Revised: September 18, 2025

Enable Secure Boot for Cisco Catalyst Center

Secure boot

Secure boot helps you to ensure that Cisco hardware platforms run authentic and unmodified code. Secure boot establishes a root of trust to prevent your network devices from running unauthorized or malicious software.

The root of trust starts with the firmware as it can't be modified. The Cisco Integrated Management Controller (Cisco IMC) and BIOS firmware include the Unified Extensible Firmware Interface (UEFI) secure boot certificates. These certificates are organized in a hierarchy as defined by the UEFI specification. This hierarchy can't be modified after it's loaded on the system.

Hierarchy

This hierarchy contains certificates specific to Cisco, and the certificate private keys are securely maintained offline in the Cisco software image management engine:

PK → KEK → DB

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

Boot order

During the Catalyst Center UCS system boot, the firmware validates itself and then activates the UEFI key hierarchy for the Catalyst Center platform based on the product ID (PID).

After secure boot is activated, the system can boot only the software that is signed by the UEFI secure boot Catalyst Center certificate. To successfully boot from a CD-ROM, USB flash drive, or hard disk, ensure that you have the correct Catalyst Center signature. After secure boot is enabled, it can't be disabled in the Cisco IMC and BIOS.

Requirements

This table lists the secure boot requirements.

Secure boot requirement	Description
Hardware	
Appliance	DN2-HW-APL DN2-HW-APL-L DN2-HW-APL-XL
Firmware	
UCS firmware	4.0(4h)
Firmware for C220 (DN2-HW-APL, DN2-HW-APL-L)	https://software.cisco.com/download/home/286318809/type/283850974/release/4.0(4h)

Secure boot requirement	Description
Firmware for C480 (DN2-HW-APL-XL)	https://software.cisco.com/download/home/286318818/type/283850974/release/4.0(4h)
BIOS	
BIOS for C220 (DN2-HW-APL, DN2-HW-APL-L)	http://10.106.0.171/C220M5-BIOS-4.0.4i_DNAC.cap
BIOS for C480 (DN2-HW-APL-XL)	http://10.106.0.171/C480M5-BIOS-4.0.4h_DNAC.cap

Install the Cisco IMC firmware

Step 1 Extract the firmware installation files:

a) Download the Cisco Host Upgrade Utility ISO file from cisco.com.

b) Extract the firmware installation files from the firmware for C220 and C480.

Step 2 Log in to the Cisco IMC GUI with admin privileges.

Step 3 Click the **Navigation** pane and choose **Admin**.

Step 4 From the **Admin** drop-down list, choose **Firmware Management**.

Step 5 In the **Firmware Management** dialog box, check the **BMC** check box, and click **Update**.

Step 6 In the **Update Firmware** dialog box, click **Install BMC Firmware through Browser Client**.

Step 7 Choose the file that you want to install:

a) Click **Browse**.

b) In the **Choose File** dialog box, navigate to and choose the .bin file that you want to install.

Step 8 In the **Update Firmware** dialog box, click **Install Firmware**.

Activate the Cisco IMC firmware

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**.

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 that you want to activate, and then click **Activate Firmware**.

After you click **Activate Firmware**, the Cisco IMC shuts down and reboots. The reboot process can take up to 15 minutes.

Install the Cisco IMC BIOS

Step 1 Download the BIOS for C220 and C480.

Step 2 Log in to the Cisco IMC GUI with admin privileges.

Step 3 Click the **Navigation** pane and choose **Admin**.

Step 4 From the **Admin** drop-down list, choose **Firmware Management**.

Step 5 In the **Firmware Management** dialog box, check the **BIOS** check box and click **Update**.

Step 6 In the **Update Firmware** dialog box, click **Install BIOS Firmware through Browser Client**.

Step 7 Choose the file that you want to install:

a) Click **Browse**.

b) In the **Choose File** dialog box, navigate to and choose the .cap file that you want to install.

Step 8 In the **Update Firmware** dialog box, click **Install Firmware**.

Activate the Cisco IMC BIOS

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**.

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 click **Activate Firmware**.

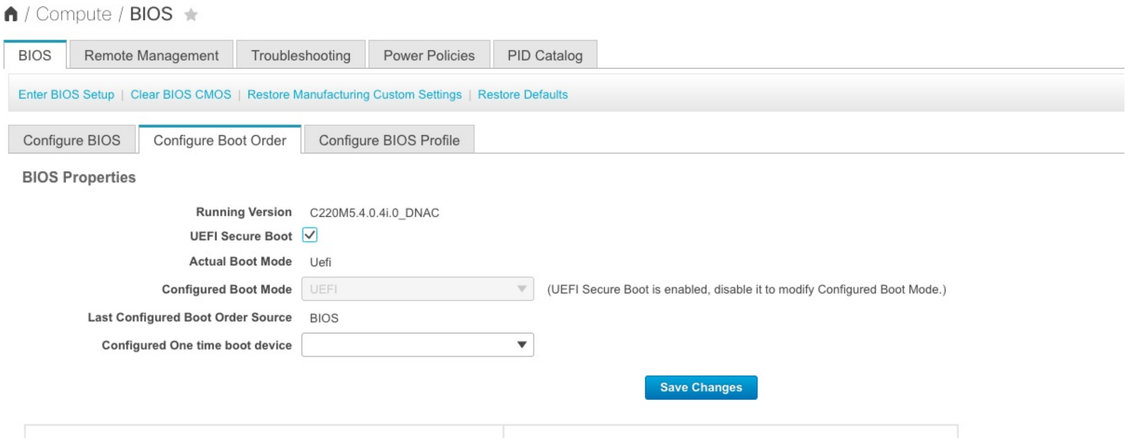
Enable the UEFI secure boot mode

Step 1 Log in to the Cisco IMC GUI with admin privileges.

Step 2 Click the **Navigation** pane and choose **Compute** > **BIOS**.

Step 3 In the **BIOS** tab, click the **Configure Boot Order** tab.

Step 4 Check the **UEFI Secure Boot** check box and click **Save Changes**.



BIOS Properties

Running Version: C220M5.4.0.4i.0_DNAC

UEFI Secure Boot: ☑

Actual Boot Mode: Uefi

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

Last Configured Boot Order Source: BIOS

Configured One time boot device:

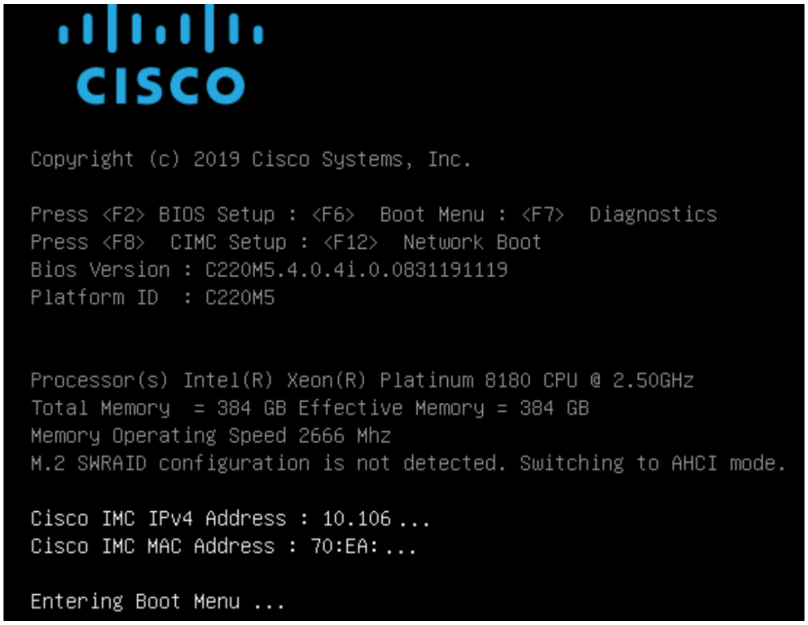
The machine reboots.

Configure the boot order

Configure the first EFI boot order option to the Hard Disk Drive (HDD). Based on the mode of installation, the second boot order option can be:

- Cisco IMC-mapped DVD,
- KVM-mapped DVD, or
- USB flash drive.

Step 1 Restart the machine and while BIOS is loading, press **F2** to enter the BIOS setup.



```
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 ...
```

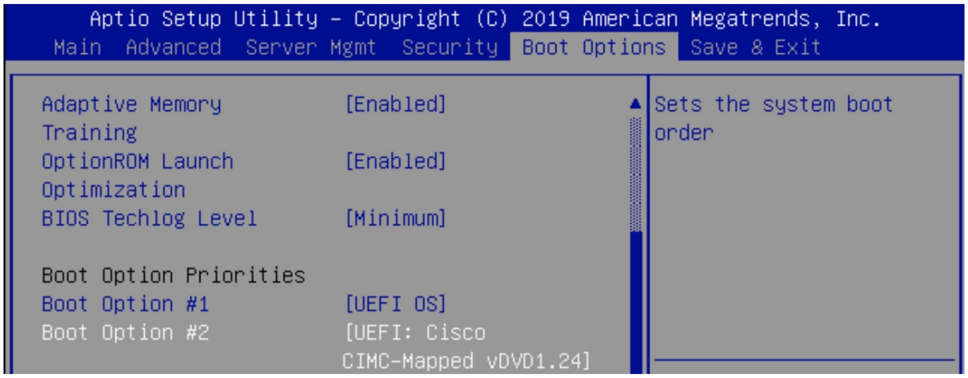
Step 2 In the Navigation pane, click the **Boot Options** tab.

Step 3 From the **Boot Options** tab, scroll down to the **Boot Option Priorities** area.

Step 4 In the **Boot Option Priorities** area, set the **Boot Option #1** field to **UEFI OS** (the HDD).

Step 5 Set the **Boot Option #2** field to one of these options:

- **Cisco IMC Mapped DVD** (tested)
- **USB flash drive** (not tested)
- **KVM Mapped DVD** (not tested)

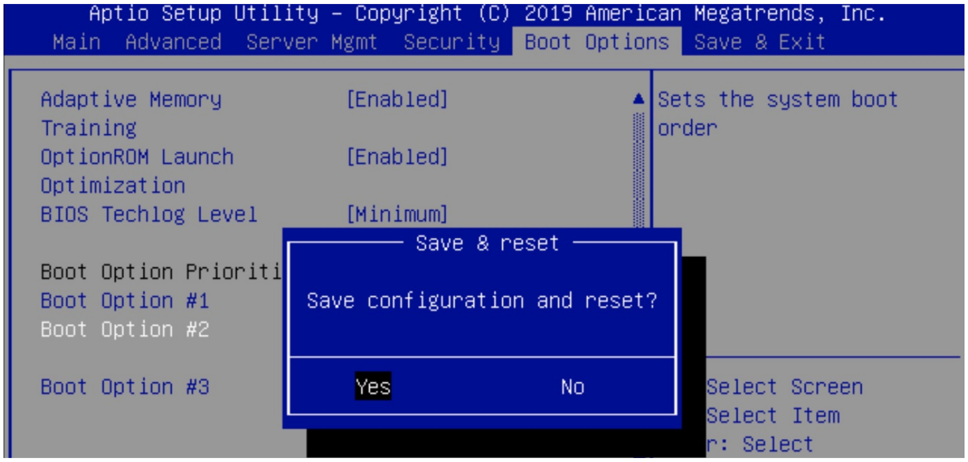


```
    Aptio Setup Utility – Copyright (C) 2019 American Megatrends, Inc.
  Main  Advanced  Server Mgmt  Security  Boot Options  Save & Exit

  Adaptive Memory             [Enabled]              Sets the system boot
  Training                                           order
  OptionROM Launch            [Enabled]
  Optimization
  BIOS Techlog Level          [Minimum]

  Boot Option Priorities
  Boot Option #1              [UEFI OS]
  Boot Option #2              [UEFI: Cisco
                              CIMC-Mapped vDVD1.24]
```

In this example figure, **Boot Option #2** is set to **Cisco IMC Mapped DVD**.

Note Before you set the boot order, map the secure boot-enabled ISO. Without mapping, these options are unavailable. This mapping is also needed for **USB flash drive** to view it as an option.

Step 6 Press **F10** and save the configuration.



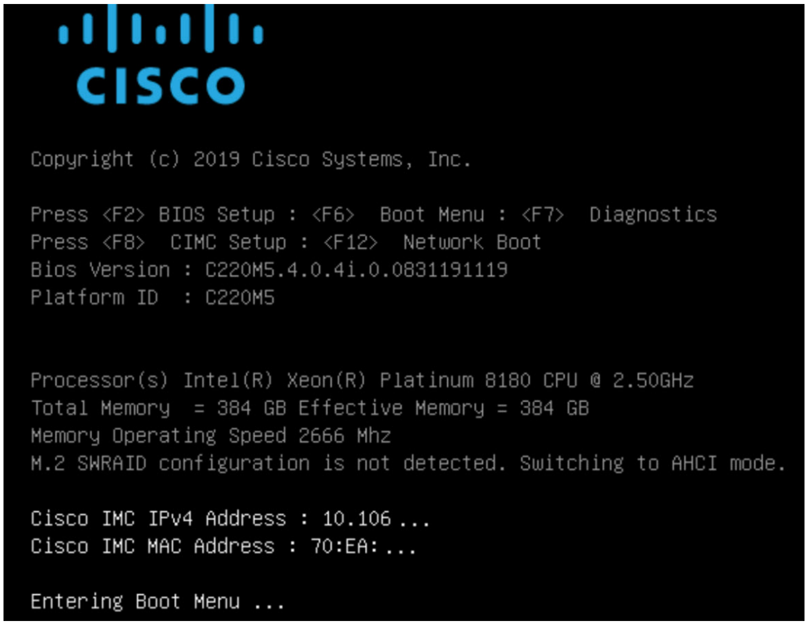
```
   Aptio Setup Utility – Copyright (C) 2019 American Megatrends, Inc.
 Main  Advanced  Server Mgmt  Security  Boot Options  Save & Exit

 Adaptive Memory           [Enabled]          ▲ Sets the system boot
 Training                                       order
 OptionROM Launch          [Enabled]
 Optimization
 BIOS Techlog Level        [Minimum]
                      ─────── Save & reset ───────
 Boot Option Prioriti
 Boot Option #1        Save configuration and reset?
 Boot Option #2

 Boot Option #3           Yes              No        Select Screen
                                                     Select Item
                                                     r: Select
```

Install Catalyst Center

Step 1 Ensure that the:

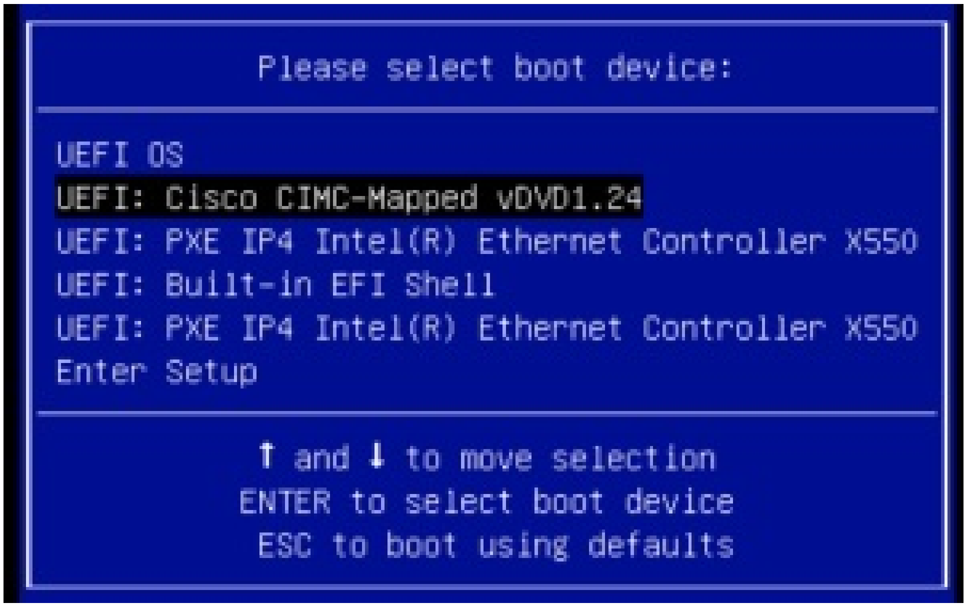
- Secure boot-enabled Catalyst Center ISO is available in the USB flash drive.
- ISO is either connected to the Catalyst Center appliance, or mapped through the Cisco IMC Mapped DVD option or KVM Mapped DVD option. We recommend that you use the Cisco IMC Mapped DVD option.

Step 2 Restart the appliance and while the BIOS is loading, press **F6** to enter the Boot Selection.



```
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 ...
```

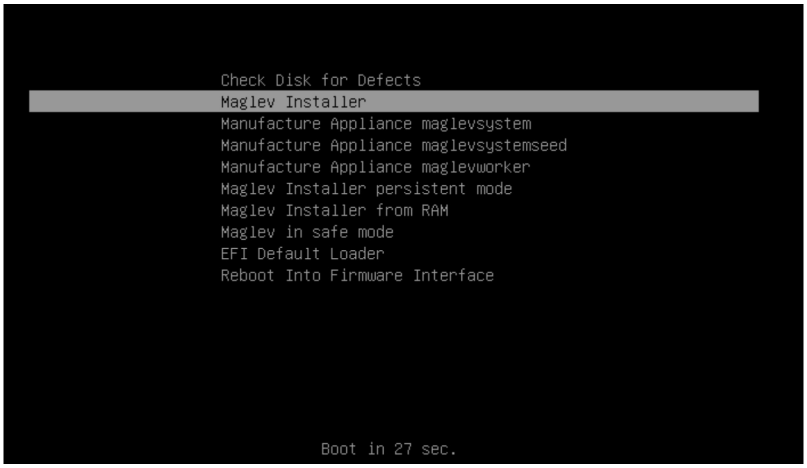
Step 3 Choose the ISO boot drive from the **Cisco IMC Mapped DVD** (tested), **USB flash drive** (not tested), or **KVM Mapped DVD** (not tested).



```
Please select boot device:

UEFI OS
UEFI: Cisco CIMC-Mapped vDVD1.24
UEFI: PXE IP4 Intel(R) Ethernet Controller X550
UEFI: Built-in EFI Shell
UEFI: PXE IP4 Intel(R) Ethernet Controller X550
Enter Setup

↑ and ↓ to move selection
ENTER to select boot device
ESC to boot using defaults
```

In this example image, the chosen ISO boot drive is **Cisco IMC Mapped DVD** (tested).

Step 4 Choose the **Maglev Installer** mode, which is the default in the System Boot menu, to proceed with the installation.

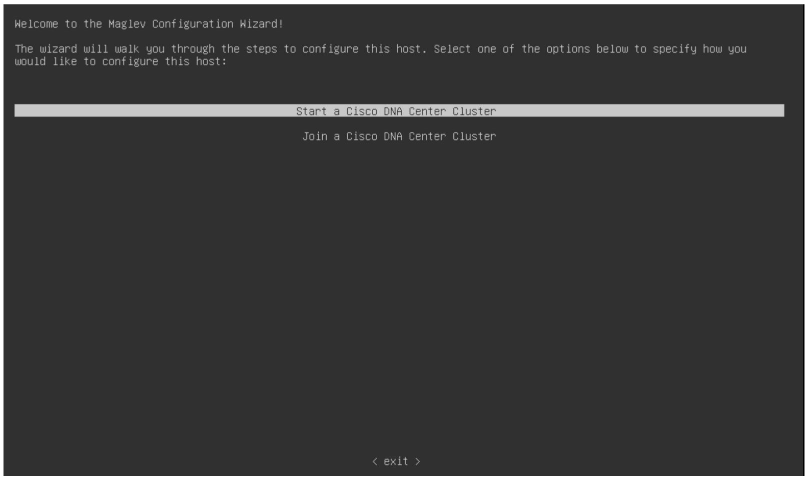


```
Check Disk for Defects
Maglev Installer
Manufacture Appliance maglevsystem
Manufacture Appliance maglevsystemseed
Manufacture Appliance maglevworker
Maglev Installer persistent mode
Maglev Installer from RAM
Maglev in safe mode
EFI Default Loader
Reboot Into Firmware Interface

Boot in 27 sec.
```

Note Currently, only the **Maglev Installer** mode is supported. Pressing any key other than **Enter** in this menu, causes the menu to freeze. Either press **Enter** or wait until it times out and proceed with the default option. As a workaround, restart the appliance and begin again from Step 1.

Step 5 Use the same procedure in the Maglev Configuration wizard as in a regular Catalyst Center installation.

For more information about the Maglev Configuration wizard, see the *Cisco Catalyst Center Installation Guide*.


Welcome to the Maglev Configuration Wizard!

The wizard will walk you through the steps to configure this host. Select one of the options below to specify how you would like to configure this host:

Start a Cisco DNA Center Cluster
Join a Cisco DNA Center Cluster
< exit >

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 speed of the USB flash drive or the network speed of the Cisco IMC Mapped DVD. The installation takes at least 3 to 4 hours to complete.

  The installation comprises two stages:

  - Stage one is copying files, which usually takes a period of time and depends on the speed between the ISO and Catalyst Center appliance.
  - Stage two is postreboot, which usually takes approximately 45 minutes.

- In some appliances, 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 postinstallation (also called the postreboot) continues. *Maintain these settings at all times.*

Verify secure boot

This section explains how to:

- verify that the ISO image supports EFI boot,
- verify the disk UEFI secure boot, and
- verify the extensible firmware interface image signature.

Verify that the ISO image supports EFI boot

Step 1 Use these commands to verify that the ISO image that you use to install Catalyst Center 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

Secure boot recognizes only VFAT/FAT16 partitions. Therefore, you must format the USB flash drive as VFAT. 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 7.

To burn an ISO to a new USB flash drive, complete these steps:

1. Download the secure boot-compatible ISO from cisco.com.

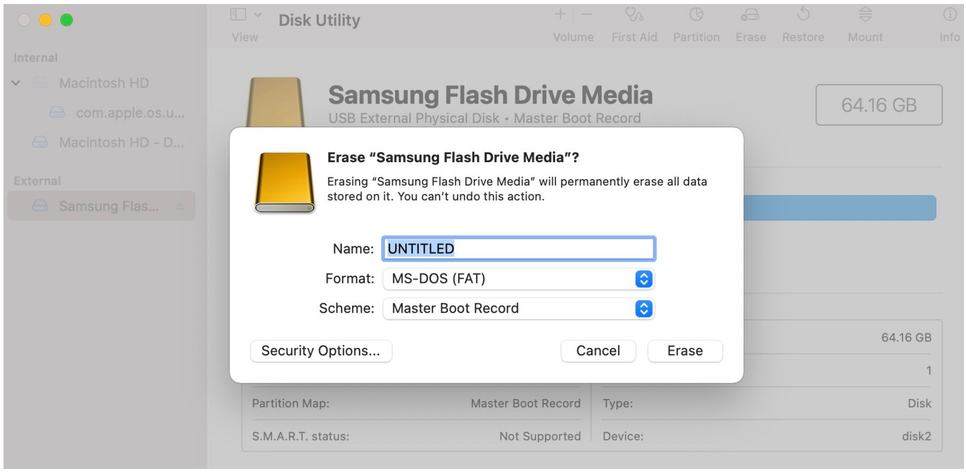
   Use a USB flash drive with at least 64 GB, as the ISO requires at least 33 GB.

2. Format the USB flash drive as "MS-DOS (FAT)" using the Mac "Disk Utility".

3. Use Etcher to burn the secure boot-compatible ISO to the USB flash drive.

   For more information, see "Prepare the Appliance for Configuration" in the *Cisco Catalyst Center Installation Guide*.

   The Catalyst Center appliance, which has secure boot enabled in its Cisco IMC, detects the ISO on the USB flash drive.



Erase "Samsung Flash Drive Media"?

Erasing "Samsung Flash Drive Media" will permanently erase all data stored on it. You can't undo this action.

Name: UNTITLED

Format: MS-DOS (FAT)

Scheme: Master Boot Record

64.16 GB

1

Partition Map: Master Boot Record

Type: Disk

S.M.A.R.T. status: Not Supported

Device: disk2

Verify the disk UEFI secure boot

After installation, the **fat16** partition contains the **esp** flag.

```
$ 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 efivars** shows the efivarfs mounted.

Verify the extensible firmware interface image signature

Catalyst Center images are signed using the SHA-256 hash algorithm. The signature uses the PKCS7 scheme with the RSA-2048 key.

Step 1 After the system boots in secure boot, enter these 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, which contains the EFI boot images.
- **mount | grep efivarfs**: lists the EFI variable file system (efivarfs).

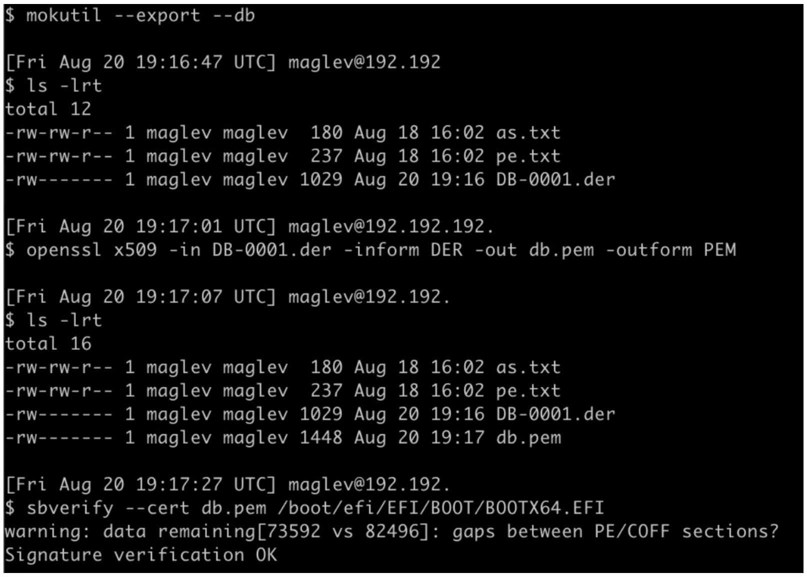
A disk that is booted by secure boot contains these sample EFI boot images:

```
/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 these commands:

- **mokutil --sb-state**: shows whether 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
$ 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.
$ 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.
$ sbverify --cert db.pem /boot/efi/EFI/BOOT/BOOTX64.EFI
warning: data remaining[73592 vs 82496]: gaps between PE/COFF sections?
Signature verification OK
```