



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
- [Reimage the Appliance](#), on page 13

Preparation for Appliance Configuration Overview

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

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



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

Enable Browser Access to Cisco Integrated Management Controller

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

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



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

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

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

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

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

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

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

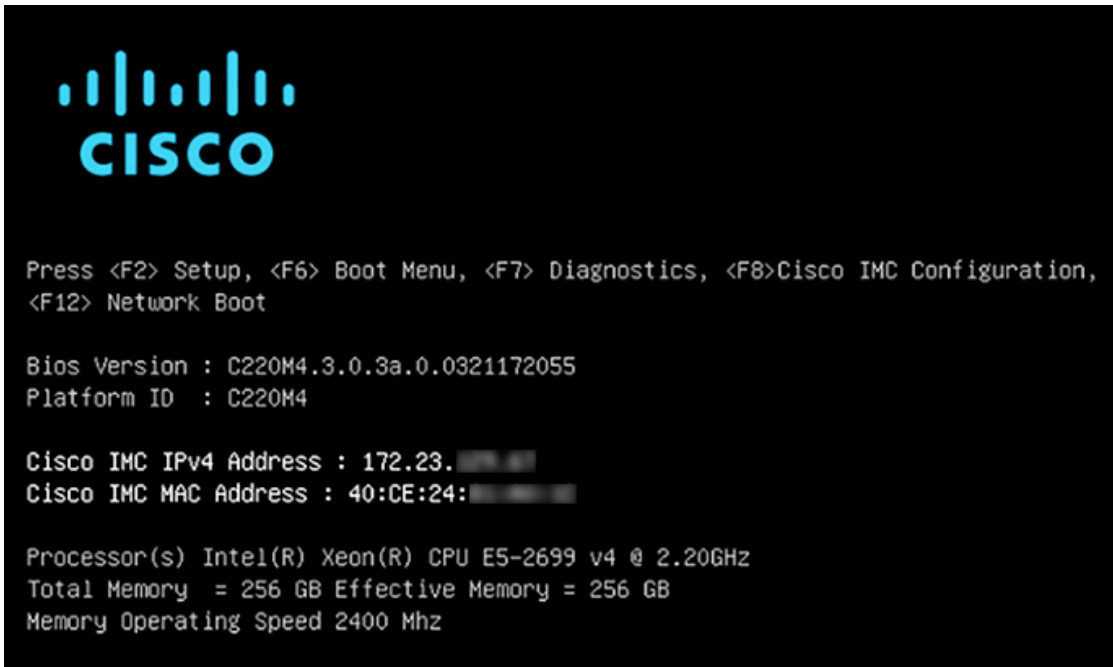
Step 1 Access the appliance console by attaching either of the following:

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

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

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

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



```

Cisco
CISCO

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

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

Cisco IMC IPv4 Address : 172.23. [redacted]
Cisco IMC MAC Address : 40:CE:24: [redacted]

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

```

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

```

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

- Step 5** Enter the default CIMC user password (the default on a new appliance is *password*) in the **Enter current CIMC Password** field.

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

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

```

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

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

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

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

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

```

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

```

Step 9 Perform the following actions:

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

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

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

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

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

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

**Step 13**

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

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

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

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

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

Step 14

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

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

Execute Preconfiguration Checks

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

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

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

Step 1

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

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


The screenshot displays the Cisco IMC Chassis Summary page. The top navigation bar includes the Cisco logo, the title 'Cisco Integrated Management Controller', and user information 'admin@1' for device '-C220-FCH212'. The main content area is divided into four sections:

- Server Properties:** Lists hardware details such as Product Name (UCS C220 M4SX), Serial Number (FCH212), PID (UCSC-C220-M4SX), UUID (1DB0E03F-59AF-4B5B-BAB7-), BIOS Version (C220M4.3.1.3c.0.0307181404), and Asset Tag (Unknown).
- Cisco Integrated Management Controller (Cisco IMC) Information:** Shows system identifiers like Hostname (C220-FCH212), IP Address (172.25), MAC Address (70:79:F0), Firmware Version (3.1(3a)), Current Time (UTC) (Tue Aug 14 15 2018), Local Time (Tue Aug 14 15 2018 UTC +0000), and Timezone (UTC).
- Chassis Status:** A list of health indicators with status icons: Power State (On), Overall Server Status (Good), Temperature (Good), Overall DIMM Status (Good), Power Supplies (Good), Fans (Good), Locator LED (Off), and Overall Storage Status (Good).
- Server Utilization:** A bar chart showing utilization percentages for Overall, CPU, Memory, and IO. The y-axis ranges from 0 to 100%. The chart shows low utilization for all categories.

At the bottom right, there are 'Save Changes' and 'Reset Values' buttons.

Step 2

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

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

Cisco Integrated Management Controller

admin@1 -C220-FCH212

Networking / NTP Setting

Network Network Security NTP Setting

NTP Properties

NTP Enabled:

Server 1:

Server 2:

Server 3:

Server 4:


Status: NTP service disabled

Save Changes Reset Values

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

Note Cisco IMC does not support NTP authentication.

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

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

Cisco Integrated Management Controller

Inventory / Cisco VIC Adapters

CPU Memory PCI Adapters Power Supplies Cisco VIC Adapters Network Adapters

Cisco VIC Adapters

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

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

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

CDN Support f	PCI ROM CLP	Disabled
PCH SATA	All Onboard LOM Ports	Enabled
LOM Port 1 Optio	LOM Port 2 OptionROM	Enabled
All PCIe Slots Optio	PCIe Slot:1 OptionROM	Enabled
PCIe Slot:2 Optio	PCIe Slot:MLOM OptionROM	Enabled
PCIe Slot:HBA Optio	PCIe Slot:FrontPcie1 OptionROM	Disabled
PCIe Slot:FrontPcie2 Optio	PCIe Slot:MLOM Link Speed	Auto
PCIe Slot:Riser1 Link .	PCIe Slot:Riser2 Link Speed	GEN3
PCIe Slot:FrontPcie1 Link	PCIe Slot:FrontPcie2 Link Speed	Auto
PCIe Slot:HBA Link '		

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

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

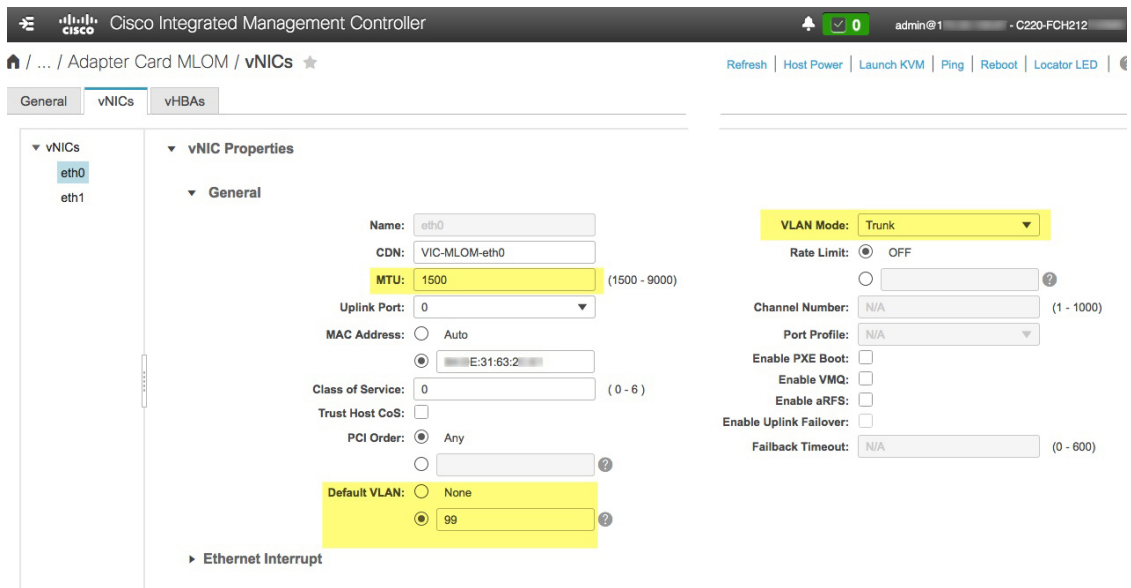
The screenshot displays the Cisco IMC configuration page for the Adapter Card MLOM. The page is organized into several sections:

- Adapter Card Properties:** Includes fields for PCI-Slot (MLOM), Vendor (Cisco Systems Inc), Product Name (UCS VIC 1227), Product ID (UCSC-MLOM-CSC-02), Serial Number (146J9L2), and Version ID (V01). It also shows Hardware Revision (3), Cisco IMC Management Enabled (no), Configuration Pending (no), ISCSI Boot Capable (True), CDN Capable (True), and usNIC Capable (True).
- Firmware:** Shows Running Version (4.1(3a)), Backup Version (4.1(3a)), Startup Version (4.1(3a)), and Bootloader Version (4.1(3a)). The status is 'Fwupdate never issued'.
- External Ethernet Interfaces:** This section is expanded to show details for Port-0 and Port-1.
 - Port-0:** MAC Address: E:31:63:2, Link State: Link Down, Encap: CE, Admin Speed: 10Gbps, Operating Speed: -.
 - Port-1:** MAC Address: E:31:63:2, Link State: Link Down, Encap: CE, Admin Speed: 10Gbps, Operating Speed: -.

At the bottom right of the configuration page, there are dropdown menus for Port-0 and Port-1, both set to 'Auto'.

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

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



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

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



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

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

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

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

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

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

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

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

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

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

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

MySwitch#
```

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

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

```

switchport mode trunk
switchport voice vlan dot1p
end

```

```
MySwitch#
```

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

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

Vlan	Mac Address	Type	Ports
99	xxx.e.3161.1000	DYNAMIC	Te1/1/3

Total Mac Addresses for this criterion: 1

```
MySwitch#
```

What to do next

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

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

Reimage the Appliance

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

- Step 1** Download the Cisco DNA Center ISO image and verify that it is a genuine Cisco image.
See [Verify the Cisco DNA Center Image, on page 15](#).
- Step 2** Create a bootable USB drive that contains the Cisco DNA Center ISO image.
See [Create a Bootable USB Flash Drive, on page 16](#).
- Step 3** Reinitialize the three virtual drives that are managed by your appliance's RAID controller:
- Log in to Cisco IMC and start a KVM session.
 - 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) is displayed.

```

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

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

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

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

```

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

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

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

```

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

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

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

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

```

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

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

Step 4 Reinstall Cisco DNA Center onto your appliance.

See [Install the Cisco DNA Center ISO Image, on page 18](#).

Verify the Cisco DNA Center Image

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

Before you begin

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

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

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

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

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

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

For example:

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

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

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

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

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

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

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

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

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

Create a Bootable USB Flash Drive

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

Before you begin:

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



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

Using Etcher

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

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

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

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


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

- Auto-unmount on success
- Validate write on success

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

Step 5 Click **Select Image**.

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

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

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

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

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

Using the Linux CLI

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

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

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

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

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

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

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

Using the Mac CLI

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

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

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

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

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

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

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

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

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

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

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

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

Install the Cisco DNA Center ISO Image

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

Before you begin

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

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

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

Step 3 Power on or power cycle the appliance:

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

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

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

The boot device selection menu appears.

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

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

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

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