

# Enable Secure Boot for Cisco DNA Center

First Published: 2021-10-25

## Secure Boot

The Cisco Integrated Management Controller (Cisco IMC) and BIOS firmware contains the Unified Extensible Firmware Interface (UEFI) secure boot certificates in a hierarchy as defined by the UEFI specification. This hierarchy is immutable once it is loaded on the system. The root of trust begins from the firmware because of immutability. The following hierarchy contains Cisco-specific certificates; the certificate private keys are maintained securely offline in the Cisco software image management engine.

### PK → KEK → DB

The root of trust is in the firmware, which hosts the platform key (PK), the key exchange key (KEK), and the key database (DB). The PK validates the certificates in the KEK; the KEK validates the certificates in the DB. The DB contains the end entity certificate, which is used to verify the signatures of all boot programs. The PK, KEK, and DB are referred to as *auth variables* in UEFI secure boot terms.

During the Cisco DNA Center UCS system boot, the firmware validates itself and then activates the UEFI key hierarchy for the Cisco DNA Center platform based on the product ID (PID). After secure boot is activated, the system can only boot software that is signed by the UEFI secure boot Cisco DNA Center certificate. If you try to boot a CD-ROM, USB flash drive, or hard disk without the correct Cisco DNA Center signature, the boot operation fails. After secure boot is enabled, it cannot be disabled in the Cisco IMC and BIOS.

To verify that the image boots with the correct signature, see [Verify the Extensible Firmware Interface Image Signature, on page 15](#).

## Hardware and Software Requirements

The following table lists the hardware and software requirements for secure boot and Cisco DNA Center. Confirm that the Cisco DNA Center ISO that you are using is enabled with secure boot.

Cisco DNA Center images are signed using the SHA-256 hash algorithm. The signature scheme is PKCS7, signed with the RSA-2048 key.

Secure Boot Requirement	Description
<b>Hardware</b>	
Appliance	DN2-HW-APL DN2-HW-APL-L DN2-HW-APL-XL
<b>Firmware</b>	
UCS firmware	4.0(4h)

Secure Boot Requirement	Description
Firmware for C220 (DN2-HW-APL, DN2-HW-APL-L)	<a href="https://software.cisco.com/download/home/286318809/type/283850974/release/4.0(4h)">https://software.cisco.com/download/home/286318809/type/283850974/release/4.0(4h)</a>
Firmware for C480 (DN2-HW-APL-XL)	<a href="https://software.cisco.com/download/home/286318818/type/283850974/release/4.0(4h)">https://software.cisco.com/download/home/286318818/type/283850974/release/4.0(4h)</a>
<b>BIOS</b>	
BIOS for C220 (DN2-HW-APL, DN2-HW-APL-L)	<a href="http://10.106.0.171/C220M5-BIOS-4.0.4i_DNAC.cap">http://10.106.0.171/C220M5-BIOS-4.0.4i_DNAC.cap</a>
BIOS for C480 (DN2-HW-APL-XL)	<a href="http://10.106.0.171/C480M5-BIOS-4.0.4h_DNAC.cap">http://10.106.0.171/C480M5-BIOS-4.0.4h_DNAC.cap</a>

## Installation Workflow

The workflow to install and enable secure boot for Cisco DNA Center involves the following steps:

1. Install and activate the Cisco IMC firmware.
2. Install and activate the BIOS.
3. Change the settings in the Cisco IMC and BIOS, and install secure boot-enabled Cisco DNA Center.

## Install the Cisco IMC Firmware

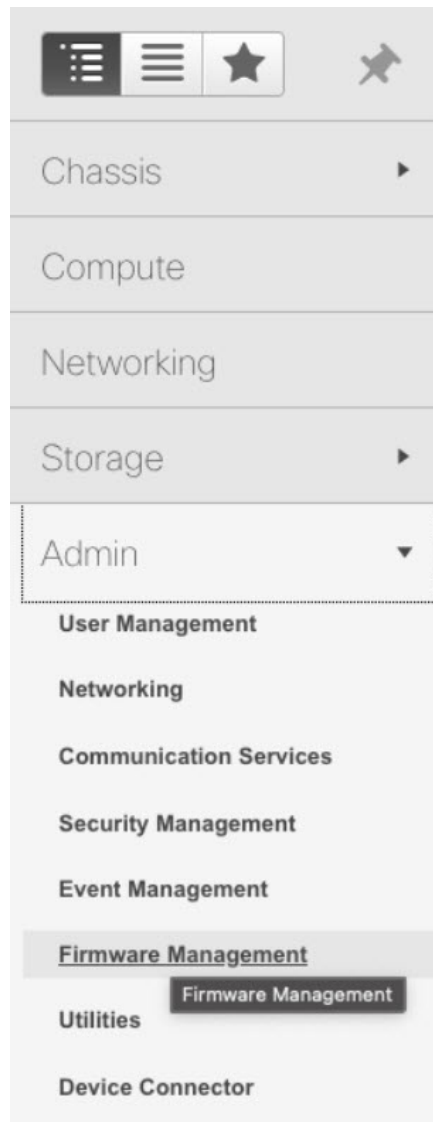
### Install the Cisco IMC Firmware Through the Browser

#### Before you begin

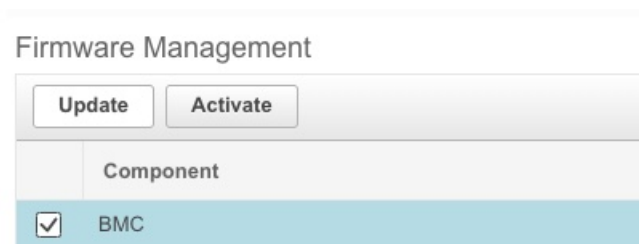
- Log in to the Cisco IMC GUI as a user with admin privileges.
- Obtain the Cisco Host Upgrade Utility ISO file from [cisco.com](http://cisco.com) and extract the firmware installation files from the firmware for [C220](#) and [C480](#).

#### Procedure

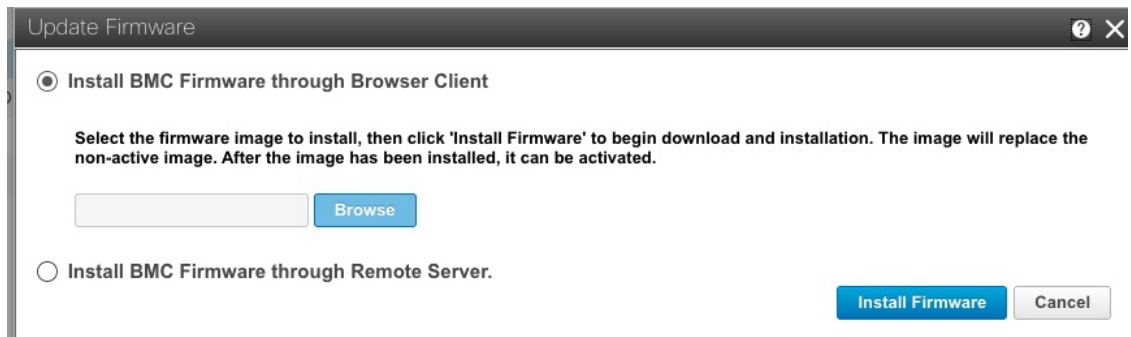
- 
- Step 1** In the Cisco IMC GUI, click the Navigation pane and choose **Admin**.
- Step 2** From the **Admin** drop-down list, choose **Firmware Management**.  
The **Firmware Management** dialog box appears.



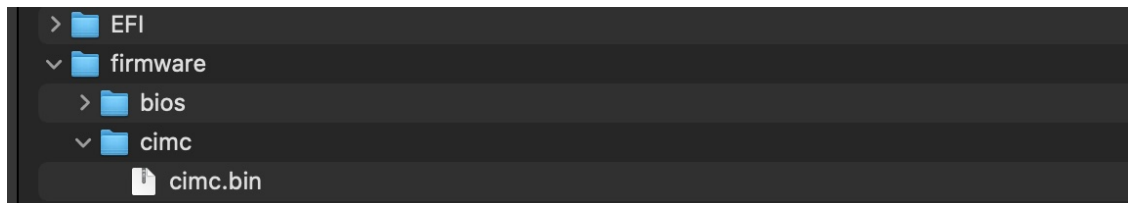
**Step 3** In the **Firmware Management** dialog box, check the **BMC** check box and click **Update**.



**Step 4** In the **Update Firmware** dialog box, click **Install BMC Firmware through Browser Client**, and then click **Browse**.



**Step 5** In the **Choose File** dialog box, navigate to the .bin file that you want to install.



**Step 6** In the **Update Firmware** dialog box, click **Install Firmware**.

## Activate the Installed Cisco IMC Firmware

### Before you begin

Install the Cisco IMC firmware on the server.

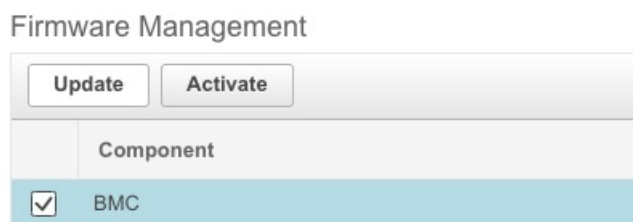
### Procedure

**Step 1** In the Cisco IMC GUI, click the Navigation pane and choose **Admin**.

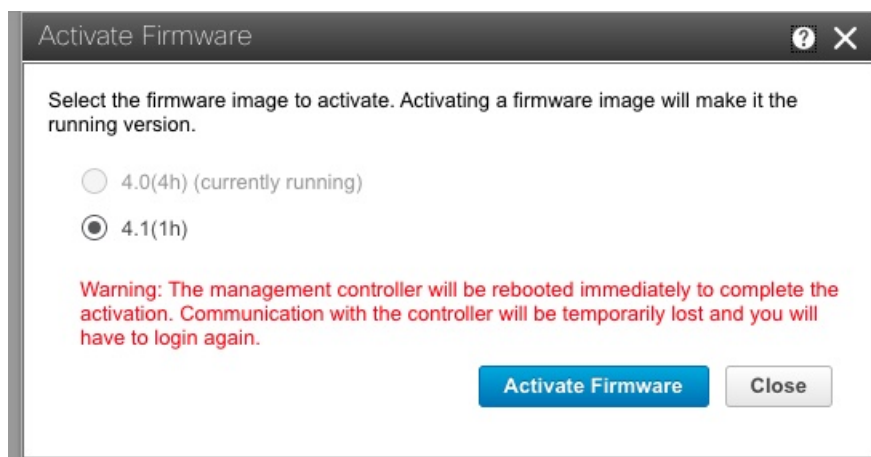
**Step 2** From the **Admin** drop-down list, choose **Firmware Management**.

The **Firmware Management** dialog box appears.

**Step 3** In the **Firmware Management** dialog box, check the **BMC** check box and click **Activate**.



**Step 4** In the **Activate Firmware** dialog box, select the firmware image to activate, and then click **Activate Firmware**.



**Note** After you press **Activate Firmware**, the Cisco IMC shuts down and reboots. This shouldn't take more than 15 minutes.

## Install the BIOS

### Install the Cisco IMC BIOS Through the Browser

#### Before you begin

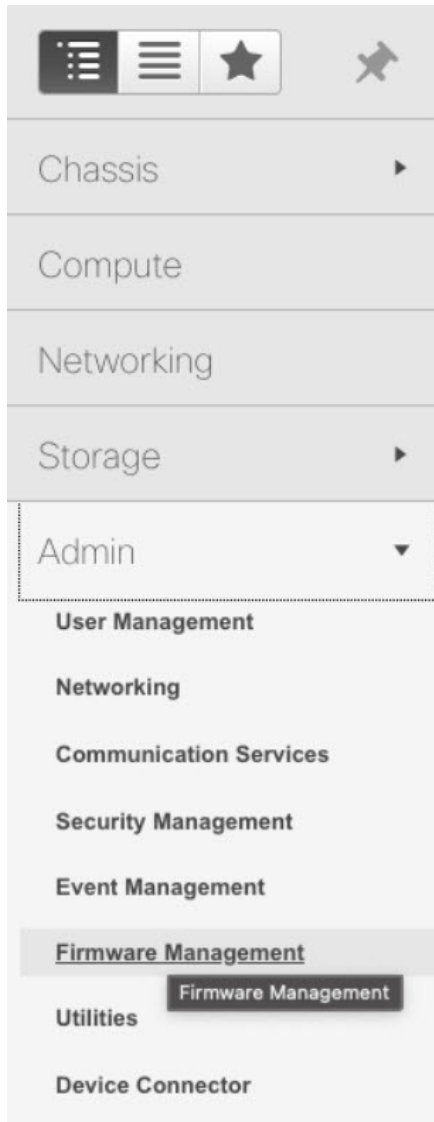
- Log in to the Cisco IMC GUI as a user with admin privileges.
- Download the BIOS for [C220](#) and the BIOS for [C480](#).

#### Procedure

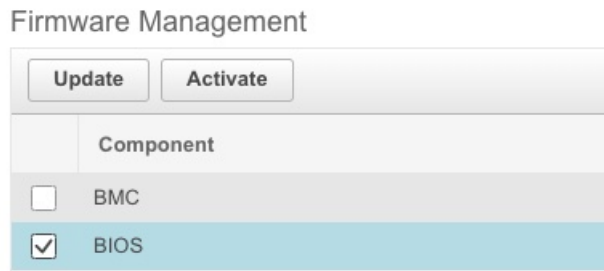
**Step 1** In the Cisco IMC GUI, click the Navigation pane and choose **Admin**.

**Step 2** From the **Admin** drop-down list, choose **Firmware Management**.

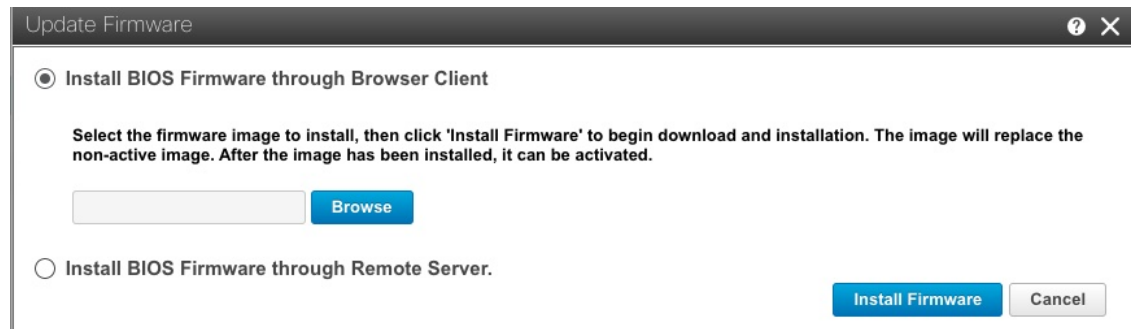
The **Firmware Management** dialog box appears.



**Step 3** In the **Firmware Management** dialog box, check the **BIOS** check box and click **Update**.



**Step 4** In the **Update Firmware** dialog box, click **Install BIOS Firmware through Browser Client**, and click **Browse**.



**Step 5** In the **Choose File** dialog box, navigate to the .cap file that you want to install.

**Step 6** In the **Update Firmware** dialog box, click **Install Firmware**.

## Activate the Installed BIOS Firmware

### Before you begin

Install the Cisco IMC firmware on the server.

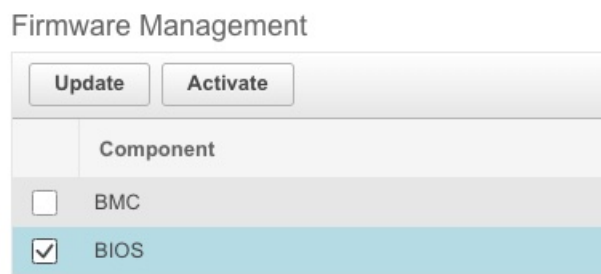
### Procedure

**Step 1** In the Cisco IMC GUI, click the Navigation pane and choose **Admin**.

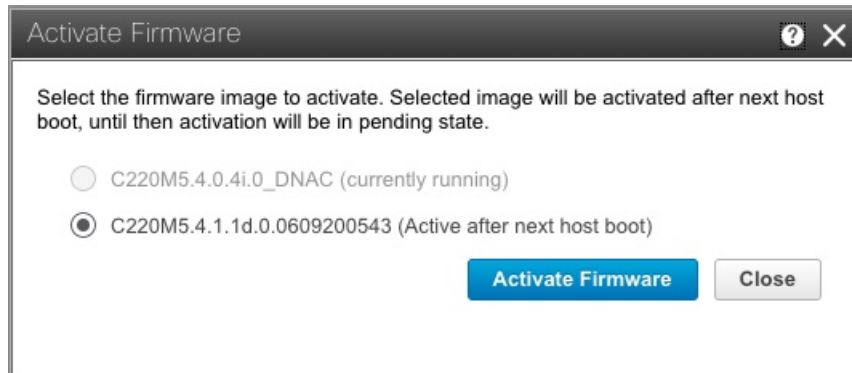
**Step 2** From the **Admin** drop-down list, choose **Firmware Management**.

The **Firmware Management** dialog box appears.

**Step 3** In the **Firmware Management** dialog box, check the **BIOS** check box and click **Activate**.



**Step 4** In the **Activate Firmware** dialog box, select the firmware image to activate, and then click **Activate Firmware**.



---

## Change the Cisco IMC and BIOS Settings and Install Cisco DNA Center

The workflow to change the settings for the Cisco IMC and BIOS and to install Cisco DNA Center involves the following steps:

1. Enable the UEFI secure boot mode.
2. Configure the boot order.
3. Install Cisco DNA Center.

### Enable the UEFI Secure Boot Mode

#### Before you begin

Log in to the Cisco IMC GUI as a user with admin privileges.

#### Procedure

- 
- Step 1** In the Cisco IMC GUI, click the Navigation pane and choose **Compute > BIOS** to view the **BIOS** tab.
  - Step 2** In the **BIOS** tab, click the **Configure Boot Order** tab.
  - Step 3** Check the **UEFI Secure Boot** check box, and click **Save Changes**.



🏠 / Compute / BIOS ★

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

[Enter BIOS Setup](#) | [Clear BIOS CMOS](#) | [Restore Manufacturing Custom Settings](#) | [Restore Defaults](#)

Configure BIOS | **Configure Boot Order** | Configure BIOS Profile

**BIOS Properties**

Running Version C220M5.4.0.4i.0\_DNAC

UEFI Secure Boot

Actual Boot Mode Uefi

Configured Boot Mode  (UEFI Secure Boot is enabled, disable it to modify Configured Boot Mode.)

Last Configured Boot Order Source BIOS

Configured One time boot device

[Save Changes](#)

**Note** After you click **Save Changes**, the machine reboots.

## Configure the Boot Order

Configure the first EFI boot order option to the Hard Disk Drive (HDD). The second boot order option can be either the Cisco IMC Mapped DVD, KVM Mapped DVD, or USB flash drive (which is based on your mode of installation).

### Before you begin

Restart the machine, and while BIOS is loading, press **F2** to enter the BIOS setup.

```

Cisco
Copyright (c) 2019 Cisco Systems, Inc.

Press <F2> BIOS Setup : <F6> Boot Menu : <F7> Diagnostics
Press <F8> CIMC Setup : <F12> Network Boot
Bios Version : C220M5.4.0.4i.0.0831191119
Platform ID : C220M5

Processor(s) Intel(R) Xeon(R) Platinum 8180 CPU @ 2.50GHz
Total Memory = 384 GB Effective Memory = 384 GB
Memory Operating Speed 2666 Mhz
M.2 SWRAID configuration is not detected. Switching to AHCI mode.

Cisco IMC IPv4 Address : 10.106 ...
Cisco IMC MAC Address : 70:EA:...

Entering Boot Menu ...

```

**Procedure**

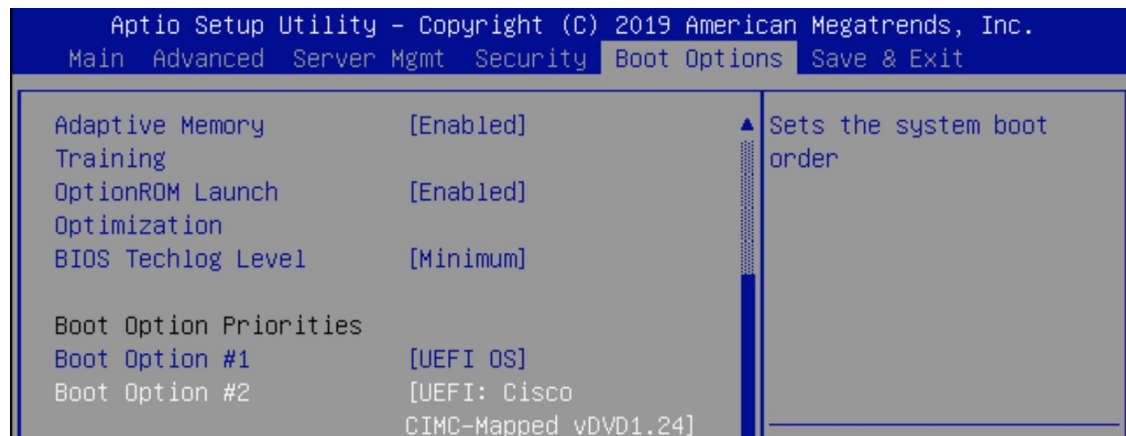
**Step 1** In the Navigation pane, click the **Boot Options** tab.

**Step 2** From the **Boot Options** tab, scroll down to the **Boot Option Priorities** area.

**Step 3** In the **Boot Option Priorities** area, set the **Boot Option #1** field to **UEFI OS**.

**Note** UEFI OS is the HDD.

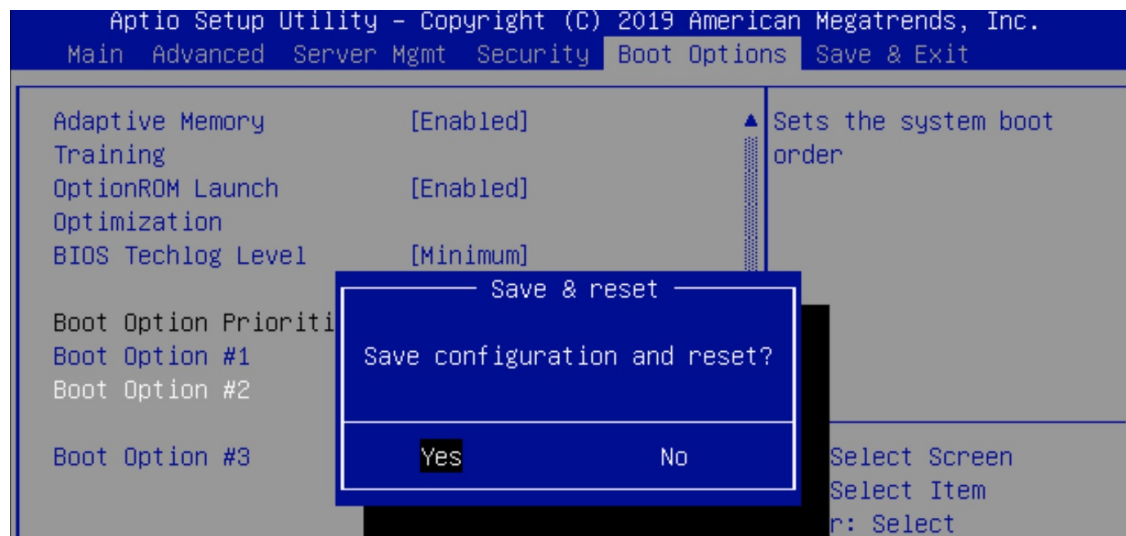
**Step 4** Set the **Boot Option #2** field to **Cisco IMC Mapped DVD (Tested)**, **USB flash drive (Not Tested)**, or **KVM Mapped DVD (Not Tested)**.



The preceding example screenshot shows that **Boot Option #2** is set to **Cisco IMC Mapped DVD**.

**Note** If the ISO is not mapped, you will not see these options. Before you set the boot order, map the secure boot-enabled ISO. (This also applies to the **USB flash drive** option because without mapping the ISO, it will not appear as an option.)

**Step 5** Press **F10** and save the configuration.



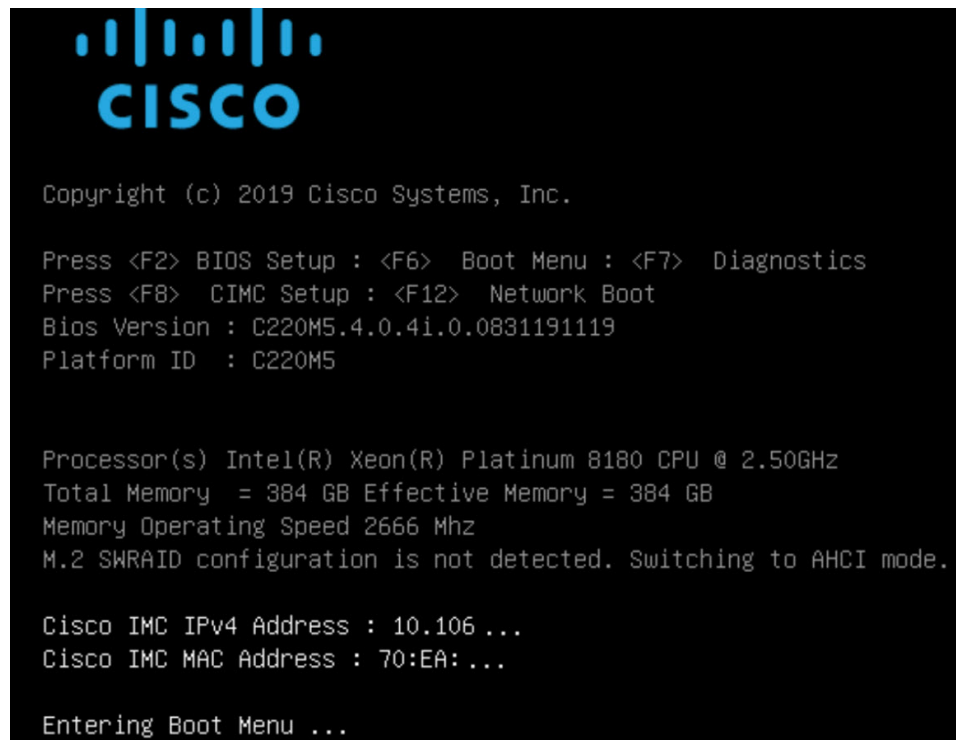
## Install Cisco DNA Center

### Before you begin

The secure boot-enabled Cisco DNA Center ISO must be available in the USB flash drive. Also, the ISO must either be connected to the Cisco DNA Center machine, or mapped via the Cisco IMC Mapped DVD option (recommended) or KVM Mapped DVD option (not recommended).

### Procedure

**Step 1** Restart the machine, and while the BIOS is loading, press **F6** to enter the Boot Selection.



```

      |||||
      CISCO

Copyright (c) 2019 Cisco Systems, Inc.

Press <F2> BIOS Setup : <F6> Boot Menu : <F7> Diagnostics
Press <F8> CIMC Setup : <F12> Network Boot
Bios Version : C220M5.4.0.4i.0.0831191119
Platform ID : C220M5

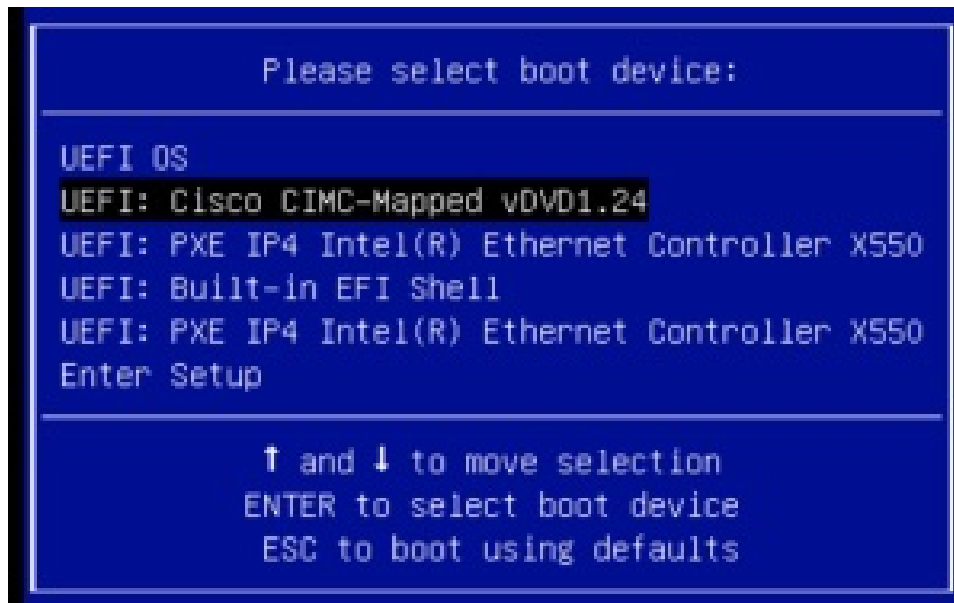
Processor(s) Intel(R) Xeon(R) Platinum 8180 CPU @ 2.50GHz
Total Memory = 384 GB Effective Memory = 384 GB
Memory Operating Speed 2666 Mhz
M.2 SWRAID configuration is not detected. Switching to AHCI mode.

Cisco IMC IPv4 Address : 10.106 ...
Cisco IMC MAC Address : 70:EA:...

Entering Boot Menu ...

```

**Step 2** Choose the ISO boot drive from the **Cisco IMC Mapped DVD** (Tested), **USB flash drive** (Not Tested), or **KVM Mapped DVD** (Not Tested).



The preceding example screenshot shows the chosen ISO boot drive as **Cisco IMC Mapped DVD (Tested)**.

- Step 3** Choose the **Maglev Installer** mode, which is the default in the System Boot menu, to proceed with the installation.



**Note** Currently, only the **Maglev Installer** mode is supported. If you press any key other than **Enter** in this menu, the menu freezes. Either press **Enter** or wait until it times out and proceed with the default option. There is an open bug for this problem, and Cisco is actively working on providing a solution. One workaround is to restart the machine and begin again from Step 1.

- Step 4** The Maglev Configuration wizard follows the same procedure as in a regular Cisco DNA Center installation. For more information about the Maglev Configuration wizard, see the [Cisco DNA Center Installation Guide](#).



- Note**
- In the **Maglev Installer** mode, first complete the configuration. Then, the system files start copying from the ISO to the HDD. Installation time depends on the USB flash drive speed or Cisco IMC Mapped DVD network speed. Expect a minimum of 3 to 4 hours for the installation to complete. Installation is completed in two stages. Stage one is copying files, which usually takes a period of time and depends on the speed between the ISO and Cisco DNA Center machine. Stage two is post-reboot, which usually takes approximately 45 minutes.
  - In a few machines, such as the Cisco UCS C220 M5 and Cisco (GEN 2) 44 Core, there is a chance of the boot order being altered. If you are using the same screen to start a cluster, unmap the HTTP/NFS mapping if it was done by HTTP or NFS. If it was completed by the USB flash drive, either remove the USB flash drive or disable it. Then, restart the machine. Now, the UEFI OS (HDD) is selected, and the post-installation (also called the post-reboot) continues. **Maintain these settings at all times.**

## Verify That the ISO Image Supports EFI Boot

### Procedure

**Step 1** Enter the following commands to verify that the ISO image supports EFI boot:

```
sudo bash
lodev=$(losetup --show -f uber_ISO_FILE.iso)
echo $lodev
parted $lodev print
losetup -d $lodev
```

**Step 2** In the output for the **parted** command, locate the EFI boot partition. For example:

```
Model: Loopback device (loopback)
Disk /dev/loop9: 22.2GB
Sector size (logical/physical): 512B/512B
```

```

Partition Table: gpt
Disk Flags:

Number  Start   End     Size   File system  Name              Flags
  1      32.8kB  346kB   313kB                Gap0              hidden, msftdata
  2      346kB   135MB   134MB   fat16         EFI boot partition boot, hidden, esp
  3      135MB   22.2GB  22.1GB   hfs+          Gap1              hidden, msftdata
    
```

## Considerations When Burning an ISO to a USB Flash Drive

Because secure boot recognizes only VFAT/FAT16 partitions, the USB flash drive must be VFAT formatted. Use an ISO writing tool, such as Etcher (<https://www.balena.io/etcher/>), to flash the ISO to the USB flash drive. Confirm that the ISO is secure UEFI bootable; see [Verify That the ISO Image Supports EFI Boot, on page 13](#).

Burning an ISO to a new USB flash drive involves the following steps:

1. Download the secure boot-enabled ISO from [cisco.com](http://cisco.com).
2. The USB flash drive must be at least 64 GB. (The ISO itself is at least 33 GB.)
3. Format the USB flash drive with "MS-DOS (FAT)" using the Mac "Disk Utility."
4. Use Etcher to burn the secure boot-enabled ISO to the USB flash drive. See "Prepare the Appliance for Configuration" in the [Cisco DNA Center Installation Guide](#).
5. The Cisco DNA Center appliance detects the ISO on the USB flash drive, whose Cisco IMC is enabled with secure boot.



## Verify the Disk UEFI Secure Boot

After installation, the **fat16** partition contains the **esp** flag, as follows:

```

$ sudo parted /dev/sda print

Disk /dev/sda: 215GB
    
```

```

Sector size (logical/physical): 512B/512B
Partition Table: gpt
Disk Flags:

Number  Start   End     Size    File system  Name      Flags
  1      1049kB 2097kB 1049kB             primary  bios_grub
  2      2097kB 51.2GB 51.2GB  ext4         primary
  3      51.2GB 51.5GB 251MB  fat16        primary  boot, esp
  4      51.5GB 215GB 163GB  ext4         primary

```

The output of **mount | grep efivarfs** shows the efivarfs mounted.

## Verify the Extensible Firmware Interface Image Signature

Cisco DNA Center images are signed using the SHA-256 hash algorithm. The signature scheme is PKCS7, signed with the RSA-2048 key.

### Procedure

**Step 1** After the system boots in secure boot, enter the following commands:

- **bootctl status:** Displays the UEFI secure boot information, which also includes the EFI image used for booting.
- **mokutil --db:** Lists the secure boot certificate, which is used to verify the signature on the EFI boot images.
- **mount | grep /boot/efi:** Lists the EFI partition that contains the EFI boot images.
- **mount | grep efivarfs:** Lists the EFI variable file system (efivarfs).

A disk that is booted by secure boot contains the following sample EFI boot images:

```

/boot/efi/EFI/BOOT/BOOTX64.EFI
/boot/efi/linux/dnac-1.7-5.4.0-73-generic.efi
/boot/efi/linux/dnac_rescue-1.7-5.4.0-73-generic.efi

```

**Step 2** To verify the EFI image signature, enter the following commands:

- **mokutil --sb-state:** Indicates whether or not secure boot is enabled.
- **mokutil --export --db:** Exports the DB certificate as the file `DB-0001.der`.
- **openssl x509 -in DB-0001.der -inform DER -out db.pem -outform PEM:** Converts the DER certificate to PEM format.
- **sbverify --cert db.pem /boot/efi/EFI/BOOT/BOOTX64.EFI:** Verifies the signature. If the signature is valid, the command output returns **Signature verification OK**.

- **osslsigncode verify /boot/efi/EFI/BOOT/BOOTX64.EFI**: Verifies the signature if the `osslsigncode` package is installed in the system.

```
$ mokutil --export --db

[Fri Aug 20 19:16:47 UTC] maglev@192.192.192
$ ls -lrt
total 12
-rw-rw-r-- 1 maglev maglev 180 Aug 18 16:02 as.txt
-rw-rw-r-- 1 maglev maglev 237 Aug 18 16:02 pe.txt
-rw----- 1 maglev maglev 1029 Aug 20 19:16 DB-0001.der

[Fri Aug 20 19:17:01 UTC] maglev@192.192.192.
$ openssl x509 -in DB-0001.der -inform DER -out db.pem -outform PEM

[Fri Aug 20 19:17:07 UTC] maglev@192.192.192.
$ ls -lrt
total 16
-rw-rw-r-- 1 maglev maglev 180 Aug 18 16:02 as.txt
-rw-rw-r-- 1 maglev maglev 237 Aug 18 16:02 pe.txt
-rw----- 1 maglev maglev 1029 Aug 20 19:16 DB-0001.der
-rw----- 1 maglev maglev 1448 Aug 20 19:17 db.pem

[Fri Aug 20 19:17:27 UTC] maglev@192.192.192.
$ sbverify --cert db.pem /boot/efi/EFI/BOOT/BOOTX64.EFI
warning: data remaining[73592 vs 82496]: gaps between PE/COFF sections?
Signature verification OK
```



---

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2021 Cisco Systems, Inc. All rights reserved.