Managing the Server

This chapter includes the following sections:

- Server Boot Order, on page 1
- Configuring Power Policies, on page 15
- Configuring DIMM Blocklisting, on page 26
- Configuring BIOS Settings, on page 27
- BIOS Profiles, on page 29
- Secure Boot Certificate Management, on page 33
- Persistent Memory Modules, on page 37

Server Boot Order

Using Cisco IMC, you can configure the order in which the server attempts to boot from available boot device types. In the legacy boot order configuration, Cisco IMC allows you to reorder the device types but not the devices within the device types. With the precision boot order configuration, you can have a linear ordering of the devices. In the web UI or CLI you can change the boot order and boot mode, add multiple devices under each device types, rearrange the boot order, set parameters for each device type.

When you change the boot order configuration, Cisco IMC sends the configured boot order to BIOS the next time that server is rebooted. To implement the new boot order, reboot the server after you make the configuration change. The new boot order takes effect on any subsequent reboot. The configured boot order remains until the configuration is changed again in Cisco IMC or in the BIOS setup.

Note The actual boot order differs from the configured boot order if either of the following conditions occur:

- BIOS encounters issues while trying to boot using the configured boot order.
- A user changes the boot order directly through BIOS.
- BIOS appends devices that are seen by the host but are not configured from the user.

Note When you create a new policy using the configure boot order feature, BIOS tries to map this new policy to the devices in the system. It displays the actual device name and the policy name to which it is mapped in the **Actual Boot Order** area. If BIOS cannot map any device to a particular policy in Cisco IMC, the actual device name is stated as **NonPolicyTarget** in the **Actual Boot Order** area.

Note During Cisco IMC 2.0(x) upgrade, the legacy boot order is migrated to the precision boot order. The previous boot order configuration is erased and all device types configured before updating to 2.0 version are converted to corresponding precision boot device types and some dummy devices are created for the same device types. you can view these devices in the **Configured Boot Order** area in the web UI. To view these devices in the CLI, enter **show boot-device** command. During this the server's actual boot order is retained and it can be viewed under actual boot order option in web UI and CLI.

When you downgrade Cisco IMC prior to 2.0(x) verison the server's last legacy boot order is retained, and the same can be viewed under **Actual Boot Order** area. For example:

- If you configured the server in a legacy boot order in 2.0(x) version, upon downgrade a legacy boot order configuration is retained.
- If you configured the server in a precision boot order in 2.0(x), upon downgrade the last configured legacy boot order is retained.

Important

- S3260 M4 servers support both Legacy and Precision Boot order configuration through Cisco IMC GUI and CLI interfaces.

  For S3260 M5 servers, you must manually configure the intended boot order through Cisco IMC GUI or CLI interfaces.
- Boot order configuration prior to 2.0(x) is referred as legacy boot order. If your running version is 2.0(x), then you cannot configure legacy boot order through web UI, but you can configure through CLI and XML API. In the CLI, you can configure it by using **set boot-order HDD,PXE** command. Even though, you can configure legacy boot order through CLI or XML API, in the web UI this configured boot order is not displayed.
- Legacy and precision boot order features are mutually exclusive. You can configure either legacy or precision boot order. If you configure legacy boot order, it disables all the precision boot devices configured. If you configure precision boot order, then it erases legacy boot order configuration.

Configuring the Precision Boot Order

Before you begin

You must log in as a user with admin privileges to configure server the boot order.

Step 1 In the **Navigation** pane, click the **Compute** menu.

Step 2 In the **Compute** menu, select a server.

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

Step 4 In the **BIOS Properties** area, click **Configure Boot Order** at the bottom of the page.

Configure Boot Order dialog box is displayed.

Step 5 In the **Configure Boot Order** dialog box, update the following properties:

Basic Tab

Name	Description
Device Types table	The server boot options. You can select one or more of the following: • **HDD**—Hard disk drive • **FDD**—Floppy disk drive • **CDROM**—Bootable CD-ROM or DVD • **PXE**—PXE boot • **EFI**—Extensible Firmware Interface
>>	Moves the selected device type to the **Boot Order** table.
<<	Removes the selected device type from the **Boot Order** table.
Boot Order table	Displays the device types from which this server can boot, in the order in which the boot will be attempted.
Down	Moves the selected device type to a higher priority in the **Boot Order** table.
Up	Moves the selected device type to a higher priority in the **Boot Order** table.
Save Changes	Click this button to save the changes made.
Close button	Closes the dialog box without saving any changes and the existing configuration is applied when the server is rebooted.

Advanced Tab

The following list of links are displayed under **Add Boot Device** pane.

- **Add Local HDD**
- **Add PXE Boot**
- **Add SAN Boot**
- **Add iSCSI Boot**
- **Add USB**
- **Add Virtual Media**
- **Add PCHStorage**
- **Add UEFISHELL**

- **Add NVME**
- **Add Local CDD**
- **Add HTTP Boot**

In the **Advanced Boot Order Configuration** pane, the devices are displayed after they are added. You can perform the following actions by selecting the appropriate buttons:

- **Enable or Disable**
- **Modify**
- **Delete**
- **Clone**
- **Re-Apply**
- **Move Up**
- **Move Down**

Step 6 Click **Save Changes**.

Additional device types might be appended to the actual boot order, depending on what devices you have connected to your server.

What to do next

Reboot the server to boot with your new boot order.

Managing a Boot Device

Before you begin

You must log in as a user with admin privileges to add device type to the server boot order.

Step 1 In the **Navigation** pane, click the **Compute** menu.

Step 2 In the **Compute** menu, select a server.

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

Step 4 In the **BIOS Properties** area, click **Configure Boot Order**.

A dialog box with boot order instructions appears.

Step 5 In the **Configure Boot Order** dialog box, from the **Add Boot Device** table, choose the device that you want add to the boot order.

To add the local HDD device, click **Add Local HDD**, and update the following parameters:

Name	Description
Name field	The name of the device. **Note** Once created, you cannot rename the device.
State drop-down list	The visibility of the device by BIOS. This can be one of the following: • **Enabled**—The device is visible to BIOS in a boot order configuration. • **Disabled**—The device is not visible to BIOS in a boot configuration.
Order field	The order of the device in the available list of devices. Enter between 1 and n, where n is the number of devices.
Slot field	The slot in which the device is installed. Enter the slot number from the available range.
Add Device button	Adds the device to the **Boot Order** table.
Cancel button	Closes the dialog box without saving any changes made while the dialog box was open.

To add the PXE device, click **Add PXE**, and update the following parameters:

Name	Description
Name field	The name of the device. This name cannot be changed after the device has been created.
State drop-down list	The visibility of the device by BIOS. The state can be one of the following: • **Enabled**—The device is visible to BIOS in a boot order configuration. • **Disabled**—The device is not visible to BIOS in a boot order configuration.
Order field	The order of the device in the available list of devices. Enter between 1 and n, where n is the number of devices.
Slot field	The slot in which the device is installed. Enter the slot number from the available range.
MAC Address	MAC address of the network ethernet interface. **Note** This option is available only on some C-Series servers.
Port field	The port of the slot in which the device is present. Enter a number between 0 and 255.

To add the SAN boot device, click **Add SAN Boot**, and update the following parameters:

Name	Description
Name field	The name of the device. This name cannot be changed after the device has been created.
State drop-down list	The visibility of the device by BIOS. The state can be one of the following: • **Enabled**—The device is visible to BIOS in a boot order configuration. • **Disabled**—The device is not visible to BIOS in a boot order configuration.
Order field	The order of the device in the available list of devices. Enter between 1 and n, where n is the number of devices.
Slot field	The slot in which the device is installed. Enter the slot number from the available range.
LUN field	Logical unit in a slot where the device is present. Enter a number between 0 and 255.
Save Changes button	Adds the device to the **Boot Order** table, and saves the changes.
Cancel button	Closes the dialog box without saving any changes made while the dialog box was open.

To add the iSCSI boot device, click **Add iSCSI Boot**, and update the following parameters:

Name	Description
Name field	The name of the device. This name cannot be changed after the device has been created.
State drop-down list	The visibility of the device by BIOS. The state can be one of the following: • **Enabled**—The device is visible to BIOS in a boot order configuration. • **Disabled**—The device is not visible to BIOS in a boot order configuration.
Order field	The order of the device in the available list of devices. Enter between 1 and n, where n is the number of devices.
Slot field	The slot in which the device is installed. Enter the slot number from the available range.
Port field	The port of the slot in which the device is present. Enter a number between 0 and 255. **Note** In case of a VIC card, use a vNIC instance instead of the port number.
Save Changes button	Adds the device to the **Boot Order** table, and saves the changes.

Name	Description
Cancel button	Closes the dialog box without saving any changes made while the dialog box was open.

To add the SD card, click **Add SD Card**, and update the following parameters:

Note This option is available only on some UCS C-Series servers.

Name	Description
Name field	The name of the device. This name cannot be changed after the device has been created.
State drop-down list	The visibility of the device by BIOS. This can be one of the following: • **Enabled**—The device is visible to BIOS in a boot order configuration. • **Disabled**—The device is not visible to BIOS in a boot configuration.
Order field	The order of the device in the available list of devices. Enter between 1 and n, where n is the number of devices.
Save Changes button	Adds the device to the **Boot Order** table.
Cancel button	Closes the dialog box without saving any changes made while the dialog box was open.

To add the USB device, click **Add USB**, and update the following parameters:

Name	Description
Name field	The name of the device. This name cannot be changed after the device has been created.
Sub Type drop-down list	The subdevice type under a certain device type. This can be one of the following: • **CD** • **FDD** • **HDD**
State drop-down list	The visibility of the device by BIOS. This can be one of the following: • **Enabled**—The device is visible to BIOS in a boot order configuration. • **Disabled**—The device is not visible to BIOS in a boot order configuration.
Order field	The order of the device in the available list of devices. Enter between 1 and n, where n is the number of devices.
Save Changes button	Adds the device to the **Boot Order** table.

Name	Description
Cancel button	Closes the dialog box without saving any changes made while the dialog box was open.

To add the virtual media, click **Virtual Media**, and update the following parameters:

Name	Description
Name field	The name of the device. This name cannot be changed after the device has been created.
Sub Type drop-down list	The subdevice type under a certain device type. This could be any one of the following: • **KVM Mapped DVD** • **Cisco IMC Mapped DVD** • **KVM Mapped HDD** • **Cisco IMC Mapped HDD** • **KVM Mapped FDD**
State drop-down list	The visibility of the device by BIOS. The state can be one of the following: • **Enabled**—The device is visible to BIOS in a boot order configuration. • **Disabled**—The device is not visible to BIOS in a boot order configuration.
Order field	The order of the device in the available list of devices. Enter between 1 and n, where n is the number of devices.
Save Changes button	Adds the device to the **Boot Order** table.
Cancel button	Closes the dialog box without saving any changes made while the dialog box was open.

To add the PCH storage device, click **PCH Storage**, and update the following parameters:

Name	Description
Name field	The name of the device. This name cannot be changed after the device has been created.
State drop-down list	The visibility of the device by BIOS. This can be one of the following: • **Enabled**—The device is visible to BIOS in a boot order configuration. • **Disabled**—The device is not visible to BIOS in a boot order configuration.
Order field	The order of the device in the available list of devices. Enter between 1 and n, where n is the number of devices.

Name	Description
LUN field	Logical unit in a slot where the device is present. • Enter a number between 0 and 255 • SATA in AHCI mode—Enter a value between 1 and 10 • SATA in SWRAID mode—Enter 0 for SATA , and enter 1 for SATA **Note** SATA mode is available only on some UCS C-Series servers.
Save Changes button	Adds the device to the **Boot Order** table.
Cancel button	Closes the dialog box without saving any changes made while the dialog box was open.

To add the UEFI shell device, click **Add UEFI Shell**, and update the following parameters:

Name	Description
Name field	The name of the device. This name cannot be changed after the device has been created.
State drop-down list	The visibility of the device by BIOS. The state can be one of the following: • **Enabled**—The device is visible to BIOS in a boot order configuration. • **Disabled**—The device is not visible to BIOS in a boot order configuration.
Order field	The order of the device in the available list of devices. Enter between 1 and n, where n is the number of devices.
Add Device button	Adds the device to the **Boot Order** table.
Cancel button	Closes the dialog box without saving any changes made while the dialog box was open.

To add the HTTP boot device device, click **Add HTTP Boot**, and update the following parameters:

Note The following OS (ISOs) are supported for HTTP Boot device:

- SLES 12.x
- RHEL 8.2
- ESX 6.5

The following OS (ISOs) are not supported for HTTP Boot device:

- Windows 2016
- Windows 2019

Name	Description
Name field	The name of the device. This name cannot be changed after the device has been created. You can enter between 1 and 30 characters, containing alphanumerics, - (hyphen) and _ (underscore). The name cannot begin with hyphen or underscore.
State drop-down list	The visibility of the device by BIOS. The state can be one of the following: • **Enabled**—The default option. The device is visible to BIOS in a boot order configuration. • **Disabled**—The device is not visible to BIOS in a boot order configuration.
Order field	The order of the device in the available list of devices. The default option is 1.
MAC Address field	MAC address of the network ethernet interface.
IP Type drop-down list	The type of IP. Select any one of the following options displayed in the drop-down list: • None • IPv4 • IPv6 The default value is None.
Slot field	The slot in which the device is installed. Enter the slot number from the available range. Enter the required value from the below list: • SIOC1 • SIOC2 • IOESLOT1 • IOESLOT2 • SBLOM1 • Any number between 1 and 255
Port field	The port of the slot in which the device is present. Enter a number between 0 and 255.

Name	Description
IP Config Type drop-down list	The type of IP configuration. The following options are displayed in the drop-down list: • **None** • **DHCP** • **Static** For **DHCP** IP configuration, the following fields are displayed, depending on the IP type that you have selected: • **MAC Address** • **IP Type** • **Slot** • **Port** For **Static** IP configuration, the following fields are displayed, depending on the IP type that you have selected: • **URI** • **IP Address** • **IPv4 Netmask** or **IPv6 Netmask** • **IPv4 Gateway** or **IPv6 Gateway** • **IPv4 Preferred DNS server** or **IPv6 Preferred DNS server**
URI field	The Uniform Resource Identifier HTTP server path location. You can enter between 1 and 255 characters.
Save Changes button	Saves the changes and adds the device to the **Boot Order** table.
Cancel button	Closes the dialog box without saving any changes made while the dialog box was open.

Overview to UEFI Secure Boot

You can use Unified Extensible Firmware Interface (UEFI) secure boot to ensure that all the EFI drivers, EFI applications, option ROM or operating systems prior to loading and execution are signed and verified for authenticity and integrity, before you load and execute the operating system. You can enable this option using either web UI or CLI. When you enable UEFI secure boot mode, the boot mode is set to UEFI mode and you cannot modify the configured boot mode until the UEFI boot mode is disabled.

Note If you enable UEFI secure boot on a nonsupported OS, on the next reboot, you cannot boot from that particular OS. If you try to boot from the previous OS, an error is reported and recorded the under system software event in the web UI. You must disable the UEFI secure boot option using Cisco IMC to boot from your previous OS.

Important Also, if you use an unsupported adapter, an error log event in Cisco IMC SEL is recorded. The error messages is displayed that says:

System Software event: Post sensor, System Firmware error. EFI Load Image Security Violation. [0x5302] was asserted .

UEFI secure boot is supported on the following components:

Components	Types
Supported OS	• Windows Server 2019 • Windows Server 2016 • ESX 6.7 • ESX 6.5 • ESXi 7.0 • ESXi 8.0 • Linux
QLogic PCI adapters	• 8362 dual port adapter • 2672 dual port adapter
Fusion-io	
LSI	• LSI MegaRAID SAS 9240-8i • LSI MegaRAID SAS 9220-8i • LSI MegaRAID SAS 9265CV-8i • LSI MegaRAID SAS 9285CV-8e • LSI MegaRAID SAS 9285CV-8e • LSI MegaRAID SAS 9266-8i • LSI SAS2008-8i mezz • LSI Nytro card • RAID controller for UCS Storage (SLOT-MEZZ) • Host Bus Adapter (HBA)

Enabling UEFI Secure Boot

Step 1 In the **Navigation** pane, click the **Compute** menu.

Step 2 In the **Compute** menu, select a server.

Step 3 In the work pane, click the **BIOS** tab.

Step 4 In the **BIOS Properties** area of the **Configure Boot Order** tab, check **UEFI Secure Boot** checkbox.

Note If checked, the boot mode is set to UEFI secure boot. You cannot modify the **Configure Boot Mode** until UEFI secure boot option is disabled.

Note In case of RFD (Reset Factory Default), you must re-enable UEFI Secure Boot.

If you enable UEFI secure boot on a nonsupported OS, on the next reboot, you cannot boot from that particular OS. If you try to boot from the previous OS, an error is reported and recorded under the system software event in the web UI. You must disable the UEFI secure boot option by using Cisco IMC to boot from your previous OS.

Step 5 Click **Save Changes**.

What to do next

Reboot the server to have your configuration boot mode settings take place.

Disabling UEFI Secure Boot

Step 1 In the **Navigation** pane, click the **Compute** menu.

Step 2 In the **Compute** menu, select a server.

Step 3 In the work pane, click the **BIOS** tab.

Step 4 In the **BIOS Properties** area, uncheck the **UEFI Secure Boot** check box.

Step 5 Click **Save Changes**.

What to do next

Reboot the server to have your configuration boot mode settings take place.

Viewing the Actual Server Boot Order

The actual server boot order is the boot order actually used by BIOS when the server last booted. The actual boot order can differ from the boot order configured in Cisco IMC.

Step 1 In the **Navigation** pane, click the **Compute** menu.

Step 2 In the **Compute** menu, select a server.

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

Step 4 In the **BIOS Properties** area, click **Configure Boot Order**.

This area displays the boot order devices configured through Cisco IMC as well as the actual boot order used by the server BIOS.

The **Configured Boot Devices** section displays the boot order (**Basic** or **Advanced**) configured through Cisco IMC. If this configuration changes, Cisco IMC sends this boot order to BIOS the next time that server boots. The Basic configuration allows you to specify only the device type. The Advanced configuration allows you to configure the device with specific parameters such as slot, port and LUN.

To change the configured boot order, or to restore the previously configured boot order, administrators can click the **Configure Boot Order** button. To have these changes take effect immediately, reboot the server. You can verify the new boot order by refreshing the **BIOS** tab.

Note This information is only sent to BIOS the next time the server boots. Cisco IMC does not send the boot order information to BIOS again until the configuration changes.

The **Actual Boot Devices** section displays the boot order actually used by BIOS when the server last booted. The actual boot order will differ from the configured boot order if either of the following conditions occur:

- The BIOS encounters issues while trying to boot using the configured boot order.
- A user changes the boot order directly through the BIOS. To override any manual changes, you can change the configured boot order through Cisco IMC and reboot the server.

Note When you create a new policy using the configured boot order, BIOS tries to map this new policy to the device or devices present in the system. It displays the actual device name and the policy name to which it is mapped under the **Actual Boot Order** area. If BIOS cannot map any device found to a particular policy in Cisco IMC, then the actual device name is stated as **NonPolicyTarget** under the **Actual Boot Order** area.

Configuring a Server to Boot With a One-Time Boot Device

You can configure a server to boot from a particular device only for the next server boot, without disrupting the currently configured boot order. Once the server boots from the one time boot device, all its future reboots occur from the previously configured boot order.

Before you begin

You must log in as a user with admin privileges to configure server the boot order.

Step 1 In the **Navigation** pane, click the **Compute** menu.

Step 2 In the **Compute** menu, select a server.

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

Step 4 In the **BIOS Properties** area, select an option from the **Configured One Time Boot Device** drop-down.

Note The host boots to the one time boot device even when configured with a disabled advanced boot device.

Creating a Server Asset Tag

Before you begin

You must log in with user or admin privileges to perform this task.

Step 1 In the **Navigation** pane, click the **Chassis** menu.

Step 2 In the **Chassis** menu, click **Summary**.

Step 3 In the **Chassis Properties** area, update the **Asset Tag** field.

Step 4 Click **Save Changes**.

Configuring Power Policies

Configuring the Power Restore Policy

The power restore policy determines how power is restored to the server after a chassis power loss.

Before you begin

You must log in with admin privileges to perform this task.

Step 1 In the **Navigation** pane, click the **Compute** menu.

Step 2 In the **Compute** menu, select a server.

Step 3 In the work pane, click the **Power Policies** tab.

Step 4 In the **Power Restore Policy** area, update the following fields:

Name	Description
Power Restore Policy drop-down list	The action to be taken when chassis power is restored after an unexpected power loss. This can be one of the following: • **Power Off**—The server remains off until it is manually restarted. • **Power On**—The server is allowed to boot up normally when power is restored. The server can restart immediately or, optionally, after a fixed or random delay. • **Restore Last State**—The server restarts and the system attempts to restore any processes that were running before power was lost.

Name	Description
Power Delay Type drop-down list	If the selected policy is **Power On**, the restart can be delayed with this option. This can be one of the following: • **fixed**—The server restarts after a fixed delay. • **random**—The server restarts after a random delay. **Note** This option is available only for some C-Series servers.
Power Delay Value field	If a fixed delay is selected, once chassis power is restored and the Cisco IMC has finished rebooting, the system waits for the specified number of seconds before restarting the server. Enter an integer between 0 and 240. **Note** This option is available only for some C-Series servers.

Step 5 Click **Save Changes**.

Power Characterization

The chassis power characterization range is calculated and derived from individual server node power characterization status, and from the power requirements of all the unmanageable components of the chassis.

This range varies for each configuration, so you need to run the power characterization every time a configuration changes.

To help you use the power characterization range appropriately for the different power profiles, the system represents the chassis' minimum power as auto profile minimum and custom profile minimum. However, custom power profile minimum is the actual minimum power requirement of the current chassis configuration. For more information see the section Run Power Characterization.

Running Power Characterization

Before you begin

You must log in with admin privileges to perform this task.

Step 1 In the **Navigation** pane, click the **Chassis** menu.

Step 2 In the **Chassis** menu, click **Power Management**.

Step 3 In the **Power Cap Configuration** tab, click the **Run Power Characterization** link.

A confirmation box appears that says the host is going to be either powered on or rebooted depending on the current power state. Review the message and click **OK** to close the dialog box.

You can verify the progress of the power characterization in the **Status** field. The status can be one of the following:

- **Not Run on One Server**— When the power characterization status is **Not Run** on any one server node.

- **Not Run**— When the power characterization status is **Not Run** on both the server nodes.
- **Failed on One Server**— When the power characterization status is **Failed** on any one server.
- **Completed Successfully**—When the power characterization status is **Completed Successfully** on both the server nodes.
- **Running**— When the power characterization status is **Running** on any one of the server nodes.
- **Failed**— When the power characterization status is **Failed** on both the server nodes.

After power characterization action is performed, the platform power limit range is populated under the **Recommended Power Cap** area as a minimum and maximum power in watts.

Power Profiles

Power capping determines how server power consumption is actively managed. When you enable power capping option, the system monitors power consumption and maintains the power below the allocated power limit. If the server cannot maintain the power limit or cannot bring the platform power back to the specified power limit within the correction time, power capping performs actions that you specify in the Action field under the Power Profile area.

You can configure multiple profiles with the following combinations: automatic and thermal profiles; and custom and thermal profiles. These profiles are configured by using either the web user interface, command line interface, or XML API. In the web UI, the profiles are listed under the Power Capping area. In the CLI, the profiles are configured when you enter the **power-cap-config** command. You can configure the following power profiles for power capping feature:

- Automatic Power Limiting Profile
- Custom Power Limiting Profile
- Thermal Power Limiting Profile

Automatic power limiting profile sets the power limit of the individual server boards based on server priority selected by you, or as detected by the system, based on the server utilization sensor (which is known as manual or dynamic priority selection). The limiting values are calculated within the manageable chassis power budget and applied to the individual server, and the priority server is allocated with its maximum power limiting value, while the other server with the remaining of the manageable power budget. Power limiting occurs at each server board platform level that affects the overall chassis power consumption.

Custom power limiting profile allows you to set an individual server board’s power limit from the Web UI or command line interface within the chassis power budget. In this scenario you can specify an individual server power limit.

Thermal power profile allows you to enable thermal failure power capping, which means you can set a specific platform temperature threshold and it sets P (min-x) as the power limit to be applied on the temperature threshold.

Resetting Power Profiles to Default

Before you begin

You must log in with admin privileges to perform this task.

Step 1 In the **Navigation** pane, click the **Chassis** menu.

Step 2 In the **Chassis** menu, click **Power Management**.

Step 3 In the **Power Cap Configuration** tab, click the **Reset Profiles to Default** link.

Note This action resets all the power profile settings to factory default values and disables power capping.

Configuring the Power Capping Settings

You can enable power characterization only on some Cisco UCS C-Series servers.

Before you begin

You must log in with admin privileges to perform this task.

Step 1 In the **Navigation** pane, click the **Chassis** menu.

Step 2 In the **Chassis** menu, click **Power Management**.

Step 3 In the **Chassis Power Characterization Details** area, review the following information:

Name	Description
Chassis Power Characterization Status field	Displays the progress of the power characterization. This can be one of the following: • **Not Run on One Server**— When the power characterization status is **Not Run** on any one server node. • **Not Run**— When the power characterization status is **Not Run** on both the server nodes. • **Failed on One Server**— When the power characterization status is **Failed** on any one server. • **Completed Successfully**—When the power characterization status is **Completed Successfully** on both the server nodes. • **Running**— When the power characterization status is **Running** on any one of the server nodes. • **Failed**— When the power characterization status is **Failed** on both the server nodes.

Name	Description
Chassis Power Characterization Range	It is composed of the following: • **Auto Profile Minimum**— The minimum value to be used for the user allocated chassis power to enable **Auto Profile**. **Note** The **Auto Profile Minimum** option is available only when both server nodes are present. • **Custom Profile Minimum**— The minimum value to be used for the user allocated chassis power to enable **Custom Profile** • **Maximum**— Maximum value for both Auto and Custom profiles.
Server Power Details	When you move the mouse over the Help icon, the server power details are displayed in a table.

Step 4 In the **Power Capping and Profiles Configuration** area, complete the following fields:

Name	Description
Enable Power Capping check box	If checked, this enables the power capping capability of the system, and allows you to select and set the parameters for individual power capping profiles. **Note** If disabled, you cannot configure or modify individual power capping profiles in the **Power Profiles** area.
User Allocated Chassis Power field	Power budget that you allocate to a chassis, in watts.
Chassis Manageable Power field	Maximum power that a chassis can manage, in watts. It is a part of the User Allocated Chassis power that is manageable.

Step 5 Click **Save Changes**.

What to do next

Configure the individual power profiles.

Configuring Auto Power Profile

Note The Auto tab is visible only when both server nodes are present in the chassis.

Before you begin

You must log in with admin privileges to perform this task.

Step 1 In the **Navigation** pane, click the **Chassis** menu.

Step 2 In the **Chassis** menu, click **Power Management**.

Step 3 In the **Auto** tab of the **Power Cap Configuration** tab, complete the following fields:

Name	Description
Enable Profile check box	If checked, enables the power profile for editing.
Allow Throttle check box	If checked, it forces the processor to use more aggressive power management mechanisms such as CPU throttling states (T-states) and memory bandwidth throttling to maintain the power limit, in addition to the regular internal mechanisms.
Priority Selection drop-down list	This can be one of the following: • **Manual**— When you manually assign priority to a server node. It could be either server 1 or server 2. • **Dynamic**— CMC dynamically decides to assign priority to a server node based on server utilization. The server that is utilized more at any given time is selected as a priority server.
Correction Time field	The time in seconds in which the platform power should be brought back to the specified power limit before taking the action specified in the **Action** field. The valid range is 1 to 600 seconds.
Priority Server drop-down list	Select an option to manually assign priority to a server. This can be one of the following: • **Server 1** • **Server 2** **Note** This option is available when you select **Manual** from the **Priority Selection** drop-down list.
Exception Action drop-down list	The action to be performed if the specified power limit is not maintained within the correction time. • **Alert**—Logs the event to the Cisco IMC SEL. • **Alert and Shutdown**—Logs the event to the Cisco IMC SEL, and gracefully shuts down the host.

Name	Description
Power Limit field **Server 1** **Server 2**	Displays the power cap limit assigned to server 1 and server 2 in auto profile.

Step 4 In the **Suspend Period** area, click the **Configure** link to set the time period in which the power capping profile is not active.

What to do next

Configure the custom power profile.

Configuring Custom Power Profile

Before you begin

You must log in with admin privileges to perform this task.

Step 1 In the **Navigation** pane, click the **Chassis** menu.

Step 2 In the **Chassis** menu, click **Power Management**.

Step 3 In the **Custom** tab of the **Power Cap Configuration** tab, complete the following fields:

Name	Description
Component field	Component for which you want to enable the **Custom Power** profile.
Enabled check box	If checked, enables the power profile for editing.
Power Limit field	Enter a value in the range suggested by the tooltip.
Exception Action drop-down list	The action to be performed if the specified power limit is not maintained within the correction time. • **Alert**—Logs the event to the Cisco IMC SEL. • **Alert and Shutdown**—Logs the event to the Cisco IMC SEL, and gracefully shuts down the host.
Correction Time field	The time in seconds in which the platform power should be brought back to the specified power limit before taking the action specified in the **Action** field. The valid range is 1 to 600 seconds.
Allow Throttling field	Forces the processor to use more aggressive power management mechanisms such as, CPU the throttling states (T-states) and memory bandwidth throttling to maintain the power limit, in addition to the regular internal mechanisms.

Name	Description
Suspend Period field	Allows you to suspend power capping for a chosen period of time.

What to do next

Configure the thermal power profile.

Configuring Thermal Power Profile

Before you begin

You must log in with admin privileges to perform this task.

Step 1 In the **Navigation** pane, click the **Chassis** menu.

Step 2 In the **Chassis** menu, click **Power Management**.

Step 3 In the **Thermal** tab of the **Power Cap Configuration** tab, complete the following fields:

Name	Description
Component field	Component for which you want to enable the **Thermal Power** profile.
Enabled field	Enables the power profile for editing.
Temperature field	Enter a temperature value crossing which the thermal profile should be applied. The valid range is 1 to 40.
Power Limit field	Displays the power cap limit that is minimum for the given server.

Viewing Power Monitoring Summary

This option is available only on some Cisco UCS C-Series servers.

Step 1 In the **Navigation** pane, click the **Chassis** menu.

Step 2 In the **Chassis** menu, click **Power Management**.

Step 3 On the **Work** pane, click the **Power Monitoring** tab.

Step 4 In the **Power Monitoring Summary** area, review the following information:

The following tables display the power consumed by the system and its components since the last time it was rebooted.

Name	Description
Monitoring Period	The time of monitoring the power consumed by the system since the last time it was rebooted. The monitoring period is displayed in Day HH:MM:SS format.

Note **Monitoring Period** is displayed under **Chassis**.

Platform, **CPU**, and **Memory** areas are available under **Server 1** and **Server 2**.

Step 5 In the **Platform** area, review the following information:

Name	Description
Current	The power currently being used by the server, CPU, and memory in watts.
Minimum	The minimum number of watts consumed by the server, CPU, and memory since the last time it was rebooted.
Maximum	The maximum number of watts consumed by the server, CPU, and memory since the last time it was rebooted.
Average	The average amount of power consumed by the server, CPU, and memory in watts over the defined period of time.

Step 6 In the **CPU** area, review the following information:

Name	Description
Current	The power currently being used by the CPU in watts.
Minimum	The minimum number of watts consumed by the CPU since the last time it was rebooted.
Maximum	The maximum number of watts consumed by the CPU since the last time it was rebooted.
Average	The average amount of power consumed by the server, CPU, and memory in watts over the defined period of time.

Step 7 In the **Memory** area, review the following information:

Name	Description
Current	The power currently being used by the memory, in watts.
Minimum	The minimum number of watts consumed by the memory since the last time it was rebooted.
Maximum	The maximum number of watts consumed by the memory since the last time it was rebooted.
Average	The average amount of power consumed by the memory in watts over the defined period of time.

Step 8 In the **Chart Properties** area, review and update the chart, component, and view the power consumption details.

Name	Description
Chart Settings	Enables you to configure the chart properties and the way data is displayed in the chart.
Download Power Statistics and Server Utilization Data	Enables you to download the power statistics and host server utilization information. The files are downloaded to your local download folder. **Note** If the file size of the already downloaded statistics file is less than 256 KB, then when you download, another set of files is downloaded, one for the power statistics and the other for host server utilization. If the size of the existing files exceeds 256 KB, then the next set of files overwrites the existing ones.

Name	Description
Chart drop-down list	Allows you to collect the trends of power consumption from every server for the selected duration. This can be one of the following: • **Last Hour**— Plots the chart for every five minutes • **Last Day**—Plots the chart for every hour from the current time. • **Last Week**—Plots the chart for each day.
Component drop-down list	The component for which you want to view the power consumption over the selected duration. This can be one of the following: • **Chassis** • ***Server 1*** • ***Server 2***
Domain drop-down list	The default value displayed is **Platform**.
Plot button	Displays the power consumed by the selected component for the specified duration.
Chart/Table View (Appears on mouse-over)	Select to view power monitoring summary in either **Chart** or **Table** view.

Name	Description
Chart Type (Appears on mouse-over)	Select the type of chart you wish to view. This could be one of the following: • Line Chart— Power monitoring data appears in lines. • Column Chart— Power monitoring data appears as a column. **Default Chart**: Line Chart. **Note** When the **Chart** drop-down list is selected as **Last Week**, and more than one Component is selected, the Column chart is not displayed, and by default the Line chart is displayed. The following message is displayed in such a scenario: `For the selected Configuration, Column graph cannot be plotted. Reverting to Line Graph.`
Current check box	If checked, the chart displays the current power consumed by the selected component for the selected duration.
Average check box	If checked, the plot displays the average amount of power consumed by the selected component for the selected duration.
Maximum check box	If checked, the plot displays the maximum number of watts consumed by the selected component for the selected duration.
Minimum check box	If checked, the plot displays the minimum number of watts consumed by the selected component for the selected duration.

Configuring the Chart Properties

Step 1 In the **Navigation** pane, click the **Chassis** menu.

Step 2 In the **Chassis** menu, click **Power Management**.

Step 3 On the **Work** pane, click the **Power Monitoring** tab.

Step 4 In the **Chart Properties** area, click the **Chart Settings** icon to configure the following fields:

Name	Description
Show Range Filter check box	If checked, displays the range filter content.
Show X Axis Labels check box	If checked, displays the X Axis labels for the power monitoring summary.

Name	Description
Show Y Axis Labels check box	If checked, displays the Y Axis labels for the power monitoring summary.
Show Markers check box	If checked, displays the markers for the X and Y axis data.
Y-Axis Interval Value field (1 - 1020)	Select the interval value in wattage. Default value is 20.

The power reading chart plots power consumption values of different components for the selected duration. These power consumption values are captured from the time that the host is powered on. When a power profile is enabled, the power limit is plotted in the chart as a red line. This plot can be used to determine the power consumption trend of the system. To view the configured power limit values of a particular domain, move the mouse over these trend lines.

Note These trend lines are not displayed if the profile is disabled on the **Power Cap Configuration** tab.

Step 5 Click **Save Changes**.

Downloading Power Statistics and Server Utilization Data

This option is available only on some Cisco UCS C-Series servers.

Before you begin

You must log in with admin privileges to perform this task.

Step 1 In the **Navigation** pane, click the **Chassis** menu.

Step 2 In the **Chassis** menu, click **Power Management**.

Step 3 On the **Work** pane, click the **Power Monitoring** tab.

Step 4 In the **Power Monitoring** tab, click **Download Power Statistics and Server Utilization Data**.

The files are downloaded to your local download folder.

Note If the file size of the already downloaded statistics file is less than 256 KB, then when you download, another set of files is downloaded, one for the power statistics and the other for host server utilization. If the size of the existing files exceeds 256 KB, then the next set of files overwrites the existing ones.

Configuring DIMM Blocklisting

DIMM Block Listing

In Cisco IMC, the state of the Dual In-line Memory Module (DIMM) is based on SEL event records. A DIMM is marked bad if the BIOS encounters a non-correctable memory error or correctable memory error with 16000 error counts during memory test execution during BIOS post. If a DIMM is marked bad, it is considered a non-functional device.

If you enable DIMM blocklisting, Cisco IMC monitors the memory test execution messages and blocklists any DIMM that encounters memory errors at any given point of time in the DIMM SPD data. This allows the host to map out those DIMMs.

DIMMs are mapped out or blocklisted only when Uncorrectable errors occur. When a DIMM gets blocklisted, other DIMMs in the same channel are ignored or disabled, which means that the DIMM is no longer considered bad.

Note DIMMs do not get mapped out or blocklisted for 16000 Correctable errors.

Enabling DIMM Block Listing

Before you begin

- You must log in with admin privileges.

Step 1 In the **Navigation** pane, click the **Compute** menu.
Step 2 In the **Compute** menu, select a server.
Step 3 In the work pane, click the **Inventory** tab.
Step 4 In the **Memory** pane's **DIMM Block Listing** area, click the **Enable DIMM Block List** check box.

Configuring BIOS Settings

Configuring BIOS Settings

Before you begin

You must log in with admin privileges to perform this task.

Step 1 In the **Navigation** pane, click the **Compute** menu.
Step 2 In the **Compute** menu, select a server.
Step 3 In the work pane, click the **BIOS** tab.
Step 4 In the **Actions** area, click **Configure BIOS**.
Step 5 Refer BIOS Parameters by Server Model to update the following tabs:

- I/O
- Server Management
- Security
- Processor

- Memory
- Power/Performance

Note The BIOS parameters available depend on the model of the server that you are using. For descriptions and information about the options for each BIOS setting, see *BIOS Parameters by Server Model* chapter in this guide.

Important A BIOS parameter available in one tab may affect the parameters on all available tabs, not just the parameters on the tab that you are viewing.

Entering BIOS Setup

Before you begin

- The server must be powered on.
- You must log in with admin privileges to perform this task.

Step 1 In the **Navigation** pane, click the **Compute** menu.
Step 2 In the **Compute** menu, select a server.
Step 3 In the work pane, click the **BIOS** tab.
Step 4 In the **Actions** area, click **Enter BIOS Setup**.
Step 5 Click **OK** at the prompt.
Enables enter BIOS setup. On restart, the server enters the BIOS setup.

Clearing the BIOS CMOS

Before you begin

- The server must be powered on.
- You must log in with admin privileges to perform this task.

Step 1 In the **Navigation** pane, click the **Compute** menu.
Step 2 In the **Compute** menu, select a server.
Step 3 In the work pane, click the **BIOS** tab.
Step 4 In the **Actions** area, click **Clear BIOS CMOS**.
Step 5 Click **OK** to confirm.
Clears the BIOS CMOS.

Restoring BIOS Manufacturing Custom Settings

Before you begin

- The server must be powered on.
- You must log in with admin privileges to perform this task.

Step 1 In the **Navigation** pane, click the **Compute** menu.
Step 2 In the **Compute** menu, select a server.
Step 3 In the work pane, click the **BIOS** tab.
Step 4 In the **Actions** area, click **Restore Manufacturing Custom Settings**.
Step 5 Click **Yes** if you wish to reboot the server immediately.
Step 6 Click **OK** to confirm.

Restoring BIOS Defaults

Before you begin

- The server must be powered on.
- You must log in with admin privileges to perform this task.

Step 1 In the **Navigation** pane, click the **Compute** menu.
Step 2 In the **Compute** menu, select a server.
Step 3 In the work pane, click the **BIOS** tab.
Step 4 In the **Actions** area, click **Restore Defaults**.
Step 5 Click **Yes** if you wish to reboot the server immediately.
Step 6 Click **OK** to confirm.

BIOS Profiles

On the Cisco UCS server, default token files are available for every S3260 server platform, and you can configure the value of these tokens using the Graphic User Interface (GUI), CLI interface, and the XML API interface. To optimize server performance, these token values must be configured in a specific combination.

Configuring a BIOS profile helps you to utilize pre-configured token files with the right combination of the token values. Some of the pre-configured profiles that are available are virtualization, high-performance, low power, and so on. You can download the various options of these pre-configured token files from the Cisco website and apply it on the servers through the BMC.

You can edit the downloaded profile to change the value of the tokens or add new tokens. This allows you to customize the profile to your requirements without having to wait for turnaround time.

Uploading a BIOS Profile

You can upload a BIOS profile either from a remote server location or through a browser client.

Before you begin

You must log in with admin privileges to perform this task.

Step 1 In the **Navigation** pane, click the **Compute** menu.

Step 2 In the **Compute** menu, select a server.

Step 3 In the work pane, click the **BIOS** tab.

Step 4 Click the **Configure BIOS Profile** tab.

Step 5 To upload the BIOS profile using a remote server location, in the **BIOS Profile** area, click the **Upload** button.

Step 6 In the **Upload BIOS Profile** dialog box, update the following fields:

Name	Description
Upload BIOS Profile from drop-down list	The remote server type. This can be one of the following: • **TFTP** • **FTP** • **SFTP** • **SCP** • **HTTP**
Server IP/Hostname field	The IP address or hostname of the server on which the BIOS profile information is available. Depending on the setting in the Upload BIOS Profile from drop-down list, the name of the field may vary.
Path and Filename field	The path and filename of the BIOS profile on the remote server.
Username field	Username of the remote server.
Password field	Password of the remote server.

Name	Description
Upload button	Uploads the selected BIOS profile. **Note** If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print_ID> Do you wish to continue?*. Click Yes or No depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
Cancel button	Closes the wizard without making any changes to the firmware versions stored on the server.

Step 7 To upload the BIOS profile using a browser client, in the **BIOS Profile** area, click the **Upload** button.

Step 8 In the **Upload BIOS Profile** dialog box, update the following fields:

Name	Description
File field	The BIOS profile that you want to upload.
Browse button	Opens a dialog box that allows you to navigate to the appropriate file.

What to do next

Activate a BIOS profile.

Activating a BIOS Profile

Before you begin

You must log in with admin privileges to perform this task.

Step 1 In the **Navigation** pane, click the **Compute** menu.

Step 2 In the **Compute** menu, select a server.

Step 3 In the work pane, click the **BIOS** tab.

Step 4 Click the **Configure BIOS Profile** tab.

Step 5 Select a BIOS profile from the **BIOS Profile** area and click **Activate**.

Step 6 At the prompt, click **Yes** to activate the BIOS profile.

Deleting a BIOS Profile

Before you begin

You must log in with admin privileges to perform this task.

Step 1 In the **Navigation** pane, click the **Compute** menu.
Step 2 In the **Compute** menu, select a server.
Step 3 In the work pane, click the **BIOS** tab.
Step 4 Select a BIOS profile from the **BIOS Profile** area and click **Delete**.
Step 5 At the prompt, click **OK** to delete the BIOS profile.

Backing up a BIOS Profile

Before you begin

You must log in with admin privileges to perform this task.

Step 1 In the **Navigation** pane, click the **Compute** menu.
Step 2 In the **Compute** menu, select a server.
Step 3 In the work pane, click the **BIOS** tab.
Step 4 Select a BIOS profile from the **BIOS Profile** area and click **Take Backup**.
Step 5 At the prompt, click **OK** to take a backup of the BIOS profile.

What to do next

Activate a BIOS profile.

Viewing BIOS Profile Details

Before you begin

You must log in with admin privileges to perform this task.

Step 1 In the **Navigation** pane, click the **Compute** menu.
Step 2 In the **Compute** menu, select a server.
Step 3 In the work pane, click the **BIOS** tab.
Step 4 Select a BIOS profile from the **BIOS Profile** area and click **Details**.
Step 5 Review the following information in the **BIOS Profile Details** window:

Name	Description
Token Name column	Displays the token name of the BIOS profile.
Display Name column	Displays the user name of the BIOS profile.
Profile Value column	Displays the value that was provided in the uploaded file.
Actual Value column	Displays the value of the active BIOS configuration.

Secure Boot Certificate Management

Beginning with 4.2(2a) release, Cisco IMC allows you to upload up to ten certificates for configured secure HTTP Boot device. You can also delete and upload a new certificate for the specific boot device configured. Cisco IMC allows you to upload up to ten root CA Certificates.

Viewing Secure Boot Certificate Details

You can view the details of a secure boot certificate, which is already uploaded.

Before you begin

You must log in with admin privileges to perform this task. log in as admin

Step 1 In the **Navigation** pane, click the **Compute** menu.

Step 2 In the **Compute** menu, select a server.

Step 3 In the work pane, click the **BIOS** tab.

Step 4 Click the **Secure Boot Certificate Management** tab.

Step 5 From the certificates table, select the certificate, which you wish to view.

Step 6 Click the **View Secure Boot Certificate** icon above the table.

Step 7 **View Secure Boot Certificate** dialog box is displayed.

You can view the following information:

Table 1: General Area

Field	Description
Certificate ID field	Displays the certificate ID assigned by Cisco IMC.
Serial Number field	The serial number for the server.
Valid From field	Certificate validity start date.
Valid To field	Certificate expiry date.

Table 2: Subject Area

Field	Description
Country Code field	Country code of the certificate.
Locality field	Locality of the certificate.
State Name field	State of the certificate.
Organization Name field	Organization of the certificate.
Organization Unit field	Organization unit of the certificate.
Common Name field	Certificate name.

Table 3: Issuer Area

Field	Description
Country Code field	Country code of the issuer.
Locality field	Locality of the issuer.
State Name field	State of the issuer.
Organization Name field	Organization of the issuer.
Organization Unit field	Organization unit of the issuer.
Common Name field	Issuer name.

Uploading Secure Boot Certificate

You can upload a boot certificate either from a remote server location or from local location.

Before you begin

- You must log in with admin privileges to perform this task. log in as admin
- If you wish to upload using Local upload, ensure that the certificate file resides on a locally accessible file system.
- Ensure that the generated certificate is of type server.
- The following certificate formats are supported:
  - .crt
  - .cer
  - .pem

Step 1 In the **Navigation** pane, click the **Compute** menu.

Step 2 In the **Compute** menu, select a server.

Step 3 In the work pane, click the **BIOS** tab.

Step 4 Click the **Secure Boot Certificate Management** tab.

Step 5 To upload the boot certificate, click the upload button (+).

Step 6 You can upload the certificate using one of the following methods:

- Paste the certificate directly in the paste certificate text field
- Upload from local location
- Upload from remote location

In the **Add Secure Boot Certificate**dialog box, update the fields as per your the method you wish to upload the certificate:

Table 4: Add Secure Boot Certificate

Field	Description
Paste Secure Boot Certificate radio button	Allows you to copy the entire content of the signed certificate and paste it in the Paste certificate content text field. **Note** Ensure the certificate is signed before uploading.
Upload from local radio button	Allows you to browse and navigate to the location of the authorities certificate file that you want to add.

Field	Description

Upload from remote location radio button	Allows you to choose the certificate from a remote location and Upload it. Enter the following details:
	• **Upload Secure Boot Certificate from**—
	  • TFTP Server
	  • FTP Server
	  • SFTP Server
	  • SCP Server
	  • HTTP Server
	• **Server IP/Hostname**—The IP address or hostname of the server on which the certificate file should be stored. Depending on the setting in the Upload Certificate from drop-down list, the name of the field may vary.
	• **Path and Filename**—The path and filename Cisco IMC should use when uploading the file to the remote server.
	• **Username**—The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP.
	• **Password**—The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.

Upload Secure Boot Certificate button	Allows you to Upload the certificate to the server.

Deleting a Secure Boot Certificate

You can delete a boot certificate which is already uploaded on Cisco IMC.

Before you begin

You must log in with admin privileges to perform this task. log in as admin

Step 1 In the **Navigation** pane, click the **Compute** menu.

Step 2 In the **Compute** menu, select a server.

Step 3 In the work pane, click the **BIOS** tab.

Step 4 Click the **Secure Boot Certificate Management** tab.

Step 5 From the certificates table, select the certificate, which you wish to delete.

Step 6 Click the **Delete Secure Boot Certificate** icon above the table.

Step 7 Click **Yes** to confirm.

Persistent Memory Modules

Cisco UCS S-Series Release 4.0(4) introduces support for the Intel® Optane™ Data Center persistent memory modules on the UCS M5 servers that are based on the Second Generation Intel® Xeon® Scalable processors. These persistent memory modules can be used only with the Second Generation Intel® Xeon® Scalable processors.

Persistent memory modules are non-volatile memory modules that bring together the low latency of memory and the persistence of storage. Data stored in persistent memory modules can be accessed quickly compared to other storage devices, and is retained across power cycles.

For detailed information about configuring persistent memory modules, see the Cisco UCS: Configuring and Managing Intel® Optane™ Data Center Persistent Memory Modules Guide.