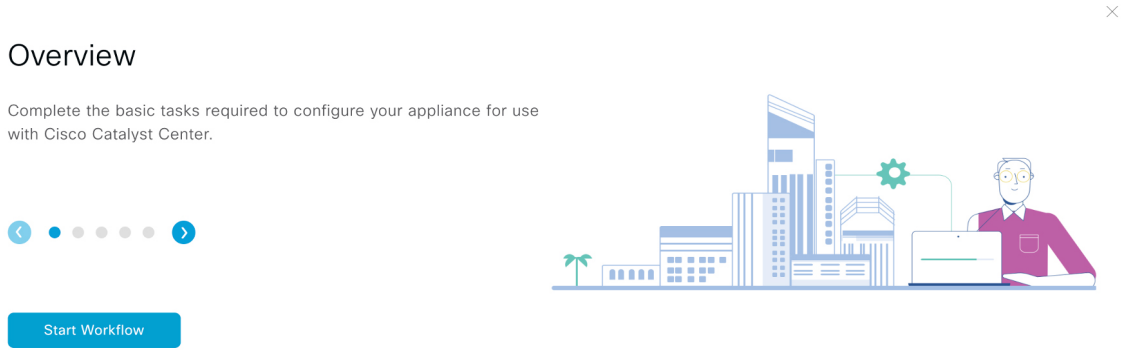


f) Click the **Join a Cisco Catalyst Center Cluster** radio button, then click **Next**.



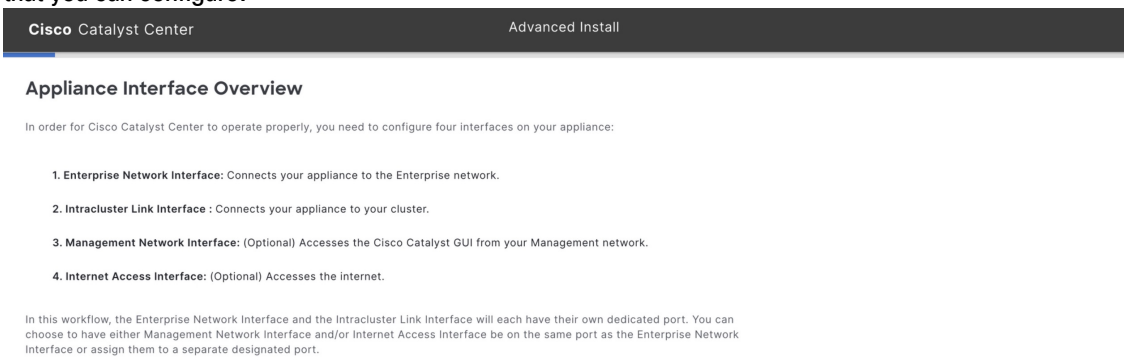
g) Click the **Advanced Install** radio button, then click **Start**.

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



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.

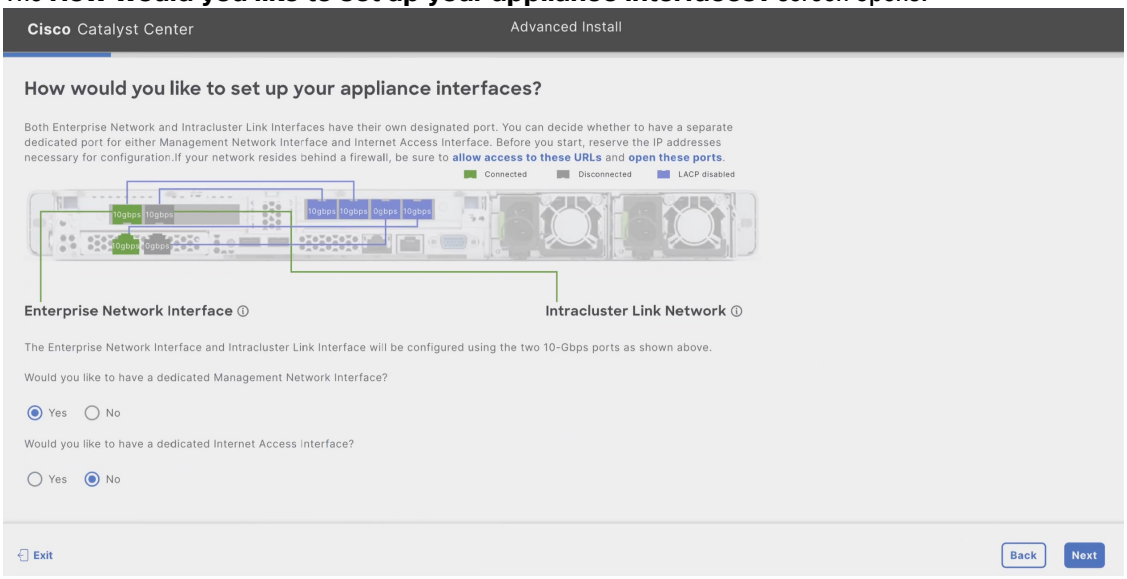


Important

At a minimum, you must configure the interfaces on your appliance's Enterprise and Cluster ports, as they are required for Catalyst 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, click **Exit** to exit the wizard immediately. Be sure you have completed all of the steps provided in Execute preconfiguration tasks on page 71 before resuming configuration or contacting the Cisco Technical Assistance Center (TAC).

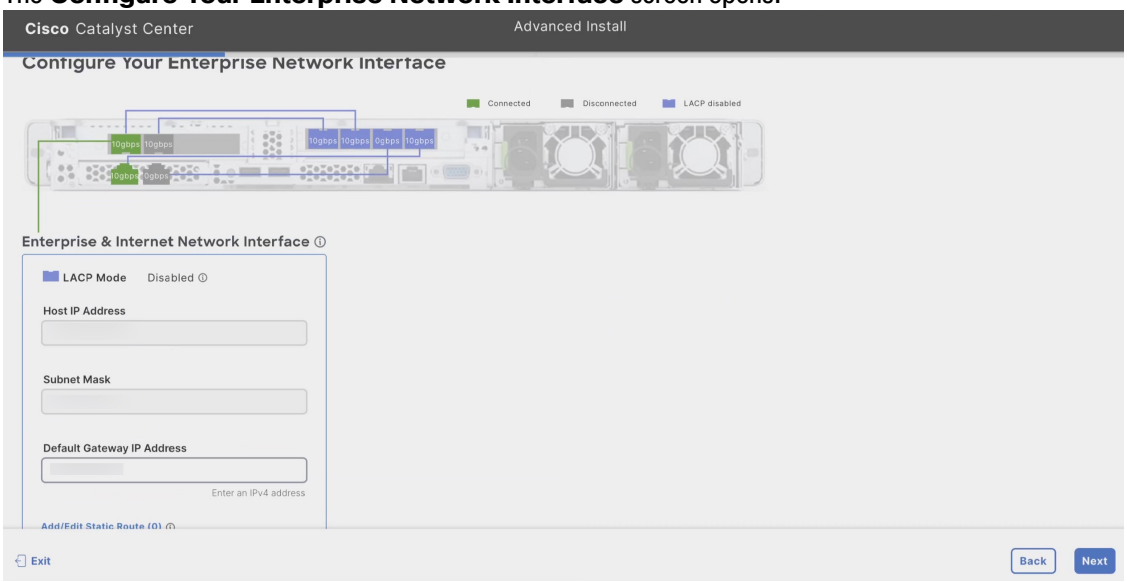
2. Complete the Advanced Install configuration wizard:
   a) Click **Next**.

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



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

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



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

As explained in Interface cable connections on page 28, this is a required interface used to link the appliance to the enterprise network. Refer to Required IP addresses and subnets on page 31 and Required configuration information on page 53 for a more detailed description of the values you need to enter.

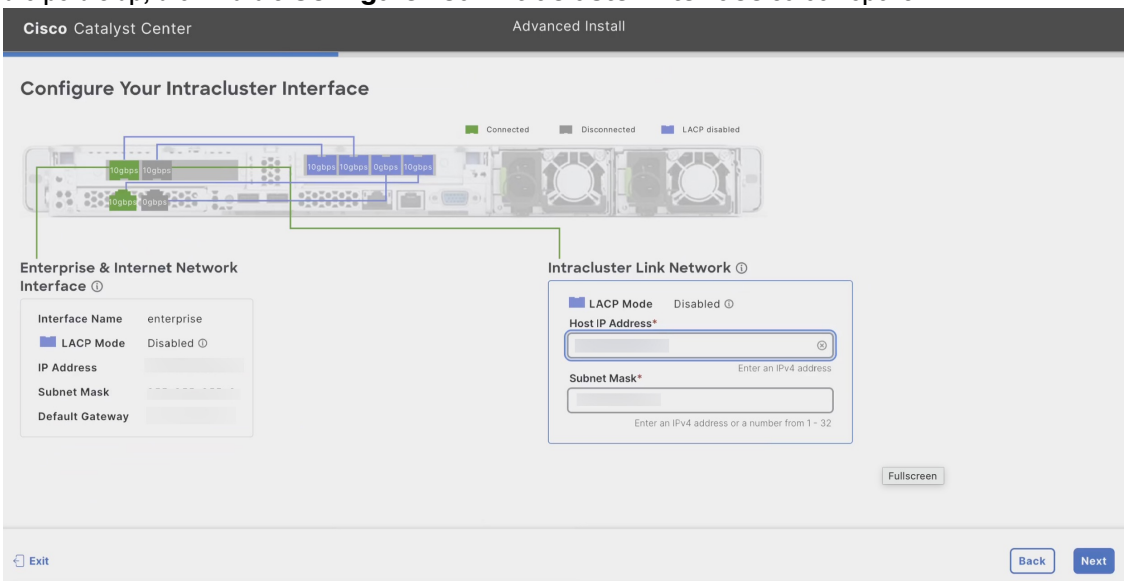
Table 44: Secondary node entries for the Enterprise interface

LACP Mode slider	Select one of these network interface controller (NIC) bonding modes for the Enterprise interface: • **Active-Backup 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. • **LACP mode**: 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. For more information about Catalyst Center's implementation of NIC bonding, refer to NIC bonding overview on page 74.
Host IP Address field	Enter the IP address for the Enterprise interface. This is required.
Subnet Mask field	Enter the netmask for the interface's IP address. This is required.

Default Gateway IP Address field	Enter a default gateway IP address to use for the interface. **Important** 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. **Note** You designated this interface to use the default gateway assigned to it by a DHCP server. Complete these steps to specify a different gateway: 1. Delete the IP address that is currently listed in this field and then click **Exit**. This will bring you back to the first wizard screen. 2. Return to the Enterprise port's wizard screen and enter the gateway IP address you want to use.
DNS field	Enter the IP address of the preferred DNS server. To enter additional DNS servers, click the **Add** (**+**) icon. **Important** • Configure up to three DNS servers per node in your cluster. Problems can occur if you configure more than three DNS servers for an appliance. • For NTP, ensure port 123 (UDP) is open between Catalyst Center and your NTP server.

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 continue 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.



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

As explained in Interface cable connections on page 28, this required port is used to link the appliance to your cluster. Refer to Required IP addresses and subnets on page 31 and Required configuration information on page 53 for a more detailed description of the values you need to enter.

Note

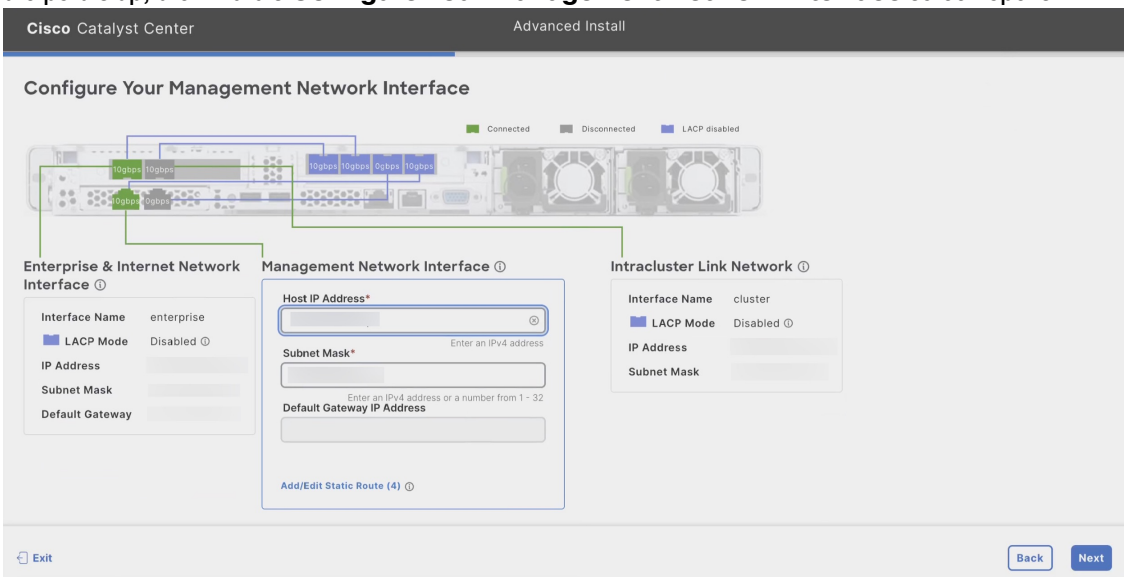
- If you opted to configure the Enterprise and Internet Access interfaces on the same port, complete this step and then continue to Step 2e (which describes how to configure your Management interface).
- If you opted to configure the Enterprise and Management interfaces on the same port, complete this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

Table 45: Secondary node entries for the Intracluster interface

LACP Mode slider	Select one of these NIC bonding modes for the Intracluster interface: • **Active-Backup 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. • **LACP mode**: 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. **Important** If you want to enable LACP mode on your appliance's Intracluster interface, do so now. You won't be able to after you complete this wizard. For more information about Catalyst Center's implementation of NIC bonding, refer to NIC bonding overview on page 74.
Host IP Address field	Enter the IP address for the Intracluster interface. This is required. **Note** You cannot change the address of the Intracluster interface later.
Subnet Mask field	Enter the netmask for the interface'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 continue 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.



e) (Optional) Enter configuration values for the Management interface, then click **Next**.

As explained in Interface cable connections on page 28, this port is used to access the Catalyst Center GUI from your management network. If you chose to configure a dedicated Management interface, enter the information described in this table. (Refer to Required IP addresses and subnets on page 31 and Required configuration information on page 53 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 2g.

Table 46: Secondary node entries for the Management interface

Host IP Address field	Enter the IP address for the Management interface. This is required.
Subnet Mask field	Enter the netmask for the interface's IP address. This is required.
Default Gateway IP Address field	Enter a default gateway IP address to use for the interface. **Important** 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.

DNS field	Enter the IP address of the preferred DNS server. 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 Catalyst Center and your NTP server.

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 continue 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, provided you have selected a dedicated **Internet Access Interface** during setting up your appliance interface.

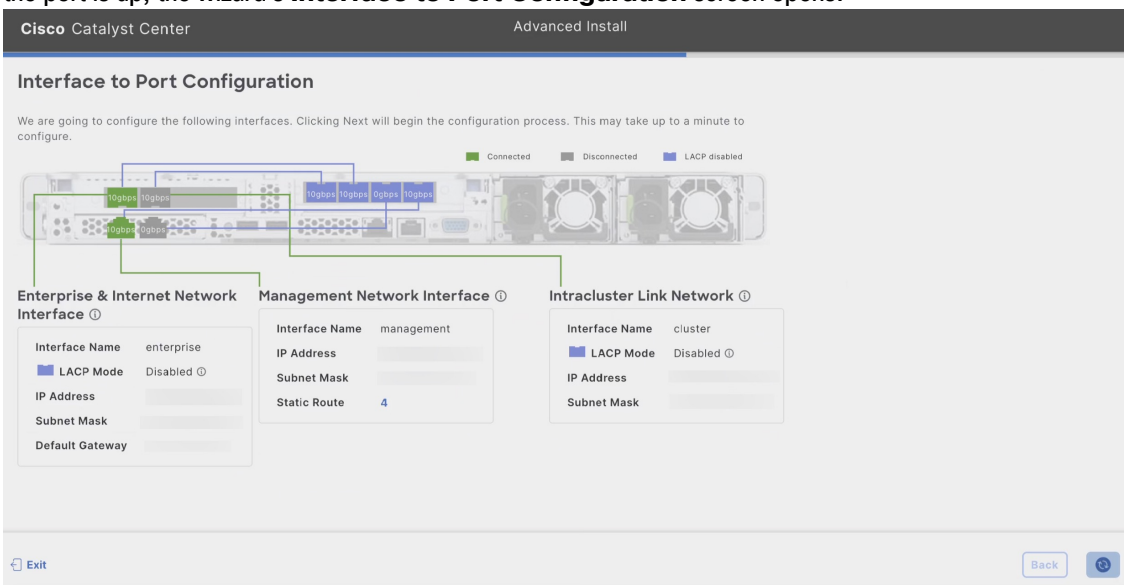
f) (Optional) Enter configuration values for the Internet Access interface, then click **Next**.

As explained in Interface cable connections on page 28, this is an optional port used to link the appliance to the Internet when you cannot do so through the Enterprise port. If you decided to configure a dedicated Internet Access interface, enter the information described in this table. (Refer to Required IP addresses and subnets on page 31 and Required configuration information on page 53 for a more detailed description of the values you need to enter.)

Table 47: Secondary node entries for the Internet Access interface

Host IP Address field	Enter the IP address for the Internet Access interface.
Subnet Mask field	Enter the netmask for the interface'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 interface. **Important** 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.
DNS field	Enter the IP address of the preferred DNS server. 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 Catalyst Center and your NTP server.

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 continue 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.

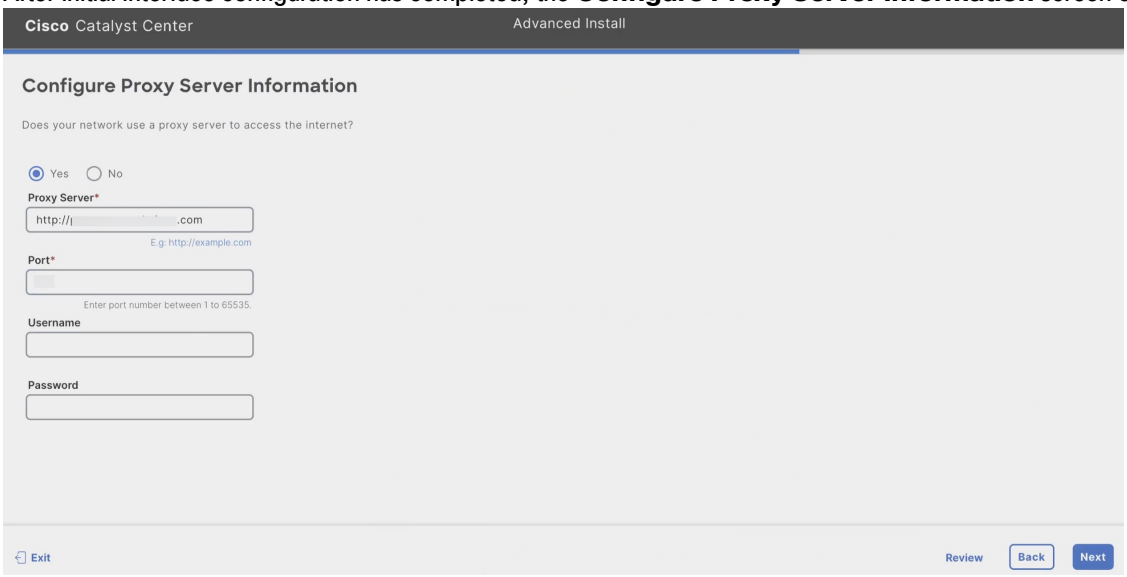


g) Review the settings that you have entered for the secondary node's interfaces.

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

h) When you are happy with the interface settings, click **Next**.

After initial interface configuration has completed, the **Configure Proxy Server Information** screen opens.



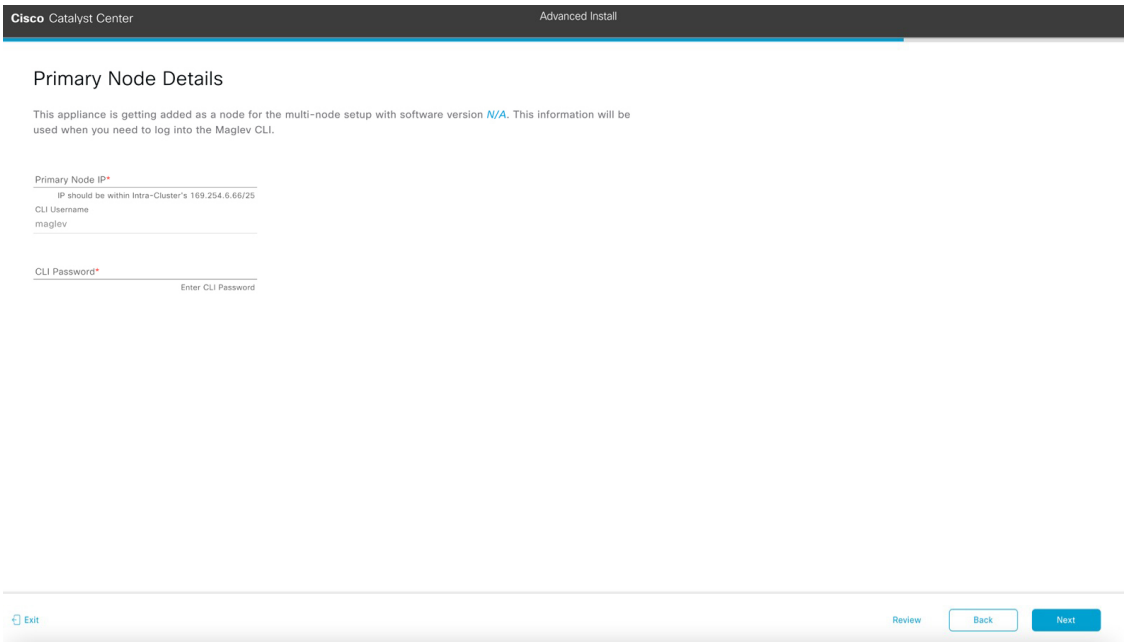
i) Do one of these task and then click **Next**:

- 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 this table:

Table 48: Secondary node entries for proxy server settings

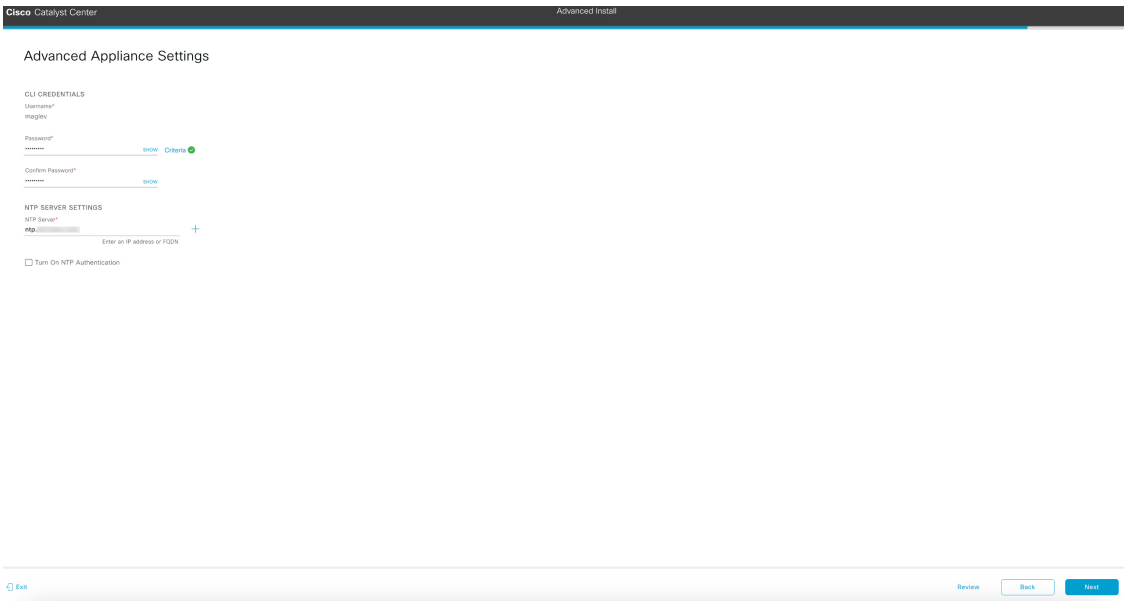
Proxy Server field	Enter the URL or host name of an HTTPS network proxy used to access the Internet. **Note** Connection from Catalyst Center to the HTTPS proxy is supported only through HTTP in this release.
Port field	Enter the port your appliance used to access the network proxy.
Username field	Enter 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 continue with the wizard. If the settings you have entered are valid, the wizard's **Primary Node Details** screen opens.



j) 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.



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

Table 49: Secondary node entries for advanced appliance settings

CLI Credentials

Enter and confirm the password for the `maglev` user.

Important

Ensure that this password complies with the Password requirements on page 56.

NTP Server Settings

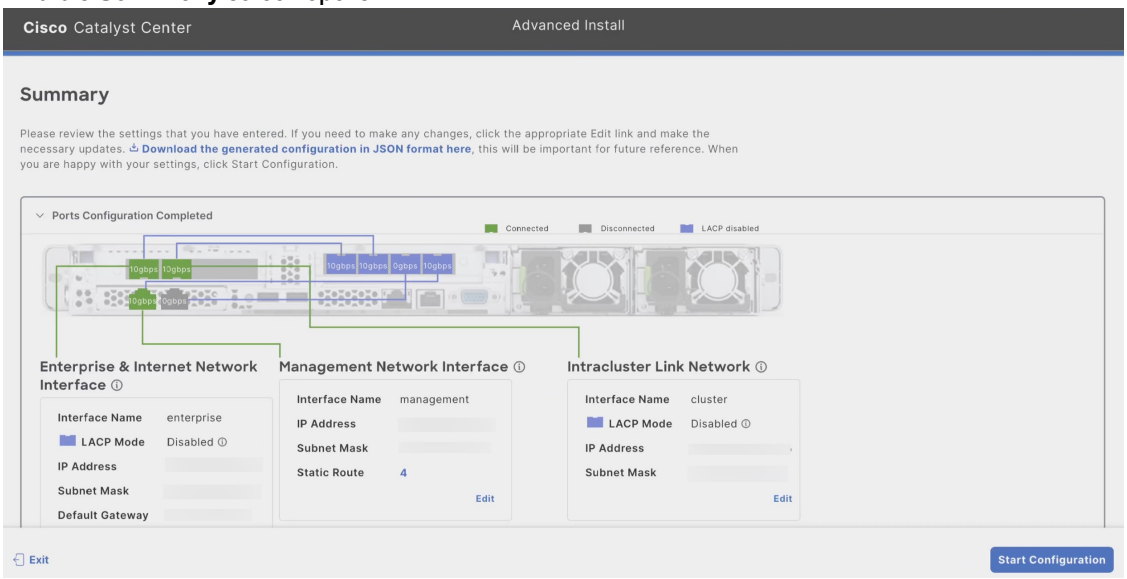
NTP Server field	Enter at least one NTP server address or hostname. To enter additional NTP server addresses or hostnames, click the **Add** (**+**) icon. For a production deployment, Cisco recommends that you configure a minimum of three NTP servers.

Turn On NTP Authentication check box	To enable the authentication of your NTP server before it's synchronized with Catalyst Center, check this check box and then enter this information: • The NTP server's key ID. Valid values range between 1 and 4294967295 (2^32-1). This value corresponds to the key ID that's defined in the NTP server's key file. • 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.

Note

Ensure that you enter a key ID and key value for each NTP server that you configured in the previous field.

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 continue with the wizard. If the settings you have entered are valid, the wizard's **Summary** screen opens.



Note

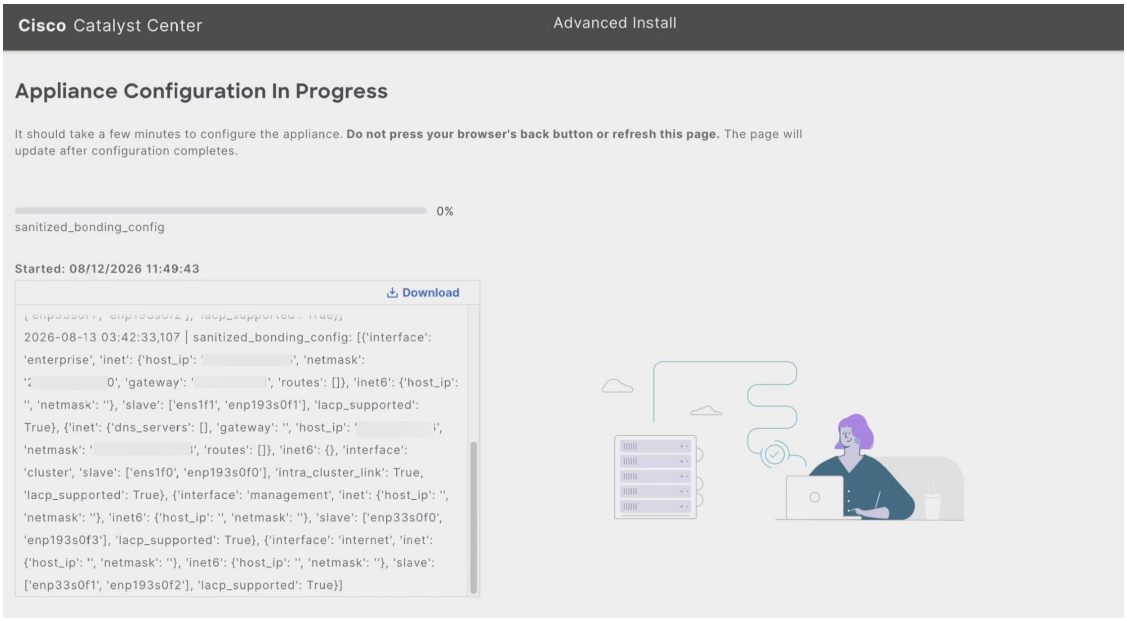
To download the appliance configuration as a JSON file, click the **here** link.

l) 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.

m) To complete the configuration of your Catalyst 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.



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, complete the first-time setup: First-time setup workflow on page 178.

Upgrade to the latest Catalyst Center release

You can upgrade to the latest Catalyst Center release.

For information about upgrading your current release of Catalyst Center, see the *Cisco Catalyst Center Upgrade Guide*.

7 Complete First-Time Setup

Topics:

- First-time setup workflow
- Compatible browsers
- Log in to Catalyst Center for the first time
- Complete the Quick Start workflow
- Catalyst Center setup methods
- Integrate Cisco ISE with Catalyst Center
- Configure authentication and policy servers
- Configure SNMP properties

Provides information on initial setup of the Catalyst Center appliance.

First-time setup workflow

Information about the Catalyst Center appliance installation.

After you finish configuring all of the Catalyst Center appliances you have installed, do the tasks described in this chapter to prepare Catalyst Center for production use. Consider these 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). Complete this step after you have configured the SNMP settings for your appliances.

Compatible browsers

Information about Catalyst Center browser support.

The Catalyst Center GUI is compatible with these 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 Catalyst Center be equipped with 64-bit operating systems and browsers.

Log in to Catalyst Center for the first time

After you have installed and configured the Catalyst Center appliance, follow these steps to log in to its GUI for the first time.

After you have installed and configured the Catalyst Center appliance, follow these steps to log in to its GUI for the first time. You will log in for the first time as the admin superuser (with the username admin and the SUPER-ADMIN-ROLE assigned).

> **Note**
>
> Use a compatible, HTTPS-enabled browser when accessing Catalyst Center. For more information, refer to Compatible browsers on page 178.

Before you begin

Make sure that you have this information on hand, so you can log in to Catalyst Center:

- The *admin* superuser username and password that you specified while configuring your Catalyst Center appliance.
- The information described in Required first-time setup information.

Procedure

1. Access the Catalyst Center GUI:

a) After the Catalyst Center appliance reboot completes, do one of these tasks:

- If you used the browser-based configuration wizard: Click **Open Catalyst Center Virtual Appliance** on the last page of the wizard.
- If you used the Maglev Configuration wizard: Launch a compatible, HTTPS-enabled browser. Then enter the host IP address to access the Catalyst Center GUI, using **`HTTPS://`** and the IP address of the Catalyst Center GUI, which appears at the end of the configuration process.

One of these messages appears (depending on the browser you are using):

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

b) Click **Advanced** to continue.

One of these 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 about how Catalyst Center uses certificates, refer to "Certificate and private key support" in the *Cisco Catalyst Center Administrator Guide*.

c) Do one of these tasks to continue:

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

2. Log in to Catalyst Center:

a) After the Catalyst Center login window opens, do one of these configuration wizard completion tasks:

- With Maglev configuration wizard completion and selection of the **Start using DNAC pre manufactured cluster** option, enter the admin username (**admin**) and password (**P@ssword9**).
- With Maglev configuration wizard completion and selection of the **Start configuration of DNAC in advanced mode** option, enter the admin username (**admin**) and password that you configured for your Catalyst Center appliance.
- With Install configuration wizard completion, enter the admin username (**admin**) and paste the password (**P@ssword9**) that you copied from the last wizard window.
- With Advanced Install configuration wizard completion, enter the admin username (**admin**) and password that you set when you configured your Catalyst Center appliance.

b) Click **Log In**.

3. Configure a new admin user, as a security measure:
   a) Enter this information:
      - **Roles**: Confirm that the `SUPER-ADMIN` role is already set.
      - **New Username**: Enter the admin user username.
      - **Email**: Enter the admin user email address.
      - **New Password** and **Confirm Password**: Enter the admin user password. Ensure that this password complies with the Password requirements on page 56.

        Note

        Changing the default password is critical to network security, especially when the people who set up the appliance are not the same people who will serve as its administrators.

   b) Click **Submit**.

   Catalyst Center logs you out.

4. Log back in to Catalyst Center:
   a) Click **Log In**.
   b) Enter the new admin username and password that you just configured.
   c) Click **Log In**.

   You are prompted to authenticate using your cisco.com credentials, which are used to register software downloads and receive system communications.

5. Click **Authenticate**.

   Note

   If you don't want to authenticate now, click **Skip** instead.

6. Confirm that an activation code is listed in the **Activate your device** pop-up window, then click **Next**.

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

7. Review the documents and 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 Catalyst Center.

What to do next

You can continue with the first-time setup by completing either the Quick Start workfow or one of the enhanced setup methods. For more information, refer to Complete the Quick Start workflow on page 181 and Catalyst Center setup methods on page 186.

Complete the Quick Start workflow

Describes how to discover devices and enable telemetry collection for those devices.

Complete this workflow to discover the devices that Catalyst Center will manage and enable the collection of telemetry from those devices.

> **Note**
>
> Alternatively, you can set up Catalyst Center using one of the enhanced setup methods. For more information, refer to Catalyst Center setup methods on page 186.

After 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.

Before you begin

Ensure that you meet these prerequisites:

- Initial setup: You successfully logged in to Catalyst Center for the first time and created a new admin user. For more information, refer to Log in to Catalyst Center for the first time on page 178.
- Required information: You have the information described in on hand.

  This includes:

  - User access planning: A list of users who need access to the system, including their roles, unique passwords, and privilege settings.
  - Service integration (optional): If you plan to use an IPAM server or Cisco Identity Services Engine (ISE), have the relevant URL and login information ready.

Procedure

1. In the **Quick Start Overview** slider, select **Let's Do it**.
2. In the **Discover Devices: Provide IP Ranges** screen, enter this information and then select **Next**:
   - The name for the device discovery job.
   - The IP address ranges of the devices you want to discover. Select **+** to enter additional ranges.
   - Specify whether you want to designate your appliance's loopback address as its preferred management IP address. For more information, refer to the "Preferred management IP address" topic in the "Discover Your Network" chapter of the *Cisco Catalyst Center User Guide*.
3. In the **Discover Devices: Provide Credentials** screen, enter the information described in Device credential information on page 182 for the type of credentials you want to configure and then select **Next**.

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

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

5. In the **Enable Telemetry** screen, check the network components that you want Catalyst Center to collect telemetry for and then select **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.

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

     Catalyst 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 home page after the Quick Start workflow has completed.

What to do next

- Select **View Discovery** to open the **Discovery** page and confirm that the devices in your network have been discovered.
- Select 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.
- Select 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 Catalyst Center has already scheduled to run.
- Select the **Workflow Home** link to access guided workflows that will help you set up and maintain your network.

Device credential information

Describes the information that needs to be entered in the **Discover Devices: Provide Credentials** screen.

This table describes the information you need to enter in the **Discover Devices: Provide Credentials** screen when completing the Quick Start workflow.

Table 50: Description of device credential fields

Field	Description
CLI (SSH) Credentials	
Username	Username used to log in to the CLI of the devices in your network.

Field	Description
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.

SNMP Credentials: SNMPv2c Read tab

> **Note**
>
> Catalyst 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, refer to Configure the primary node using the Maglev wizard.

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.

SNMP Credentials: SNMPv2c Write tab

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.

SNMP Credentials: SNMPv3

Name/Description	Name or description of the SNMPv3 credentials.
Username	Username associated with the SNMPv3 credentials.

Field	Description
Mode	Security level that SNMP messages require: • **No Authentication, No Privacy** (noAuthnoPriv): Does not provide authentication or encryption. • **Authentication, No Privacy** (authNoPriv): Provides authentication, but does not provide encryption. • **Authentication and Privacy** (authPriv): Provides both authentication and encryption. **Note** When FIPS mode is enabled, Catalyst Center only supports **Authentication and Privacy** mode.
Authentication Password	Password required to gain access to information from devices that use SNMPv3. The password must be at least eight characters in length. Note the following points: • 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 Catalyst Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.

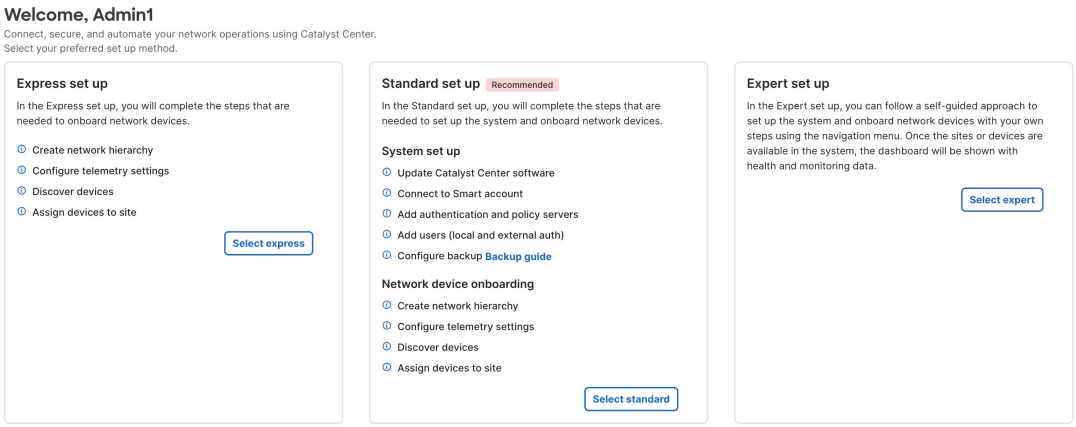
Field	Description
Authentication Type	Hash-based Message Authentication Code (HMAC) type used when either **Authentication and Privacy** or **Authentication, No Privacy** is set as the authentication mode: • **SHA**: HMAC-SHA authentication. • **MD5**: HMAC-MD5 authentication. **Note** Catalyst Center does not support this authentication type when FIPS mode is enabled.
Privacy Type	Privacy type. (Enabled if you select **Authentication and Privacy** as **Mode**.) Choose one of the following privacy types: • **AES128**: 128-bit CBC mode AES for encryption. • **CISCOAES192**: 192-bit CBC mode AES for encryption on Cisco devices. • **CISCOAES256**: 256-bit CBC mode AES for encryption on Cisco devices. **Note** • Privacy types CISCOAES192 and CISCOAES256 are supported only for use with Discovery and Inventory features. Assurance features are not supported. • Privacy type AES128 is supported for Discovery, Inventory, and Assurance.
Privacy Password	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. **Note** • 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 Catalyst Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.

Field	Description
NETCONF	
Port	The NETCONF port that Catalyst Center should use in order to discover wireless controllers that run Cisco IOS-XE.

Catalyst Center setup methods

You can set up Catalyst Center using one of the available setup methods.

When you log in for the first time, the Quick Start workflow automatically starts. To view the enhanced setup methods, exit the Quick Start workflow and go to the default home page. The default home page displays the available setup methods.



If you have SUPER-ADMIN-ROLE or NETWORK-ADMIN-ROLE permissions, you can set up Catalyst Center using one of these methods:

- Express setup: This setup helps you onboard network devices. For instructions, see Complete the express setup method.
- Standard setup: This recommended setup helps you set up the system and onboard network devices. For instructions, see Complete the standard setup method.
- Expert setup: This self-directed setup allows you to independently set up the system and onboard network devices. We recommend this option for expert users only. For instructions, see Complete the expert setup on page 191.

Note

If you start one setup method and later decide that you'd prefer to use a different setup method, you can change your selected method. Return to the default home page and click **Select <setup method name>** to start a different setup method.

Complete the express setup

Follow these steps to set up Catalyst Center using the express setup method.

Follow these steps to set up Catalyst Center using the express setup method.

Before you begin

Ensure that you successfully completed Log in to Catalyst Center for the first time on page 178.

Procedure

1. From the home page, click **Select express**.

   The express setup method starts and opens the **Design** > **Network Hierarchy** page. The **Express set up** slide-in pane displays the steps to complete this setup method.

   Tip

   - We recommend that you complete the steps in the order that they are presented.
   - You can view the relevant page for any step by clicking **Go to this step**.
   - You can close the **Express set up** slide-in pane at any time by clicking **Exit**. In the dialog box, click **Exit** again.
   - After you complete at least one of the listed steps, you can reopen this slide-in pane by clicking **Express set up** in the top-right portion of Catalyst Center.
   - You can view all completed steps by scrolling to the end of this slide-in pane and opening the **<Number of> steps completed** section. To mark a completed step as incomplete, check the **Mark as complete** check box for that step. The step becomes incomplete, and the progress bar updates to reflect this change.

2. Complete the create network hierarchy step.
   a) On the **Design** > **Network Hierarchy** page, create the network hierarchy—including areas, buildings, and floors.

      For instructions, refer to the "Design the Network Hierarchy" chapter in the *Cisco Catalyst Center User Guide*.

   b) Under **Create network hierarchy**, check the **Mark as complete** check box for this step.

      The progress bar updates and indicates that one of four steps is complete.

3. Complete the telemetry settings step.
   a) Under **Configure telemetry settings**, click **Go to this step**.
   b) On the **Design** > **Network Settings** page for **Telemetry**, configure the required telemetry settings for telemetry data collection.

      For instructions, refer to "Configure syslog, SNMP traps, NetFlow Collector servers, and wired client data collection using telemetry" in the *Cisco Catalyst Center User Guide*.

   c) Under **Configure telemetry settings**, check the **Mark as complete** check box for this step.

      The progress bar updates and indicates that two of four steps are complete.

4. Complete the discover devices step.
   a) Under **Discover devices**, click **Go to this step**.

      The onboard devices workflow begins.

   b) Discover your devices by completing the onboard devices workflow.

For instructions, refer to "Do Discovery" in the *Cisco Catalyst Center User Guide*.

c) Under **Discover devices**, check the **Mark as complete** check box for this step.

The progress bar updates and indicates that three of four steps are complete.

5. Complete the assign devices to site step.
   a) Under **Assign devices to site**, click **Go to this step**.
   b) On the **Provision** > **Inventory** page, assign your devices to the relevant sites.

   For instructions, refer to "Assign an unprovisioned device to a site" or "Assign a provisioned device to a different site" in the *Cisco Catalyst Center User Guide*.

   c) Under **Assign devices to site**, check the **Mark as complete** check box for this step.

   The progress bar updates and indicates that four of four steps are complete. A completion message summarizes the number of created sites and discovered devices.

6. Click **Launch home page** to complete the express setup of Catalyst Center.

   The home page displays when the express setup of Catalyst Center is complete.

> **Note**
>
> The system may take some time to display discovered devices on the home page.

Complete the standard setup

Follow these steps to set up Catalyst Center using the standard setup method.

Follow these steps to set up Catalyst Center using the standard setup method.

Before you begin

Ensure that you successfully completed Log in to Catalyst Center for the first time on page 178.

Procedure

1. From the home page, click **Select standard**.

   The standard setup method starts and opens the **System** > **Software Management** page. The **Standard set up** slide-in pane displays the steps to complete this setup method.

Tip

- We recommend that you complete the steps in the order that they are presented.
- You can view the relevant page for any step by clicking **Go to this step**.
- You can close the **Standard set up** slide-in pane at any time by clicking **Exit**. In the dialog box, click **Exit** again.
- After you complete at least one of the listed steps, you can reopen this slide-in pane by clicking **Standard set up** in the top-right portion of Catalyst Center.
- You can view all completed steps by scrolling to the bottom of this slide-in pane and opening the **<Number of> steps completed** section. To mark a completed step as incomplete, check the **Mark as complete** check box for that step. The step becomes incomplete, and the progress bar updates to reflect this change.

2. Complete the update the Catalyst Center software step.
   a) On the **System** > **Software Management** page, update the Catalyst Center software to the latest recommended version.

      For instructions, refer to the *Cisco Catalyst Center Upgrade Guide*.

   b) Under **Update Catalyst Center software**, check the **Mark as complete** check box for this step.

      The progress bar updates and indicates that one of nine steps is complete.

3. Complete the connect to smart account step.
   a) Under **Connect to Smart account**, click **Go to this step**.
   b) On the **Smart Account** page, connect your Cisco Smart Account to your Smart Licensing account.

      For instructions, refer to "Configure Smart Account" in the *Cisco Catalyst Center Administrator Guide*.

   c) Under **Connect to Smart account**, check the **Mark as complete** check box for this step.

      The progress bar updates and indicates that two of nine steps are complete.

4. Complete the add authentication and policy servers step.
   a) Under **Add authentication and policy servers**, click **Go to this step**.
   b) On the **Authentication and Policy Servers** page, add either a Cisco Identity Services Engine (Cisco ISE) or AAA server.

      Catalyst Center uses AAA servers for user authentication or Cisco ISE for both user authentication and access control. For instructions, refer to "Configure authentication and policy servers" in the *Cisco Catalyst Center Administrator Guide*.

   c) Under **Add authentication and policy servers**, check the **Mark as complete** check box for this step.

      The progress bar updates and indicates that three of nine steps are complete.

5. Complete the add users step.
   a) Under **Add users (local and external auth)**, click **Go to this step**.
   b) On the **User Management** page, add the required users, so they can access Catalyst Center.

      For instructions, refer to "Create an internal user" in the *Cisco Catalyst Center Administrator Guide*.

   c) If your network requires using an external server for authentication and authorization of external users, enable external authentication.

For instructions, refer to "Configure external authentication" in the *Cisco Catalyst Center Administrator Guide*.

d) Under **Add users (local and external auth)**, check the **Mark as complete** check box for this step.

The progress bar updates and indicates that four of nine steps are complete.

6. Complete the configure backup step.
   a) Under **Configure backup**, click **Go to this step**.
   b) On the **System** > **Backup & Restore** page, configure a remote server to back up your automation and Assurance data from Catalyst Center and connect a remote server to restore automation and Assurance data from Catalyst Center.

   For instructions, refer to "Configure the location to store backup files" and "Restore data from backups" in the *Cisco Catalyst Center Administrator Guide*.

   c) Under **Configure backup**, check the **Mark as complete** check box for this step.

   The progress bar updates and indicates that five of nine steps are complete.

7. Complete the create network hierarchy step.
   a) Under **Create network hierarchy**, click **Go to this step**.
   b) On the **Design** > **Network Hierarchy** page, create the network hierarchy–including areas, buildings, and floors.

   For instructions, refer to the "Design the Network Hierarchy" chapter in the *Cisco Catalyst Center User Guide*.

   c) Under **Create network hierarchy**, check the **Mark as complete** check box for this step.

   The progress bar updates and indicates that six of nine steps are complete.

8. Complete the telemetry settings step.
   a) Under **Configure telemetry settings**, click **Go to this step**.
   b) On the **Design** > **Network Settings** page for **Telemetry**, configure the required telemetry settings for telemetry data collection.

   For instructions, refer to "Configure syslog, SNMP traps, NetFlow Collector servers, and wired client data collection using telemetry" in the *Cisco Catalyst Center User Guide*.

   c) Under **Configure telemetry settings**, check the **Mark as complete** check box for this step.

   The progress bar updates and indicates that seven of nine steps are complete.

9. Complete the discover devices step.
   a) Under **Discover devices**, click **Go to this step**.

   The onboard devices workflow begins.

   b) Discover your devices by completing the onboard devices workflow.

   For instructions, refer to "Do Discovery" in the *Cisco Catalyst Center User Guide*.

   c) Under **Discover devices**, check the **Mark as complete** check box for this step.

   The progress bar updates and indicates that eight of nine steps are complete.

10. Complete the assign devices to site step.
    a) Under **Assign devices to site**, click **Go to this step**.
    b) On the **Provision** > **Inventory** page, assign your devices to the relevant sites.

    For instructions, refer to "Assign an unprovisioned device to a site" or "Assign a provisioned device to a different site" in the *Cisco Catalyst Center User Guide*.

c) Under **Assign devices to site**, check the **Mark as complete** check box for this step.

The progress bar updates and indicates that nine of nine steps are complete. A completion message summarizes the number of created sites and discovered devices.

11. Click **Launch home page** to complete the standard setup of Catalyst Center.

The home page displays when the standard setup of Catalyst Center is complete.

> **Note**
>
> The system may take some time to display discovered devices on the home page.

Complete the expert setup

Follow these steps to set up Catalyst Center using the expert setup method.

Follow these steps to set up Catalyst Center using the expert setup method.

Before you begin

> **Note**
>
> We recommend that only expert network administrators use this setup method. This method does not provide detailed setup instructions. The express and standard setup methods provide step-by-step instructions. For more information, see Catalyst Center setup methods on page 186.

Before you begin

Ensure that you successfully completed Log in to Catalyst Center for the first time on page 178.

Procedure

1. From the home page, click **Select expert**.
2. In the **Expert set up** dialog box, click **Ok** to continue.
3. Set up Catalyst Center as required for your network.

   For general instructions on setting up your network, consider referring to this information:

   - Refer to the "Design the Network Hierarchy" chapter in the *Cisco Catalyst Center User Guide*.
   - Refer to the "Discover Your Network" chapter in the *Cisco Catalyst Center User Guide*.
   - Refer to the "Manage Your Inventory" chapter in the *Cisco Catalyst Center User Guide*.

   After you complete device discovery, the default home page is displayed–indicating that you completed the expert setup of Catalyst Center.

Integrate Cisco ISE with Catalyst Center

Explains how to integrate Cisco ISE and Catalyst Center.

Catalyst 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 Catalyst Center, any device that Catalyst Center discovers, along with relevant configuration and other data, is pushed to Cisco ISE. You can use Catalyst Center to discover devices and then apply both Catalyst Center and Cisco ISE functions to them because these devices will be displayed in both the applications. Catalyst 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 Catalyst Center site hierarchy, Catalyst Center devices are pushed to Cisco ISE. Any updates to a Catalyst 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**
>
> Catalyst 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 Catalyst Center, ensure that you have met these prerequisites:

- You have deployed one or more Cisco ISE hosts on your network. For information on supported Cisco ISE versions, see the *Catalyst 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 Catalyst 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, Catalyst 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 Catalyst 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 decide 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 Catalyst Center.
- Catalyst 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 Catalyst Center and Cisco ISE on these ports: 443, 5222, 8910, and 9060.
- The Cisco ISE host on which pxGrid is enabled must be reachable from Catalyst 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.
- Catalyst 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 Catalyst Center deployment. For more information, see the **alt_names** section in the *Catalyst Center Security Best Practices Guide*.

> **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 Catalyst Center, see the "Integration with Catalyst Center" topic in the *Cisco Identity Services Engine Administrator Guide*.

Procedure

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, choose **API Settings** > **API Service Settings**.
g) Enable **ERS (Read/Write)** and click **OK**.
h) Click **Save**.

2. Add the Cisco ISE node to Catalyst Center as a AAA server:

a) Log in to the Catalyst Center GUI.
b) From the main menu, 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 select **ISE** from the drop-down list.
e) Enter these 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 Catalyst Center system certificate as the pxGrid client certificate (sent to ISE to authenticate the Catalyst Center system as a pxGrid client), check the **Use Catalyst 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, Catalyst 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 Catalyst 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 select the protocol that must be used by checking the check box for **RADIUS** or **TACACS**
    - Enter the required values in these fields: **Authentication Port**, **Accounting Port**, **Retries**, and **(Timeout seconds)**.

> **Note**
>
> This option is available only if third-party certificates are used by Catalyst Center. If Catalyst Center uses the default self-signed system certificate, 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 select **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.

3. Verify that Catalyst Center is connected to Cisco ISE, and that the Cisco ISE SGT groups and devices are pushed to Catalyst Center:
   a) Log in to the Catalyst Center GUI.
   b) From the main menu, choose **System** > **System 360**.
   c) In the Identity Services Engine (ISE) pane, verify that the status of all listed ISE servers is displayed as **Available** or **Configured**.
   d) In the Identity Services Engine (ISE) pane, click the **Update** link.
   e) From the **Authentication and Policy Servers** window, verify that the status of the Cisco ISE AAA server is still **Active**.
4. Verify that Cisco ISE is connected to Catalyst Center and that the connection has subscribers:
   a) Log in to the Cisco ISE nodes that are shown as pxGrid servers in the **Identity Services Engine (ISE)** pane.
   b) Choose **Administration** > **pxGrid Services** and click the **Web Clients** tab.

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

Group-Based Access Control: policy data migration and synchronization

When you install or upgrade Catalyst Center, you must migrate policy data from Cisco ISE. This ensures that the policy data in Catalyst Center and in Cisco ISE is synchronized. This synchronization must complete before you can use the Group-Based Access Control policy functionality.

When you start using Catalyst Center

In earlier releases of Catalyst Center, the Group-Based Access Control policy function stored some policy Access Contracts and Policies locally in Catalyst Center. Catalyst 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 Catalyst 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 Catalyst Center, these steps are necessary before you can use the Group-Based Access Control capabilities.

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

What is “migration and synchronization”?

Catalyst Center reads all the Group-Based Access Control policy data in the integrated Cisco ISE and compares that data with the policy data in Catalyst 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 Catalyst Center.

How does migration and synchronization work?

Usually, the policy data in Cisco ISE and in Catalyst 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. This 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 Catalyst Center.
  - When the Name and SGT value are the same, nothing is changed. The information in Catalyst 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 Catalyst Center, a new Security Group is created in Catalyst Center. The new Security Group is given the default association of “Default_VN.”
  - When a Cisco ISE Security Group SGT value exists in Catalyst Center, but the names do not match, the name from Cisco ISE Security Group replaces the name of that Security Group in Catalyst 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 Catalyst 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 Catalyst Center.

- When the SGACL and Contract have the same name and content, there is no need for further action. The information in Catalyst 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 Catalyst Center is discarded.

When the SGACL name does not exist in Catalyst 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, Catalyst 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 done 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 Catalyst 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 Catalyst Center.
- The Cisco ISE default policy is checked and migrated to Catalyst Center.

Note

Catalyst 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 Catalyst 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 Catalyst 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 Catalyst 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 Catalyst Center.

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

- **Manage Group-Based Access Control policy in Catalyst Center**: If this option is selected, all management of Group-Based Access Control Policy is done in Catalyst 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 Catalyst Center. The policy uses the default policy, and you can select a new contract for those policies after completing the migration. If there was an problem migrating the default policy, the default policy is set to "Permit."

- **Manage Group-Based Access Control Policy in Cisco ISE**: If this option is selected, Catalyst 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 Catalyst Center and Cisco ISE**: This option is not recommended for general use, because policy changes made in Cisco ISE are not synchronized with Catalyst 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

Instructions to configure AAA server and Cisco ISE for Catalyst Center.

Catalyst 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 do both policy and AAA functions, make sure that Catalyst Center and Cisco ISE are integrated.
- If FIPS mode is enabled for Catalyst Center, ensure that you enable KeyWrap when integrating Catalyst Center and Cisco ISE. Refer to Step 2e in Integrate Cisco ISE with Catalyst Center.

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

- If you are using another product (not Cisco ISE) to do AAA functions, make sure to do these tasks:
  - Register Catalyst Center with the AAA server, including defining the shared secret on both the AAA server and Catalyst Center.
  - Define an attribute name for Catalyst Center on the AAA server.
  - For a Catalyst 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 *Catalyst Center Compatibility Matrix*. For information on installing Cisco ISE, refer to the *Cisco Identity Services Engine Install and Upgrade guides*.
  - If you have a standalone ISE deployment, you must integrate Catalyst 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, Catalyst 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 Catalyst 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 decide 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 Catalyst Center and Cisco ISE on these ports: 443, 5222, 8910, and 9060.
- The Cisco ISE host on which pxGrid is enabled must be reachable from Catalyst 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 Catalyst Center system certificate must list both the Catalyst 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*.

Procedure

1. From the main menu, choose **System** > **Settings** > **External Services** > **Authentication and Policy Servers**.
2. From the **Add** drop-down list, select **AAA** or **ISE**.
3. To configure the primary AAA server, enter this 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.
4. To configure a Cisco ISE server, enter these 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 this 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.

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 Catalyst Center system certificate as the pxGrid client certificate (sent to Cisco ISE to authenticate the Catalyst Center system as a pxGrid client), check the **Use Catalyst 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, Catalyst 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 Catalyst 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 Catalyst 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 Catalyst 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.

6. Click **Add**.
7. To add a secondary server, repeat the preceding steps.

Configure SNMP properties

Information about configuring SNMP properties, including retries and timeouts.

You can configure the retry and timeout values for SNMP.

Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can do this procedure. For more information, see the *Cisco Catalyst Center Administrator Guide*.

Procedure

1. From the main menu, choose **System** > **Settings** > **Device Settings** > **SNMP**.
2. Configure these 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 Catalyst 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.
3. Click **Save**.

Note

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

8 Troubleshoot the Deployment

Topics:

- Troubleshooting tasks
- Log out
- Reconfigure the appliance using the Configuration wizard
- Power cycle the appliance

Guides you in troubleshooting the Catalyst Center appliance deployment.

Troubleshooting tasks

Links to troubleshooting tasks you can use when the appliance has problems.

When troubleshooting issues with the appliance configuration, follow these steps:

1. If you are currently using the Catalyst Center GUI, Log out on page 206.
2. To reconfigure the appliance hardware, log in to the CIMC GUI, as explained in Enable browser access to the Cisco Integrated Management Controller on page 66.
3. To change the appliance configuration, launch and use the Maglev Configuration wizard, as explained in Reconfigure the appliance using the Configuration wizard on page 206.

For more information about the appliance network adapters, see the Managing Adapters section of the *Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide*. 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

Instructions to log out of the Catalyst 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.

To log out of the Catalyst Center GUI, from the top-right corner, click your displayed username and select **Log Out**.

This ends your session and logs you out.

Reconfigure the appliance using the Configuration wizard

Instructions to reconfigure a Catalyst Center appliance and update its settings using Configuration wizard.

To reconfigure an appliance and update its settings, you must use the Configuration wizard. 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 configuring the appliance, use the Configuration wizard only to change this limited set of appliance setting:

- 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 need the Linux username (*maglev*) and password that are currently configured on the target appliance.

Procedure

1. Point your browser to the Cisco IMC IP address set during the Cisco IMC GUI configuration and log in to the Cisco IMC GUI as the Cisco IMC user (see Enable browser access to the Cisco Integrated Management Controller on page 66).

   After you log in, the appliance shows the **Cisco Integrated Management Controller Chassis Summary** window.
2. In the hyperlinked menu at the top of the window, select **Launch KVM** and then select **HTML based KVM**.

   The KVM console opens in a separate window or tab automatically. Use it to monitor the progress of the configuration and respond to the Maglev Configuration wizard prompts.
3. When prompted, enter the Linux password.
4. Enter this command to access the Configuration wizard.

   sudo maglev-config update

   In Catalyst Center 2.3.7.7 onwards:

   - Change the **maglev** user password by specifying a new one in the **Linux Password** and **Re-enter Linux Password** fields. Ensure that this password complies with the requirements described in Password requirements on page 56. Leave these fields blank to continue using the current password.
   - You can make the other configuration setting changes without entering the **maglev** user password.
5. The Configuration wizard provides an abbreviated version of the series of screens shown in, for example, Configure a secondary node using the Maglev wizard on page 110. Make changes to the settings provided, if required. After you finish making changes on each screen, select **[Next]**, as needed, to continue through the Configuration wizard.
6. At the end of the configuration process, a message appears, stating that the Configuration wizard is now ready to apply your changes. These 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.

   Select **proceed>>** to complete the installation. The Configuration wizard applies your changes.

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

Power cycle the appliance

Procedures to stop or start a warm reset on Catalyst Center appliance.

Complete one of these procedures on your Catalyst Center appliance to either stop it or start a warm restart. You can stop the appliance before you make hardware repairs, or you can initiate a warm restart after you have corrected software issues.

> **Note**
>
> Complete the SSH procedure to perform a graceful shutdown of your appliance. Only complete the Cisco IMC procedure if Catalyst Center is unresponsive and cannot be rebooted via SSH.

Using SSH

Instructions to halt or reset (warm reset) the Catalyst Center appliance 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 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 14.
- The Linux username (*maglev*) and the password that is currently configured on the target appliance.

Procedure

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

   ssh maglev@*Enterprise-port's-IP-address* **-p 2222**
2. When prompted, enter the Linux password.
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.
4. Review the command output that is displayed as the host shuts down.
5. If you halted your appliance, power up the Maglev root process by turning the appliance back on, using the front-panel power button.

Using the Cisco IMC GUI

Instructions to halt or reset (warm reset) the Catalyst Center appliance using Cisco IMC GUI.

To halt your appliance or perform a warm restart using the Cisco IMC GUI, complete these steps.

Before you begin

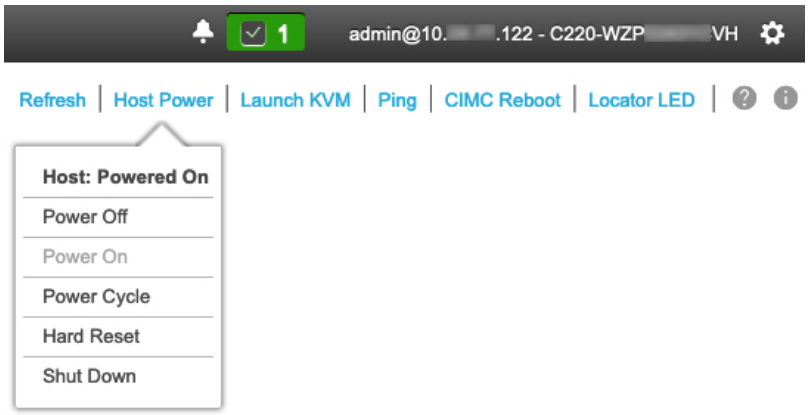
Note that any hardware changes you make using the Cisco IMC GUI will be applied after the appliance reboots.

> **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.

Procedure

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 the Cisco Integrated Management Controller on page 66).

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

2. Reboot the appliance by choosing **Host Power** > **Power Cycle**.

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

A Review High Availability Cluster Deployment Scenarios

Topics:

- New HA deployment
- Existing HA deployment of the primary node with standard interface configurations
- Existing HA deployment of primary node with nonstandard interface configurations
- Activate HA
- Additional HA deployment considerations

HA cluster deployment scenarios for Catalyst Center.

Catalyst Center's implementation of HA is described in the *Cisco Catalyst 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 decide to continue, complete these tasks:

1. Complete the deployment procedure that is appropriate for your network:
   - New HA deployment on page 212
   - Existing HA deployment of the primary node with standard interface configurations on page 212
   - Existing HA deployment of primary node with nonstandard interface configurations on page 213
2. Activate HA on your Catalyst Center cluster.
3. Refer to Additional HA deployment considerations on page 214 and make any additional telemetry or wireless controller configurations that are necessary.

New HA deployment

Instructions for installing a new HA cluster for Catalyst Center.

To install a new HA cluster, complete these steps:

Procedure

1. Configure the first installed appliance as the primary node:
   - If you are configuring an appliance using the Maglev Configuration wizard, refer to Configure the primary node using the Maglev wizard on page 87.
   - If you are configuring an appliance using the browser-based configuration wizard, refer to Configure the Appliance Using the Browser-Based Wizard on page 129.
2. Configure the second and third appliances in the cluster:
   - If you are configuring an appliance using the Maglev Configuration wizard, refer to Configure a secondary node using the Maglev wizard on page 110.
   - If you are configuring an appliance using the browser-based configuration wizard, refer to Configure a secondary node using the Advanced Install configuration wizard on page 158.

Existing HA deployment of the primary node with standard interface configurations

Instructions for deploying an existing Catalyst Center HA cluster, where the primary node uses standard interface configurations.

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

Procedure

1. Upgrade the primary node to the latest release of Catalyst Center.

   For information about upgrading your current release of Catalyst Center, see the *Cisco Catalyst Center Upgrade Guide*.
2. Confirm that you are using the required interface cable configurations on the primary node.

   Refer to Interface cable connections on page 28.
3. Update the virtual IP address (if the virtual IP address is not yet added).

   Refer to Reconfigure the appliance using the Configuration wizard on page 206.
4. Configure the second and third appliances in the cluster:
   - If you are configuring appliances using the Maglev Configuration wizard, refer to Configure a secondary node using the Maglev wizard on page 110.
   - If you are configuring appliances using the browser-based configuration wizard, refer to the "Configure a secondary appliance using the Advanced Install Configuration wizard" topic specific to your appliance.

5. Check the GlusterFS size:
   a) Contact the Cisco TAC to obtain a challenge token.
   b) Open a restricted shell and run the **sudo du -h /data/maglev/srv/maglev-system/glusterfs/mnt/bricks/default_brick/ | tail -1 | awk '{print $1}'** command.

   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 on page 213.

Existing HA deployment of primary node with nonstandard interface configurations

Instructions for deploying an existing Catalyst Center HA cluster, where the primary node uses nonstandard interface configurations.

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

Procedure

1. Upgrade the primary node to the latest release of Catalyst Center.

   For information about upgrading your current release of Catalyst Center, see the *Cisco Catalyst Center Upgrade Guide*.

2. Create a backup of the remote repository.

   See the "Backup and Restore" chapter in the *Cisco Catalyst Center Administrator Guide*.

3. Reimage the primary node with the required interface cable configuration.

   See Interface cable connections on page 28 and Install the Catalyst Center ISO image on page 82. Ensure that the VIP has been configured correctly on the primary node.

4. Install the same set of packages on the primary node that you selected during the backup.
5. Using the backup file that you created in Step 2, restore the remote repository's data.
6. Configure the second and third appliances in the cluster.
   - If you are configuring appliances using the Maglev Configuration wizard, refer to Configure a secondary node using the Maglev wizard on page 110.
   - 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.

Activate HA

Instructions to activate HA on Catalyst Center.

Catalyst Center's implementation of HA is described in the *Cisco Catalyst Center High Availability Guide*. Determine if HA is suitable for your production environment after reviewing the information. If you decide to continue, complete these steps for deployment:

1. From the main menu, choose **System** > **Settings** > **System Configuration** > **High Availability**.

2. Click **Activate High Availability**.

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

> **Note**
>
> Catalyst Center goes into maintenance mode every time you restore the database, upgrade your system (not a package upgrade), and activate HA (as described).

Additional HA deployment considerations

Additional configurations for an existing HA deployment.

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

Telemetry

Telemetry configuration for a device.

If you enabled telemetry for a device without enabling the VIP, complete these steps:

Procedure

1. Use the **sudo maglev-config update** command to update the cluster VIP.
2. Disable telemetry on the device:
   a. From the Catalyst Center home page, select **Network Telemetry** from the **Tools** area.

      The **Network Telemetry** window appears.

   b. Click the **Site View** tab.

   c. Check the check box of the device on which you want to disable telemetry, and then choose **Actions** > **Disable Telemetry**.
3. Reenable telemetry using the profile associated with the device previously.

Wireless controller

Wireless controller configuration.

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