Managing the Server

This chapter includes the following sections:

- Viewing Overall Server Status, page 1
- Configuring the Server Boot Order Using the CIMC GUI, page 3
- Configuring the Boot Order Using the BIOS Setup Menu, page 6
- Resetting the Server, page 7
- Shutting Down the Server, page 7
- Locking or Unlocking Cisco IOS CLI Configuration Changes, page 8
- Managing Server Power, page 8
- Configuring BIOS Settings, page 13
- Configuring Trusted Platform Module, page 26

Viewing Overall Server Status

Procedure

Step 1 In the **Overall Server Status** area of the **Navigation** pane, click the blue health report link to refresh the **Server Summary** pane.

Step 2 (Optional) Review the following information in the **Server Status** area of the **Server Summary** pane:

Note The following list shows all possible status fields. The actual fields displayed depend on the type of E-Series Server that you are using.

Name	Description
Power State field	The current power state.

Name	Description
Overall Server Status field	The overall status of the server. This can be one of the following: • **Memory Test In Progress—**The server is performing a self-test of the installed memory. This condition normally occurs during the boot process. • **Good** • **Moderate Fault** • **Severe Fault**
Temperature field	The temperature status. This can be one of the following: • **Good** • **Fault** • **Severe Fault** You can click the link in this field to view more temperature information.
Processors field	The overall status of the processors. This can be one of the following: • **Good** • **Fault** Click the link in this field to view more information about the processors.
Memory field	The overall status of the memory modules. This can be one of the following: • **Good** • **Fault** • **Severe Fault** Click the link in this field to view detailed status information.
Overall DIMM Status field	The overall status of the DIMM modules. This can be one of the following: • **Good** • **Fault** • **Severe Fault** Click the link in this field to view detailed status information.

Name	Description
Overall Storage Status field	The overall status of all controllers. This can be one of the following: • **Good** • **Moderate Fault** • **Severe Fault** Click the link in this field to view detailed status information.

Configuring the Server Boot Order Using the CIMC GUI

Before You Begin

Log into CIMC as a user with admin privileges.

Procedure

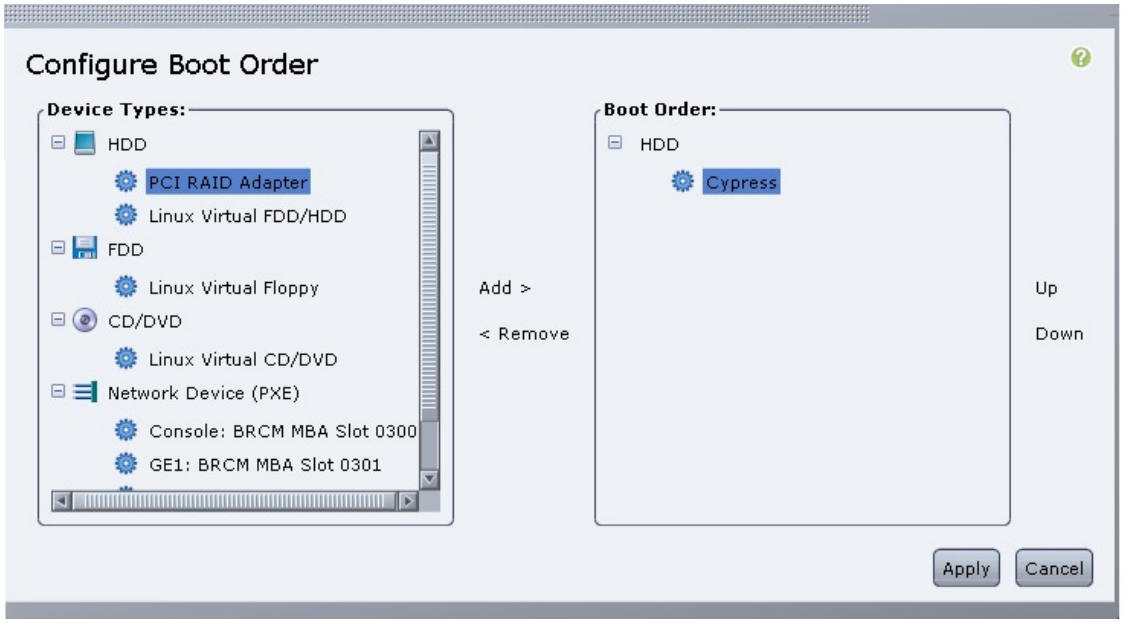
Step 1 In the **Navigation** pane, click the **Server** menu.

Step 2 On the **Server** tab, click **BIOS**.

Step 3 In the **Actions** area, click **Configure Boot Order**.

The **Configure Boot Order** dialog box appears.

Figure 1: Configure Boot Order Dialog Box



Step 4 In the **Configure Boot Order** dialog box, complete the following fields as appropriate:

Name	Description
Device Types table	The server boot options. This can be the following: • **HDD—**Hard disk drive. Contains the following options: ◦ **Cypress** ◦ **PCI RAID Adapter** ◦ **Linux Virtual FDD/HDD** ◦ **SSD Hard Drive** • **FDD—**Floppy disk drive. Contains the following option: ◦ **Linux Virtual Floppy** • **CD/DVD—**Bootable CD-ROM. Contains the following option: ◦ **Linux Virtual CD/DVD** • **Network Devices (PXE)—**PXE boot. Contains the following options: ◦ **Console** ◦ **GE1** ◦ **GE2** ◦ **GE3** ◦ **TE2** ◦ **TE3** **Note** The PXE boot options vary depending on the platform. For instance, the M3 servers use TE2 and TE3 instead of GE2 and GE3. • **Internal EFI Shell—**Internal Extensible Firmware Interface.
Add >	Moves the selected device type to the **Boot Order** table.
< Remove	Removes the selected device type from the **Boot Order** table.
Boot Order table	Displays the device types from which this server can boot, in the order in which the boot will be attempted.
Up	Moves the selected device type to a higher priority in the **Boot Order** table.
Down	Moves the selected device type to a lower priority in the **Boot Order** table.

Step 5 Click **Apply**.
Additional device types may be appended to the actual boot order, depending on what devices you have connected to your server.

What to Do Next

Reboot the server to boot with your new boot order.

Configuring the Boot Order Using the BIOS Setup Menu

Use this procedure if you want the server to boot from an external bootable device, such as a USB or an external CD-ROM drive that is directly connected to the E-Series Server or NCE.

Procedure

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

Step 2 In the work pane, click **Host Image Mapping** tab.

Step 3 From the **Actions** area, click **Launch KVM Console**.
The **KVM Console** opens in a separate window.

Step 4 From the **Server Summary** page, click **Power Cycle Server** to reboot the server.

Step 5 When prompted, press **F2** during bootup to access the BIOS setup menu.
The **Aptio Setup Utility** appears, which provides the BIOS setup menu options.

Step 6 Click the **Boot** tab.

Step 7 Scroll down to the bottom of the page below the **Boot Options Priority** area. The following boot option priorities are listed:

- Floppy Drive BBS Priorities
- Network Device BBS Priorities
- Hard Drive BBS Priorities
- CD/DVD ROM Drive BBS Priorities

Step 8 Use the **Up** or **Down arrow keys** on your keyboard to highlight the appropriate option.

Step 9 Press **Enter** to select the highlighted field.

Step 10 Choose the appropriate device as Boot Option 1.

Step 11 Press **F4** to save changes and exit.
The **Main** tab of the BIOS setup displays the device that you configured as Boot Option 1.

Resetting the Server

Before You Begin

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

Procedure

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

Step 2 In the work pane, click **Host Image Mapping** tab.

Step 3 In the **Actions** area, click **Hard Reset Server**.
A dialog box with the message **Hard Reset the Server?** appears.

Step 4 Click **OK**.

Shutting Down the Server

Before You Begin

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

Procedure

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

Step 2 In the work pane, click **Host Image Mapping** tab.

Step 3 In the **Actions** area, click **Shut Down Server**.
A dialog box with the message **Shut Down the Server?** appears.

Note The Citrix XenServer does not gracefully shut down when you click **Shut Down Server** or when you press the power button on the front panel of the E-Series Server.

Step 4 Click **OK**.

Note The NIM E-Series NCE might take up to 60 seconds to shut down. After two or three shut down attempts, if the NIM E-Series NCE does not shut down, enter the following commands from the router:

1. Router # **hw-module subslot 0/***NIM-slot-number* **stop**
2. Router # **hw-module subslot 0/***NIM-slot-number* **start**

Locking or Unlocking Cisco IOS CLI Configuration Changes

Use this procedure to allow or prevent configuration changes to be made using the Cisco IOS CLI.

Before You Begin

- Log into CIMC as a user with admin privileges.

Procedure

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

Step 2 In the work pane, click **Host Image Mapping** tab.

Step 3 To allow configuration changes to be made using the Cisco IOS CLI, from the **Actions** area, click **Unlock IOS Configuration Changes**.
The button in the GUI changes to **Lock IOS Configuration Changes**.

Step 4 To prevent configuration changes to be made using the Cisco IOS CLI, from the **Actions** area, click **Lock IOS Configuration Changes**.
If you do use the Cisco IOS CLI to make configuration changes, a warning message displays and the configuration is ignored.

The button in the GUI changes to **Unlock IOS Configuration Changes**.

Step 5 In the confirmation window, click **OK**.

Managing Server Power

Powering On the Server

Note If the server was powered off by any means other than through CIMC, it will not become active immediately when powered on. The server will remain in standby mode until CIMC completes initialization.

Before You Begin

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

Procedure

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

Step 2 In the work pane, click **Host Image Mapping** tab.

Step 3 In the **Actions** area, click **Power On Server**.

A dialog box with the message **Power on the server?** appears.

Step 4 Click **OK**.

Powering Off the Server

Note This procedure is not applicable to the NIM E-Series NCE.

Before You Begin

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

Procedure

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

Step 2 In the work pane, click **Host Image Mapping** tab.

Step 3 In the **Actions** area, click **Power Off Server**.
A dialog box with the message **Power Off the Server?** appears.

Step 4 Click **OK**.

Note For the NIM E-Series NCE, we recommend that you click **Shut Down Server**. If a power off is necessary, use the following commands from the router:

1. Router # **hw-module subslot 0**/*NIM-slot-number* **stop**
2. Router # **hw-module subslot 0**/*NIM-slot-number* **start**

Power Cycling the Server

Note This procedure is not applicable to the NIM E-Series NCE.

Before You Begin

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

Procedure

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

Step 2 In the work pane, click **Host Image Mapping** tab.

Step 3 In the **Actions** area, click **Power Cycle Server**.
A dialog box with the message **Power Cycle the Server?** appears.

Step 4 Click **OK**.

Note
- Power cycling the server is the same as pressing the physical power button to power off and then powering on the server.
- Power hard-reset is the same as pressing the physical reset button on the server.

Note For the NIM E-Series NCE, we recommend that you click **Shut Down Server**. If a power cycle is necessary, use one of the following commands from the router:

- **1** Router # **hw-module subslot 0/***NIM-slot-number* **stop**
  2 Router # **hw-module subslot 0/***NIM-slot-number* **start**
- Router # **hw-module subslot 0/***NIM-slot-number* **reload**

  Note This command power-cycles the module. The CIMC and server reboot.

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.

Note On a NIM, the power restore policy option is not configurable through CIMC 3.1.x GUI. Other configuration methods (CLI, XMLAPI) must be used. All configuration methods, including GUI, are supported in CIMC 3.2.x.

Note This feature is supported only on ISR 4K routers, not on ISR G2. For ISR G2, refer to the BIOS configuration in CIMC.

Procedure

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

Step 2 On the **Server** tab, click **Power Policies**.

Step 3 In the **Power Restore Policy** area, update the following field:

Name	Description
Power Restore Policy drop-down list	The action to be taken when chassis power is restored after an unexpected power loss. This can be one of the following: • **Power Off—**The server remains off until it is manually restarted. • **Power On—**The server is allowed to boot up normally when power is restored. • **Restore Last State—**Restores the server to the same power state (off or on) that it was in when the power was lost. This is the default action.

Step 4 Click **Save Changes**.

Locking or Unlocking the Server's Front Panel Power Button

Note This procedure is applicable to E-Series Servers and the SM E-Series NCE. This procedure is not applicable to the EHWIC E-Series NCE and the NIM E-Series NCE.

Use this procedure to enable or disable the physical power button, which is located on the front panel of the physical server.

Before You Begin

- Log in to CIMC as a user with admin privileges.
- Power off the server.

Procedure

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

Step 2 In the work pane, click **Host Image Mapping** tab.

Step 3 To disable the power button, from the **Actions** area, click **Lock Front Panel Power Button**.
The power button is disabled. You cannot use the front panel power button to turn the server power on or off.

The button in the GUI changes to **Unlock Front Panel Power Button**.

Step 4 To enable the power button, from the **Actions** area, click **Unlock Front Panel Power Button**.
The power button is enabled. You can use the front panel power button to turn the server power on or off.

The button in the GUI changes to **Lock Front Panel Power Button**.

Step 5 In the confirmation window, click **OK**.

Locking or Unlocking the Server's Front Panel Reset Button

Note This procedure is applicable to E-Series Servers and the SM E-Series NCE. This procedure is not applicable to the EHWIC E-Series NCE and the NIM E-Series NCE.

Use this procedure to enable or disable the reset button, which is located on the front panel of the physical server.

Before You Begin

- Log in to CIMC as a user with admin privileges.
- Power off the server.

Procedure

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

Step 2 In the work pane, click **Host Image Mapping** tab.

Step 3 To disable the reset button, from the **Actions** area, click **Lock Front Panel Reset Button**.
The reset button is disabled. You cannot use the front panel reset button to reset the server.

The button in the GUI changes to **Unlock Front Panel Reset Button**.

Step 4 To enable the reset button, from the **Actions** area, click **Unlock Front Panel Reset Button**.
The reset button is enabled. You can use the front panel reset button to reset the server.

The button in the GUI changes to **Lock Front Panel Reset Button**.

Step 5 In the confirmation window, click **OK**.

Configuring BIOS Settings

Activating the Backup BIOS

On rare occasions, the BIOS image might get corrupted. To recover from a corrupt BIOS image, activate the backup BIOS to boot the system.

Note The backup BIOS image is factory installed. It cannot be upgraded.

Before You Begin

- Log into CIMC as a user with admin privileges.

Procedure

Step 1 In the **Navigation** pane, click the **Server** menu.
Step 2 On the **Server** tab, click **BIOS**.
Step 3 In the **Actions** area, click **Activate Backup BIOS**.
Step 4 In the confirmation window, click **OK**.

Configuring Advanced BIOS Settings

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

Before You Begin

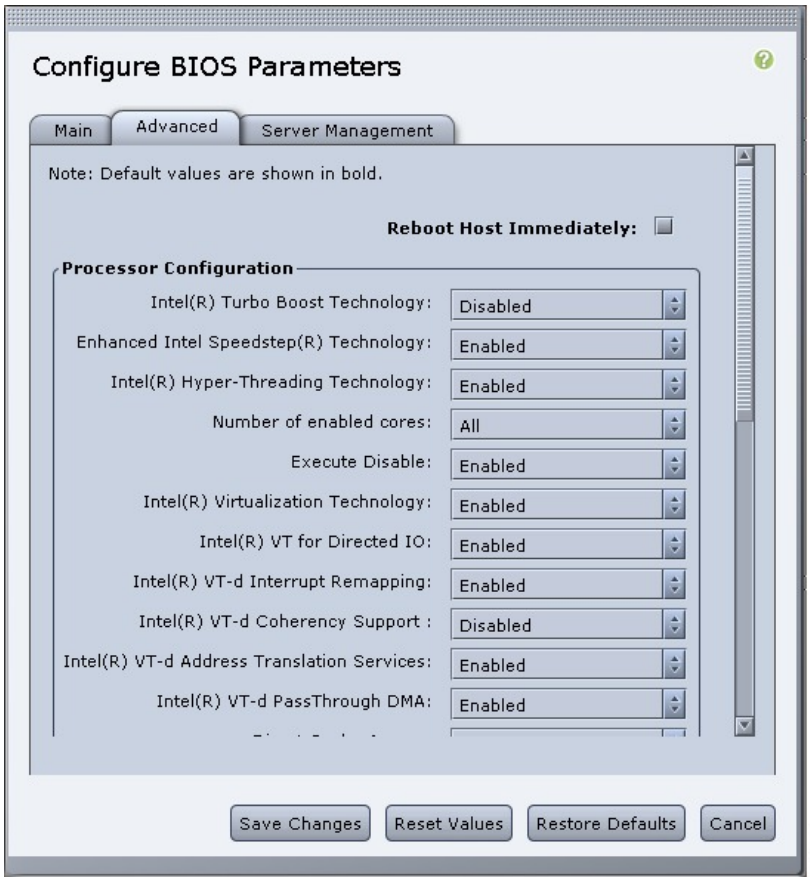
You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Server** menu.
Step 2 On the **Server** tab, click **BIOS**.
Step 3 In the **Actions** area, click **Configure BIOS**.
The **Configure BIOS Parameters** dialog box appears.

Step 4 In the **Configure BIOS Parameters** dialog box, click the **Advanced** tab.

Figure 2: Advanced Tab



Step 5 Check or clear the **Reboot Host Immediately** checkbox.
If checked, the server is rebooted immediately after you make changes to the BIOS parameters.

To specify that the server should not reboot automatically, clear this check box. Any parameter changes will take effect the next time the server is rebooted.

Note This step is not applicable to the NIM E-Series NCE.

Step 6 In the **Advanced** tab, update the BIOS settings fields.

Step 7 Click **Save Changes**.

Configuring Server Management BIOS Settings

Before You Begin

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

Procedure

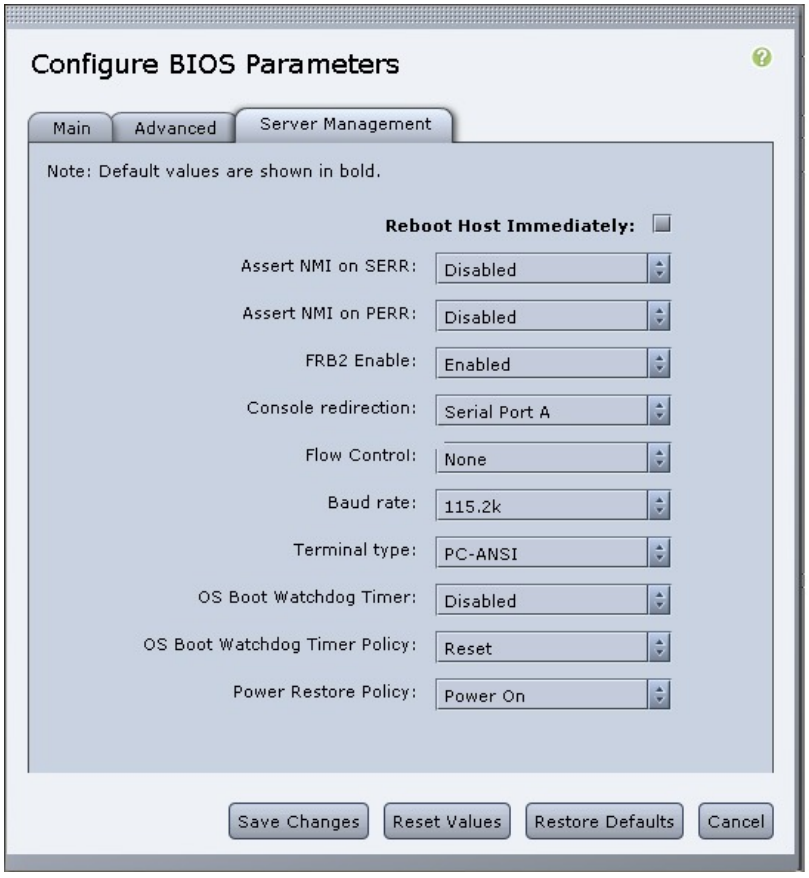
Step 1 In the **Navigation** pane, click the **Server** menu.

Step 2 On the **Server** tab, click **BIOS**.

Step 3 In the **Actions** area, click **Configure BIOS**.
The **Configure BIOS Parameters** dialog box appears.

Step 4 In the **Configure BIOS Parameters** dialog box, click the **Server Management** tab.

Figure 3: Server Management Tab



Step 5 Check or clear the **Reboot Host Immediately** checkbox.
If checked, the server is rebooted immediately after you make changes to the BIOS parameters.

To specify that the server should not reboot automatically, clear this check box. Any parameter changes will take effect the next time the server is rebooted.

Note This step is not applicable to the NIM E-Series NCE.

Step 6 In the **Server Management** tab, update the BIOS settings fields.

Step 7 Click **Save Changes**.

Clearing the BIOS CMOS

Note On rare occasions, troubleshooting a server may require you to clear the server's BIOS CMOS memory. This procedure is not part of the normal maintenance of a server.

Before You Begin

- Log into CIMC as a user with admin privileges.
- Power off the server.

Procedure

Step 1 In the **Navigation** pane, click the **Server** menu.
Step 2 On the **Server** tab, click **BIOS**.
Step 3 In the **Actions** area, click **Clear BIOS CMOS**.
Step 4 In the confirmation window, click **OK**.

Clearing the BIOS Password

Before You Begin

- Log into CIMC as a user with admin privileges.

Procedure

Step 1 In the **Navigation** pane, click the **Server** menu.
Step 2 On the **Server** tab, click **BIOS**.
Step 3 In the **Actions** area, click **Clear BIOS Password**.
Step 4 In the confirmation window, click **OK**.

What to Do Next

Reboot the server for the clear password operation to take effect. You are prompted to create a new password when the server reboots.

Server BIOS Settings

The tables in the following sections list the server BIOS settings that you can view and configure.

Note We recommend that you verify the support for BIOS settings in your server. Depending on your installed hardware, some settings may not be supported.

Main BIOS Settings

Name	Description
Reboot Host Immediately Not displayed for the NIM E-Series NCE.	If checked, the server is rebooted immediately after you click **Save Changes**. To specify that the server should not reboot automatically, clear this check box. Any parameter changes will take effect the next time the server is rebooted.

Advanced: Processor BIOS Settings

Name	Description
Intel Turbo Boost Technology **Intel Turbo Boost Technology**	Whether the processor uses Intel Turbo Boost Technology, which allows the processor to automatically increase its frequency if it is running below power, temperature, or voltage specifications. This can be one of the following: • **Disabled—**The processor does not increase its frequency automatically. • **Enabled—**The processor utilizes Turbo Boost Technology if required.
Enhanced Intel Speedstep Technology	Whether the processor uses Enhanced Intel SpeedStep Technology, which allows the system to dynamically adjust processor voltage and core frequency. This technology can result in decreased average power consumption and decreased average heat production. This can be one of the following: • **Disabled—**The processor never dynamically adjusts its voltage or frequency. • **Enabled—**The processor utilizes Enhanced Intel SpeedStep Technology and enables all supported processor sleep states to further conserve power. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.

Name	Description
Intel Hyper-Threading Technology	Whether the processor uses Intel Hyper-Threading Technology, which allows multithreaded software applications to execute threads in parallel within each processor. This can be one of the following: • **Disabled—**The processor does not permit hyperthreading. • **Enabled—**The processor allows for the parallel execution of multiple threads. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.
Number of Enabled Cores	Sets the state of logical processor cores in a package. If you disable this setting, Hyper Threading is also disabled. This can be one of the following: • **All—**Enables multi processing on all logical processor cores. • **1** through *n***—**Specifies the number of logical processor cores that can run on the server. To disable multi processing and have only one logical processor core running on the server, select 1. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.
Execute Disable	Classifies memory areas on the server to specify where application code can execute. As a result of this classification, the processor disables code execution if a malicious worm attempts to insert code in the buffer. This setting helps to prevent damage, worm propagation, and certain classes of malicious buffer overflow attacks. This can be one of the following: • **Disabled—**The processor does not classify memory areas. • **Enabled—**The processor classifies memory areas. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.

Name	Description
Intel Virtualization Technology	Whether the processor uses Intel Virtualization Technology (VT), which allows a platform to run multiple operating systems and applications in independent partitions. This can be one of the following: • **Disabled—**The processor does not permit virtualization. • **Enabled—**The processor allows multiple operating systems in independent partitions. **Note** If you change this option, you must power cycle the server before the setting takes effect.
Intel VT for Directed IO	Whether the processor uses Intel Virtualization Technology for Directed I/O (VT-d). This can be one of the following: • **Disabled—**The processor does not use virtualization technology. • **Enabled—**The processor uses virtualization technology.
Intel VT-d Interrupt Remapping	Whether the processor supports Intel VT-d Interrupt Remapping. This can be one of the following: • **Disabled—**The processor does not support remapping. • **Enabled—**The processor uses VT-d Interrupt Remapping as required.
Intel VT-d Coherency Support	Whether the processor supports Intel VT-d Coherency. This can be one of the following: • **Disabled—**The processor does not support coherency. • **Enabled—**The processor uses VT-d Coherency as required.
Intel VT-d Address Translation Services	Whether the processor supports Intel VT-d Address Translation Services (ATS). This can be one of the following: • **Disabled—**The processor does not support ATS. • **Enabled—**The processor uses VT-d ATS as required.
Intel VT-d PassThrough DMA	Whether the processor supports Intel VT-d Pass-through DMA. This can be one of the following: • **Disabled—**The processor does not support pass-through DMA. • **Enabled—**The processor uses VT-d Pass-through DMA as required.

Name	Description
Direct Cache Access	Allows processors to increase I/O performance by placing data from I/O devices directly into the processor cache. This setting helps to reduce cache misses. This can be one of the following: • **Disabled—**Data from I/O devices is not placed directly into the processor cache. • **Enabled—**Data from I/O devices is placed directly into the processor cache.
Processor C3 Report	Whether the processor sends the C3 report to the operating system. This can be one of the following: • **Disabled—**The processor does not send the C3 report. • **ACPI C2—**The processor sends the C3 report using the ACPI C2 format. • **ACPI C3—**The processor sends the C3 report using the ACPI C3 format.
Processor C6 Report	Whether the processor sends the C6 report to the operating system. This can be one of the following: • **Disabled—**The processor does not send the C6 report. • **Enabled—**The processor sends the C6 report.
Hardware Prefetcher	Whether the processor allows the Intel hardware prefetcher to fetch streams of data and instruction from memory into the unified second-level cache when necessary. This can be one of the following: • **Disabled—**The hardware prefetcher is not used. • **Enabled—**The processor uses the hardware prefetcher when cache issues are detected. **Note** You must select **Custom** in the **CPU Performance** drop-down list to specify this value. For any value other than **Custom**, this option is overridden by the setting in the selected CPU performance profile.

Name	Description
Adjacent Cache-Line Prefetch	Whether the processor uses the Intel Adjacent Cache-Line Prefetch mechanism to fetch data when necessary. This can be one of the following: • **Disabled—**The Adjacent Cache-Line Prefetch mechanism is not used. • **Enabled—**The Adjacent Cache-Line Prefetch mechanism is used when cache issues are detected. **Note** You must select **Custom** in the **CPU Performance** drop-down list in order to specify this value. For any value other than **Custom**, this option is overridden by the setting in the selected CPU performance profile.
Package C State Limit	The amount of power available to the server components when they are idle. This can be one of the following: • **C0 state—**The server provides all server components with full power at all times. This option maintains the highest level of performance and requires the greatest amount of power. • **C2 state—** System level coordination is in progress resulting in high power consumption. There might be performance issues until the coordination is complete. • **C6 state—**When the CPU is idle, the system reduces the power consumption further than with the C3 option. This option saves more power than C0 or C2, but there might be performance issues until the server returns to full power. • **C7 state—**When the CPU is idle, the server makes a minimal amount of power available to the components. This option saves the maximum amount of power but it also requires the longest time for the server to return to high performance mode. • **No Limit—**The server may enter any available C state. **Note** This option is used only if **CPU C State** is enabled.

Name	Description
Patrol Scrub	Whether the system actively searches for, and corrects, single bit memory errors even in unused portions of the memory on the server. This can be one of the following: • **Disabled—**The system checks for memory ECC errors only when the CPU reads or writes a memory address. • **Enabled—**The system periodically reads and writes memory searching for ECC errors. If any errors are found, the system attempts to fix them. This option may correct single bit errors before they become multi-bit errors, but it may adversely affect performance when the patrol scrub is running.
Demand Scrub	Whether the system allows a memory scrub to be performed on demand. This can be one of the following: • **Disabled—**The system does not allow a memory scrub to be performed on demand. • **Enabled—**The system allows a memory scrub to be performed on demand. If errors occur, the system attempts to fix them or marks the location as unreadable. This process makes the system run faster with fewer data processing errors.
Device Tagging	Whether the system allows devices and interfaces to be grouped based on a variety of information, including descriptions, addresses, and names. This can be one of the following: • **Disabled—**The system does not allow the devices and interfaces to be grouped. • **Enabled—**The system allows the devices and interfaces to be grouped.

Advanced: Serial Port BIOS Settings

Name	Description
Serial A Enable	Whether serial port A is enabled or disabled. This can be one of the following: • **Disabled—**The serial port is disabled. • **Enabled—**The serial port is enabled.

Advanced: USB BIOS Settings

Name	Description
USB Port 0	Whether the processor uses USB port 0. This can be one of the following: • **Disabled—**The server does not use the USB port 0. • **Enabled—**The processor uses the USB port 0.
USB Port 1	Whether the processor uses USB port 1. This can be one of the following: • **Disabled—**The server does not use the USB port 1. • **Enabled—**The processor uses the USB port 1.

Server Management BIOS Settings

Name	Description
Reboot Host Immediately Not displayed for the NIM E-Series NCE.	If checked, the server is rebooted immediately after you click **Save Changes**. To specify that the server should not reboot automatically, clear this check box. Any parameter changes will take effect the next time the server is rebooted.
Assert NMI on SERR	Whether the BIOS generates a non-maskable interrupt (NMI) and logs an error when a system error (SERR) occurs. This can be one of the following: • **Disabled—**The BIOS does not generate an NMI or log an error when a SERR occurs. • **Enabled—**The BIOS generates an NMI and logs an error when a SERR occurs. You must enable this setting if you want to enable **Assert NMI on PERR**.
Assert NMI on PERR	Whether the BIOS generates a non-maskable interrupt (NMI) and logs an error when a processor bus parity error (PERR) occurs. This can be one of the following: • **Disabled—**The BIOS does not generate an NMI or log an error when a PERR occurs. • **Enabled—**The BIOS generates an NMI and logs an error when a PERR occurs. You must enable **Assert NMI on SERR** to use this setting.

Name	Description
FRB2 Enable	Whether the FRB2 timer is used by CIMC to recover the system if it hangs during POST. This can be one of the following: • **Disabled—**The FRB2 timer is not used. • **Enabled—**The FRB2 timer is started during POST and used to recover the system if necessary.
Console Redirection	Allows a serial port to be used for console redirection during POST and BIOS booting. After the BIOS has booted and the operating system is responsible for the server, console redirection is irrelevant and has no effect. This can be one of the following: • **Disabled—**No console redirection occurs during POST. • **Serial Port A—**Enables serial port A for console redirection during POST. This option is valid for blade servers and rack-mount servers. Note that **Serial Port A** option also requires that you enabled **Serial Port A** in the Advanced menu. **Note** If you enable this option, you also disable the display of the Quiet Boot logo screen during POST.
Flow Control	Whether a handshake protocol is used for flow control. Request to Send/Clear to Send (RTS/CTS) helps to reduce frame collisions that can be introduced by a hidden terminal problem. This can be one of the following: • **None—**No flow control is used. • **RTS-CTS—**RTS/CTS is used for flow control. **Note** This setting must match the setting on the remote terminal application.
Baud Rate	What BAUD rate is used for the serial port transmission speed. If you disable Console Redirection, this option is not available. This can be one of the following: • **9.6k—**A 9600 BAUD rate is used. • **19.2k—**A 19200 BAUD rate is used. • **38.4k—**A 38400 BAUD rate is used. • **57.6k—**A 57600 BAUD rate is used. • **115.2k—**A 115200 BAUD rate is used. **Note** This setting must match the setting on the remote terminal application.

Name	Description
Terminal Type	What type of character formatting is used for console redirection. This can be one of the following: • **PC-ANSI—**The PC-ANSI terminal font is used. • **VT100—**A supported vt100 video terminal and its character set are used. • **VT100-PLUS—**A supported vt100-plus video terminal and its character set are used. • **VT-UTF8—**A video terminal with the UTF-8 character set is used. **Note** This setting must match the setting on the remote terminal application.
OS Boot Watchdog Timer	Whether the BIOS programs the watchdog timer with a specified timeout value. If the operating system does not complete booting before the timer expires, the CIMC resets the system and an error is logged. This can be one of the following: • **Disabled—**The watchdog timer is not used to track how long the server takes to boot. • **Enabled—**The watchdog timer tracks how long the server takes to boot. If the server does not boot within the length of time specified in the **OS Boot Watchdog Timer Timeout** field, the CIMC logs an error and takes the action specified in the **OS Boot Watchdog Policy** field.
OS Boot Watchdog Timer Policy	The action the system takes when the watchdog timer expires. This can be one of the following: • **Do Nothing—**The state of the server power does not change when the watchdog timer expires during OS boot. • **Power Down—**The server is powered off if the watchdog timer expires during OS boot. • **Reset—**The server is reset if the watchdog timer expires during OS boot. **Note** This option is only applicable if you enable the OS Boot Watchdog Timer.

Common Controls

The buttons described in the following table are available in all **Configure BIOS Parameters** tabs.

Name	Description
Save Changes button	Saves the settings for the BIOS parameters on all three tabs and closes the wizard. If the **Reboot Host Immediately** check box is checked, the server is rebooted immediately and the new BIOS settings go into effect. Otherwise, the changes are saved until the server is manually rebooted.
Reset Values button	Restores the values of the BIOS parameters on all three tabs to the settings that were in effect when this dialog box was opened.
Restore Defaults button	Sets the BIOS parameters on all three tabs to their default settings.
Cancel button	Closes the dialog box without making any changes.

Configuring Trusted Platform Module

The Trusted Platform Module (TPM) is a component that can securely store artifacts that are used to authenticate the server. These artifacts can include passwords, certificates, or encryption keys. A TPM can also be used to store platform measurements that help ensure that the platform remains trustworthy. Authentication (ensuring that the platform can prove that it is what it claims to be) and attestation (a process helping to prove that a platform is trustworthy and has not been breached) are necessary steps to ensure safer computing in all environments. It is a requirement for the Intel Trusted Execution Technology (TXT) security feature, which must be enabled in the BIOS settings for a server equipped with a TPM. TPM is enabled by default on these servers.

To check the status of TPM, follow this procedure:

Procedure

Step 1 Power on the system.

Step 2 As soon as the first logo screen appears, immediately press the **F2** key, or the **DEL** key if you have a desktop, to enter the **BIOS**.

Step 3 In the **BIOS** menu, go to **Advanced** option, and then select the **Trusted Computing** page. You can see the TPM information.