



Cisco Digital Network Architecture Center Appliance Installation Guide, Release 1.1

First Published: 2017-11-07

Last Modified: 2018-01-29

Americas Headquarters

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

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: <http://www.cisco.com/go/trademarks>. 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. (1110R)

© 2017-2018 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

Install the Cisco DNA Center Appliance 1

- About the Appliance Installation 1
- Standalone Mode Requirements 3
- Cluster Mode Requirements 4
 - Secure Multi-Host Cluster 6
- Cisco DNA Center Appliance 6
 - Physical Specifications 6
 - Environmental Specifications 7
 - Power Specifications 8
 - 770 W AC Power Supply 8
 - Cisco DNA Center Appliance Front and Rear Panels 9
 - Summary of Appliance Series Features 11
 - Cisco DNA Center Appliance Ports Reference 12
- Prepare for Appliance Installation 14
 - Unpack and Inspect the Appliance 14
 - Review the Installation Warnings and Guidelines 15
 - Review the Rack Requirements 16
- Connect and Power On the Appliance 17
- Check the LEDs 17
 - Front Panel LEDs and Buttons 17
 - Rear Panel LEDs and Buttons 19
- Configure CIMC 21

CHAPTER 2

Configure the Cisco DNA Center Appliance 25

- Review Cisco DNA Center Configuration Wizard Parameters 25
- Configure Cisco DNA Center as a Single Host Using the Wizard 29
- Configure Cisco DNA Center as a Multi-Host Cluster Using the Wizard 33

CHAPTER 3**Perform Post-Installation Tasks 39**

- About Post-Installation Tasks 39
- Use a Web Browser to Access Cisco DNA Center 40
- Log In to Cisco DNA Center For the First Time 40
- Integrate Cisco ISE With DNA Center 41
- Configure an IP Address Manager 43
- Configure Authentication and Policy Servers 44
- Configure SNMP Properties 46
- Log Out of DNA Center 46
- Reconfigure the Appliance Using the Wizard 47
- Power-Cycle the Appliance 48



Install the Cisco DNA Center Appliance

- [About the Appliance Installation, page 1](#)
- [Standalone Mode Requirements, page 3](#)
- [Cluster Mode Requirements, page 4](#)
- [Cisco DNA Center Appliance, page 6](#)
- [Prepare for Appliance Installation, page 14](#)
- [Connect and Power On the Appliance, page 17](#)
- [Check the LEDs, page 17](#)
- [Configure CIMC, page 21](#)

About the Appliance Installation

Cisco DNA Center is available as a physical appliance, with the DNA Center ISO image pre-installed and tested. You can deploy this appliance within your network in one of two modes:

- **Standalone:** As a single host offering all DNA Center functions. This option is often preferred for initial or test deployments and in smaller network environments.
- **Cluster:** As one of a maximum of three hosts, with DNA Center sharing all of its services and data among the hosts. This is the preferred option for high availability and best performance at scale.

If you choose standalone mode for initial deployment, you can still add more appliances later to form a cluster. The following table details the the installation tasks and order of installation for both options.

Table 1: Cisco DNA Center Appliance Installation

Step	Description
1	<p>Review the pre-installation requirements for the DNA Center appliance for the mode you are planning to deploy:</p> <ul style="list-style-type: none"> • See Standalone Mode Requirements, on page 3. • See Cluster Mode Requirements, on page 4.
2	<p>Review information about the appliance and its specifications, including the following:</p> <ul style="list-style-type: none"> • Physical • Environmental • Power • Front and rear panels <p>See Cisco DNA Center Appliance, on page 6.</p>
3	<p>Review information about DNA Center port usage.</p> <p>See Cisco DNA Center Appliance Ports Reference, on page 12.</p>
4	<p>Unpack, inspect and review operational warnings about the appliance.</p> <p>See Prepare for Appliance Installation, on page 14.</p>
5	<p>Install the appliance in a rack.</p> <p>See Review the Rack Requirements, on page 16.</p>
6	<p>Connect power to the appliance and power it on.</p> <p>See Connect and Power On the Appliance, on page 17.</p>
7	<p>Check the appliance LEDs to ensure the appliance is functional.</p> <p>See Check the LEDs, on page 17.</p>
8	<p>Configure CIMC.</p> <p>See Configure CIMC.</p>
9	<p>Review the kinds of information you will need to supply when running the configuration wizard.</p> <p>See Review Cisco DNA Center Configuration Wizard Parameters, on page 25.</p>

Step	Description
10	<p>Use the wizard to configure DNA Center for use:</p> <ul style="list-style-type: none"> • To configure the appliance for standalone use, or as the first host in a cluster, see Configure Cisco DNA Center as a Single Host Using the Wizard, on page 29. • To configure the appliance as the second or third host in a cluster, see Configure Cisco DNA Center as a Multi-Host Cluster Using the Wizard, on page 33.
11	<p>Get DNA Center ready for use in a production environment.</p> <p>See About Post-Installation Tasks, on page 39.</p>

Standalone Mode Requirements

Review the following requirements before installing a Cisco DNA Center appliance installation.

Multi-Host Requirements

If you are planning to install the appliance as the first host in a cluster, or as an additional host in a cluster, see [Cluster Mode Requirements, on page 4](#) instead.

Networking Interface Requirements

In a production installation, you must connect the DNA Center appliance's network ports to your network. Cisco recommends the following cable connections:

- First 10Gb port in the VIC: Connect to an access switch with connections to the enterprise network.
- First embedded 1Gb interface: Connect to your dedicated management network. Cisco strongly recommends that you create such a network if it does not already exist.
- Second 10Gb port in the VIC: This port is reserved for DNA Center intra-cluster communications. While it is possible to leave this unconnected if you are installing in standalone mode, doing so will make it much more difficult to move to a clustered configuration later. Cisco recommends that you connect it to an access switch with connections to the network and data center where you would install additional DNA Center hosts. Note that cluster installations must have all their members in the same network and in the same data center. DNA Center does not support installation of cluster members in different networks and locations (despite the resemblance to high-availability clustering).
- 1Gb Ethernet dedicated out-of-band management port: This interface allows you to access the appliance's instance of the Cisco Integrated Management Console (CIMC), which is used to maintain DNA Center and the Cisco UCS hardware chassis. Connect this interface to your management network.

The second embedded 1Gb interface is optional. You may connect this interface to any isolated network with a static route. Cisco recommends that you leave it unconnected and unconfigured unless you have a special need for this type of connection.

For a diagram showing all of these ports, see the back-panel illustration in [Cisco DNA Center Appliance Front and Rear Panels, on page 9](#).

IP Address Requirements

Before beginning the installation, ensure that your network has sufficient IP addresses available to assign to each of the DNA Center appliance ports you plan on using.

You will need a minimum of four addresses: one for the connection to the enterprise network, one for embedded 1Gb dedicated management port, one for the 10Gb cluster port, and one for the 1Gb dedicated OOB management port. You will need five if you will also use the second embedded 1Gb interface for a static-route connection.

You will also need the following additional IP address and dedicated IP subnets, applied during installation of the standalone host in anticipation of future clustering:


- **Cluster Virtual IP Address:** Identifies a virtual IP address to be used for all traffic between any future cluster and your enterprise network. If you are using a firewall proxy with the cluster, be sure to see the information about picking a cluster virtual IP in the topic [Secure Multi-Host Cluster](#), on page 6.
- **Services Subnet:** Identifies two dedicated IP subnets for DNA Center to use in managing its own services. These two dedicated IPv4 Services management subnets must not conflict or overlap with any other subnets in use in the enterprise network, or with each other. The minimum size of the subnets is 21 bits; the recommended size is 20 bits to 16 bits.
- **Cluster Services Subnet:** Identifies one dedicated IP subnet for DNA Center to use in managing its clustering services. This dedicated IPv4 subnet cluster-service management subnet must not conflict or overlap with any other subnet in use in the enterprise network, including the dedicated DNA Center Services management subnets.

Internet Access Requirements

By default, DNA Center is configured to access Cisco.com via the internet, in order to:

- Download product updates, licenses, and device software updates.
- Send product-improvement and usage information to Cisco.

The internet connection for downloads is a firm requirement. Product improvement telemetry is optional. If you do not want to participate in the Cisco product improvement program, you can opt out by disabling the telemetry collection parameter in the installed DNA Center's System Settings.

To disable the telemetry collection parameter, log into DNA Center and select  > **System Settings** > **Settings** > **Telemetry Collection**. Uncheck the **Telemetry Collection** checkbox, then click **Update**.

Cluster Mode Requirements

Review the following requirements before beginning the Cisco DNA Center appliance installation in cluster mode.

Multi-Host Requirements

You can install a maximum of three DNA Center hosts in a cluster (or multi-host) deployment.

Networking Interface Requirements

In a production installation, you must connect the DNA Center appliance's network ports to your network. Cisco recommends the following cable connections:

- First 10Gb port in the VIC: Connect to an access switch with connections to the enterprise network.
- First embedded 1Gb interface: Connect to your dedicated management network. Cisco strongly recommends that you create such a network if it does not already exist.

- **Second 10Gb port in the VIC:** This port is reserved for DNA Center intra-cluster communications. Connect it to an access switch with connections to the network and data center where you will install the additional DNA Center hosts in the cluster. Note that cluster installations must have all their members in the same network and in the same data center. DNA Center does not support installation of cluster members in different networks and locations (despite the resemblance to high-availability clustering).
- **1Gb Ethernet dedicated out-of-band management port:** This interface allows you to access the appliance's instance of the Cisco Integrated Management Console (CIMC), which is used to maintain DNA Center and the Cisco UCS hardware chassis. Connect this interface to your management network.

The second embedded 1Gb interface is optional. You may connect this interface to any isolated network with a static route. Cisco recommends that you leave it unconnected and unconfigured unless you have a special need for this type of connection.

For a diagram showing all of these ports, see the back-panel illustration in [Cisco DNA Center Appliance Front and Rear Panels](#), on page 9.

IP Address Requirements

Before beginning the installation, ensure that your network has sufficient IP addresses available to assign to each of the DNA Center appliance ports you plan on using.

You will need a minimum of four addresses: one for the connection to the enterprise network, one for embedded 1Gb dedicated management port, one for the 10Gb cluster port, and one for the 1Gb dedicated OOB management port. You will need five if you will also use the second embedded 1Gb interface for a static-route connection.

You will also need the following additional IP address and dedicated IP subnets, applied during installation of the first host in the cluster:


- **Cluster Virtual IP Address:** Identifies the virtual IP address used for all traffic between the cluster and your enterprise network..
- **Services Subnet:** Identifies a dedicated IP subnet for DNA Center to use in managing its own services. The dedicated IPv4 Services Subnet must not conflict or overlap with any other subnet in use in the enterprise network, including the Cluster Services Subnet. The minimum size of the subnet is 21 bits; the recommended size is 20 bits to 16 bits..
- **Cluster Services Subnet:** Identifies one dedicated IP subnet for DNA Center to use in managing its clustering services. The dedicated IPv4 Cluster Services subnet must not conflict or overlap with any other subnet in use in the enterprise network, including the dedicated DNA Center Services Subnet. Size recommendation is the same as for the Services Subnet..

Internet Access Requirements

By default, DNA Center is configured to access Cisco.com via the internet, in order to:

- Download product updates, licenses, and device software updates.
- Send product-improvement and usage information to Cisco.

The internet connection for downloads is a firm requirement. Product improvement telemetry is optional. If you do not want to participate in the Cisco product improvement program, you can opt out by disabling the telemetry collection parameter in the installed DNA Center's System Settings.

To disable the telemetry collection parameter, log into DNA Center and select  > **System Settings** > **Settings** > **Telemetry Collection**. Uncheck the **Telemetry Collection** checkbox, then click **Update**.

Secure Multi-Host Cluster

If a host fails within a multi-host configuration, the time for the cluster to recover is usually 20 minutes.

In a multi-host cluster with three hosts, if a single host (host A) is removed from the cluster for any reason, and the second host (host B) fails, then the last host (host C) will also immediately fail. To remove the failed node, log into the healthy node and execute the following CLI: **maglev node remove**. This will remove the faulty node from the cluster. To add back the removed node, you must reinstall it using the Configuration Wizard's Add to cluster option.

To enable external authentication with a AAA server in a multi-host environment, you must configure all individual DNA Center host IP addresses and the Virtual IP address for the multi-host cluster on the AAA server.

In certain circumstances, you may have only two operational hosts within a multi-host cluster (three hosts). For example, when in the process of setting up a multi-host cluster, you may have only two hosts set up before configuring the third or if a single host fails in your existing multi-host cluster. In these cases, the following functionality is unsupported for a multi-host cluster (three hosts) consisting of only two operational hosts:

- Upgrading the software version
- Installing the applications
- Restoring a backup file
- Restarting the cluster
- Removing an active host, when there is an already a faulty host that exists and there is no reachability (IP connectivity) to the multi-host cluster



Important

The above functionality is only supported on a multi-host cluster that consists of three hosts.

Simultaneous removal of two hosts from a multi-host cluster (three hosts) at once or a simultaneous addition of two hosts to a multi-host cluster (three hosts) at once is not supported.

DNA Center does not support shutting down two hosts in a three-host cluster running a High Availability (HA) configuration. Only a single host at a time can be shut down and restarted when performing maintenance or troubleshooting in a three-host cluster with HA.

Cisco DNA Center Appliance

Cisco supplies DNA Center on a physical appliance with an ISO image loaded on the appliance storage. The Cisco DNA Center appliance part number is DN1-HW-APL. You must physically install the appliance on your network, and then configure it using CIMC and the installation wizard.

Physical Specifications

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

Table 2: Physical Specifications

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

Environmental Specifications

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

Table 3: Environmental Specifications

Description	Specification
Temperature, operating	41 to 95°F (5 to 35°C) Derate the maximum temperature by 1°C per every 1000 ft. (305 meters) of altitude above sea level.
Temperature, non-operating (when the server is stored or transported)	–40 to 149°F (–40 to 65°C)
Humidity (RH), operating	10 to 90%, non-condensing at 82°F (28°C)
Humidity, non-operating	5 to 93% at 82°F (28°C)
Altitude, operating	0 to 10,000 ft. (3,000 m)
Altitude, non-operating (when the server is stored or transported)	0 to 40,000 ft. (12,192 m)

Description	Specification
Sound power level Measure A-weighted per ISO7779 LwAd (Bels) Operation at 73°F (23°C)	5.4
Sound pressure level Measure A-weighted per ISO7779 LpAm (dBA) Operation at 73°F (23°C)	37

Power Specifications

The specifications for the Cisco DNA Center appliance power supply are listed in the following section.

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



Caution

Do not mix power supply types in the appliance. Both power supplies must be identical.

770 W AC Power Supply

The following table lists the specifications for the dual 770 W AC power supply (Cisco part number UCSC-PSU1-770W) supplied with the Cisco DNA Center appliance.

Table 4: AC Power Supply Specifications

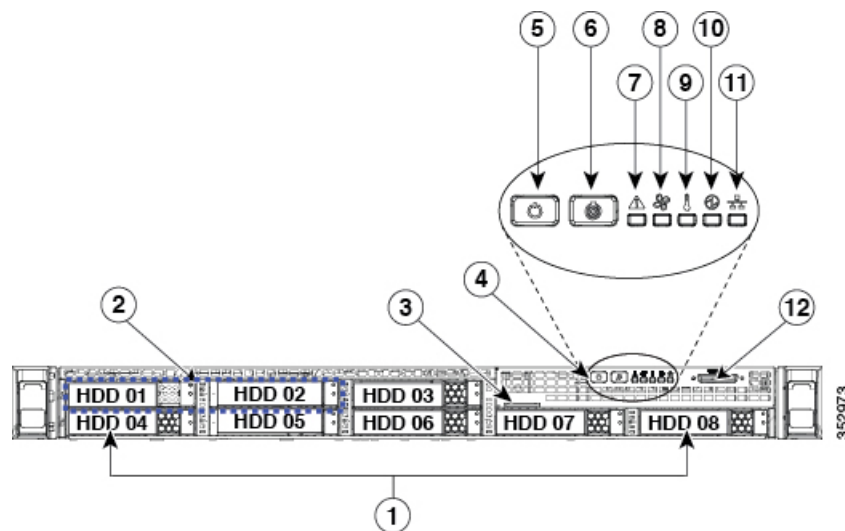
Description	Specification
AC input voltage	Nominal range: 100–120 VAC, 200–240 VAC (Range: 90–132 VAC, 180–264 VAC)
AC input frequency	Nominal range: 50 to 60Hz (Range: 47–63 Hz)
Maximum AC input current	9.5 A at 100 VAC 4.5 A at 208 VAC
Maximum input volt-amperes	950 VA at 100 VAC
Maximum output power per PSU	770 W
Maximum inrush current	15 A (sub-cycle duration)

Description	Specification
Maximum hold-up time	12 ms at 770 W
Power supply output voltage	12 VDC
Power supply standby voltage	12 VDC
Efficiency rating	Climate Savers Platinum Efficiency (80Plus Platinum certified)
Form factor	RSP2
Input connector	IEC320 C14

Cisco DNA Center Appliance Front and Rear Panels

The following figure displays the front panel of the Cisco DNA Center appliance.

Figure 1: Front Panel, Cisco DNA Center Appliance (DN1-HW-APL)

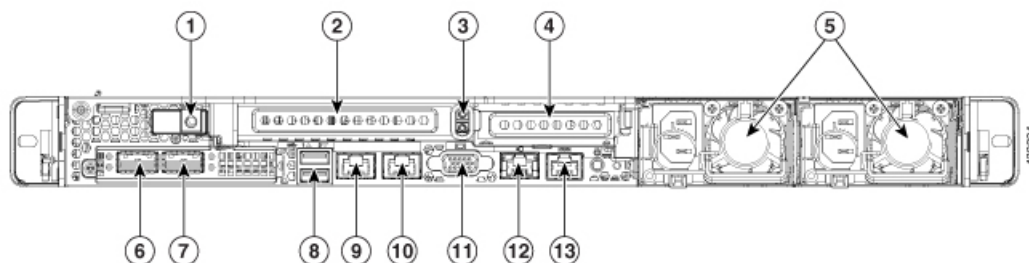


Component	Description
1	Drives (eight 2.5-inch SDD drives)
2	Drive bays 1 and 2 support SAS/SATA and NVMe PCIe solid state drives (SSDs).
3	Pull-out asset tag
4	Operations panel buttons and LEDs

Component	Description
5	Power button/power status LED
6	Unit identification button/LED
7	System status LED
8	Fan status LED
9	Temperature status LED
10	Power supply status LED
11	Network link activity LED
12	KVM connector (used with KVM cable that provides two USB 2.0, one VGA, and one serial connector)

The following figure displays the rear panel of the Cisco DNA Center appliance.

Figure 2: Rear Panel, Cisco DNA Center Appliance (DN1-HW-APL)



Release 1.1 Figure Callouts

Component	Description
1	Grounding-lug hole (for DC power supplies)
2	PCIe riser 1/slot 1
3	Rear unit identification button/LED
4	PCIe riser 2/slot 2
5	Power supplies (up to two, redundant as 1+1)
6	Second 10Gb port on Virtual Interface Card (VIC) 1227. Used for intra-cluster communications. Connect to an access switch with connections to other nodes in the cluster. This port appears in the Configuration Wizard as enp10s0.

Component	Description
7	First 10Gb port on Cisco Virtual Interface Card (VIC) 1227. Connect to an access switch with connections to the enterprise network. This port appears in the Configuration Wizard as enp9s0.
8	USB 3.0 ports (two)
9	1Gb Ethernet dedicated out-of-band management port. Reserved for OOB management of DNA Center and the appliance chassis using CIMC. Connect to the dedicated management network. This port does not appear when using the Configuration Wizard.
10	Serial port (RJ-45 connector)
11	VGA video port (DB-15)
12	First embedded (on the motherboard) Intel i350 1Gb ethernet controller port. Reserved for OOB management of the DNA Center software. Connect to the dedicated management network. This port appears in the Configuration Wizard as enp1s0f0.
13	Second embedded 1Gb ethernet controller port. Optional, intended for connecting to an isolated network with a static route. This port appears in the Configuration Wizard as enp1s0f1.

Summary of Appliance Series Features

The following table lists the Cisco DNA Center appliance features.

Table 5: Cisco DNA Appliance Series Features

Feature	Description
Chassis	One rack-unit (1RU) chassis.
Processors	Up to two Intel Xeon CPU E5-2699 2.20 GHz v4 series processor family CPUs.
Memory	24 slots for registered DIMMs (RDIMMs) or load-reduced DIMMs (LRDIMMs) (12 each CPU).
Baseboard management	<p>BMC, running Cisco Integrated Management Controller (Cisco IMC) firmware.</p> <p>Depending on your port configuration and Cisco IMC (CIMC) settings, you can access CIMC either through the IP address assigned to the 1Gb dedicated management port or the second 10Gb VIC port.</p>

Feature	Description
Network and Management I/O	Supported connectors: <ul style="list-style-type: none"> • Two 10Gb Ethernet ports on the Cisco UCS Virtual Interface Card (VIC) 1227 • One 1Gb Ethernet dedicated management port • Two 1Gb BASE-T Ethernet LAN ports • One RS-232 serial port (RJ-45 connector) • One 15-pin VGA2 connector • Two USB3 3.0 connectors • One front-panel KVM connector that is used with the KVM cable, which provides two USB 2.0, one VGA, and one serial (DB-9) connector
Power	Dual AC power supplies, 770 W AC each. Do not mix power supply types or wattages in the server. Redundant as 1+1.
Cooling	Six hot-swappable fan modules for front-to-rear cooling.
Storage	Eight 2.5-inch Small Form Factor (SFF) solid state drives (SSDs).
Disk Management (RAID)	Three pre-configured RAID settings: RAID 1 on slots 1 and 2, RAID 1 on slots 3 and 4, and RAID 10 on slots 5, 6, 7, and 8. These settings are not user-configurable.
Video	VGA video resolution up to 1920 x 1200, 16 bpp at 60 Hz, and up to 256 MB of video memory.

Cisco DNA Center Appliance Ports Reference

The following tables list the Cisco DNA Center appliance ports that permit incoming and outgoing traffic. You should ensure that these ports are open for both incoming and outgoing traffic flows.

Ensure that proper protections exist in your network for accessing port 2222. For example, you can configure a proxy gateway or secure subnets to access this port.

Table 6: Cisco DNA Center Appliance Incoming Traffic Port Reference

Port Number	Permitted Traffic	Protocol (TCP or UDP)
2222	SSH	TCP
80	HTTP	TCP

Port Number	Permitted Traffic	Protocol (TCP or UDP)
123	NTP	UDP
162	SNMP	UDP
443	HTTPS	TCP
16026	SCEP	TCP

Table 7: Cisco DNA Center Appliance Outgoing Traffic Port Reference

Port Number	Permitted Traffic	Protocol (TCP or UDP)
22	SSH (to the network devices)	TCP
23	Telnet (to the network devices)	TCP
53	DNS	UDP
80	<p>Port 80 may be used for an outgoing proxy configuration.</p> <p>Additionally, other common ports such as 8080 may also be used when a proxy is being configured by the DNA Center configuration wizard (if a proxy is already in use for your network).</p> <p>To access Cisco supported certificates and trust pools, you can configure your network to allow for outgoing IP traffic from the controller to Cisco addresses at the following URL:</p> <p>http://www.cisco.com/security/pki/</p>	TCP
123	NTP	UDP
161	SNMP agent	UDP
443	HTTPS	TCP

The following table lists the ports that permit incoming IP traffic to DNA Center:

Table 8: Cisco DNA Center Appliance IP Traffic Port Reference

Protocol (TCP or UDP)	Port Number	Traffic Type
TCP	22	SSH
TCP	2222	SSH
TCP	80	HTTP
TCP	443	HTTPS
UDP	67	bootps
UDP	123	NTP
UDP	162	SNMP
TCP	16026	SCEP

Additionally, you can configure your network to allow for outgoing IP traffic from DNA Center to Cisco addresses at the following URL: <http://www.cisco.com/security/pki/>. DNA Center uses the IP addresses listed at the above URL to access Cisco supported certificates and trust pools.

Prepare for Appliance Installation

This section provides information about preparing the Cisco DNA Center appliance for installation.

Unpack and Inspect the Appliance



Caution

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



Tip

Keep the shipping container in case the appliance requires shipping in the future.

**Note**

The chassis is thoroughly inspected before shipment. If any damage occurred during transportation or any items are missing, contact your customer service representative immediately.

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

Review the Installation Warnings and Guidelines

**Warning**

To prevent the system from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of: 40° C (104° F). Statement 1047

**Warning**

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

**Warning**

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

**Warning**

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

**Caution**

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

**Caution**

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

When you are installing an appliance, use the following guidelines:

- Plan your site configuration and prepare the site before installing the appliance. See the [Cisco UCS Site Preparation Guide](#) for help with recommended site planning and preparation tasks.
- Ensure that there is adequate space around the appliance to allow for servicing the appliance and for adequate airflow. The airflow in this appliance is from front to back.
- Ensure that the air-conditioning meets the thermal requirements listed in the [Environmental Specifications, on page 7](#).
- Ensure that the cabinet or rack meets the requirements listed in the following "Rack Requirements" topic.
- Ensure that the site power meets the power requirements listed in the [770 W AC Power Supply, on page 8](#). If available, you can use an uninterruptible power supply (UPS) to protect against power failures.

Review the Rack Requirements

This topic explains the requirements for installing the appliance in standard open racks.

The rack must be of the following type:

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

Connect and Power On the Appliance

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

Step 1

Attach a supplied power cord to each power supply in the appliance and then attach the power cord to a grounded AC power outlet. See [Power Specifications, on page 8](#) for details.

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

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

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

For more information on these and other appliance LEDs, see [Check the LEDs, on page 17](#).

Step 2

Connect a USB keyboard and VGA monitor to the server, using the supplied KVM cable connected to the KVM connector on the front panel.

Alternatively, you can use the VGA and USB ports on the rear panel. However, you cannot use the front panel VGA and the rear panel VGA at the same time. If you are connected to one VGA connector and you then connect a video device to the other connector, the first VGA connector is disabled.

What to Do Next

Continue by following the procedure in [Configure CIMC, on page 21](#).

Check the LEDs

When the Cisco DNA Center appliance has been started up and is running, observe the state of the front-panel and rear-panel LEDs and buttons. The following topics describe the LEDs and buttons, their colors, and the appliance power state, activity, and other important hardware status indicators that they provide.

Front Panel LEDs and Buttons

The following table describes the Cisco DNA Center appliance front-panel LEDs and buttons.

The minimum network interface speed for the appliance should be 1 GB a second.

Table 9: Front Panel LEDs and Buttons

LED Name	State
Front Panel LEDs and Buttons	<p>Off—There is no AC power to the appliance.</p> <p>Amber—The appliance is in standby power mode. Power is supplied only to the CIMC and some motherboard functions.</p> <p>Green—The appliance is in main power mode. Power is supplied to all server components.</p>
Identification	<p>Off—The Identification LED is not in use.</p> <p>Blue—The Identification LED is activated.</p>
System status	<p>Green—The appliance is running in a normal operating condition.</p> <p>Green, blinking—The appliance is performing system initialization and memory checks.</p> <p>Amber, steady—The appliance is in a degraded operational state, which may be due to one of the following:</p> <ul style="list-style-type: none"> – Power supply redundancy is lost. – CPUs are mismatched. – At least one CPU is faulty. – At least one DIMM is faulty. – At least one drive in a RAID configuration failed. <p>Amber, blinking—The appliance is in a critical fault state, which may be due to one of the following:</p> <ul style="list-style-type: none"> – Boot failed. – Fatal CPU and/or bus error is detected. – Server is in an over-temperature condition.
Fan status	<p>Green—All fan modules are operating properly.</p> <p>Amber, steady—One fan module has failed.</p> <p>Amber, blinking—Critical fault, two or more fan modules have failed.</p>
Temperature status	<p>Green—The appliance is operating at normal temperature.</p> <p>Amber, steady—One or more temperature sensors have exceeded a warning threshold.</p> <p>Amber, blinking—One or more temperature sensors have exceeded a critical threshold</p>

LED Name	State
Power supply status	<p>Green—All power supplies are operating normally.</p> <p>Amber, steady—One or more power supplies are in a degraded operational state.</p> <p>Amber, blinking—One or more power supplies are in a critical fault state.</p>
Network link activity	<p>Off—The Ethernet link is idle.</p> <p>Green—One or more Ethernet LOM ports are link-active, but there is no activity.</p> <p>Green, blinking—One or more Ethernet LOM ports are link-active, with activity.</p>
Hard drive fault	<p>Off—The hard drive is operating properly.</p> <p>Amber—The hard drive has failed.</p> <p>Amber, blinking—The device is rebuilding.</p>
Hard drive activity	<p>Off—There is no hard drive in the hard drive sled (no access, no fault).</p> <p>Green—The hard drive is ready.</p> <p>Green, blinking—The hard drive is reading or writing data.</p>

Rear Panel LEDs and Buttons

The following table describes the Cisco DNA Center appliance rear panel LEDs and buttons.

The minimum network interface speed for the appliance is 1Gbps on 10Gb connections, and 100Mbps on 1Gb connections.

Table 10: Rear Panel LEDs and Buttons

LED Name	State
Power supply fault	<p>Off—The power supply is operating normally.</p> <p>Amber, blinking—An event warning threshold has been reached, but the power supply continues to operate.</p> <p>Amber, solid—A critical fault threshold has been reached, causing the power supply to shut down (for example, a fan failure or an over-temperature condition).</p>

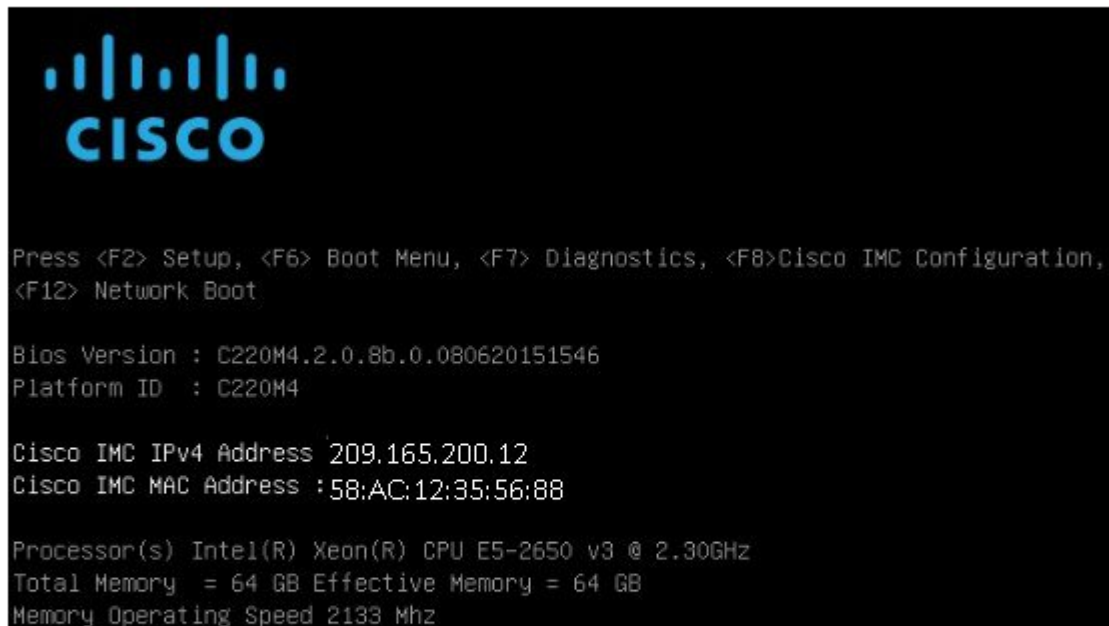
LED Name	State
Power supply AC OK	Off—There is no AC power to the power supply. Green, blinking—AC power OK, DC output not enabled. Green, solid—AC power OK, DC outputs OK.
1 Gb Ethernet dedicated management link speed	Off—link speed is 10 Mbps or less. Amber—link speed is 100 Mbps. Green—link speed is 1 Gbps.
1 Gb Ethernet dedicated management link status	Off—No link is present. Green—Link is active. Green, blinking—Traffic is present on the active link.
1 Gb Ethernet link speed	Off—link speed is 10 Mbps or less. Amber—link speed is 100 Mbps. Green—link speed is 1 Gbps.
1 Gb Ethernet link status	Off—No link is present. Green—Link is active. Green, blinking—Traffic is present on the active link.
10 Gb Ethernet link speed	Off—link speed is 100 Mbps or less. Amber—link speed is 1 Gbps. Green—link speed is 10 Gbps.
10 Gb Ethernet link status	Off—No link is present. Green—Link is active. Green, blinking—Traffic is present on the active link.
Identification	Off—The Identification LED is not in use. Blue—The Identification LED is activated.

Configure CIMC

After rack-mounting the appliance and connecting the network cabling, use the Cisco IMC Configuration Utility (CIMC) to assign the appliance an IP address and gateway.

-
- Step 1** Attach a keyboard and monitor to the USB ports on the rear panel of the appliance or by using a KVM cable and connector to access the appliance console.
- Step 2** Plug in the power cord.
- Step 3** Press the **Power** button to boot the appliance. Watch for the prompt to press **F8** as shown in the CIMC boot screen.

Figure 3: CIMC Boot Screen



Step 4 During bootup, press **F8** to open the CIMC Configuration Utility. The CIMC Configuration Utility screen appears.

Figure 4: CIMC Configuration Utility Screen

```

Cisco IMC Configuration Utility Version 2.0  Cisco Systems, Inc.
*****
NIC Properties
NIC mode                                NIC redundancy
Dedicated:      [X]                    None:          [X]
Shared LOM:     [ ]                    Active-standby: [ ]
Cisco Card:     [ ]                    Active-active:  [ ]
  Riser1:       [ ]                    VLAN (Advanced)
  Riser2:       [ ]                    VLAN enabled:   [ ]
  MLom:         [ ]                    VLAN ID:        1
Shared LOM Ext: [ ]                    Priority:       0
IP (Basic)
IPV4:           [X]                    IPV6:          [ ]
DHCP enabled    [ ]
CIMC IP:        209.165.200.12
Prefix/Subnet:  255.255.254.0
Gateway:        209.165.200.13
Pref DNS Server: 0.0.0.0
*****
<Up/Down>Selection  <F10>Save  <Space>Enable/Disable  <F5>Refresh  <ESC>Exit
<F1>Additional settings

```

Step 5 In the Configuration Utility window, change the following fields as specified:

- **NIC mode**—Select Dedicated.
- **IP (Basic)**—Select IPV4.
- **CIMC IP**—Enter the IP address of the CIMC.
- **Prefix/Subnet**—Enter the subnet of the CIMC.
- **Gateway**—Enter the Gateway address.
- **Pref DNS Server**—Enter the preferred DNS server address, if available.

- **NIC Redundancy**—None

Step 6 Press **F1** to specify additional settings.

Step 7 Make the following changes on the Additional Settings window:

- For **Common Properties**, enter a hostname for CIMC.
- For **Common Properties**, turn off Dynamic DNS.
- Turn off the **Factory Defaults**.
- Enter the admin password. If you leave the password field blank, the default password is *password*.
- Enter new **Port Properties** or accept the default.
- Turn off the **Port Profiles**.

Step 8 Press **F10** to save the settings.

Step 9 Press **escape** to exit and reboot the server.

Step 10 After the settings are saved, open a browser and enter the following URL:
`https://CIMC_ip_address` where `CIMC_IP_address` is the IP address that you entered in Step 5.

What to Do Next

Continue by using CIMC and the configuration wizard to configure the appliance for use in your standalone or cluster deployment, as follows:

If you are configuring the appliance for use as a standalone host, or as the first host in a cluster deployment, see [Configure Cisco DNA Center as a Single Host Using the Wizard](#), on page 29.

If you are adding the appliance as the second or third host in a cluster, see [Configure Cisco DNA Center as a Multi-Host Cluster Using the Wizard](#), on page 33.



Configure the Cisco DNA Center Appliance

- [Review Cisco DNA Center Configuration Wizard Parameters, page 25](#)
- [Configure Cisco DNA Center as a Single Host Using the Wizard, page 29](#)
- [Configure Cisco DNA Center as a Multi-Host Cluster Using the Wizard, page 33](#)

Review Cisco DNA Center Configuration Wizard Parameters

When DNA Center configuration begins, an interactive configuration wizard prompts you to enter configuration parameter information. The following table describes the parameters for which the wizard will prompt you, and the information you will need to enter in order to complete the configuration.

Table 11: Cisco DNA Center Configuration Wizard Parameters

Configuration Wizard Prompt	Description	Example
Host IP address	Enter a host IP address for each of the ports you are going to use. If installing the host in standalone mode, this will mean, at minimum, addresses for the ports connecting the host to the enterprise network and to the management network. If installing the host in cluster mode, this will also include an address for the port connecting the host to other hosts in the cluster. These must be valid IPv4 addresses.	10.0.0.12
Netmask	Enter a netmask for the IP address. This must be a valid IPv4 netmask.	255.255.255.0

Configuration Wizard Prompt	Description	Example
Default Gateway IP address	Enter a default gateway IP address. This must be a valid IPv4 address for the default gateway.	10.12.13.1
DNS Servers	Enter a DNS server address. This must be a valid IPv4 address for the primary DNS server. Enter either a single IP address for a single primary server, or multiple IP addresses separated by spaces for multiple DNS servers.	10.15.20.25
Static Routes	Enter the IP address and subnet mask for a manually specified route for this interface, including the gateway IP. We recommend that you always specify at least one static route for the interface connecting to the fabric underlay.	204.2.0.0/255.255.0.0/ <i>gatewayIP</i> Enter either a single IP address and subnet mask for a single static route, or a space-separated list of multiple IP addresses/masks for multiple static routes (including their gateway IPs.
Cluster Link	If you are installing the first node in a cluster: Select the checkbox to indicate that the port you are configuring is the link to a DNA Center cluster. If not installing in cluster mode: Leave this checkbox unselected. The IP address you assign to the port must be a physical IP.	Does not apply
Configure IPv6 Address	Reserved for future use.	Does not apply
HTTPS Proxy	Enter the URL of any network proxy used to access the network.	https://proxy.mycompany.com:8080
HTTPS Proxy Username	Enter the username used to access the proxy.	MyUserName
HTTPS Proxy Password	Enter the password used to access the proxy.	MyPass901&
Cluster Virtual IP Address	Identifies the virtual IP address used for all traffic between the cluster and your enterprise network.	192.126.15.20

Configuration Wizard Prompt	Description	Example
Maglev Master Node	<p>Identifies the IP address of the intra-cluster port (the second 10Gb VIC port) on the first host in the cluster. You are prompted for this only when configuring the second and third hosts in a cluster.</p> <p>You must enter in this field the same physical IP you configured for the intra-cluster port IP on the first node in the cluster.</p>	10.0.0.12
Username	<p>Identifies the Linux administrator for the Maglev Master Node (the first host in the cluster). You are prompted for this only when configuring the second and third hosts in a cluster.</p> <p>Enter maglev.</p>	maglev
Password	<p>Identifies the Linux Password you have configured for the Maglev Master Node (the first host in the cluster). You are prompted for this only when configuring the second and third hosts in a cluster.</p>	MyPass1\$
Linux Password	<p>Enter a Linux password.</p> <p>Identifies the Linux administrator password that is used for CLI access to the Maglev roots and clients. This is the password for the "maglev" user. You must create this password because there is no default. The password must meet the following requirements:</p> <ul style="list-style-type: none"> • Eight character minimum length. • Does NOT contain a tab or a line break. • Does contain characters from at least three of the following categories: <ul style="list-style-type: none"> ◦ Uppercase alphabet ◦ Lowercase alphabet ◦ Numeral ◦ Special characters (for example, ! or #) 	MyPass1\$

Configuration Wizard Prompt	Description	Example
(Optional) Password Generation Seed	<p>Instead of creating and entering your own Linux administrator password, you can enter a seed phrase and press Generate Password to have the configuration wizard generate a random and secure password using that seed phrase.</p> <p>If you choose to enter a seed phrase, the generated password will be displayed in the Auto Generated Password field, where you can further edit it.</p>	WhenAprilLastInDooryard
(Optional) Auto Generated Password	<p>If you choose to enter a seed phrase, the generated password (including your seed phrase) will be displayed in this field. If desired, you can either use this password "as is", or you can further edit this auto generated password.</p> <p>You must select Use Generated Password to save the password and have it used automatically.</p>	N/A
Administrator Passphrase	<p>Enter the admin password.</p> <p>Identifies the password used for web access to DNA Center. You must create this password because there is no default. The password must meet the following requirements:</p> <ul style="list-style-type: none"> • Eight character minimum length. • Does NOT contain a tab or a line break. • Does contain characters from at least three of the following categories: <ul style="list-style-type: none"> ◦ Uppercase alphabet ◦ Lowercase alphabet ◦ Numeral ◦ Special characters (for example, ! or #) 	MyIseYPass2

Configuration Wizard Prompt	Description	Example
NTP Servers	<p>Enter a primary NTP server address.</p> <p>This must be a valid IPv4 address or hostname of a Network Time Protocol (NTP) server.</p> <p>Before you deploy DNA Center, make sure that the time on the DNA Center appliance system clock is current and that you are using a Network Time Protocol (NTP) server that is keeping the correct time.</p>	<p>10.12.13.10</p> <p>Enter either a single IP address for a single NTP primary server, or multiple IP addresses separated by spaces for several NTP servers. We recommend that you configure three NTP servers for your deployment.</p>
Services Subnet	<p>Enter a dedicated IP subnet for DNA Center to use in managing its own services.</p> <p>The dedicated IPv4 Services Subnet must not conflict or overlap with any other subnet in use in the enterprise network, including the Cluster Services Subnet. The minimum size of the subnet is 21 bits; the recommended size is 20 bits to 16 bits.</p>	10.60.0.0/21
Cluster Services Subnet	<p>Enter a dedicated IP subnet for DNA Center to use in managing its clustering services.</p> <p>The dedicated IPv4 Cluster Services subnet must not conflict or overlap with any other subnet in use in the enterprise network, including the dedicated DNA Center Services Subnet. Size recommendation is the same as for the Services Subnet.</p>	10.100.0.0/16

Configure Cisco DNA Center as a Single Host Using the Wizard

Perform the steps in the following procedure to use the wizard to configure DNA Center as a standalone host, or as the first host in a multi-host cluster.

Before You Begin

Ensure that you have:

- Racked, connected and powered up the host by following the recommended procedures in this guide.
- Configured CIMC for use with the host. See [Configure CIMC](#).

- Reviewed and gathered the information for which the configuration wizard will prompt you. See [Review Cisco DNA Center Configuration Wizard Parameters](#).

- Step 1** Use a browser and the assigned CIMC IP address to log in to the CIMC Setup Utility. The IP address was set during the CIMC configuration you performed, as explained in [Configure CIMC](#). The default username for the server is admin. The default password is *password*.
- Step 2** Choose **Macros > Static Macros > Ctrl-Alt-Del** to reboot the host.
- Step 3** Review the **Welcome to the Maglev Configuration Wizard!** screen and choose the **Start a DNA-C cluster** option to begin.
- Step 4** Enter configuration values for the **NETWORK ADAPTER #1** on the host. The configuration wizard discovers and prompts you to confirm values for the network adapter or adapters on your host.

Host IP address	Enter the IP address for the port that connects the host to the enterprise network (the first 10Gb VIC port). The wizard validates the value entered and issues an error message if incorrect. If you receive an error message, check that the IP exists and that the port is cabled correctly. If you entered the wrong IP and get an error, use <<back to re-enter the IP.
Netmask	Enter the netmask for the network adapter's IP address.
Default Gateway IP address	Enter a default gateway IP address to use for the network adapter. If no other routes match the traffic, traffic will be routed through this IP address.
DNS Servers	Enter the IP address of the DNS server for the network adapter. If entering multiple DNS servers, separate the IP addresses in the list with commas.
Static Routes	If required for your network, enter a space separated list of static routes in this format: <network>/<netmask>/<gateway> Static routes, which define explicit paths between two routers, cannot be automatically updated; you must manually reconfigure static routes when network changes occur. You should use static routes in environments where network traffic is predictable and where the network design is simple. You should not use static routes in large, constantly changing networks because static routes cannot react to network changes.

Cluster Link	Select the checkbox to indicate that the port you are configuring will be the link to a DNA Center cluster. If not installing in cluster mode: Leave this checkbox unselected. The IP address you assign to the port must be a physical IP.
Configure IPv6 Address	Reserved for future use. Leave this field blank.

When you are ready, enter **next>>** to proceed. After entering **next>>**, the wizard validates the values you entered.

After validation, you are prompted to enter values for each of the remaining adapters, in order of discovery. Repeat the process you used for the first network adapter, configuring each as per their cabling to their respective networks. When you are finished with each adapter's settings, enter **next>>** to proceed.

Step 5 Enter configuration values for any **NETWORK PROXY** you are using.

HTTPS Proxy	Enter the URL of the network proxy.
HTTPS Proxy Username	Enter the user name used to access the network proxy.
HTTPS Proxy Password	Enter the password used to access the network proxy.

When you are ready, enter **next>>** to proceed.

Step 6 Enter configuration values for any **MAGLEV CLUSTER DETAILS**.

Cluster Virtual IP Address	Enter a virtual IP address to be used for all traffic between any future cluster installation and your enterprise network.
-----------------------------------	--

When you are ready, enter **next>>** to proceed.

Step 7 Enter values for the **USER ACCOUNT SETTINGS**.

Linux Password	<p>Enter a Linux password.</p> <p>The Linux password is used to ensure security for the Maglev root and clients located on the host. Access to the Maglev root and clients requires this password.</p> <p>The default username is maglev and cannot be changed</p> <p>The Linux password is encrypted and hashed in the DNA Center database.</p>
Re-enter Linux Password	Confirm the Linux password by entering it a second time.

Password Generation Seed	<p>(Optional) Instead of creating and entering your own password in the above Linux Password fields, you can enter a seed phrase and have the wizard generate a random and secure password using that seed phrase.</p> <p>Enter a seed phrase and then press <Generate Password> to generate the password.</p>
Auto Generated Password	<p>(Optional) The seed phrase appears as part of a random and secure password. If desired, you can either use this password "as is", or you can further edit this auto generated password.</p> <p>Press <Use Generated Password> to save the password.</p> <p>When finished with the password, be sure to save it to a secure location for future reference.</p>
Administrator Passphrase	<p>Enter an administrator passphrase.</p> <p>The administrator passphrase is encrypted and hashed in the DNA Center database.</p>
Re-enter Administrator Passphrase	<p>Confirm the administrator passphrase by entering it a second time.</p>

When you are finished, enter **next>>** to proceed.

Step 8 Enter configuration values for **NTP SERVER SETTINGS**.

NTP servers	<p>Enter a single NTP server address or a list of NTP servers, each separated by a space.</p> <p>We recommend that, for redundancy purposes, you configure at least three NTP servers for your deployment.</p> <p>Cisco routers and switches can also be configured as NTP servers.</p>
--------------------	---

When you are ready, enter **next>>** to proceed.

Step 9 Enter configuration values for **MAGLEV ADVANCED SETTINGS**:

Services Subnet	<p>Enter a dedicated IP subnet for DNA Center to use in managing its own services.</p> <p>The dedicated IPv4 Services Subnet must not conflict or overlap with any other subnet in use in the enterprise network, including the Cluster Services Subnet. The minimum size of the subnet is 21 bits; the recommended size is 20 bits to 16 bits.</p>
------------------------	---

Cluster Services Subnet	<p>Enter a dedicated IP subnet for DNA Center to use in managing its clustering services.</p> <p>The dedicated IPv4 Cluster Services Subnet must not conflict or overlap with any other subnet in use in the enterprise network, including the DNA Center Services Subnet. Size recommendation is the same as for the Services Subnet.</p>
--------------------------------	--

When you are finished, enter **next>>** to proceed.

Step 10

A final message appears stating that the wizard is now ready to proceed with applying the configuration. The following options are available:

- **[back]**—Review and verify your configuration settings.
- **[cancel]**—Discard your configuration settings and exit the configuration wizard.
- **[proceed]**—Save your configuration settings and begin applying them.

Enter **proceed>>** to complete the installation. After entering **proceed>>**, the configuration wizard applies the configuration values that you entered above.

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

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 console.

What to Do Next

When this task is complete:

If you are deploying DNA Center in standalone mode only, begin performing the required post-installation tasks. See [About Post-Installation Tasks, on page 39](#).

If you are deploying DNA Center in a cluster configuration, review and follow the multi-host configuration procedure for the second host in the multi-host cluster. See [Configure Cisco DNA Center as a Multi-Host Cluster Using the Wizard, on page 33](#).

Configure Cisco DNA Center as a Multi-Host Cluster Using the Wizard

Perform the steps in this procedure to configure DNA Center on your host and to join it to another, pre-existing host to create a cluster. Configuring DNA Center on multiple hosts to create a cluster is the best way to ensure that your deployment has both high availability and good performance at scale.

**Caution**

- When joining a host to a cluster as described in the procedure below, there is no merging of the data on the two hosts. The data that currently exists on the host that is joining the cluster is erased and replaced with the data that exists on the cluster that it is being joined to.
- When joining the additional hosts to form a cluster, be sure to join only a single host at a time. You should not join multiple hosts at the same time, as doing so will result in unexpected behavior.
- You should also expect some service downtime when adding hosts to or removing them from a cluster. Services will need to be redistributed across the hosts and the system will be down for periods during that process.
- If you have enabled HA (high availability) for the cluster, you must toggle the HA slide button once you have joined all three nodes. Doing so will rebalance DNA Center services across the three nodes.

Before You Begin

You must have already configured DNA Center on the first host in your planned multi-host cluster following the steps in the previous procedure, [Configure Cisco DNA Center as a Single Host Using the Wizard](#), on page 29.

The following procedure must be run on the second and third hosts that you are joining to the cluster. When joining each new host to the cluster, you must specify the first host in the cluster as the Master Node.

- Step 1** Use a browser and the assigned CIMC IP address to log in to the CIMC Setup Utility. The IP address was set during the CIMC configuration you performed, as explained in [Configure CIMC](#). The default username for the server is admin. The default password is *password*.
- Step 2** Choose **Macros > Static Macros > Ctrl-Alt-Del** to reboot the host.
- Step 3** Review the **Welcome to the Maglev Configuration Wizard!** screen and choose the **Join a DNA-C cluster** option to begin.
- Step 4** Enter configuration values for the **NETWORK ADAPTER #1** on the host. The configuration wizard discovers and prompts you to confirm values for the network adapter or adapters on your host.

Host IP address	Enter the IP address for the port that connects this host to the enterprise network (the first 10Gb VIC port). The wizard validates the value entered and issues an error message if incorrect. If you receive an error message, check that the IP exists and that the port is cabled correctly. If you entered the wrong IP and get an error, use <<back to re-enter the IP.
Netmask	Enter the netmask for the network adapter's IP address.
Default Gateway IP address	Enter a default gateway IP address to use for the network adapter. If no other routes match the traffic, traffic will be routed through this IP address.

DNS Servers	Enter the IP address of the DNS server for the network adapter. If entering multiple DNS servers, separate the IP addresses in the list with commas.
Static Routes	<p>If required for your network, enter a space separated list of static routes in this format: <network>/<netmask>/<gateway></p> <p>Static routes, which define explicit paths between two routers, cannot be automatically updated; you must manually reconfigure static routes when network changes occur. You should use static routes in environments where network traffic is predictable and where the network design is simple. You should not use static routes in large, constantly changing networks because static routes cannot react to network changes.</p>
Cluster Link	Select the checkbox to indicate that the port you are configuring will be the link to the DNA Center cluster.
Configure IPv6 Address	Reserved for future use. Leave this field blank.

When you are ready, enter **next>>** to proceed. After entering **next>>**, the wizard validates the values you entered.

After validation, you are prompted to enter values for each of the remaining adapters, in order of discovery. Repeat the process you used for the first network adapter, configuring each as per their cabling to their respective networks. When you are finished with each adapter's settings, enter **next>>** to proceed.

Step 5 Enter configuration values for any **NETWORK PROXY** you are using.

HTTPS Proxy	Enter the URL of the network proxy.
HTTPS Proxy Username	Enter the user name used to access the network proxy.
HTTPS Proxy Password	Enter the password used to access the network proxy.

When you are ready, enter **next>>** to proceed.

Step 6 Enter configuration values for any **MAGLEV CLUSTER DETAILS**.

Maglev Master Node	Enter the IP address of the intra-cluster port on the first host in the cluster (the "Master Node").
Username	Enter maglev.
Password	Enter the Linux Password configured for the first host in the cluster.

When you are ready, enter **next>>** to proceed.

Step 7

Enter values for the **USER ACCOUNT SETTINGS**.

Linux Password	<p>Enter a Linux password.</p> <p>The Linux password is used to ensure security for the Maglev root and clients located on this host. Access to the Maglev root and clients requires this password.</p> <p>The default username is maglev and cannot be changed</p> <p>The Linux password is encrypted and hashed in the DNA Center database.</p>
Re-enter Linux Password	<p>Confirm the Linux password by entering it a second time.</p>
Password Generation Seed	<p>(Optional) Instead of creating and entering your own password in the above Linux Password fields, you can enter a seed phrase and have the wizard generate a random and secure password using that seed phrase.</p> <p>Enter a seed phrase and then press <Generate Password> to generate the password.</p>
Auto Generated Password	<p>(Optional) The seed phrase appears as part of a random and secure password. If desired, you can either use this password "as is", or you can further edit this auto generated password.</p> <p>Press <Use Generated Password> to save the password.</p> <p>When finished with the password, be sure to save it to a secure location for future reference.</p>
Administrator Passphrase	<p>Enter an administrator passphrase.</p> <p>The administrator passphrase is encrypted and hashed in the DNA Center database.</p>
Re-enter Administrator Passphrase	<p>Confirm the administrator passphrase by entering it a second time.</p>

When you are finished, enter **next>>** to proceed.

Step 8

Enter configuration values for **NTP SERVER SETTINGS**.

NTP servers	<p>Enter a single NTP server address or a list of NTP servers, each separated by a space.</p> <p>We recommend that, for redundancy purposes, you configure at least three NTP servers for your deployment.</p> <p>Cisco routers and switches can also be configured as NTP servers.</p>
--------------------	---

When you are ready, enter **next>>** to proceed.

Step 9

A final message appears stating that the wizard is now ready to proceed with applying the configuration. The following options are available:

- **[back]**—Review and verify your configuration settings.
- **[cancel]**—Discard your configuration settings and exit the configuration wizard.
- **[proceed]**—Save your configuration settings and begin applying them.

Enter **proceed>>** to complete the installation. After entering **proceed>>**, the configuration wizard applies the configuration values that you entered above.

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

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 console.

What to Do Next

When this task is complete:

If you are deploying DNA Center in a multi-host configuration and need to add another host: Repeat this procedure for the third and final host.

If you are finished adding hosts to the cluster: Perform the post-installation tasks needed to get the cluster ready for use in a production environment. See [About Post-Installation Tasks](#), on page 39.



Perform Post-Installation Tasks

- [About Post-Installation Tasks, page 39](#)
- [Use a Web Browser to Access Cisco DNA Center, page 40](#)
- [Log In to Cisco DNA Center For the First Time, page 40](#)
- [Integrate Cisco ISE With DNA Center, page 41](#)
- [Configure an IP Address Manager, page 43](#)
- [Configure Authentication and Policy Servers, page 44](#)
- [Configure SNMP Properties, page 46](#)
- [Log Out of DNA Center, page 46](#)
- [Reconfigure the Appliance Using the Wizard, page 47](#)
- [Power-Cycle the Appliance, page 48](#)

About Post-Installation Tasks

Once you have finished installing Cisco DNA Center, you will need to perform the tasks in the following table to complete the installation and prepare DNA Center for production use.

The following table lists the steps for installing the appliance.

Table 12: DNA Center Post-Installation Tasks

Step	Description
1	Make sure you are using a compatible browser to access DNA Center. See Use a Web Browser to Access Cisco DNA Center, on page 40 .

Step	Description
2	<p>Log in to DNA Center for the first time. During this first administrative login, you will be prompted to:</p> <ol style="list-style-type: none"> 1 Provide a new password for the admin superuser. 2 Enter the Cisco.com user ID and password your organization uses to download software images and receive email communications from Cisco. 3 Enter the Cisco.com user ID and password your organization uses to manage its Smart Account licenses. 4 Configure the IP address manager (IPAM) server you plan to use with DNA Center. <p>For details on the first three tasks, see Log In to Cisco DNA Center For the First Time, on page 40. For details on the fourth, see Configure an IP Address Manager, on page 43.</p>
3	<p>Set up policy and AAA servers, including Cisco Identity Services Engine (ISE).</p> <p>See Configure Authentication and Policy Servers, on page 44.</p>
4	<p>Configure basic SNMP polling parameters.</p> <p>See Configure SNMP Properties, on page 46.</p>
5	<p>If you need to troubleshoot problems with a DNA Center host's low-level configuration: Log out of DNA Center, reconfigure the host using the configuration wizard, and then power-cycle the host.</p> <p>See Log Out of DNA Center, on page 46, Reconfigure the Appliance Using the Wizard, on page 47, Power-Cycle the Appliance, on page 48.</p>

Use a Web Browser to Access Cisco DNA Center

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

- Google Chrome—version 62.0 or later.
- Mozilla Firefox—version 54.0 or later.

Log In to Cisco DNA Center For the First Time

After you have installed the DNA Center appliance, you can log into its web-based interface for the first time. You must use only supported HTTPS-enabled browsers when accessing DNA Center. For a list of supported browsers, see [Use a Web Browser to Access Cisco DNA Center](#), on page 40.

When logging in for the first time as the system admin (super user), you will be asked to complete a first-time setup wizard that helps you enhance system security and complete basic setup tasks. Although you can skip each of the steps in the wizard, Cisco recommends that you complete all of them as indicated, so that your system is ready to go immediately.

Before You Begin

In order to complete the first-time setup wizard, you will need the following information:

- A new password for the admin superuser. Resetting the admin superuser password is an important way to enhance operational security if, for example, personnel who will not be DNA Center users or administrators installed the DNA Center software.
- The Cisco.com user ID and password your organization uses to register software downloads and receiving system communications via email.
- The Cisco.com Smart Account user ID and password your organization uses for managing your device and software licenses.
- The host name, URL, admin user name and admin password of the third-party IP address manager (IPAM) server you plan to use with DNA Center. The current release supports InfoBlox or Bluecat .

-
- Step 1** After the DNA Center appliance reboot has completed, launch your browser.
- Step 2** Enter the host IP address to access the DNA Center GUI.
Use HTTPS and the IP address of the DNA Center GUI that was displayed at the end of the configuration process.
- Step 3** After entering the IP address in the browser, a message stating that "Your connection is not private" appears. Ignore the message and click the **Advanced** link.
- Step 4** After clicking the **Advanced** link, a message stating that the site's security certificate is not trusted appears. Ignore the message and click the link. The DNA Center **Login** window appears.
This message appears because the controller uses a self-signed certificate. You will have the option to upload a trusted certificate using the GUI.
- Step 5** In the **Login** window, enter the administrator username and password that you configured when you configured DNA Center. Then click **Log In**.
- Step 6** The **Reset Login** window appears. Enter the old password, then enter and confirm a new password for the admin superuser. Then click **Save**.
- Step 7** The **Enter Cisco.com ID** window appears. Enter the user ID and password for the Cisco.com user, then click **Next**.
- Step 8** The **Smart Account** window appears. Enter the user ID and password for your organization's Smart Account, then click **Next**.
- Step 9** The **IP Address Manager** window appears. Enter the server and admin information for the external IP address manager your organization will use, and specify its type (for example, InfoBlox). Then click **Next**.
- Step 10** The software **EULA** window appears. Click **Next** to accept the software End User License Agreement and continue.
- Step 11** The **Ready To Go!** window appears. Click on any of the links displayed to start discovering devices and constructing your network hierarchy, or click **Go** to display the main DNA Center dashboard.
-

Integrate Cisco ISE With DNA Center

This release of DNA Center provides a mechanism to create a trusted communications link with Cisco Identity Services Engine (ISE) and permit the two applications to share data with one another in a secure manner.

Once ISE is registered with DNA Center, any device ISE discovers, along with relevant configuration and other data, is pushed to DNA Center. Users can use either application to discover devices and then apply both DNA Center and ISE functions to them, as these devices will be exposed in both applications. DNA Center and ISE devices are all uniquely identified by their device names.

Similarly, DNA Center devices, as soon as they are provisioned and belong to a particular site in the DNA Center site hierarchy, are pushed to ISE. Any updates to a DNA Center device (such as changes to IP address, SNMP or CLI credentials, ISE shared secret, and so on) will flow to the corresponding device instance on ISE automatically. When a DNA Center device is deleted, it is removed from ISE as well. Please note that DNA Center devices are pushed to ISE only when these devices are associated to a particular site where ISE is configured as its AAA server.

Finally, when properly configured, you can use Cisco ISE as a AAA server, to authorize and authenticate DNA Center users. You can also use a server other than Cisco ISE to perform this function (for details on this option, see [Configure Authentication and Policy Servers](#), on page 44).

Follow the steps below to integrate ISE with DNA Center.

Before You Begin

Before attempting to integrate ISE with Cisco DNA Center, be sure you have met the following pre-requisites:

- You have deployed one or more ISE version 2.3 hosts on your network. If you have a multi-host ISE deployment, integrating with the ISE admin node is recommended.
For information on installing ISE, see the [Cisco Identity Services Engine Installation Guide, Release 2.3](#).
- The PxGrid service must be enabled on the ISE host with which you plan to integrate DNA Center. The procedure below explains how to enable this service.
- The ISE admin node on which PxGrid is enabled must be reachable on the IP address of the eth0 interface of ISE from DNA Center.
- The ISE node can reach the fabric underlay network via the appliance NIC.
- The ISE node has SSH enabled
- The ISE CLI and GUI user accounts must use the same username and password
- The ISE admin node certificate must contain the ISE IP address or fully-qualified domain name (FQDN) in either the certificate subject name or the SAN.
- The DNA Center system certificate must contain the DNA Center appliance IP or FQDN in either the certificate subject name or the SAN.


Step 1

Enable ISE Services on the ISE host, as follows:

- a) Log into the ISE node with which you want to integrate.
- b) Select **Administration > Deployment**.
- c) Select the host name of the ISE node with which you will integrate and, under the **General Settings** tab, make sure the following boxes are checked: **Enable SXP Service**, **Enable Passive Identity Service**, and **pxGrid**.
- d) Click **Save**.
- e) Click the **Profiling Configuration** tab and ensure that (at a minimum) the following probes are selected: **RADIUS**, **SNMPQUERY**.

- f) Select **Administration > Settings > ERS Settings** and click **Enable ERS for Read/Write**. Click **OK** at the notification prompt.

Step 2 Add the ISE node to DNA Center as a AAA server, as follows:


- a) Log in to the DNA Center web-based GUI.
- b) Click , then select **System Settings**.
- c) Under the Cisco ISE panel, select the **Configure Settings** link.
- d) On the **Settings - Authentication and Policy Servers** page, click the large plus (+) icon to display the AAA settings.
- e) Click the **Cisco ISE** slider to ensure that all of the ISE-related fields are shown.
- f) Enter the ISE management IP address in the **IP address** field.
- g) Enter the **Shared Secret** used to secure communications between your network devices and ISE.
- h) Enter the corresponding ISE admin credentials in the **Username** and **Password** fields.
- i) Enter the **FQDN** for the ISE node.
- j) Enter the **Subscriber Name** (for example: dnacenter).
- k) The **SSH Key** is optional and may be left blank.

Step 3 When you are finished populating these fields, click **Update** and wait for the server status to show as Active.

Step 4 Verify that ISE is connected to DNA Center and that the connection has subscribers, as follows:

- a) Log into the ISE node.
- b) Select **Administration > pxGrid Services**. You should see that a subscriber with the name you entered (for example: dnacenter) is currently online.
- c) If the subscriber status is Pending, select **Total Pending Approval > Approve All Clients** to approve this subscriber. The subscriber status should change to online.

Step 5 Verify that DNA Center is connected to ISE and that ISE SGT groups and devices are being pushed to DNA Center, as follows:

- a) Log in to the DNA Center web-based GUI.
- b) Click , and then select **System Settings**.
- c) Under the Cisco ISE panel, select the **Configure Settings** link.
- d) On the **Settings - Authentication and Policy Servers** page, click the large plus (+) icon to display the AAA settings.
- e) Verify that the status for the Cisco ISE AAA server is still Active.
- f) Select **Policy > Registry > Scalable Groups**. You should see ISE SGT groups in the list of Scalable Groups.

Configure an IP Address Manager

You can configure DNA Center to communicate with an external IP address manager.

Before You Begin

You should have an external IP address manager already set up and functional.

Step 1 From the DNA Center **Home** page, click the gear icon (⚙️) and then choose **System Settings > Settings > IP Address Manager**.

Step 2 In the **IP Address Manager** section, enter the required information in the following fields:

Server Name	Name of server.
Server URL	IP address of server.
Username	Required username for server access.
Password	Required password for server access.
Provider	<p>Select a provider from the drop-down menu.</p> <p>Note When selecting BlueCat as your provider, ensure that your user has been granted API access in the BlueCat Address Manager. Refer to your BlueCat documentation for information about configuring API access for your user or users.</p>

Step 3 Click **Apply** to apply and save your settings.

What to Do Next

Click the **System 360** tab and check to ensure that your external IP address manager configuration was successful.


Configure Authentication and Policy Servers

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

Before You Begin

- If you are using Cisco ISE 2.3 or later to perform both policy and AAA functions, make sure that DNA Center and Cisco ISE are integrated as described in the section [Integrate Cisco ISE With DNA Center, on page 41](#).
- If you are using another product (not Cisco ISE 2.3 or later) to perform AAA functions, make sure to do the following:
 - Register DNA Center with the AAA server, including defining the shared-secret on both the AAA server and DNA Center.

- Define an attribute name for DNA Center on the AAA server.
- For a DNA Center multi-host cluster configuration, define all individual host IP addresses and the virtual IP address for the multi-host cluster on the AAA server.

Step 1 From the DNA Center **Home** page, click  and then choose **System Settings > Settings > Authentication and Policy Servers**.

Step 2 Click  **Add**.

Step 3 Configure the primary AAA server by providing the following information:

- **Server IP Address**—IP address of the AAA server.
- **Shared Secret**—Key for device authentications. The shared secret can be up to 128 characters in length.

Step 4 To configure a AAA server (not Cisco ISE), leave the **Cisco ISE Server** button in the **Off** position and proceed to the next step.

To configure a Cisco ISE server, click the **Cisco ISE server** button to the **On** position and enter information in the following fields:

- **Cisco ISE**—Setting that indicates whether the server is a Cisco ISE server. Click the **Cisco ISE** setting to enable Cisco ISE.
- **Username**—Name that is used to log in to the Cisco ISE command-line interface (CLI).
- **Password**—Password for the Cisco ISE CLI username.
- **FQDN**—Fully qualified domain name (FQDN) of the Cisco ISE server. The FQDN consists of two parts, a hostname and the domain name, in the following format:
hostname.domainname.com.
For example, the FQDN for a Cisco ISE server might be ise.cisco.com.
- **Subscriber Name**—A unique text string, for example `dnac`, that is used during DNA Center to Cisco ISE integration to setup a new pxGrid client in Cisco ISE.
- **SSH Key**—Diffie-Hellman-Group14-SHA1 SSH key used to connect and authenticate with Cisco ISE.

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

- **Protocol**—**TACACS** or **RADIUS**. Radius is the default.
Note You can only choose one option. The option that is dimmed is the chosen option. To select the other option, you need to choose it and then manually deselect the other option.
- **Authentication Port**—Port used to relay authentication messages to the AAA server. The default is UDP port 1812.
- **Accounting Port**—Port used to relay important events to the AAA server. The information in these events is used for security and billing purposes. The default UDP port is 1813.
- **Retries**—Number of times that DNA Center attempts to connect with the AAA server before abandoning the attempt to connect. The default number of attempts is 1.

- **Timeout**—The length of time that device waits for the AAA server to respond before abandoning the attempt to connect.

Step 6 Click **Add**.

Step 7 To add a secondary server, repeat Step 2 through Step 6.

Configure SNMP Properties

You can configure retry and timeout values for SNMP.

Before You Begin

Only a user with SUPER-ADMIN-ROLE or NETWORK-ADMIN-ROLE permissions may perform this procedure. For more information, see the *Cisco Digital Network Architecture Center Administrator Guide*.

Step 1 From the DNA Center **Home** page, click the gear icon (⚙️) and then choose **System Settings > Settings > SNMP Properties**.

Step 2 Configure the following fields:

Table 13: SNMP Properties

Field	Description
Retries	Number of attempts to connect to the device. Valid values are from 0-4. The default is 3.
Timeout (in Seconds)	Number of seconds DNA Center waits when trying to establish a connection with a device before timing out. Valid values are from 5-120 in intervals of 5 seconds. The default is 5.

Step 3 Click **Apply**.

Note To return to the default settings, click **Revert to Defaults**.

Log Out of DNA Center

To log out of Cisco DNA Center, click ⚙️ and then select **Log Out**. This ends your session and logs you out.

For security reasons, we recommend that you log out when you complete your administrative session. If you do not log out, DNA Center logs you out automatically after 30 minutes of inactivity.

Reconfigure the Appliance Using the Wizard

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

Perform the steps in this procedure to change the DNA Center configuration wizard settings, including the external network settings, NTP server address, and/or password for the Linux maglev user. The external network settings that can be changed include:

- Host IP address
- DNS server
- Default gateway
- NTP servers
- Static routes

Step 1

Using a Secure Shell (SSH) client, log into the DNA Center appliance.

Log in using the IP address that you specified using the configuration wizard, on port 2222.

The recommended IP address to enter for the SSH client is the IP address that you configured for the OOB management network adapter (this is the 1Gb Ethernet dedicated OOB management port).

Step 2

When prompted, enter your Linux username (maglev) and password for SSH access.

Step 3

Enter the following command to access the configuration wizard.

```
$ sudo maglev-config update
```

If prompted for the maglev user's password, enter it again.

Step 4

After making your configuration change(s), continue through the configuration process to the final message.

Step 5

At the end of the configuration process, a final message appears stating that the wizard is now ready to proceed with applying the configuration.

The following options are available:

- **[back]**—Review and verify your configuration settings.
- **[cancel]**—Discard your configuration settings and exit the configuration wizard.
- **[proceed]**—Save your configuration settings and begin applying them.

Enter **proceed>>** to complete the installation. After entering **proceed>>**, the configuration wizard applies the configuration values that you entered above.

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

Power-Cycle the Appliance

Under certain circumstances (such as when troubleshooting problems), you may want to power-cycle (power down and then power up) the appliance. This procedure describes how to perform this task.

Before You Begin

Be sure you have installed the Cisco DNA Center appliance following the procedures in this guide.

-
- Step 1** Using a Secure Shell (SSH) client, log into the DNA Center appliance with the IP address that you specified using the configuration wizard, on port 2222.
The IP address to enter for the SSH client is the IP address that you configured for the network adapter that connects the host to the enterprise network.
- Step 2** When prompted, enter your Linux username (maglev) and password for SSH access.
- Step 3** Power down the host by entering the following command:
- ```
$ sudo shutdown -h now
```
- Enter your password a second time when prompted.
- Step 4** Review the command output as the host shuts down.  
The **sudo shutdown** command also powers off the host.
- Step 5** Power up the Maglev root process by turning the appliance back on.
-