Prepare the Appliance for Configuration

• Preparation for Appliance Configuration Overview, on page 1
• Enable Browser Access to Cisco Integrated Management Controller, on page 1
• Execute Preconfiguration Checks, on page 6
• Disable the Network Interface Card, on page 8
• Reimage the Appliance, on page 14

Preparation for Appliance Configuration Overview

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

1. Enable browser access to the appliance's Cisco IMC (see Enable Browser Access to Cisco Integrated Management Controller).

2. Use Cisco IMC to check and adjust important hardware and switch settings (see Execute Preconfiguration Checks).

3. If the Intel X710-DA4 network interface card (NIC) that shipped with your appliance is currently enabled, you need to disable it (see Disable the Network Interface Card, on page 8).

4. Cisco DNA Center software is preinstalled on your appliance, but you may need to reinstall the software in certain situations (such as before you change the current cluster link configuration). If this is the case, you must also complete the tasks described in Reimage the Appliance.

Note

If you do not need to reimage your appliance, proceed to Appliance Configuration Overview.

Enable Browser Access to Cisco Integrated Management Controller

After installing the appliance, as described in Appliance Installation Workflow, use the Cisco IMC configuration utility to assign an IP address and gateway to the appliance's CIMC port. This gives you access to the Cisco IMC GUI, which you should use to configure the appliance.
After you complete the Cisco IMC setup, log in to Cisco IMC and run the tasks listed in Execute Preconfiguration Checks to ensure correct configuration.

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

2. Click ID 1, and then Modify User.
3. Enter the new password in the Change Password field, and then click Save.

---

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

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

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

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

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

---

Step 4
As soon as the boot screen is displayed, press F8 to perform Cisco IMC configuration.

The CIMC configuration utility displays the CIMC User Details screen, as shown below.
Step 5  Enter the default CIMC user password (the default on a new appliance is password) in the Enter current CIMC Password field.

Step 6  Enter and confirm the new CIMC user password in the Enter new CIMC password and Re-Enter new CIMC password fields.

When you press Enter after entering the new password in the Re-Enter new CIMC password field, the Cisco IMC configuration utility displays the NIC Properties screen, as shown below.

Step 7  Perform the following actions:

- NIC mode: Select Dedicated.
- IP (Basic): Select IPV4.
- CIMC IP: Enter the IP address of the CIMC port.
- Prefix/Subnet: Enter the subnet mask for the CIMC port IP address.
- Gateway: Enter the IP address of your preferred default gateway.
**Pref DNS Server**: Enter the IP address of your preferred DNS server.

**NIC Redundancy**: Select None.

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

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

![Common Properties Screen](image)

**Step 9**
Perform the following actions:

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

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

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

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

https://CIMC_ip_address, where CIMC_ip_address is the Cisco IMC port IP address that you entered in Step 7.
Your browser displays a main Cisco IMC GUI login window similar to the one shown below.

---

**Step 13**

Log in using the Cisco IMC user ID and password you set in Step 5. If the login is successful, your browser displays a **Cisco Integrated Management Controller Chassis Summary** window similar to the one shown below.
Execute Preconfiguration Checks

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

1. Synchronize the appliance hardware with the Network Time Protocol (NTP) servers you use to manage your network. These must be the same NTP servers whose hostnames or IPs you gathered for use when planning your implementation, as explained in Required IP Addresses and Subnets. This is a critical task that ensures that your Cisco DNA Center data is synchronized properly across the network.

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

---

Step 1

Login to the appliance’s CIMC using the CIMC IP address, user ID and password you set in Enable Browser Access to Cisco Integrated Management Controller. If login is successful, your browser displays the Cisco Integrated Management Controller Chassis Summary window, as shown below.

![Chassis Summary Window](image)

Step 2

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

a) With the Chassis Summary window displayed, click the icon to display the CIMC menu.

b) From the CIMC menu, select Admin > Networking > NTP Setting. CIMC displays the NTP Setting tab.

c) Make sure the NTP Enabled box is checked, then enter up to four NTP server host names or addresses in the four numbered Server fields, as in the example shown below.
d) When you are finished, click **Save Changes**. Cisco IMC will validate your entries, then begin to synchronize the time on the appliance hardware with the time on the NTP servers.

**Note** Unlike the previous generation of Cisco DNA Center appliances, second generation appliances do not use a virtual interface card (VIC). You do not need to configure the network interface card (NIC) that comes installed on your second generation appliance to support high throughput in Cisco IMC, as this is already enabled by default.

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

a) Using a Secure Shell (SSH) client, log into the switch to be configured and enter EXEC mode at the switch prompt.

b) Enter the following series of commands to configure the switch port:

```
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
```

**Note** These commands are examples only.

**Important** The switch port on Cisco DNA Center second generation appliances must be set to access mode in order to function properly. Trunk mode is not supported, as it is on first generation appliances.

c) Run the command **show interface tengigabitethernet portID** and verify that the port is connected and 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)
```
### Disable the Network Interface Card

If your appliance ships with the Intel X710-DA4 network interface card (NIC) enabled, you must disable it by completing the following procedure. If you do not disable the card, your appliance will contain four extra interfaces, which could negatively affect your configuration.

#### Step 1

Confirm that you have a Cisco DNA Center appliance and that it has the Intel X710-DA4 NIC installed.

a) Log in to the appliance’s Cisco IMC.

b) In the **Summary** window’s **Server Properties** area, confirm that the following values are set:

- **PID:** DN2-HW-APL for a 44 core appliance, DN2-HW-APL-L for a 56 core appliance, or DN2-HW-APL-XL for a 112 core appliance (see the following example).

---

**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

### What to do next

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

- If you need to reinstall Cisco DNA Center software before you configure your appliance, see Reimage the Appliance.

- If you are ready to configure your appliance, proceed to Appliance Configuration Overview.
• BIOS Version: This value should start with either **C220M5** for a 44 and 56 core appliance or **C480M5** for a 112 core appliance (see the following example).

![Server Properties](image)

**Server Properties**

| Product Name: | FH224 |
| Serial Number: | 6C2-1W-AW-XX |
| UUID: | 6FF202AA-EEF9-4DF4-9FE4-01c.0.0.706181854 |
| BIOS Version: | XE801AA |
| Description: | Unknown |

**Cisco Integrated Management Controller**

| Hostname: | C480-FH224 |
| IP Address: | 10.195.10.10 |
| MAC Address: | A8:B4:56:80:AA:XX |
| Firmware Version: | 4.0(1a) |
| Current Time (UTC): | Wed Nov 6 18:51:54 2019 |
| Local Time: | Wed Nov 6 10:51:54 2019 PST -08 |
| Timezone: | America/Los_Angeles |

**c) Choose **Chassis > Inventory > Network Adapters.**

d) In the **Network Adapters** table, confirm that the Intel X710-DA4 Quad Port network adapter is listed for one of the following slots:

- For a 44 or 56 core appliance, **Slot 2**.
- For a 112 core appliance, **Slot 12** (see the following example).  

![Network Adapters](image)

**Step 2** Confirm that your appliance’s PCIe card is disabled:

a) Choose **Chassis > Compute.**

The **BIOS > Configure BIOS > I/O** tab opens.

b) Set the following parameters to **Disabled**, then click **Save**:

- For a 44 or 56 core appliance, **PCIe Slot 2 OptionROM** and **PCIe Slot 2 Link Speed**.
- For a 112 core appliance, **PCIe Slot 12 OptionROM** and **PCIe Slot 12 Link Speed** (see the following example).
c) Do one of the following:

- If you were able to set these two parameters to **Disabled** for your appliance, reboot your appliance and then proceed with its configuration. You do not need to complete the rest of this procedure.

- If you have a 112 core appliance and only see one of these parameters displayed in the **I/O** tab, proceed to Step 3 and complete the rest of this procedure.

**Step 3**

Boot into your appliance’s BIOS:

a) From Cisco IMC, start a KVM session.

b) Power cycle the appliance by clicking the **Host Power** link and then choosing **Power Cycle**.

c) During startup, press the **F2** key as soon as you see the following screen to boot into your appliance’s BIOS and open the Aptio Setup Utility.
Step 4  Disable the PCIe card:

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

b) In the **LOM and PCIe Slots Configuration** tab, choose **PCIE Link Speed Configuration**.
c) In the **PCIE Link Speed Configuration** tab, scroll down to PCIE SlotID: 12’s **Link Enable** option and then press **Enter**.

d) Choose **Disable**, then press **ENTER**.

Your screen should look like the following example:
e) Press the **ESC** key twice to return to the main BIOS menu, then open the **Save & Exit** tab.
f) Choose the **Save Changes and Reset** option, then press **Enter**.
Reimage the Appliance

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

**Step 1** Download the Cisco DNA Center ISO image and verify that it is a genuine Cisco image.
See [Verify the Cisco DNA Center ISO Image](#).

**Step 2** Create a bootable USB drive that contains the Cisco DNA Center ISO image.
See [Create a Bootable USB Drive](#).

**Step 3** Reinitialize the three virtual drives that are managed by your appliance’s RAID controller:

a) Log into CIMC and start a KVM session.

b) Power on or power cycle the appliance by choosing one of the following menu options:

   - **Power > Power On System**
   - **Power > Power Cycle System (cold boot)**

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

<table>
<thead>
<tr>
<th>ID</th>
<th>LUN</th>
<th>VENDOR</th>
<th>PRODUCT</th>
<th>REVISION</th>
<th>CAPACITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>0</td>
<td>ATA</td>
<td>INTEL SSDSC2BB48</td>
<td>CS01</td>
<td>457862MB</td>
</tr>
<tr>
<td>0</td>
<td>A0AG0</td>
<td>Virtual Drive</td>
<td>RAID1</td>
<td>457862MB</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>A0AG0</td>
<td>Virtual Drive</td>
<td>RAID1</td>
<td>457862MB</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>A0AG0</td>
<td>Virtual Drive</td>
<td>RAID1</td>
<td>457862MB</td>
<td></td>
</tr>
</tbody>
</table>

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

Press <Ctrl><R> to run MegaRAID Configuration Utility.

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

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

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

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

**Important** After you have disabled your appliance’s NIC, if you reset your appliance to the default settings in Cisco IMC (*Admin > Utilities > Reset to factory Default*), you will need to complete this procedure again.
This opens the drive’s Advanced Properties screen.

e) In the resulting menu, choose Initialization > Fast Initialization.
f) Repeat Steps 3b through 3e for the other virtual drives on your appliance.

Step 4
Reinstall Cisco DNA Center onto your appliance.

See Install the Cisco DNA Center ISO Image.

---

**Verify the Cisco DNA Center ISO Image**

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

**Before you begin**

Obtain the location of the Cisco DNA Center ISO image (either via email or contact with the Cisco support team).

---

**Step 1**
Download the Cisco DNA Center ISO image (.iso) from the location specified by Cisco.

**Step 2**
Download the Cisco public key (cisco_image_verification_key.pub) for signature verification from the location specified by Cisco.

**Step 3**
Download the secure hash algorithm (SHA512) checksum file for the ISO image from the location specified by Cisco.

**Step 4**
Obtain the ISO image’s signature file (.sig) from Cisco support via email or by download from the secure Cisco website (if available).

**Step 5**
(Optional) Perform a SHA verification to determine whether the ISO image was corrupted due to a partial download. Run one of the following commands (depending upon your operating system):
• On a Linux system: `sha512sum ISO-image-filename`
• On a Mac system: `shasum -a 512 ISO-image-filename`

Microsoft Windows does not include a built-in checksum utility, but you can install a utility from Microsoft at this link: http://www.microsoft.com/en-us/download/details.aspx?id=11533. Compare the output of the command above (or Microsoft Windows utility) to the SHA512 checksum file downloaded earlier in Step 3. If the command output fails to match, download the ISO image again and run the appropriate command a second time. If the output still fails to match, contact Cisco support.

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

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

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

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

**Step 7**  After confirming you have downloaded a Cisco ISO image, create a bootable USB drive that contains the Cisco DNA Center ISO image. See Create a Bootable USB Drive.

---

**Create a Bootable USB Drive**

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

Before you begin:

• Download and verify your copy of the Cisco DNA Center ISO image. See Verify the Cisco DNA Center ISO Image.
• Confirm that the USB flash drive you are using has a capacity of at least 32 GB.

**Using Etcher**

---

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

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

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

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

**Step 3**  Click the gear icon in the upper right corner of the window and verify that the following Etcher settings are set:

• Auto-unmount on success
• Validate write on success
Step 4  Click Back to return to the main window.

Step 5  Click Select Image.

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

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

1. Click Select drive.
2. Click the radio button for the correct USB drive, then click Continue.

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

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

Using the Linux CLI  

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

a) Insert a flash drive into your machine's USB port.

b) Open a Linux shell and run the following command: `lsblk`

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

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

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

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

For example, to create a bootable USB drive using an ISO image named `CDNAC-SW-1.3.iso`, you would run the following command: `time sudo dd if=/data/tmp/CDNAC-SW-1.3.iso of=/dev/sdd bs=4M && sync`

Using the Mac CLI  

Step 1  Determine the disk partition associated with your USB flash drive:
a) Open a Terminal window and run the following command: `diskutil list`

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

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

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

**Step 2**

Unmount the flash drive's partition: `diskutil unmountDisk flash-drive-partition`

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

**Step 3**

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

Continuing our example, let's assume that you are working with a Cisco DNA Center 1.3 ISO image named `CDNAC-SW-1.3.iso`. You would run the following command, which creates a macOS disk image named `CDNAC-1.3.dmg`:

`hdiutil convert -format UDRW -o CDNAC-1.3 CDNAC-SW-1.3.iso`

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

**Step 4**

Create a bootable USB drive: `sudo dd if=macOS-image-filename of=flash-drive-partition bs=1m`

Continuing our example, you would run the following command: `sudo dd if=CDNAC-1.3.dmg of=/dev/disk2 bs=1m`

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

---

**Install the Cisco DNA Center ISO Image**

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

**Before you begin**

Create the bootable USB drive from which you will install the Cisco DNA Center ISO image. See Create a Bootable USB Drive.

**Step 1**

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

**Step 2**

Log into CIMC and start a KVM session.

**Step 3**

Power on or power cycle the appliance:

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

**Step 4**

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

**Step 5**

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

The boot device selection menu appears.

**Step 6**

Select your USB drive and then press Enter.
Step 7  In the GNU GRUB bootloader window, choose **Manufacture Cisco DNA appliance** and then press **Enter**.

**Note**  The bootloader will automatically boot the Maglev Installer instead if you do not make a selection within 30 seconds. Ensure that you make your selection before then.

When installation of the Cisco DNA Center ISO image completes, the installer reboots and opens the Maglev Configuration wizard's welcome screen. Depending on whether you are going to configure a master or secondary cluster node, proceed to Step 4 in either **Configure the Master Node Using the Maglev Wizard** or **Configure Add-On Nodes Using the Maglev Wizard**.
Install the Cisco DNA Center ISO Image