



Managing the Server

This chapter includes the following sections:

- [Toggling the Locator LED, page 1](#)
- [Toggling the Front Locator LED for the Chassis, page 2](#)
- [Toggling the Locator LED for a Hard Drive, page 2](#)
- [Selecting a Time Zone, page 3](#)
- [Managing the Server Boot Order, page 6](#)
- [Resetting the Server, page 16](#)
- [Shutting Down the Server, page 16](#)
- [Managing Server Power, page 17](#)
- [Configuring Power Policies, page 19](#)
- [Configuring Fan Policies, page 27](#)
- [Managing the Flexible Flash Controller, page 30](#)
- [Configuring DIMM Black Listing, page 49](#)
- [Configuring BIOS Settings, page 50](#)
- [Updating Firmware on Server Components, page 55](#)
- [Viewing Product ID \(PID\) Catalog Details, page 56](#)
- [Uploading and Activating PID Catalog, page 57](#)

Toggling the Locator LED

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	Server # scope chassis	Enters chassis command mode.
Step 2	Server /chassis # set locator-led {on off}	Enables or disables the chassis locator LED.
Step 3	Server /chassis # commit	Commits the transaction to the system configuration.

This example disables the chassis locator LED and commits the transaction:

```
Server# scope chassis
Server /chassis # set locator-led off
Server /chassis *# commit

Server /chassis #
```

Toggling the Front Locator LED for the Chassis

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

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	Server # scope chassis	Enters chassis command mode.
Step 2	Server /chassis # set front-locator-led {on off}	Enables or disables the chassis locator LED.
Step 3	Server /chassis # commit	Commits the transaction to the system configuration.

This example disables the chassis locator LED and commits the transaction:

```
Server# scope chassis
Server /chassis # set front-locator-led off
Server /chassis *# commit

Server /chassis #
```

Toggling the Locator LED for a Hard Drive

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

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	Server # scope chassis	Enters chassis command mode.
Step 2	Server/chassis # scope hdd	Enters hard disk drive (HDD) command mode.
Step 3	Server /chassis/hdd # set locateHDD drivenum {1 2}	Where <i>drivenum</i> is the number of the hard drive whose locator LED you want to set. A value of 1 turns the LED on while a value of 2 turns the LED off.

This example turns on the locator LED on HDD 2:

```

Server# scope chassis
Server /chassis # scope hdd
Server /chassis/hdd # locateHDD 2 1
HDD Locate LED Status changed to 1
Server /chassis/hdd # show
Name                               Status                               LocateLEDStatus
-----
HDD1_STATUS                        present                             TurnOFF
HDD2_STATUS                        present                             TurnON
HDD3_STATUS                        absent                              TurnOFF
HDD4_STATUS                        absent                              TurnOFF

Server /chassis/hdd #

```

Selecting a Time Zone

Selecting a Time Zone

Selecting a time zone helps you choose a local time zone so that you can view the local time rather than the default machine time. Cisco IMC Web UI and the CLI provide you options to choose and set a time zone of your choice.

Setting the time zone to your local time will apply the time zone variable to all the services that utilize the system timing. This impacts the logging information and is utilized in the following applications of the Cisco IMC:

- Fault summary and fault history logs
- Cisco IMC log
- rsyslog

When you set a local time, the timestamp on the applications that you can view are updated with the local time that you have chosen.

Selecting a Time Zone

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	Server # scope CIMC	Enters Cisco IMC command mode.
Step 2	Server /CIMC # timezone-select	Displays a list of continents and oceans.
Step 3	Enter the number corresponding to your continent or ocean.	A list of all the countries or regions of the chosen continent or ocean displays.
Step 4	Enter the number corresponding to the country or region that you want to set as your time zone.	If a country or a region has more than one time zones, a list of time zones in that country or region displays.
Step 5	Enter the number corresponding to time zone.	Is the above information OK? message appears.
Step 6	Enter 1 .	Continue?[y N]: prompt appears.
Step 7	Enter y if you want to set the chosen time zone.	The chosen time zone is set as the time zone for your Cisco IMC server.

This example sets the time zone:

```
Server# scope CIMC
Server /CIMC # timezone-select
```

```
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
```

- 1) Africa
- 2) Americas
- 3) Antarctica
- 4) Arctic Ocean
- 5) Asia
- 6) Atlantic Ocean
- 7) Australia
- 8) Europe
- 9) Indian Ocean
- 10) Pacific Ocean

```
#? 2
```

```
Please select a country whose clocks agree with yours.
```

- 1) Anguilla
- 2) Antigua & Barbuda
- 3) Argentina
- 4) Aruba
- 5) Bahamas
- 6) Barbados
- 7) Belize
- 8) Bolivia
- 9) Brazil
- 10) Canada
- 11) Caribbean Netherlands
- 12) Cayman Islands
- 13) Chile

- 14) Colombia
- 15) Costa Rica
- 16) Cuba
- 17) Curacao
- 18) Dominica
- 19) Dominican Republic
- 20) Ecuador
- 21) El Salvador
- 22) French Guiana
- 23) Greenland
- 24) Grenada
- 25) Guadeloupe
- 26) Guatemala
- 27) Guyana
- 28) Haiti
- 29) Honduras
- 30) Jamaica
- 31) Martinique
- 32) Mexico
- 33) Montserrat
- 34) Nicaragua
- 35) Panama
- 36) Paraguay
- 37) Peru
- 38) Puerto Rico
- 39) St Barthelemy
- 40) St Kitts & Nevis
- 41) St Lucia
- 42) St Maarten (Dutch part)
- 43) St Martin (French part)
- 44) St Pierre & Miquelon
- 45) St Vincent
- 46) Suriname
- 47) Trinidad & Tobago
- 48) Turks & Caicos Is
- 49) United States
- 50) Uruguay
- 51) Venezuela
- 52) Virgin Islands (UK)
- 53) Virgin Islands (US)

#? 49

Please select one of the following time zone regions.

- 1) Eastern Time
- 2) Eastern Time - Michigan - most locations
- 3) Eastern Time - Kentucky - Louisville area
- 4) Eastern Time - Kentucky - Wayne County
- 5) Eastern Time - Indiana - most locations
- 6) Eastern Time - Indiana - Daviess, Dubois, Knox & Martin Counties
- 7) Eastern Time - Indiana - Pulaski County
- 8) Eastern Time - Indiana - Crawford County
- 9) Eastern Time - Indiana - Pike County
- 10) Eastern Time - Indiana - Switzerland County
- 11) Central Time
- 12) Central Time - Indiana - Perry County
- 13) Central Time - Indiana - Starke County
- 14) Central Time - Michigan - Dickinson, Gogebic, Iron & Menominee Counties
- 15) Central Time - North Dakota - Oliver County
- 16) Central Time - North Dakota - Morton County (except Mandan area)
- 17) Central Time - North Dakota - Mercer County
- 18) Mountain Time
- 19) Mountain Time - south Idaho & east Oregon
- 20) Mountain Standard Time - Arizona (except Navajo)
- 21) Pacific Time
- 22) Alaska Time
- 23) Alaska Time - Alaska panhandle
- 24) Alaska Time - southeast Alaska panhandle
- 25) Alaska Time - Alaska panhandle neck
- 26) Alaska Time - west Alaska
- 27) Aleutian Islands
- 28) Metlakatla Time - Annette Island
- 29) Hawaii

#? 8

```

The following information has been given:

    United States
    Eastern Time - Indiana - Crawford County

Is the above information OK?
1) Yes
2) No
#? 1

You have chosen to set timezone settings to:

    America/Indiana/Marengo

Continue?[y|N]: y
Timezone has been updated.
The local time now is: Sun Jun 1 02:21:15 2014 EST

Server /CIMC #

```

Managing the Server Boot Order

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**

When you upgrade Cisco IMC to the latest version 2.0(x) for the first time, the legacy boot order is migrated to the precision boot order. During this process, 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) version 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**

- 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.

Viewing the Boot Device Detail

**Note**

Do not change the boot order while the host is performing BIOS power-on self test (POST).

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# scope bios	Enters the BIOS command mode.
Step 2	Server /bios # show boot-device [detail] .	Displays the detailed information of the boot device.

This example displays the details of the created bootable device:

```
Server# scope bios
Server /bios # show boot-device
Boot Device          Device Type  Device State  Device Order
-----
TestUSB              USB         Enabled      1
TestPXE              PXE         Enabled      2
Server /bios # show boot-device detail
Boot Device TestSAN:
  Device Type: SAN
  Device State: Enabled
  Device Order: 1
  Slot Id:
  Lun Id:
Boot Device TestUSB:
  Device Type: USB
  Device State: Enabled
  Device Order: 2
  Sub Type: HDD
Boot Device TestPXE:
  Device Type: PXE
  Device State: Enabled
  Device Order: 3
  Slot Id: L
  Port Number: 1
```

Configuring the Precision Boot Order



Note

Do not change the boot order while the host is performing BIOS power-on self test (POST).

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# scope bios	Enters the BIOS command mode.
Step 2	Server /bios # create-boot-device [<i>device name</i>] [<i>device type</i>].	Creates a bootable device that BIOS chooses to boot. This can be one of the following: <ul style="list-style-type: none"> • HDD—Hard disk drive • PXE—PXE boot • SAN boot • iSCSI boot • SD Card <p>Note SD card option is available only on some UCS C-Series servers.</p> • USB • Virtual Media

	Command or Action	Purpose
		<ul style="list-style-type: none"> • PCHStorage • UEFISHELL
Step 3	Server /bios # scope boot-device <i>created boot device name</i> .	Enters the management of the created bootable devices.
Step 4	Server /bios /boot-device # set values	<p>Specifies the property values for particular bootable device. You can set one or more of the following:</p> <ul style="list-style-type: none"> • cli— CLI options • state— Whether the device will be visible by BIOS. By default the device is disabled. Note If enabled, the device will overwrite the legacy boot order configuration. • slot— Slot id where the device is plugged in. • port— Port of the slot in which the device is present. • LUN— Logical unit in a slot where the device is present. • sub-type— Sub device type under a certain device type. • order— The order of the device in the available list of devices.
Step 5	Server /bios /boot-device # commit	Commits the transaction to the system configuration.

This example configures the boot order, creates a boot device, set the attributes of the new device and commit the transaction:

```

Server# scope bios
Server /bios # create boot-device TestPXE PXE
Server /bios # scope boot-device TestPXE
Server /bios /boot-device # set state Enabled
Server /bios /boot-device # set slot L
Server /bios /boot-device # set port 1
Server /bios /boot-device # set order 1
Server /bios /boot-device # commit
Enabling boot device will overwrite Legacy Boot Order configuration
Continue?[y|N]y
Server /bios /boot-device # y
Committing device configuration
Server /bios /boot-device # show detail
BIOS:
  BIOS Version: "C240M3.2.0.0.15 (Build Date: 03/16/2014)"
  Boot Order: (none)
  Boot Override Priority:
  FW Update/Recovery Status: None, OK
  UEFI Secure Boot: disabled
  Configured Boot Mode: None
  Actual Boot Mode: Legacy
  Last Configured Boot Order Source: CIMC

```

```

Server /bios/boot-device # show boot-device detail
Boot Device TestPXE:
  Device Type: PXE
  Device State: Enabled
  Device Order: 1
  Slot Id: L
  Port Number: 1

```

What to Do Next

Reboot the server to boot with your new boot order.

Modifying the Attributes of a Boot Device



Note

Do not change the boot order while the host is performing BIOS power-on self test (POST).

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# scope bios	Enters the BIOS command mode.
Step 2	Server /bios # scope boot-device <i>created boot device name.</i>	Enters the management of the created bootable devices.
Step 3	Server /bios /boot-device # set state <i>{Enabled Disabled}.</i>	Enables or disables the device. The default state is disabled. Note If enabled, the device will overwrite the legacy boot order configuration.
Step 4	Server /bios /boot-device* # set order <i>{Index 1-50}.</i>	Specifies the order of booting for particular device in the device list. Enter a number between 1 and 50 based on the total number of created device. Note When you set the boot device order individually, it is not assured that the order appears in the way it was set. So, it is recommended that to set the order for multiple devices in a single execution, use re-arrange-boot-device command.
Step 5	Server /bios /boot-device* # set port <i>{value 1-255}.</i>	Specifies the port of the slot in which the device is present. Enter a number between 1 and 255.
Step 6	Server /bios /boot-device* # commit	Commits the transaction to the system configuration.

This example modifies the attributes of an existing device:

```

Server# scope bios
Server /bios *# scope boot-device scu-device-hdd

```

```

Server /bios/boot-device # set status enabled
Server /bios/boot-device *# set order 2
Server /bios/boot-device *# set port 1
Server /bios/boot-device *# commit
Enabling boot device will overwrite boot order Level 1 configuration
Continue?[y|N]y
Server /bios/boot-device #

```

Rearranging Device Boot Order



Note

Do not change the boot order while the host is performing BIOS power-on self test (POST).

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# scope bios	Enters the BIOS command mode.
Step 2	Server /bios # rearrange boot-device [<i>device name</i>]:[<i>position</i>].	Rearranges the selected boot devices in a single execution.

This example rearranges the selected boot devices:

```

Server# scope bios
Server /bios # rearrange-boot-device TestPXE:1,TestUSB:2
Server /bios # show boot-device
Boot Device          Device Type  Device State  Device Order
-----
TestPXE              PXE         Disabled     1
TestUSB              USB         Disabled     2

Server /bios #

```

What to Do Next

Re-Applying the Boot Order Configuration



Note

Do not change the boot order while the host is performing BIOS power-on self test (POST).

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# scope bios	Enters the BIOS command mode.
Step 2	Server /bios # re-apply .	Re-applies the boot order to BIOS, if the last configured boot order source is BIOS..

This example re-applies the boot order to BIOS:

```
Server# scope bios
Server /bios # re-apply
Server /bios #
```

What to Do Next

Reboot the host after reapplying the boot order to BIOS.

Deleting an Existing Boot Device

**Note**

Do not change the boot order while the host is performing BIOS power-on self test (POST).

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# scope bios	Enters the BIOS command mode.
Step 2	Server /bios # remove-boot-device <i>device name</i>	Deletes the particular device from the boot order.

This example deletes the selected device from the device list:

```
Server# scope bios
Server /bios # remove-boot-device scu-device-hdd
Server /bios #
```

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	<ul style="list-style-type: none"> • Windows Server 2012 • Windows Server 2012 R2
Broadcom PCI adapters	<ul style="list-style-type: none"> • 5709 dual and quad port adapters • 57712 10GBASE-T adapter • 57810 CNA • 57712 SFP port
Intel PCI adapters	<ul style="list-style-type: none"> • i350 quad port adapter • X520 adapter • X540 adapter • LOM
QLogic PCI adapters	<ul style="list-style-type: none"> • 8362 dual port adapter • 2672 dual port adapter
Fusion-io	

Components	Types
LSI	<ul style="list-style-type: none"> • 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

Enabling UEFI Secure Boot Mode

Before You Begin

Procedure

	Command or Action	Purpose
Step 1	Server# scope bios	Enters the BIOS command mode.
Step 2	Server/ BIOS # set secure-boot enable disable	<p>Enables or disables UEFI secure boot.</p> <p>Note If enabled, the boot mode is set to UEFI secure mode. You cannot modify configure boot mode until UEFI secure boot mode is disabled.</p>

This example enables UEFI secure boot mode and commits the transaction

```
Server# scope bios
Server /bios # set secure-boot enable
Setting Value : enable
Commit Pending.
Server /bios *# commit
UEFI Secure boot state changed successfully. Execute 'show detail' command to check the
current status
Server /bios #
```

What to Do Next

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

Disabling UEFI Secure Boot

Procedure

	Command or Action	Purpose
Step 1	Server# scope bios	Enters the BIOS command mode.
Step 2	Server/ BIOS # set secure-boot enable disable	Enables or disables UEFI secure boot.

This example disables UEFI secure boot mode and commits the transaction

```
Server# scope bios
Server /bios # set secure-boot disable
Setting Value : enable
Commit Pending.
Server /bios *# commit
UEFI Secure boot state changed successfully. Execute 'show detail' command to check the
current status
Server /bios #
```

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

Procedure

	Command or Action	Purpose
Step 1	Server# scope bios	Enters bios command mode.
Step 2	Server /bios # show actual-boot-order [detail]	Displays the boot order actually used by the BIOS when the server last booted.

This example displays the actual boot order of the legacy boot order from the last boot:

```
Server# scope bios
Server /bios # show actual-boot-order
```

Boot Order	Type	Boot Device
1	CD/DVD	CD-ROM
2	CD/DVD	Cisco Virtual CD/DVD 1.18
3	Network Device (PXE)	Cisco NIC 23:0.0
4	Network Device (PXE)	MBA v5.0.5 Slot 0100
5	Network Device (PXE)	MBA v5.0.5 Slot 0101
6	Network Device (PXE)	MBA v5.0.5 Slot 0200

```

7          Network Device (PXE)      MBA v5.0.5 Slot 0201
8          Network Device (PXE)      Cisco NIC 22:0.0
9          Internal EFI Shell
10         FDD                        Cisco Virtual HDD 1.18
11         FDD                        Cisco Virtual Floppy 1.18

```

Server /bios #

This example displays the actual boot order of precision boot order from the last boot:

Server /bios # **show actual-boot-order**

Boot Order	Boot Device	Device Type	Boot Policy
1	IBA GE Slot 0201 v1398	PXE	TestPXE
2	IBA GE Slot 0200 v1398	PXE	NonPolicyTarget
3	IBA GE Slot 0202 v1398	PXE	NonPolicyTarget
4	IBA GE Slot 0203 v1398	PXE	NonPolicyTarget
5	"UEFI: Built-in EFI Shell "	EFI	NonPolicyTarget

Server /bios #

Resetting the Server



Important

If any firmware or BIOS updates are in progress, do not reset the server until those tasks are complete.

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters chassis command mode.
Step 2	Server /chassis # power hard-reset	After a prompt to confirm, resets the server.

This example resets the server:

```

Server# scope chassis
Server /chassis # power hard-reset
This operation will change the server's power state.
Continue?[y|N]

```

Shutting Down the Server



Important

If any firmware or BIOS updates are in progress, do not shut down the server until those tasks are complete.

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters chassis mode.
Step 2	Server /chassis # power shutdown	Shuts down the server.

The following example shuts down the server:

```
Server# scope chassis
Server /chassis # power shutdown
```

Managing Server Power

Powering On the Server

**Note**

If the server was powered off other than through the Cisco IMC, the server will not become active immediately when powered on. In this case, the server will enter standby mode until the Cisco IMC completes initialization.

**Important**

If any firmware or BIOS updates are in progress, do not change the server power until those tasks are complete.

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # power on	Turns on the server.
Step 3	At the prompt, enter y to confirm.	Turns on the server.

This example shows how to turn on the server:

```
Server# scope chassis
Server /chassis # power on
Warning: System is already powered ON, this action is ineffective.
Do you want to continue?[y|N]y
```

Powering Off the Server



Important

If any firmware or BIOS updates are in progress, do not power off the server until those tasks are complete.

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters chassis command mode.
Step 2	Server /chassis # power off	Turns off the server.

This example turns off the server:

```
Server# scope chassis
Server /chassis # power off
This operation will change the server's power state.
Continue?[y|N]y

Server /chassis # show
Power Serial Number Product Name  UUID
-----
off   Not Specified Not Specified  208F0100020F000000BEA80000DEAD00
```

Power Cycling the Server



Important

If any firmware or BIOS updates are in progress, do not power cycle the server until those tasks are complete.

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters chassis command mode.
Step 2	Server /chassis # power cycle	Power cycles the server.

This example power cycles the server:

```
Server# scope chassis
Server /chassis # power cycle
```

Configuring Power Policies

Power Capping

**Important**

This section is valid only for some UCS C-Series servers.

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.

Once power capping is enabled, you can configure multiple power profiles to either have standard or advanced power profiles with defined attributes. If you choose a standard power profile, you can set the power limit, correction time, corrective-action, suspend period, hard capping, and policy state (if enabled). If you choose an advanced power profile, in addition to the attributes of the standard power profile, you can also set the domain specific power limits, safe throttle level, and ambient temperature based power capping attributes.

**Note**

The following changes are applicable for Cisco UCS C-Series release 2.0(13) and later:

- After upgrading to the 2.0(13) release, power characterization automatically runs during the first host power on. Subsequent characterization runs only if initiated as described in section **Run Power Characterization** section.
- Also, when a server is power cycled and there is a change to the CPU or DIMM configurations, power characterization automatically runs on first host boot. For any other hardware change like PCIe adapters, GPU or HDDs, power characterization does not run. The characterized power range is modified depending on the components present after the host power cycle.

The **Run Power Characterization** option in the **Power Cap Configuration** Tab of the Web UI power cycles the host and starts power characterization.

Enabling Power Characterization

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.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters chassis command mode.
Step 2	Server /chassis # scope power-cap-config	Enters power cap command mode.
Step 3	Server /chassis # set run-pow-char-at-boot	Runs the power characterization at boot.
Step 4	Server /chassis # commit	Commits the transaction to the system.

This example shows how to automatically invoke power characterization during a host reboot:

```
Server# scope chassis
Server /chassis# scope power-cap-config
Server /chassis /power-cap-config # set run-pow-char-at-boot
Server /chassis /power-cap-config* # commit
Server /chassis/power-cap-config #
```

Configuring the Power Cap Policy

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.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters chassis command mode.
Step 2	Server /chassis # scope power-cap-config	Enters power cap command mode.
Step 3	Server /chassis /power-cap-config# set pow-cap-enable {yes no}	Enables or disables the capping of power to the server.
Step 4	Server /chassis /power-cap-config# commit	Commits the transaction to the system configuration.

This example shows how to enable the power capping policy:

```
Server# scope chassis
Server /chassis# scope power-cap-config
Server /chassis /power-cap-config # set pow-cap-enable yes
Server /chassis /power-cap-config* # commit
Server /chassis/power-cap-config #
```

Configuring Standard Power Profile

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

Before You Begin

- Power capping must be enabled.
- You must log in with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters chassis command mode.
Step 2	Server /chassis # scope power-cap-config	Enters power cap command mode.
Step 3	Server /chassis /power-cap-config# set pow-cap-enable {yes no}	Enables or disables the power capping capability of the system.
Step 4	Server /chassis /power-cap-config# scope power-profile standard	Enters the standard command mode of a power profile
Step 5	Server /chassis /power-cap-config# set allow-throttle yes no	Enables or disables the system to maintain the power limit by forcing the processor to use the throttling state (T-state) and memory throttle.
Step 6	Server /chassis /power-cap-config# set corr-time value	Sets the correction time in which the platform power should be brought back to the specified power limit before taking the action specified in the Action mode. The range is from 3 and 600 seconds. The default is 3 seconds.
Step 7	Server /chassis /power-cap-config# set except-action alert shutdown	Specifies the action to be performed if the specified power limit is not maintained within the correction time. This can be one of the following: <ul style="list-style-type: none"> • Alert—Logs the event to the Cisco IMC SEL. • Shutdown—Gracefully shuts down the host. • None—No actions are taken.
Step 8	Server /chassis /power-cap-config# set hard-cap yes no	Enables or disables the system to maintain the power consumption below the specified power limit.
Step 9	Server /chassis /power-cap-config# set pow-limit value	Specifies the power limit. Enter a value within the specified range.

	Command or Action	Purpose
Step 10	Server /chassis /power-cap-config# set susp-pd {h:m-h:m ll,Mo,Tu,We,Th,Fr,Sa,Su.}	Specifies the time period that the power capping profile is not active.
Step 11	Server /chassis /power-cap-config# commit	Commits the transaction to the system.

This example shows how to configure standard power profile:

```
Server# scope chassis
Server /chassis# scope power-cap-config
Server /chassis /power-cap-config # set pow-cap-enable yes
Server /chassis /power-cap-config* # commit
Server /chassis/power-cap-config # scope power-profile advance
Server /chassis/power-cap-config # set allow-throttle yes
Server /chassis/power-cap-config* # set corr-time 6
Server /chassis/power-cap-config* # set except-action alert
Server /chassis/power-cap-config* # set hard-cap yes
Server /chassis/power-cap-config* # set pow-limit 360
Server /chassis/power-cap-config* # set susp-pd 1:30-2:30|All
Server /chassis/power-cap-config* # commit
Server /chassis/power-cap-config #
```

Configuring Advanced Power Profile Settings

You can configure these settings only on some UCS C-Series servers.

Before You Begin

- You must enable power capping.
- You must log in with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters chassis command mode.
Step 2	Server /chassis # scope power-cap-config	Enters power cap command mode.
Step 3	Server /chassis /power-cap-config# set pow-cap-enable {yes no}	Enables or disables the power capping capability of the server.
Step 4	Server /chassis /power-cap-config# commit	Commits the transaction to the system.
Step 5	Server /chassis /power-cap-config# scope power-profile advance	Enters the advance command mode of a power profile.

	Command or Action	Purpose
Step 6	Server /chassis /power-cap-config# set allow-throttle {yes no}	Enables or disables the system to maintain the power limit by forcing the processor to use the throttling state (T-state) and memory throttle.
Step 7	Server /chassis /power-cap-config# set corr-time <i>value</i>	Sets the maximum time to take corrective actions in order to bring the platform back to the specified power limit before taking the actions specified in the Action mode. The range is from 3 and 600 seconds. The default is 3 seconds.
Step 8	Server /chassis /power-cap-config# set cpu-power-limit <i>value</i>	Specifies the power limit for the CPU. Enter power in watts within the range specified.
Step 9	Server /chassis /power-cap-config# set cpu-safe-throttle <i>value</i>	Specifies the throttling level for the CPU. The range is from 0 and 100 percentage.
Step 10	Server /chassis /power-cap-config# set except-action {alert shutdown}	Specifies the action to be performed if the specified power limit is not maintained within the correction time. This can be one of the following: <ul style="list-style-type: none"> • Alert—Reports the event to the Cisco IMC SEL. • Shutdown—Gracefully shuts down the host. • None—No actions are taken.
Step 11	Server /chassis /power-cap-config# set hard-cap {yes no}	Enables or disables the system to maintain the power consumption below the specified power limit.
Step 12	Server /chassis /power-cap-config# set mem-pow-limit <i>value</i>	Specifies the power limit for the memory. Enter power in watts within the range specified.
Step 13	Server /chassis /power-cap-config# set mem-safe-Tlvl <i>value</i>	Specifies the throttling level for the memory. The range is from 0 and 100 percentage.
Step 14	Server /chassis /power-cap-config# set fail-safe-timeout <i>value</i>	Specifies a safe throttle policy when the power capping functionality is impacted internal faults such as missing power readings for platforms or CPUs. The range is from 1 and 10 seconds.
Step 15	Server /chassis /power-cap-config# set plat-safe-Tlvl <i>value</i>	Specifies the throttling level for the platform in percentage. The range is from 0 and 100.
Step 16	Server /chassis /power-cap-config# set plat-temp <i>value</i>	Specifies the inlet temperature sensor. Enter value in Celsius.

	Command or Action	Purpose
Step 17	Server /chassis /power-cap-config# set pow-limit <i>value</i>	Specifies the power limit. Enter power in watts within the range specified.
Step 18	Server /chassis /power-cap-config# set susp-pd { <i>h:m-h:m</i> <i>ll,Mo,Tu,We,Th,Fr,Sa,Su.</i> }	Specifies the time period that the power capping profile will not be active.
Step 19	Server /chassis /power-cap-config# set thermal-power-limit <i>value</i>	Specifies the power limit to be maintained. Enter power in watts within the range specified.
Step 20	Server /power-cap # commit	Commits the transaction to the system configuration.

This example shows how to configure the advance power profile setting:

```

Server# scope chassis
Server /chassis# scope power-cap-config
Server /chassis /power-cap-config # set pow-cap-enable yes
Server /chassis /power-cap-config* # commit
Server /chassis/power-cap-config # scope power-profile advance
Server /chassis/power-cap-config # set allow-throttle yes
Server /chassis/power-cap-config* # set corr-time 6
Server /chassis/power-cap-config*# set cpu-power-limit 259
Server /chassis/power-cap-config* # set cpu-safe-Tlvl 50
Server /chassis/power-cap-config* # set except-action alert
Server /chassis/power-cap-config* # set hard-cap yes
Server /chassis/power-cap-config* # set mem-pow-limit 259
Server /chassis/power-cap-config* # set mem-safe-Tlvl 50
Server /chassis/power-cap-config* # set fail-safe-timeout 10
Server /chassis/power-cap-config* # set plat-safe-Tlvl 50
Server /chassis/power-cap-config* # set plat-temp 35
Server /chassis/power-cap-config* # set pow-limit 360
Server /chassis/power-cap-config* # set susp-pd 1:30-2:30|All
Server /chassis/power-cap-config* # set thermal-power-limit 354
Server /chassis/power-cap-config* # commit
Server /chassis/power-cap-config #

```

Resetting the Power Profiles to Defaults

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.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters chassis command mode.
Step 2	Server /chassis # scope power-cap-config	Enters power cap command mode.

	Command or Action	Purpose
Step 3	Server /chassis # set reset-power-profile-to-defaults	Resets the power profile settings to factory-default values and disables power capping.
Step 4	Server /chassis # commit	Commits the transaction to the system.

This example shows how to reset the power profile to the default settings:

```
Server# scope chassis
Server /chassis# scope power-cap-config
Server /chassis /power-cap-config # reset-power-profile-to-defaults
Server /chassis /power-cap-config* # commit
Server /chassis/power-cap-config #
```

Viewing the Power Capping Configuration

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.

Procedure

	Command or Action	Purpose
Step 1	Server # scope chassis	Enters chassis command mode.
Step 2	Server /chassis # show power-cap-config	Displays information about the power characterization.

This example shows how to view information about the power cap configuration:

```
Server #scope chassis
Server /chassis # show power-cap-config
Power Capping      Power Characterization at Boot  Power Characterization Status  Min (W)  Max
(W)
-----
yes                no                               Completed                259      580
Server /chassis #
```

Viewing the Power Statistics

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

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	Server # scope chassis	Enters chassis command mode.
Step 2	Server /chassis # show power-monitoring	Displays the power used by the server, CPU, and memory since the last time it was rebooted.

This example shows how to view the power statistics of an individual domain:

```

Server #scope chassis
Server /chassis # show power-monitoring
Domain      Current (W)  Minimum (W)  Maximum (W)  Average (W)
-----
Platform    180             160           504           180
CPU          53              33            275           53
Memory       2               2             6             2
Server /chassis #

```

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.

Procedure

	Command or Action	Purpose
Step 1	Server # Scope CIMC	Enters the Cisco IMC command mode.
Step 2	Server /CIMC # Scope power-restore-policy	Enters the power restore policy command mode.
Step 3	Server /CIMC/power-restore-policy # set policy {power-off power-on restore-last-state}	Specifies the action to be taken when chassis power is restored. Select one of the following: <ul style="list-style-type: none"> • power-off—Server power will remain off until manually turned on. This is the default action. • power-on—Server power will be turned on when chassis power is restored. • restore-last-state—Server power will return to the state before chassis power was lost.

	Command or Action	Purpose
		When the selected action is power-on , you can select a delay in the restoration of power to the server.
Step 4	Server /CIMC/power-restore-policy # set delay {fixed random}	(Optional) Specifies whether server power will be restored after a fixed or random time. The default is fixed . This command is accepted only if the power restore action is power-on .
Step 5	Server /CIMC/power-restore-policy # set delay-value delay	(Optional) Specifies the delay time in seconds. The range is 0 to 240; the default is 0.
Step 6	Server /CIMC/power-restore-policy # commit	Commits the transaction to the system configuration.

This example sets the power restore policy to power-on with a fixed delay of 180 seconds (3 minutes) and commits the transaction:

```
Server# scope CIMC
Server /CIMC # Scope power-restore-policy
Server /CIMC/power-restore-policy # set policy power-on
Server /CIMC/power-restore-policy *# commit
Server /CIMC/power-restore-policy # set delay fixed
Server /CIMC/power-restore-policy *# set delay-value 180
Server /CIMC/power-restore-policy *# commit
Server /CIMC/power-restore-policy # show detail
Power Restore Policy:
  Power Restore Policy: power-on
  Power Delay Type: fixed
  Power Delay Value(sec): 180

Server /CIMC/power-restore-policy #
```

Configuring Fan Policies

Fan Control Policies

Fan Control Policies enable you to control the fan speed to bring down server power consumption and noise levels. Prior to these fan policies, the fan speed increased automatically when the temperature of any server component exceeded the set threshold. To ensure that the fan speeds were low, the threshold temperatures of components are usually set to high values. While this behavior suited most server configurations, it did not address the following situations:

- Maximum CPU performance

For high performance, certain CPUs must be cooled substantially below the set threshold temperature. This required very high fan speeds which resulted in higher power consumption and increased noise levels.

- Low power consumption

To ensure the lowest power consumption, fans must run very slowly, and in some cases, stop completely on servers that support it. But slow fan speeds resulted in servers overheating. To avoid this situation, it is necessary to run fans at a speed that is moderately faster than the lowest possible speed.

With the introduction of fan policies, you can determine the right fan speed for the server, based on the components in the server. In addition, it allows you to configure the fan speed to address problems related to maximum CPU performance and low power consumption.

Following are the fan policies that you can choose from:

- **Balanced**

This is the default policy. This setting can cool almost any server configuration, but may not be suitable for servers with PCIe cards, since these cards overheat easily.

- **Performance**

This setting can be used for server configurations where maximum fan speed is required for high performance. With this setting, the fan speeds will run at the same speed or higher speed than that of the Balanced fan policy.

- **Low Power**

This setting is ideal for minimal configuration servers that do not contain any PCIe cards.

- **High Power**

This setting can be used for server configurations that require fan speeds ranging from 60 to 85%. This policy is ideal for servers that contain PCIe cards that easily overheat and have high temperatures. The minimum fan speed set with this policy varies for each server platform, but is approximately in the range of 60 to 85%.

- **Maximum Power**

This setting can be used for server configurations that require extremely high fan speeds ranging between 70% to 100%. This policy is ideal for servers that contain PCIe cards that easily overheat and have extremely high temperatures. The minimum fan speed set with this policy varies for each server platform, but is approximately in the range of 70 to 100%.

**Note**

Although you set a fan policy in Cisco IMC, the actual speed that the fan runs at is determined by the configuration requirements of the server. For example, if you set the fan policy to **Balanced**, but the server includes PCIe cards that overheat easily, then the speed of the fans on the server is adjusted automatically to the required minimum fan speed to prevent the overheating. If you have set a fan speed configuration higher than required, the system retains the selected fan speed. The **Applied Fan Policy** displays the actual fan speed that runs on the server.

The **Configuration Status** displays the status of the configured fan policy. This can be one of the following:

- **SUCCESS** —The selected fan policy matches the actual fan speed that runs on the server.
- **PENDING** —The configured fan policy is not in effect yet. This can be due to one of the following:
 - The server is powered off
 - The BIOS POST is not complete

- **FAN POLICY OVERRIDE**—Overrides the specified fan speed with the actual speed determined by the configuration requirements of the server.

Configuring a Fan Policy

The fan policy determines the cooling requirements for your server. Prior to setting the fan policy, you must determine if your server includes PCIe cards that overheat easily.

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope fan-policy	Enters the fan policy command mode.
Step 3	Server /chassis/fan-policy # set fan-policy	<p>Sets the fan policy for the server. It can be one of the following:</p> <ul style="list-style-type: none"> • balanced This is the default policy. This setting can cool almost any server configuration, but may not be suitable for servers with PCIe cards, since these cards overheat easily. • performance This setting can be used for server configurations where maximum fan speed is required for high performance. With this setting, the fan speeds will run at the same speed or higher speed than that of the balanced fan policy. • low-power This setting is ideal for minimal configuration servers that do not contain any PCIe cards. • high-power This setting can be used for server configurations that require fan speeds ranging from 60 to 85%. This policy is ideal for servers that contain PCIe cards that easily overheat and have high temperatures. The minimum fan speed set with this policy varies for each server platform, but is approximately in the range of 60 to 85%. • maximum-power This setting can be used for server configurations that require extremely high fan speeds ranging between 70% to 100%. This policy is ideal for servers that contain PCIe cards that easily overheat and have extremely high temperatures. The minimum fan speed set with

	Command or Action	Purpose
		this policy varies for each server platform, but is approximately in the range of 70 to 100%.
Step 4	Server /chassis/fan-policy # commit	Commits the changes to the server.

This example shows how to set the fan policy to maximum power for a server:

```
server # scope chassis
server /chassis # scope fan-policy
server /chassis/fan-policy # set fan-policy maximum-power
server /chassis/fan-policy* # commit
server /chassis/fan-policy # show detail
Fan Policy: maximum-power
Applied Fan Policy: Max Power
Configuration Status: SUCCESS
server /chassis/fan-policy #
```

Managing the Flexible Flash Controller

Cisco Flexible Flash

Some C-Series Rack-Mount Servers support an internal Secure Digital (SD) memory card for storage of server software tools and utilities. The SD card is hosted by the Cisco Flexible Flash storage adapter.

The SD storage is available to Cisco IMC as a single hypervisor (HV) partition configuration. Prior versions had four virtual USB drives. Three were preloaded with Cisco UCS Server Configuration Utility, Cisco drivers and Cisco Host Upgrade Utility, and the fourth as user-installed hypervisor. A single HV partition configuration is also created when you upgrade to the latest version of Cisco IMC or downgrade to the prior version, and reset the configuration.

For information about the Cisco software utilities and packages, see the *Cisco UCS C-Series Servers Documentation Roadmap* at this URL:

<http://www.cisco.com/go/unifiedcomputing/c-series-doc>

Card Management Feature in the Cisco Flexible Flash Controller

The Cisco Flexible Flash controller supports management of both single and two SD cards as a RAID-1 pair. With the introduction of card management, you can perform the following tasks:



Note

- If you want to upgrade from version 1.4(5e) to 1.5(4) or higher versions, you must first upgrade to version 1.5(2) and then upgrade to a higher version of Cisco IMC.
- Reset the Cisco Flexible Flash controller to load the latest Flex Flash firmware after every Cisco IMC firmware upgrade.

Action	Description
Reset Cisco Flex Flash	Allows you to reset the controller.
Reset Partition Defaults	Allows you to reset the configuration in the selected slot to the default configuration.
Synchronize Card Configuration	Allows you to retain the configuration for an SD card that supports firmware version 253 and later.
Configure Operational Profile	Allows you to configure the SD cards on the selected Cisco Flexible Flash controller.

RAID Partition Enumeration

Non-RAID partitions are always enumerated from the primary card and the enumeration does not depend on the status of the primary card.

Following is the behavior of the RAID partition enumeration when there are two cards in the Cisco Flexible Flash controller:

Scenario	Behavior
Single card	RAID partitions are enumerated if the card is healthy, and if the mode is either Primary or Secondary-active .
Dual paired cards	RAID partitions are enumerated if one of the cards is healthy. When only one card is healthy, all read/write operations occur on this healthy card. You must use UCS SCU to synchronize the two RAID partitions.
Dual unpaired cards	If this scenario is detected when the server is restarting, then neither one of the RAID partitions is enumerated. If this scenario is detected when the server is running, when a user connects a new SD card, then the cards are not managed by the Cisco Flexible Flash controller. This does not affect the host enumeration. You must pair the cards to manage them. You can pair the cards using the Reset Partition Defaults or Synchronize Card Configuration options.

Upgrading from Single Card to Dual Card Mirroring with FlexFlash

You can upgrade from a single card mirroring to dual card mirroring with FlexFlash in one of the following methods:

- Add an empty FlexFlash to the server, and then upgrade the SD firmware version from prior versions to the latest version

For information on how to complete this task, see

- Upgrade the FlexFlash firmware to the latest version and then add an empty card to the server.

Prior to using either of these methods, you must keep in mind the following guidelines:

- To create RAID1 mirroring, the empty card that you want to add to the server must be of the exact size of the card that is already in the server. Identical card size is a must to set up RAID1 mirroring.
- Ensure that the card with valid data in the Hypervisor partition is marked as the primary healthy card. You can determine this state either in the Cisco IMC GUI or from the Cisco IMC CLI. To mark the state of the card as primary healthy, you can either use the **Reset Configuration** option in the Cisco IMC GUI or run the **reset-config** command in the Cisco IMC CLI. When you reset the configuration of a particular card, the secondary card is marked as secondary active unhealthy.
- In a Degraded RAID health state all read-write transactions are done on the healthy card. In this scenario, data mirroring does not occur. Data mirroring occurs only in the Healthy RAID state.
- Data mirroring is only applicable to RAID partitions. In the C-series servers, only Hypervisor partitions operate in the RAID mode.
- If you have not configured SD cards for use with prior versions, then upgrading to the latest version loads the latest 253 firmware and enumerates all four partitions to the host.

While upgrading versions of the FlexFlash, you may see the following error message:

```
Unable to communicate with Flexible Flash controller: operation ffCardsGet, status
CY_AS_ERROR_INVALID_RESPONSE"
```

In addition, the card status may be shown as **missing**. This error occurs because you accidentally switched to an alternate release or a prior version, such as 1.4(x). In this scenario, you can either revert to the latest version, or you can switch back to the FlexFlash 1.4(x) configuration. If you choose to revert to the latest Cisco IMC version, then the Cisco FlexFlash configuration remains intact. If you choose to switch back to the prior version configuration, you must reset the Flexflash configuration. In this scenario, you must be aware of the following:

- If multiple cards are present, and you revert to a prior version, then the second card cannot be discovered or managed.
- If the card type is SD253, then you must run the **reset-config** command twice from the Cisco IMC CLI - once to reload the old firmware on the controller and to migrate SD253 to SD247 type, and the second time to start the enumeration.

Configuring the Flexible Flash Controller Properties for C220 M3, C240 M3, and C460 M4 Servers

Before You Begin

- You must log in with admin privileges to perform this task.
- Cisco Flexible Flash must be supported by your platform.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope flexflash <i>index</i>	Enters the Cisco Flexible Flash controller command mode for the specified controller. At this time, the only permissible <i>index</i> value is FlexFlash-0 .
Step 3	Server /chassis/flexflash # scope operational-profile	Enters the operational profile command mode.
Step 4	Server /chassis/flexflash/operational-profile # set raid-primary-member { slot1 slot2 }	Specifies the slot in which the primary copy of the data resides. Important Currently, Cisco Flexible Flash cards are supported in slot 1 and slot 2. Therefore, you can specify slot1 or slot2 .
Step 5	Server /chassis/flexflash/operational-profile # set raid-secondary-role { active initializing }	The role of the secondary RAID. The currently supported value is active .
Step 6	Server /chassis/flexflash/operational-profile # set read-error-count-threshold	Specifies the number of read errors that are permitted while accessing the Cisco Flexible Flash card. If the number of errors exceeds this threshold, the Cisco Flexible Flash card is disabled and you must reset it manually before Cisco IMC attempts to access it again. To specify a read error threshold, enter an integer between 1 and 255. To specify that the card should never be disabled regardless of the number of errors encountered, enter 0 (zero).
Step 7	Server /chassis/flexflash/operational-profile # set write-error-count-threshold	Specifies the number of write errors that are permitted while accessing the Cisco Flexible Flash card. If the number of errors exceeds this threshold, the Cisco Flexible Flash card is disabled and you must reset it manually before Cisco IMC attempts to access it again. To specify a write error threshold, enter an integer between 1 and 255. To specify that the card should never be disabled regardless of the number of errors encountered, enter 0 (zero).

	Command or Action	Purpose
Step 8	<pre>Server /chassis/flexflash/operational-profile # set virtual-drives-enabled list</pre>	<p>Specifies a list of virtual drives to be made available to the server as a USB-style drive. The options are as follows:</p> <ul style="list-style-type: none"> • SCU—The server can access the Cisco UCS Server Configuration Utility. • DRIVERS—The server can access the Cisco drivers volume. • HV—The server can access a user-installed hypervisor. • HUU—The server can access the Cisco Host Upgrade Utility. <p>When specifying more than one option, you must enclose the list in quotation marks ("").</p>
Step 9	<pre>Server /chassis/adapter # commit</pre>	Commits the transaction to the system configuration.

This example shows how to configure the properties of the Flash controller:

```
Server# scope chassis
Server /chassis # scope flexflash FlexFlash-0
Server /chassis/flexflash # scope operational-profile
Server /chassis/flexflash/operational-profile # set read-error-count-threshold 100
Server /chassis/flexflash/operational-profile # set write-error-count-threshold 100
Server /chassis/flexflash/operational-profile *# set raid-primary-member slot1
Server /chassis/flexflash/operational-profile # set raid-secondary-role active
Server /chassis/flexflash/operational-profile *# set virtual-drives-enabled "SCU HUU"
Server /chassis/flexflash/operational-profile *# commit
Server /chassis/flexflash/operational-profile #
```

Configuring the Flexible Flash Controller Properties for C220 M4 and C240 M4 Servers



Note

- In the **Mirror** mode, **Slot1 Read/Write Error Threshold** is applicable to both the SD cards, if two cards are present.
- In the **Util** Mode, **Slot1 Read/Write Error Threshold** is applicable to the card in slot 1 and **Slot2 Read/Write Error Threshold** is applicable to the card in slot 2.

Before You Begin

- You must log in with admin privileges to perform this task.
- Cisco Flexible Flash must be supported by your platform.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope flexflash index	Enters the Cisco Flexible Flash controller command mode for the specified controller. At this time, the only permissible <i>index</i> value is FlexFlash-0 .
Step 3	Server /chassis/flexflash # scope operational-profile	Enters the operational profile command mode.
Step 4	Server /chassis/flexflash/operational-profile # set read-error-count-slot1-threshold threshold	Specifies the number of read errors that are permitted while accessing the Cisco Flexible Flash card in slot 1. If the number of errors exceeds this threshold, the Cisco Flexible Flash card is disabled and you must reset it manually before Cisco IMC attempts to access it again. To specify a read error threshold, enter an integer between 1 and 255. To specify that the card should never be disabled regardless of the number of errors encountered, enter 0 (zero).
Step 5	Server /chassis/flexflash/operational-profile # set read-error-count-slot2-threshold threshold	Specifies the number of read errors that are permitted while accessing the Cisco Flexible Flash card in slot 2. If the number of errors exceeds this threshold, the Cisco Flexible Flash card is disabled and you must reset it manually before Cisco IMC attempts to access it again. To specify a read error threshold, enter an integer between 1 and 255. To specify that the card should never be disabled regardless of the number of errors encountered, enter 0 (zero).
Step 6	Server /chassis/flexflash/operational-profile # set write-error-count-slot1-threshold threshold	Specifies the number of write errors that are permitted while accessing the Cisco Flexible Flash card in slot 1. If the number of errors exceeds this threshold, the Cisco Flexible Flash card is disabled and you must reset it manually before Cisco IMC attempts to access it again. To specify a write error threshold, enter an integer between 1 and 255. To specify that the card should never be disabled regardless of the number of errors encountered, enter 0 (zero).
Step 7	Server /chassis/flexflash/operational-profile # set write-error-count-slot2-threshold threshold	Specifies the number of write errors that are permitted while accessing the Cisco Flexible Flash card in slot 2. If the number of errors exceeds this threshold, the Cisco Flexible Flash card is disabled and you must reset it manually before Cisco IMC attempts to access it again. To specify a write error threshold, enter an integer between 1 and 255. To specify that the card should never be disabled regardless of the number of errors encountered, enter 0 (zero).

	Command or Action	Purpose
Step 8	Server /chassis/flexflash/operational-profile # commit	Commits the transaction to the system configuration.

This example shows how to configure the properties of the Flash controller:

```
Server# scope chassis
Server /chassis # scope flexflash FlexFlash-0
Server /chassis/flexflash # scope operational-profile
Server /chassis/flexflash/operational-profile # set read-err-count-slot1-threshold 9
Server /chassis/flexflash/operational-profile *# set read-err-count-slot2-threshold 10
Server /chassis/flexflash/operational-profile *# set write-err-count-slot1-threshold 11
Server /chassis/flexflash/operational-profile *# set write-err-count-slot2-threshold 12
Server /chassis/flexflash/operational-profile *# commit
Server /chassis/flexflash/operational-profile # show detail
FlexFlash Operational Profile:
  Firmware Operating Mode: util
  SLOT1 Read Error Threshold: 9
  SLOT1 Write Error Threshold: 11
  SLOT2 Read Error Threshold: 10
  SLOT2 Write Error Threshold: 12
```

Booting from the Flexible Flash

You can specify a bootable virtual drive on the Cisco Flexible Flash card that will override the default boot priority the next time the server is restarted, regardless of the default boot order defined for the server. The specified boot device is used only once. After the server has rebooted, this setting is ignored.



Note

Before you reboot the server, ensure that the virtual drive you select is enabled on the Cisco Flexible Flash card.

After you upgrade to the latest version of Cisco IMC or downgrade to a prior version, and reset the configuration, the server boots through the HV partition only. If the prior version has valid SCU data, then the server will boot through SCU in spite of single HV partition.

Before You Begin

- You must log in with admin privileges to perform this task.
- Cisco Flexible Flash must be supported by your platform.

Procedure

	Command or Action	Purpose
Step 1	Server# scope bios	Enters the BIOS command mode.
Step 2	Server /bios # set boot-override {None HV}	The virtual drive from which the server attempts to boot the next time it is restarted. This can be one of the following:

	Command or Action	Purpose
		<ul style="list-style-type: none"> • None—The server uses the default boot order • HV—The server boots from the hypervisor virtual drive
Step 3	Server /bios # commit	Commits the transaction to the system configuration.

This example specifies that the server boots from the Cisco UCS Server Configuration Utility the next time it is restarted:

```
Server# scope bios
Server /bios # set boot-override HV
Committing the boot override BIOS will try boot to
the specified boot device first. Failure to detect
the boot device BIOS will boot from the list
configured in the BIOS boot order.
Server /bios *# commit
Server /bios #
```

Resetting the Flexible Flash Controller

In normal operation, it should not be necessary to reset the Cisco Flexible Flash. We recommend that you perform this procedure only when explicitly directed to do so by a technical support representative.



Note

This operation will disrupt traffic to the virtual drives on the Cisco Flexible Flash controller.

Before You Begin

- You must log in with admin privileges to perform this task.
- Cisco Flexible Flash must be supported by your platform.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope flexflash <i>index</i>	Enters the Cisco Flexible Flash controller command mode for the specified controller. At this time, the only permissible <i>index</i> value is FlexFlash-0 .
Step 3	Server /chassis/flexflash # reset	Resets the Cisco Flexible Flash controller.

This example resets the flash controller:

```
Server# scope chassis
Server /chassis # scope flexflash FlexFlash-0
Server /chassis/flexflash # reset
This operation will reset Cisco Flexible Flash controller.
Host traffic to VDs on this device will be disrupted.
Continue?[y|N] y

Server /chassis/flexflash #
```

Configuring the Flexible Flash Controller Cards in Mirror Mode

Configuring controller cards in mirror mode:

Before You Begin

- You must log in with admin privileges to perform this task.
- Cisco Flexible Flash must be supported by your platform.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope flexflash	Enters the Cisco Flexible Flash controller command mode for the specified controller.
Step 3	Server /chassis/flexflash # configure-cards-mirror SLOT-1.	Configures SLOT-1 as healthy primary.
Step 4	Enter y at the Enable auto sync(by default auto sync is disabled)?[y N] prompt.	Sync the card on slot 1 with the card on slot 2.
Step 5	Enter y at the Set Mirror Partition Name(Default name is Hypervisor)?[y N] prompt.	Enables you to set the name of the mirror partition.
Step 6	Enter the name of the mirror partition at the Enter Partition Name Mirror Partition Name :Hypervisor prompt.	Sets the name of the mirror partition. The following message displays: This action will mark the SLOT-1 as healthy primary slot and SLOT-2 (if card existing) as unhealthy secondary. This operation may disturb the host connectivity as well.
Step 7	Enter y at the Continue?[y N] y prompt.	Configures the cards in Mirror mode and sets the card in SLOT-1 as primary healthy and SLOT-2 (if card existing) as unhealthy secondary.

	Command or Action	Purpose
Step 8	Server /chassis/flexflash # show physical-drive	<p>(Optional) Displays the status of the configured cards.</p> <p>Note</p> <ul style="list-style-type: none"> • When the cards are configured in auto sync mode and if the cards go out of sync then syncing from a good card with the bad card will start automatically. • If the cards are configured in auto sync mode and if a card goes out of sync, then syncing from a good card starts automatically. • If the server is running with one auto mirror healthy card and if a new card is inserted then the metadata is automatically created on the new card and data syncing starts from auto mirror configured card to the new paired card.

This example shows how to configure the controller cards in mirror mode:

```

Server# scope chassis
Server /chassis # scope flexflash
Server /chassis/flexflash # configure-cards-mirror SLOT-1
Enable auto sync(by default auto sync is disabled)?[y|N]y
Set Mirror Partition Name(Default name is Hypervisor)?[y|N]y
Enter Partition Name Mirror Partition Name :hfldjslkjdfs
This action will mark the SLOT-1 as healthy primary slot and SLOT-2 (if card existing) as
unhealthy secondary.
This operation may disturb the host connectivity as well.
Continue?[y|N]y
Server /chassis/flexflash # show detail
Controller FlexFlash-0:
  Product Name: Cisco FlexFlash
  Controller HW: FX3S
  Vendor: Cypress
  Firmware Version: 1.3.2 build 159
  Firmware Operating Mode: mirror
  Firmware Configured Mode: mirror
  Has Error: No
  Error Description:
  Internal State: Disconnected
  Controller Status: OK
  Cards Manageable: Yes
  Startup Firmware Version: 1.3.2 build 159

Server /chassis/flexflash # show physical-drive
Physical Drive  Status    Controller  Card Type        Card mode        Health    Sync
Mode
-----
SLOT-1          present    FlexFlash-0  FX3S configured  mirror-primary    healthy   auto
SLOT-2          present    FlexFlash-0  FX3S configured  mirror-secondary  unhealthy auto

Server /chassis/flexflash #

```

Configuring Controller Cards in Util Mode

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope flexflash	Enters the Cisco Flexible Flash controller command mode for the specified controller.
Step 3	Server /chassis/flexflash # configure-cards-util SLOT-1	Configures card in slot-1 as Util card with four partitions - scu, huu, drivers, and user partition).
Step 4	Enter y at the Set User Partition Name on Util Card (Default name is UserPartition)?[y N] prompt.	Enables you to set the name of the user partition.
Step 5	Enter the name of the user partition at the Enter User Partiton Name:UserPartition prompt.	Sets the name of the user partition.
Step 6	Enter y at the Set Partition Name on Non Util Card(Default name is Hypervisor)?[y N] prompt.	Enables you to set the name of the single partition on non-Util card.
Step 7	Enter the name of the mirror partition at the Enter Partition Name of Non Util Card:Hypervisor prompt.	Sets the name of the non-Util partition. The following message displays: This action will create util configuration (4 partition) on SLOT-1 card and non-util configuration(1 partition) on SLOT-2 (if card existing). This operation may disturb the host connectivity as well.
Step 8	Enter y at the Continue?[y N] y prompt.	Configures the cards in the Util mode; creates four partitions of the card on SLOT-1 and sets it as primary healthy, and SLOT-2 (if card existing) as healthy secondary.
Step 9	Server /chassis/flexflash # show physical-drive	(Optional) Displays the status of the configured cards. Note On a Util card with four partitions, an extra partition is created and used during OOB update of SCU, HUU, and drivers.

This example shows how to configure the controller cards in Util mode:

```
Server# scope chassis
Server /chassis # scope flexflash
Server /chassis/flexflash # configure-cards-mirror SLOT-1
Set User Partiton Name on Util Card (Default name is UserPartition)?[y|N]y
Enter User Partiton Name :UserPartition
Set Partition Name on Non Util Card(Default name is Hypervisor)?[y|N]y
```



```

Enter Partition Name of Non Util Card :Hypervisor
This action will create util configuration (4 partitons) on SLOT-1 card and
non-util configuration(1 partition) on SLOT-2 (if card existing)
This operation may disturb the host connectivity as well.
Continue?[y|N]y

Server /chassis/flexflash # show detail
Controller FlexFlash-0:
  Product Name: Cisco FlexFlash
  Controller HW: FX3S
  Vendor: Cypress
  Firmware Version: 1.3.2 build 159
  Firmware Operating Mode: util
  Firmware Configured Mode: util
  Has Error: No
  Error Description:
  Internal State: Disconnected
  Controller Status: OK
  Cards Manageable: Yes
  Startup Firmware Version: 1.3.2 build 159

Server /chassis/flexflash # show physical-drive
Physical Drive Status Controller Card Type Card mode Health Sync
Mode
-----
SLOT-1 present FlexFlash-0 FX3S configured util healthy NA
SLOT-2 present FlexFlash-0 FX3S configured util healthy NA

Server /chassis/flexflash #

```

Configuring the Flexible Flash Controller Firmware Mode

Before You Begin

- You must log in with admin privileges to perform this task.
- Cisco Flexible Flash must be supported by your platform.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope flexflash	Enters the Cisco Flexible Flash controller command mode for the specified controller.
Step 3	Server /chassis/flexflash # configure-firmware-mode .	Switches the firmware mode from the current state to the other. The following messages appear: This action will switch firmware mode from util to mirror This operation may disturb the host connectivity as well.
Step 4	Enter y at the Continue?[y N] y prompt.	Switches the firmware mode from mirror to Util or Util to mirror.

This example shows how to configure the firmware mode of a controller:

```
Server# scope chassis
Server /chassis # scope flexflash
Server /chassis/flexflash # configure-firmware-mode
This action will switch fimrware mode from util to mirror
This operation may disturb the host connectivity as well.
Continue?[y|N]y
Server /chassis/flexflash # show detail
Controller FlexFlash-0:
  Product Name: Cisco FlexFlash
  Controller HW: FX3S
  Vendor: Cypress
  Firmware Version: 1.3.2 build 159
  Firmware Operating Mode: mirror
  Firmware Configured Mode: mirror
  Has Error: Yes
  Error Description:
  Internal State: Failed
  Controller Status: Mode Mismatch SDcard(s)
  Cards Manageable: NO
  Startup Firmware Version: 1.3.2 build 159

*+-----+
+ Based on type and number of cards please execute mirror/util Configuration +
+ (configure-mirror/configure-util) commands to start monitoring/managing SD cards +
+                                     OR                                     +
+                               Switch Firmware Operating Mode                               +
+-----+

Server /chassis/flexflash #
```

Resetting the Configuration of the Cards in the Cisco Flexible Flash Controller

You can reset the configuration of a selected slot in the Cisco Flexible Flash controller to the default configuration.

When you reset the configuration of the slots in the Cisco Flexible Flash card, the following situations occur:

- The card in the selected slot is marked as primary healthy.
- The card in the other slot is marked as secondary-active unhealthy.
- One RAID partition is created.
- The card read/write error counts and read/write threshold are set to 0.
- Host connectivity could be disrupted.

If you upgrade to the latest version and select reset configuration option, a single hypervisor (HV) partition is created, and the existing four partition configurations are erased. This may also result in data loss. You can retrieve the lost data only if you have not done any data writes into HV partition, and downgrade to prior version.

Before You Begin

- You must log in with admin privileges to perform this task.
- Cisco Flexible Flash must be supported on your server.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope flexflash index	Enters the Cisco Flexible Flash controller command mode for the specified controller. At this time, the only permissible <i>index</i> value is FlexFlash-0 .
Step 3	Server /chassis/flexflash # reset-partition-defaults primary slot ID	Resets the configuration of the selected slot to the default configuration.

This example shows how to reset the configuration from a slot to the default configuration:

```
Server# scope chassis
Server /chassis # scope flexflash FlexFlash-0
Server /chassis/flexflash # reset-partition-defaults slot1
```

This action will mark the slot1 as the healthy primary slot, and slot2 (if card exists) as unhealthy secondary active.

This operation may disturb the host connectivity as well.

Continue? [y|N] y

```
Server /chassis/flexflash/operational-profile #
```

Retaining the Configuration of the Flexible Flash Controller

You can copy the configuration of a given slot in the Cisco Flexible Flash card to the other slot. However, the slot from which the configuration is copied from must be of the SDK523 type. You can retain the configuration in the following situations:

- There are two unpaired FlexFlash
- The server is operating from a single FlexFlash, and an unpaired FlexFlash is in the other slot.
- One FlexFlash supports firmware version 253, and the other FlexFlash is unpartitioned.

Before You Begin

- You must log in with admin privileges to perform this task.
- Cisco Flexible Flash must be supported on your server.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.

	Command or Action	Purpose
Step 2	Server /chassis # scope flexflash <i>index</i>	Enters the Cisco Flexible Flash controller command mode for the specified controller. At this time, the only permissible <i>index</i> value is FlexFlash-0 .
Step 3	Server /chassis/flexflash # synchronize-card-configuration <i>primary slot ID</i>	Copies the configuration from the primary slot to the secondary slot.

This example shows how to copy the configuration from one slot to the other:

```
Server# scope chassis
Server /chassis # scope flexflash FlexFlash-0
Server /chassis/flexflash # synchronize-card-configuration slot1
```

This action will copy the config of slot1 to both the slots, mark slot1 as healthy, primary slot and slot2 (card must be present) as unhealthy secondary active. This operation may disturb the host connectivity as well.
Continue? [y|N] y

```
Server /chassis/flexflash/operational-profile #
```

Adding an ISO Image Configuration

Before You Begin

- You must log in with admin privileges to perform this task.
- Cisco Flexible Flash must be supported by your platform.
- Card must be in Util mode.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server/chassis # scope flexflash	Enters the Cisco Flexible Flash controller command mode for the specified controller.
Step 3	Server/chassis/flexflash/ # scope vd-image-configs	Enters the virtual drive configuration command mode.
Step 4	Server/chassis/flexflash/vd-image-configs # vd-image-cifs <i>virtual_drive</i> <i>//serverip/remote_share <remote_file></i>	Server username: prompt is displayed. 1 Server username: <i>server username</i> Enter a server username. 2 Server password: <i>server password</i> Enter a server password.

	Command or Action	Purpose
		3 Confirm password: <i>server password</i> Repeat the server password.
Step 5	Server/chassis/flexflash/vd-image-configs # vd-image-nfs <i>virtual_drive</i> <i>serverip:/remote_share <remote_file></i>	Server username: prompt is displayed.
Step 6	Server/chassis/flexflash/vd-image-configs # show detail	(Optional) Displays the details of the virtual drives.

```

Server # scope chassis
Server/chassis # scope flexflash
Server/chassis/flexflash # scope vd-image-configs
Server/chassis/flexflash/vd-image-configs # vd-image-cifs SCU //10.106.146.69/pdagguma
/softwares/ucs-cxx-scu-3.1.9.iso
Server/chassis/flexflash/vd-image-configs # show detail
Virtual Drive SCU:
  Mount Type: cifs
  Remote Share: //10.106.146.69/pdagguma
  Remote File: /softwares/ucs-cxx-scu-3.1.9.iso
  Mount Options:
"username=pdagguma,password*****,soft,nounix,noserverino,rsz=3072,wsz=3072"
Virtual Drive HUU:
  Mount Type: cifs
  Remote Share: //10.101
  Remote File: DFLJD_huu.iso
  Mount Options:
"username=pdagguma,password*****,soft,nounix,noserverino,rsz=3072,wsz=3072"
Virtual Drive Drivers:
  Mount Type: None
  Remote Share: None
  Remote File: None
  Mount Options: None
Server/chassis/flexflash/vd-image-configs #

```

Enabling Virtual Drives

Before You Begin

- You must log in with admin privileges to perform this task.
- Cisco Flexible Flash must be supported by your platform.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope flexflash	Enters the Cisco Flexible Flash controller command mode for the specified controller.

	Command or Action	Purpose
Step 3	Server /chassis/ flexflash # scope virtual-drive	Enters the virtual drive command mode for the specified controller.
Step 4	Server /chassis/flexflash/virtual-drive # enable-vds "SCU HUU dlfd"	Enables the virtual drives to the host.

This example shows how to enable the virtual drives to the host:

```
Server# scope chassis
Server /chassis # scope flexflash
Server /chassis/flexflash # scope virtual-drive
Server /chassis/flexflash/virtual-drive # enable-vds "SCU HUU dlfd"
Server /chassis/flexflash/virtual-drive # show detail
```

```
Virtual Drive SCU:
  VD ID: 1
  Size: 2560 MB
  VD Scope: Non-Raid
  VD Status: Healthy
  VD Type: Removable
  Read/Write: R/W
  Host Accessible: Connected
  Operation in progress: NA
  Last Operation completion status: none
Virtual Drive HUU:
  VD ID: 2
  Size: 1536 MB
  VD Scope: Non-Raid
  VD Status: Healthy
  VD Type: Removable
  Read/Write: R/W
  Host Accessible: Connected
  Operation in progress: NA
  Last Operation completion status: none
Virtual Drive Drivers:
  VD ID: 3
  Size: 8192 MB
  VD Scope: Non-Raid
  VD Status: Healthy
  VD Type: Removable
  Read/Write: R/W
  Host Accessible: Not-Connected
  Operation in progress: NA
  Last Operation completion status: none
Virtual Drive dlfd:
  VD ID: 4
  Size: 9952 MB
  VD Scope: Non-Raid
  VD Status: Healthy
  VD Type: Removable
  Read/Write: R/W
  Host Accessible: Connected
  Operation in progress: NA
  Last Operation completion status: none
Virtual Drive dfdff:
  VD ID: 5
  Size: 30432 MB
  VD Scope: Non-Raid
  VD Status: Healthy
  VD Type: Removable
  Read/Write: R/W
  Host Accessible: Not-Connected
  Operation in progress: NA
  Last Operation completion status: none
```

```
Server /chassis/flexflash/virtual-drive #
```

Erasing Virtual Drives

Before You Begin

- You must log in with admin privileges to perform this task.
- Cisco Flexible Flash must be supported by your platform.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope flexflash	Enters the Cisco Flexible Flash controller command mode for the specified controller.
Step 3	Server /chassis/ flexflash # scope virtual-drive	Enters the virtual drive command mode for the specified controller.
Step 4	Server /chassis/flexflash/virtual-drive # erase-vds "SCU HUU"	Initiates erasing FAT32.

This example shows how to erase data on the virtual drives:

```
Server# scope chassis
Server /chassis # scope flexflash
Server /chassis/flexflash # scope virtual-drive
Server /chassis/flexflash/virtual-drive # erase-vds "SCU HUU"
Server /chassis/flexflash/virtual-drive # show detail
```

```
Virtual Drive SCU:
  VD ID: 1
  Size: 2560 MB
  VD Scope: Non-Raid
  VD Status: Healthy
  VD Type: Removable
  Read/Write: R/W
  Host Accessible: Not-Connected
  Operation in progress: Erasing
  Last Operation completion status: none
Virtual Drive HUU:
  VD ID: 2
  Size: 1536 MB
  VD Scope: Non-Raid
  VD Status: Healthy
  VD Type: Removable
  Read/Write: R/W
  Host Accessible: Connected
  Operation in progress: Erase-Pending
  Last Operation completion status: none
Virtual Drive Drivers:
  VD ID: 3
  Size: 8192 MB
  VD Scope: Non-Raid
  VD Status: Healthy
  VD Type: Removable
```

```

Read/Write: R/W
Host Accessible: Not-Connected
Operation in progress: NA
Last Operation completion status: none
Virtual Drive dlfd:

Server /chassis/flexflash/virtual-drive #

```

Syncing Virtual Drives

Before You Begin

- You must log in with admin privileges to perform this task.
- Cisco Flexible Flash must be supported by your platform.
- The cards must be configured in manual mirror mode.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope flexflash	Enters the Cisco Flexible Flash controller command mode for the specified controller.
Step 3	Server /chassis/ flexflash # scope virtual-drive	Enters the virtual drive command mode for the specified controller.
Step 4	Server /chassis/flexflash/virtual-drive # sync-vds Hypervisor	<p>Syncs the virtual drives.</p> <p>Note</p> <ul style="list-style-type: none"> • If the cards are configured in auto sync mode and if a card goes out of sync, then syncing from a good card starts automatically. • If the server is running with one auto mirror healthy card and if a new card is inserted then the metadata is automatically created on the new card and data syncing starts from auto mirror configured card to the new paired card.

This example shows how to sync the virtual drives:

```

Server# scope chassis
Server /chassis # scope flexflash
Server /chassis/flexflash # scope virtual-drive
Server /chassis/flexflash/virtual-drive # sync-vds Hypervisor
Server /chassis/flexflash/virtual-drive # show detail

Virtual Drive Hypervisor:
  VD ID: 1
  Size: 30432 MB
  VD Scope: Raid
  VD Status: Degraded
  VD Type: Removable
  Read/Write: R/W

```



```
Host Accessible: Not-Connected
Operation in progress: Syncing(Manual)
Last Operation completion status: none
```

```
Server /chassis/flexflash/virtual-drive #
```

Configuring DIMM Black Listing

DIMM Black 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 blacklisting, Cisco IMC monitors the memory test execution messages and blacklists 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 blacklisted only when Uncorrectable errors occur. When a DIMM gets blacklisted, 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 blacklisted for 16000 Correctable errors.

Enabling DIMM Black Listing

Before You Begin

You must be logged in as an administrator.

Procedure

	Command or Action	Purpose
Step 1	Server# scope dimm-blacklisting /	Enters the DIMM blacklisting mode.
Step 2	Server /dimm-blacklisting # set enabled {yes no}	Enables or disables DIMM blacklisting.
Step 3	Server /dimm-blacklisting* # commit	Commits the transaction to the system configuration.

The following example shows how to enable DIMM blacklisting:

```
Server# scope dimm-blacklisting
Server /dimm-blacklisting # set enabled yes
Server /dimm-blacklisting* # commit
Server /dimm-blacklisting #
```

```
Server /dimm-blacklisting # show detail

DIMM Blacklisting:
  Enabled: yes
```

Configuring BIOS Settings

Viewing BIOS Status

Procedure

	Command or Action	Purpose
Step 1	Server# scope bios	Enters the BIOS command mode.
Step 2	Server /bios # show detail	Displays details of the BIOS status.

The BIOS status information contains the following fields:

Name	Description
BIOS Version	The version string of the running BIOS.
Boot Order	The legacy boot order of bootable target types that the server will attempt to use.
Boot Override Priority	This can be None, or HV.
FW Update/Recovery Status	The status of any pending firmware update or recovery action.
UEFI Secure Boot	Enables or Disables UEFI secure boot.
Configured Boot Mode	The boot mode in which h BIOS will try to boot the devices.
Actual Boot Mode	The actual boot mode in which BIOS booted the devices.
Last Configured Boot Order Source	The last configured boot order source by BIOS.

This example displays the BIOS status:

```
Server# scope bios
Server /bios # show detail
Server /bios # show detail
BIOS Version: "C460M1.1.2.2a.0 (Build Date: 01/12/2011)"
Boot Order: EFI,CDROM,HDD
Boot Override Priority:
```

```

FW Update/Recovery Status: NONE
FW Update/Recovery Progress: 100
Server /bios #

Server# scope bios
Server /bios # show detail
BIOS:
  BIOS Version: "C240M3.2.0.0.15 (Build Date: 03/16/2014)"
  Boot Order: (none)
  Boot Override Priority:
  FW Update/Recovery Status: None, OK
  UEFI Secure Boot: disabled
  Configured Boot Mode: Legacy
  Actual Boot Mode: Legacy
  Last Configured Boot Order Source: CIMC
Server /bios #

```

Configuring Main BIOS Settings

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# scope bios	Enters the BIOS command mode.
Step 2	Server /bios # scope main	Enters the main BIOS settings command mode.
Step 3	Configure the BIOS settings.	<p>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 one the following topics:</p> <ul style="list-style-type: none"> • Main BIOS Parameters for C22 and C24 Servers • Main BIOS Parameters for C220 and C240 Servers • Main BIOS Parameters for C460 Servers • Main Tab for C220M4 and C240M4 Servers • Main BIOS Parameters for C3160 Servers
Step 4	Server /bios/main # commit	<p>Commits the transaction to the system configuration.</p> <p>Changes are applied on the next server reboot. If server power is on, you are prompted to choose whether to reboot now.</p>

This example configures the BIOS to pause the boot upon a critical POST error and commits the transaction:

```

Server# scope bios
Server /bios # scope main
Server /bios/main # set POSTErrorPause Enabled
Server /bios/main *# commit
Changes to BIOS set-up parameters will require a reboot.
Do you want to reboot the system?[y|N] n

```

```
Changes will be applied on next reboot.
Server /bios/main #
```

Configuring Advanced BIOS Settings



Note

Depending on your installed hardware, some configuration options described in this topic may not appear.

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# scope bios	Enters the BIOS command mode.
Step 2	Server /bios # scope advanced	Enters the advanced BIOS settings command mode.
Step 3	Configure the BIOS settings.	<p>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 one the following topics:</p> <ul style="list-style-type: none"> • Advanced BIOS Parameters for C22 and C24 Servers • Advanced BIOS Parameters for C220 and C240 Servers • Advanced BIOS Parameters for C460 Servers • Advanced Tab for C220M4 and C240M4 Servers • Advanced BIOS Parameters for C3160 Servers
Step 4	Server /bios/advanced # commit	<p>Commits the transaction to the system configuration.</p> <p>Changes are applied on the next server reboot. If server power is on, you are prompted to choose whether to reboot now.</p>

This example enables low voltage DDR memory mode and commits the transaction:

```
Server# scope bios
Server /bios # scope advanced
Server /bios/advanced # set LvDDRMMode Enabled
Server /bios/advanced *# commit
Changes to BIOS set-up parameters will require a reboot.
Do you want to reboot the system?[y|N] n
Changes will be applied on next reboot.
Server /bios/advanced #
```

Configuring Server Management BIOS Settings

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# scope bios	Enters the BIOS command mode.
Step 2	Server /bios # scope server-management	Enters the server management BIOS settings command mode.
Step 3	Configure the BIOS settings.	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 one the following topics: <ul style="list-style-type: none"> • Server Management BIOS Parameters for C22 and C24 Servers • Server Management BIOS Parameters for C220 and C240 Servers • Server Management BIOS Parameters for C460 Servers • Server Management Tab for C220M4 and C240M4 Servers • Server Management Tab for C3160 Servers
Step 4	Server /bios/server-management # commit	Commits the transaction to the system configuration. Changes are applied on the next server reboot. If server power is on, you are prompted to choose whether to reboot now.

This example enables automatic detection of the BMC and commits the transaction:

```
Server# scope bios
Server /bios # scope server-management
Server /bios/server-management # set BMCnP Enabled
Server /bios/server-management *# commit
Changes to BIOS set-up parameters will require a reboot.
Do you want to reboot the system?[y|N] n
Changes will be applied on next reboot.
Server /bios/server-management #
```

Restoring BIOS Defaults

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# scope bios	Enters the BIOS command mode.
Step 2	Server /bios # bios-setup-default	Restores BIOS default settings. This command initiates a reboot.

This example restores BIOS default settings:

```
Server# scope bios
Server /bios # bios-setup-default
This operation will reset the BIOS set-up tokens to factory defaults.
All your configuration will be lost.
Changes to BIOS set-up parameters will initiate a reboot.
Continue?[y|N]y
```

Entering BIOS Setup

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# scope bios	Enters the BIOS command mode.
Step 2	Server /bios # enter-bios-setup	Enters BIOS setup on reboot.

This example enables you to enter BIOS setup:

```
Server# scope bios
Server /bios # enter-bios-setup
This operation will enable Enter BIOS Setup option.
Host must be rebooted for this option to be enabled.
Continue?[y|N]y
```

Restoring BIOS Manufacturing Custom Defaults

In instances where the components of the BIOS no longer function as desired, you can restore the BIOS set up tokens to the manufacturing default values.

**Note**

This action is only available for some C-Series servers.

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# scope bios	Enters the BIOS command mode.
Step 2	Server /bios # restore-mfg-defaults	Restores the set up tokens to the manufacturing default values.

This example shows how to restore the BIOS set up tokens to the manufacturing default values:

```
Server # scope bios
Server /bios # restore-mfg-defaults
This operation will reset the BIOS set-up tokens to manufacturing defaults.
The system will be powered on.
Continue? [y|n] N
Server /bios #
```

Updating Firmware on Server Components

**Important**

If any firmware or BIOS updates are in progress, do not reset the server until those tasks are complete.

Before You Begin

You must log in with user or admin privileges to perform this task.
Server must be powered off.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters chassis command mode.
Step 2	Server /chassis # scope firmware	Enters firmware command mode.
Step 3	Server /chassis/firmware # show detail	Displays the firmware update required on some components message.

	Command or Action	Purpose
Step 4	Server /chassis/firmware # update-all	Updates the firmware on the server components.

This example resets the server:

```
Server# scope chassis
Server /chassis # scope firmware
Server /chassis / firmware # show detail
```

Firmware update required on some components,
please run update-all (under chassis/firmware scope).

```
Server /chassis / firmware # update-all
```

Viewing Product ID (PID) Catalog Details

Procedure

	Command or Action	Purpose
Step 1	Server # scope chassis	Enters chassis command mode.
Step 2	Server /chassis # show cpu-pid	Displays the CPU PID details.
Step 3	Server /chassis # show dimm-pid	Displays the memory PID details.
Step 4	Server /chassis # show pciadapter-pid	Displays the PCI adapters PID details.
Step 5	Server /chassis # show hdd-pid	Displays the HDD PID details.

This example shows how to create view PID details

```
Server # scope chassis
Viewing CPU PID details
Server /chassis # show cpu-pid
Socket Product ID Model
-----
CPU1 UCS-CPU-E52660B Intel(R) Xeon(R) CPU E5-2660 v2 @ 2.2...
CPU2 UCS-CPU-E52660B Intel(R) Xeon(R) CPU E5-2660 v2 @ 2.2...
Viewing memory PID details
Server /chassis # show dimm-pid
Name Product ID Vendor ID Capacity Speed
-----
DIMM_A1 UNKNOWN NA Failed NA
DIMM_A2 UNKNOWN NA Ignore... NA
DIMM_B1 UCS-MR-1X162RZ-A 0xCE00 16384 MB 1866
DIMM_B2 UCS-MR-1X162RZ-A 0xCE00 16384 MB 1866
DIMM_C1 UCS-MR-1X162RZ-A 0xCE00 16384 MB 1866
DIMM_C2 UCS-MR-1X162RZ-A 0xCE00 16384 MB 1866
DIMM_D1 UCS-MR-1X162RZ-A 0xCE00 16384 MB 1866
DIMM_D2 UCS-MR-1X162RZ-A 0xCE00 16384 MB 1866
DIMM_E1 UCS-MR-1X162RZ-A 0xCE00 16384 MB 1866
DIMM_E2 UCS-MR-1X162RZ-A 0xCE00 16384 MB 1866
DIMM_F1 UCS-MR-1X162RZ-A 0xCE00 16384 MB 1866
DIMM_F2 UCS-MR-1X162RZ-A 0xCE00 16384 MB 1866
```



```

DIMM_G1          UCS-MR-1X162RZ-A      0xCE00      16384 MB    1866
DIMM_G2          UCS-MR-1X162RZ-A      0xCE00      16384 MB    1866
DIMM_H1          UCS-MR-1X162RZ-A      0xCE00      16384 MB    1866
DIMM_H2          UCS-MR-1X162RZ-A      0xCE00      16384 MB    1866

```

Viewing PCI adapters PID details

```
Server /chassis # show pciadapter-pid
```

Slot	Product ID	Vendor ID	Device ID	SubVendor ID	SubDevice ID
1	UCSC-MLOM-CSC-02	0x1137	0x0042	0x1137	0x012e

Viewing HDD PID details

```
Server /chassis # show hdd-pid
```

Disk	Controller	Product ID	Vendor	Model
1	SLOT-MEZZ	UCSC-C3X60-HD4TB	TOSHIBA	MG03SCA400
2	SLOT-MEZZ	UCS-C3X60-HD4TB	SEAGATE	ST4000NM0023
3	SLOT-MEZZ	UCSC-C3X60-HD4TB	TOSHIBA	MG03SCA400
4	SLOT-MEZZ	UCSC-C3X60-HD4TB	TOSHIBA	MG03SCA400
5	SLOT-MEZZ	UCSC-C3X60-HD4TB	TOSHIBA	MG03SCA400
6	SLOT-MEZZ	UCSC-C3X60-HD4TB	TOSHIBA	MG03SCA400
7	SLOT-MEZZ	UCSC-C3X60-HD4TB	TOSHIBA	MG03SCA400
8	SLOT-MEZZ	UCSC-C3X60-HD4TB	TOSHIBA	MG03SCA400
9	SLOT-MEZZ	UCSC-C3X60-HD4TB	TOSHIBA	MG03SCA400
10	SLOT-MEZZ	UCSC-C3X60-HD4TB	TOSHIBA	MG03SCA400
11	SLOT-MEZZ	UCSC-C3X60-HD4TB	TOSHIBA	MG03SCA400
12	SLOT-MEZZ	UCSC-C3X60-HD4TB	TOSHIBA	MG03SCA400
13	SLOT-MEZZ	UCSC-C3X60-HD4TB	TOSHIBA	MG03SCA400
14	SLOT-MEZZ	UCSC-C3X60-HD4TB	TOSHIBA	MG03SCA400
15	SLOT-MEZZ	UCS-C3X60-HD4TB	SEAGATE	ST4000NM0023
16	SLOT-MEZZ	UCS-C3X60-HD4TB	SEAGATE	ST4000NM0023
19	SLOT-MEZZ	UCSC-C3X60-HD4TB	TOSHIBA	MG03SCA400
28	SLOT-MEZZ	UCSC-C3X60-HD4TB	TOSHIBA	MG03SCA400
54	SLOT-MEZZ	UCSC-C3X60-HD6TB	SEAGATE	ST6000NM0014
55	SLOT-MEZZ	UCSC-C3X60-HD6TB	SEAGATE	ST6000NM0014
56	SLOT-MEZZ	UCSC-C3X60-HD4TB	TOSHIBA	MG03SCA400
57	SLOT-MEZZ	UCS-HD4T7KS3-E	WD	WD4001FYY...
58	SLOT-MEZZ	UCS-HD4T7KS3-E	WD	WD4001FYY...
59	SLOT-MEZZ	UCS-HD4T7KS3-E	WD	WD4001FYY...
60	SLOT-MEZZ	UCS-HD4T7KS3-E	WD	WD4001FYY...

```
Server /chassis #
```

Uploading and Activating PID Catalog

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server# /chassis scope pid-catalog	Enters the PID catalog command mode.
Step 3	Server /chassis/pid-catalog # upload-pid-catalog <i>remote-protocol IP Address PID Catalog file</i>	Specifies the protocol to connect to the remote server. It can be one of the following types: <ul style="list-style-type: none"> • TFTP • FTP • SFTP

	Command or Action	Purpose
		<ul style="list-style-type: none"> • SCP • HTTP <p>Note The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type.</p> <p>If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print_ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint.</p> <p>The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.</p>
Step 4	Server# /chassis/pid-catalog show detail	(Optional) Displays the status of the upload.
Step 5	Server# /chassis/pid-catalog activate	Activates the uploaded PID catalog.
Step 6	Server# /chassis/pid-catalog show detail	Displays the status of the activation.

This example uploads and activates the PID catalog:

```

Server # scope chassis
Server /chassis # scope pid-catalog
Uploading PID Catalog
Server /chassis/pid-catalog # upload-pid-catalog tftp 172.22.141.66
pid-ctlg-2_0_12_78_01.tar.gz
upload-pid-catalog initialized.
Please check the status using "show detail".
Server /chassis/pid-catalog #
Server /chassis/pid-catalog # show detail
    Upload Status: Upload Successful
    Activation Status: Please Activate Catalog
    Current Activated Version: N/A
Activating the uploaded PID catalog
Server /chassis/pid-catalog # activate
Successfully activated PID catalog
Server /chassis/pid-catalog # show detail
    Upload Status:
    Activation Status: Activation Successful
    Current Activated Version: 2.0(12.78).01
Server /chassis/pid-catalog #

```