Lenovo

Lenovo Edge Servers UEFI Manual

Server Model: SE350, MX1020, MX1021

Third Edition (April 2024)

Contents

Chapter 1. Lenovo Edge Server with Intel Xeon SP (3rd Gen)

This topic provides general introduction to the Unified Extensible Firmware Interface (UEFI).

UEFI is an interface packed with various features, including system information and settings, boot and runtime services, BMC settings, system event logs, and user security. This guide applies to the following server model:

- SE350
- MX1020
- MX1021

The following table details the main menu:

Table 1. Main menu details

Item	Description
Chapter 3 "System configuration and boot management**" on page 5**	Main menu
Launch Graphical System Setup	Start the graphical user interface for system setup, provisioning manager, and RAID configuration. When in Graphical System Setup, there will be no screen output to console. Please use VGA monitor for Graphical System Setup.
"System information**" on page 5**	Display the basic details of the system.
"System settings**" on page 7**	Display or modify system settings. Changes may not take effect immediately. Save any changed settings and reboot the system.
"Date and time**" on page 48**	Set the local date and time of the system.
"Start options**" on page 49**	Boot a desired selection from the primary boot sequence as specified under **Boot Manager**.
"Boot manager**" on page 50**	Change boot order, boot parameters, and boot from a file.
"BMC settings**" on page 53**	Configure the management controller.
"System event logs**" on page 57**	Clear or view the system event log.
"User security**" on page 58**	Set or change Power-On and Administrator passwords.
Save Settings	Save the changes and commit them to BMC.
Discard Settings	Discard any changes.
Load Default Settings	Load the default values for system settings.
Exit Setup Utility	Exit Setup.

Chapter 2. Get started

First launch

Perform the following steps to first launch the UEFI setup utilities.

1. (Optional) Connect the local keyboard, video, and mouse (KVM) to the server using a cable, or open the **Remote Console** page on the Lenovo XClarity Controller web user interface (XCC WebUI).
2. Power on the system and press F1.
3. If you have set the power on password, enter the correct password.
4. Wait for about 90 seconds, the setup utilities window is displayed.

Switch between graphic/text modes

The setup utilities are launched in graphic mode by default. The utilities can also be launched in text mode. You can switch between the two modes by referring to sections below.

Graphic mode to text mode

If you have entered graphic mode and need to switch to text mode, perform the following steps.

1. On the main interface, choose **UEFI Setup → System Settings → <F1> Start Control**.
2. Select **Text Setup** for **<F1> Start Control**.
3. Restart the server and press F1.
4. Wait for about 90 seconds, the setup utilities window is displayed in text mode.

Text mode to graphic mode

If you have entered text mode and need to switch to graphic mode, perform the following steps.

1. On the main interface, choose **System Settings → <F1> Start Control**.
2. Select **Tool Suite** or **Auto** for **<F1> Start Control**.
3. Restart the server and press F1.
4. Wait for about 90 seconds, the setup utilities window is displayed in graphic mode.

Chapter 3. System configuration and boot management

This chapter details system setup utility.

System information

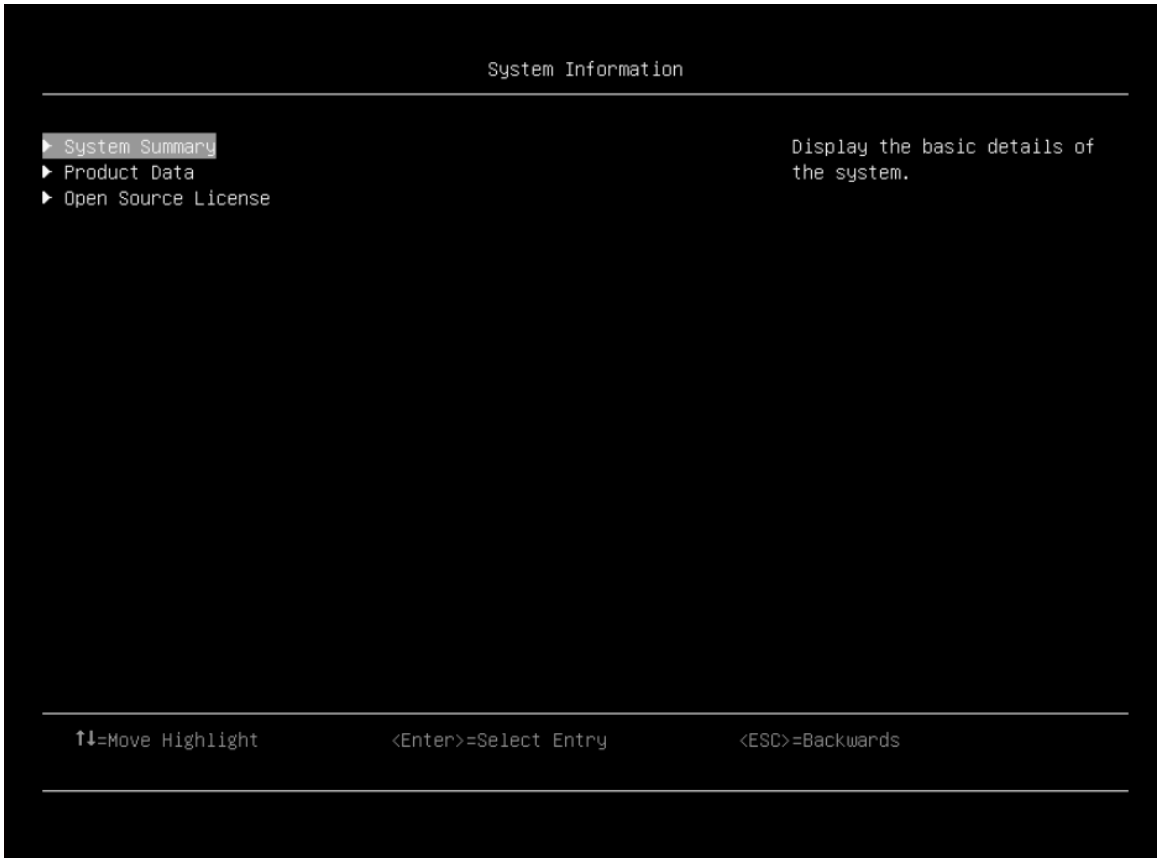


Table 2. System information details

Item	Description
“System Summary” on page 5	View the basic details of the system.
“Product Data” on page 6	View the system firmware information.
“Open Source License” on page 6	View the open source license.

System Summary

Item	Description
System Identification Data	
Machine Type/Model	View the system machine type and model.
Serial Number	View the tag for the serial number.
UUID Number	View the tag for the UUID.

Asset Tag Number	View a customer-assigned system asset tag number.
Processor	
Installed CPU Packages	View the number of installed CPU packages.
Processor Speed	View the processor speed.
Memory	
Memory Speed	View the installed memory speed.
Total Memory Size	View the total installed memory size.

Product Data

Item	Description
Host Firmware	
Build ID	View the build ID of the host firmware.
Version	View the version of the host firmware.
Build Date	View the build date of the host firmware.
BMC Firmware	
Build ID	View the build ID of the BMC firmware.
Version	View the version of the BMC firmware.
Build Date	View the build date of the BMC firmware.
Switch Firmware	
Build ID	View the build ID of the Switch firmware.

Note: The information about switch firmware will be available when the switch module is installed.

Open Source License

This is the use of open source software, which is distributed according to relevant licenses, acknowledgements and required copyright notices.

Note: The details are hardware-dependent.

System settings

Notes:

- SAS/SATA drives or NVMe drives connected to a storage controller will be displayed in the storage controller submenu: **System settings → Storage → Storage controller xxxx**.
- NVMe drives connected to the system without raid controller (sometimes using a retimer) will be displayed in one of the following pages:
  - **System settings → Foreign Devices**
  - **System settings → Storage**

Table 3. System settings details

Item	Options	Description
<F1> Start Control	• **Auto** (Default) • Tool Suite • Text Setup	Press F1 to start control.
"Devices and I/O ports" **on page 8**		View onboard devices and I/O port options.
"Driver health" **on page 17**		View the health of the controllers in the system as reported by their corresponding drivers.
"Foreign Devices" **on page 19**		View the list of foreign devices.

Table 3. System settings details (continued)

“Legacy BIOS” on page 20		Configure system UEFI firmware execution environment preferences for supporting legacy OS and legacy Option ROM.
“Memory” on page 21		View and change the memory settings.
“Network” on page 23		View and change network devices and network related settings.
“Operating modes” on page 29		Configure the operating mode based on your preference. **Note:** Power savings and performance are highly dependent on hardware configuration and the software running on the system.
“Power” on page 33		Configure power scheme options.
“Processors” on page 34		View and change the processor settings.
“Recovery and RAS” on page 39		Configure recovery policies and advanced reliability, availability, and serviceability settings.
“Security” on page 41		Configure system security settings.
“Storage” on page 47		Manage storage adapter options. Some systems may use planar devices and can be configured under the menu of **Devices and I/O Ports**.

Devices and I/O ports

This menu displays onboard devices and I/O port options.

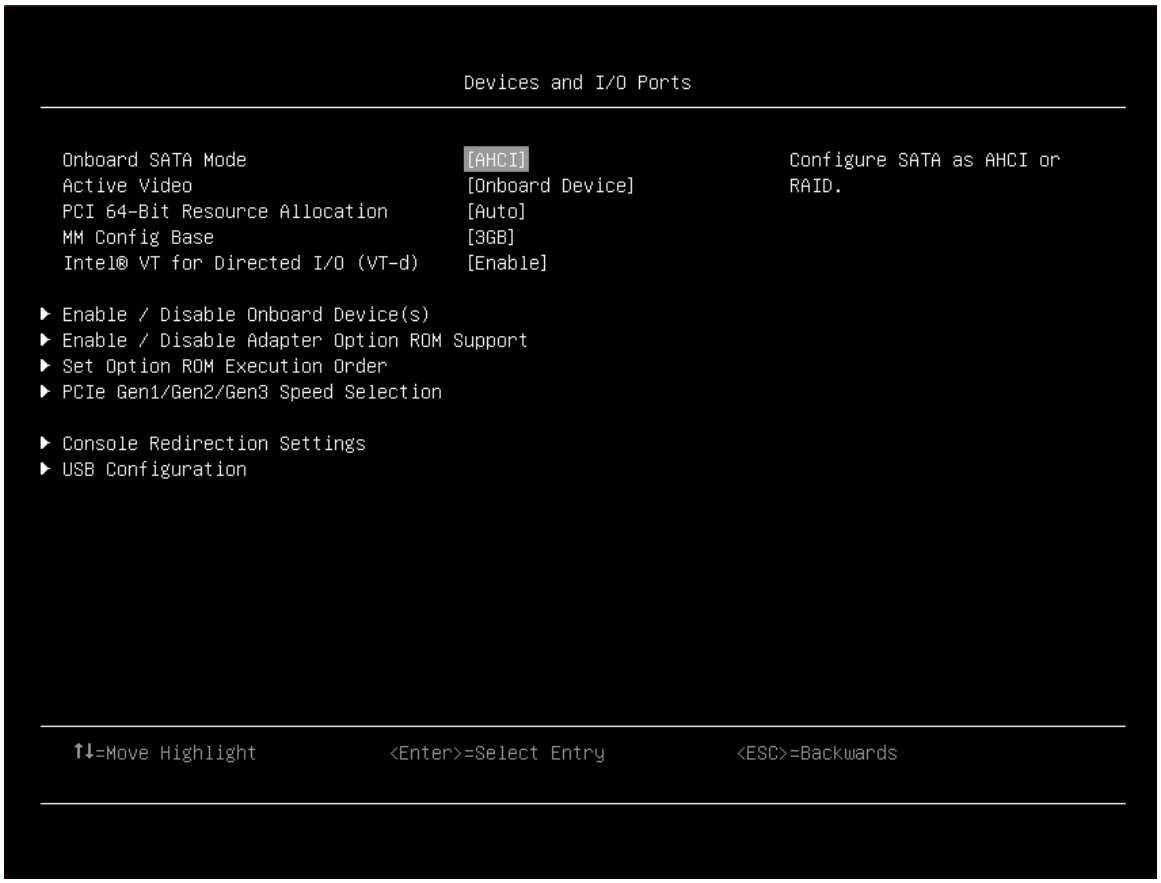


Table 4. Device and I/O Ports details

Item	Options	Description
Onboard SATA Mode	• **AHCI** (Default) • RAID	Configure SATA as AHCI or RAID. **Note:** This item is hardware dependent.
Active Video	• **Onboard Device** (Default) • Add-in Device	This setting only applies when the server has an add-in video adapter. When the option ROM is set to **Legacy** for both onboard and add-in video adapters, the Active Video setting controls which single adapter will display the System Setup utility. Regardless of this setting, the system boot early video is displayed at the onboard video only, and the management controller remote console displays the onboard video only. This setting does not affect how the OS chooses to display its graphical desktop.
PCI 64-Bit Resource Allocation	• Enable • Disable • **Auto** (Default)	• **Enable**: enable the allocation of 64-bit resources for PCI. • **Disable**: disable the allocation of 64-bit resources for PCI. • **Auto**: allocate some resources below 4GB for legacy compatibility.

Table 4. Device and I/O Ports details (continued)

MM Config Base	• **3GB** (Default) • 2GB • 1GB	The default setting of 3GB is recommended. A higher value will increase memory available to the OS below 4GB but reduce memory mapped I/O (MMIO) resource available to PCI adapters. A lower than 3GB value will increase MMIO resources but decrease memory available to OS below 4GB. If there is any issue occurred after you change the setting, you can revert to the previous setting.
Intel® VT for Directed I/O (VT-d)	• **Enable** (Default) • Disable	Enable/Disable Intel® Virtualization Technology for Directed I/O (VT-d) by reporting the I/O device assignment to VMM through DMAR ACPI Tables.
"Enable/Disable Onboard Device (s)" on page 10		Enable/disable onboard devices or slots.
"Enable/Disable Adapter Option ROM Support" on page 12		Control Legacy and UEFI-compliant adapter support. Disabling UEFI/Legacy support may adversely affect pre-boot/boot functions.
"Set Option ROM Execution Order" on page 13		Control legacy ROM load order.
"PCIe Gen1/Gen2/Gen3 Speed Selection" on page 13		Choose the generation speed for available PCIe slots.
"Console Redirection Settings" on page 15		Settings for console redirection and COM port settings.
"USB Configuration" on page 17		Disable USB storage devices or individual ports.
"Intel® VMD technology" on page 17		Press Enter to pop up the Intel® VMD for Volume Management Device Configuration menu.

Enable/Disable Onboard Device(s)

Note: The items in this menu are hardware-dependent.

Item	Options	Description
Onboard Video	• **Enable** (Default) • Disable	Disabling an entry will prevent the associated device from being enumerated during subsequent boots.
Slot 1	• **Enable** (Default) • Disable	This slot numbering is for M.2 boot adapter. Disabling an entry will prevent the associated device from being enumerated during subsequent boots.
Slot 2	• **Enable** (Default) • Disable	This slot numbering appears only when M.2 data adapter is installed at the left wing. Disabling an entry will prevent the associated device from being enumerated during subsequent boots.
Slot 3	• **Enable** (Default) • Disable	This slot numbering appears only when M.2 data adapter is installed at the left wing. Disabling an entry will prevent the associated device from being enumerated during subsequent boots.

Slot 4	• **Enable** (Default) • Disable	This slot numbering appears only when M.2 data adapter is installed at the left wing. Disabling an entry will prevent the associated device from being enumerated during subsequent boots.
Slot 5	• **Enable** (Default) • Disable	This slot numbering appears only when M.2 data adapter is installed at the left wing. Disabling an entry will prevent the associated device from being enumerated during subsequent boots.
Slot 2/3	• **Enable** (Default) • Disable	This slot numbering appears only when M.2 data adapter with hardware RAID is installed at the left wing. Disabling an entry will prevent the associated device from being enumerated during subsequent boots.
Slot 4/5	• **Enable** (Default) • Disable	This slot numbering appears only when M.2 data adapter with hardware RAID is installed at left wing. Disabling an entry will prevent the associated device from being enumerated during subsequent boots.
Slot 6	• **Enable** (Default) • Disable	This slot numbering appears when M.2 data adapter is installed at right wing or PCIe Riser is installed. Disabling an entry will prevent the associated device from being enumerated during subsequent boots.
Slot 7	• **Enable** (Default) • Disable	This slot numbering appears only when M.2 data adapter is installed at right wing. Disabling an entry will prevent the associated device from being enumerated during subsequent boots.
Slot 8	• **Enable** (Default) • Disable	This slot numbering appears only when M.2 data adapter is installed at right wing. Disabling an entry will prevent the associated device from being enumerated during subsequent boots.
Slot 9	• **Enable** (Default) • Disable	This slot numbering appears only when M.2 data adapter is installed at right wing. Disabling an entry will prevent the associated device from being enumerated during subsequent boots.
Slot 6/7	• **Enable** (Default) • Disable	This slot numbering appears only when M.2 data adapter with hardware RAID is installed at right wing. Disabling an entry will prevent the associated device from being enumerated during subsequent boots.
Slot 8/9	• **Enable** (Default) • Disable	This slot numbering appears only when M.2 data adapter with hardware RAID is installed at right wing. Disabling an entry will prevent the associated device from being enumerated during subsequent boots.

Onboard LAN 1	• **Enable** (Default) • Disable	Disabling an entry will prevent the associated device from being enumerated during subsequent boots. Disabling this entry will disable all Onboard LAN 1 Ports. All Onboard LAN 1 Port options in this page shall be grayed-out.
LAN Port 1	• **Enable** (Default) • Disable	Disabling an entry will prevent the associated device from being enumerated during subsequent boots. Gray-out when **Onboard LAN 1** is Disabled.
LAN Port 2	• **Enable** (Default) • Disable	Disabling an entry will prevent the associated device from being enumerated during subsequent boots. Gray-out when **Onboard LAN 1** is Disabled.
Onboard LAN 2	• **Enable** (Default) • Disable	Disabling an entry will prevent the associated device from being enumerated during subsequent boots. This item appears when PassThrough is present. Disabling this entry will disable all Onboard LAN 2 Ports. All Onboard LAN 2 Port options in this page shall be grayed-out.
LAN Port 3	• **Enable** (Default) • Disable	Disabling an entry will prevent the associated device from being enumerated during subsequent boots. This item appears when PassThrough is present, and will gray-out when **Onboard LAN 2** is Disabled.
LAN Port 4	• **Enable** (Default) • Disable	Disabling an entry will prevent the associated device from being enumerated during subsequent boots. This item appears when PassThrough is present, and will gray-out when **Onboard LAN 2** is Disabled.

Enable/Disable Adapter Option ROM Support

Notes:

- According to your system configuration (e.g. which riser is installed), this menu may be different.
- The items' actual order of this menu may be different from the following table because some of them are dynamically scanned.
- If any onboard/slot device option is changed to **Legacy**, onboard video option will be also changed to **Legacy** automatically. At this moment, onboard video option can't be changed, either. If you want to change onboard video option, make sure the onboard/slot device option is not legacy.

Item	Options	Description
Network	• Do not launch • **UEFI** (Default) • Legacy	Control the execution of UEFI and Legacy Network OpROM.
Storage	• Do not launch • **UEFI** (Default) • Legacy	Control the execution of UEFI and Legacy Storage OpROM.

Video	• Do not launch • **UEFI** (Default) • Legacy	Control the execution of UEFI and Legacy Video OpROM.
Other PCI devices	• Do not launch • **UEFI** (Default) • Legacy	Determine OpROM execution policy for devices other than Network, Storage, or Video.

Set Option ROM Execution Order

Note: The items in this menu are hardware-dependent.

Item	Options	Description
Set Option ROM Execution Order	• Onboard Video • Onboard LAN 1 • Onboard LAN 2 • Slot 1 • Slot 6 • Slot 2/3 • Slot 4/5 • Slot 6/7 • Slot 8/9	Select the load order for legacy PCI option ROM(s). Use the + key to execute the selected devices ROM sooner or – key to execute it later. **Notes:** • This order may be overridden for devices controlled by UEFI thunk drivers. • Slot 6 appears when PCIe Riser is installed. • Onboard LAN 2 appears when PassThrough is present. • Slot 2/3, Slot 4/5, Slot 6/7 and Slot 8/9 appear when M.2 data adapter with hardware RAID is installed at corresponding locations.

PCIe Gen1/Gen2/Gen3 Speed Selection

Note: The items in this menu are hardware-dependent.

Item	Options	Description
Slot 1	• Gen1 • Gen2 • **Gen3** (Default)	Set the PCIe slot as Generation 1, 2 or 3. **Note:** Some adapters may not operate correctly in Gen2 or Gen3. Make sure to power OFF and power ON the system for these settings to take effect.
Slot 2	• Gen1 • Gen2 • **Gen3** (Default)	Set the PCIe slot as Generation 1, 2 or 3. This slot numbering appears only when M.2 data adapter is installed at left wing. **Note:** Some adapters may not operate correctly in Gen2 or Gen3. Make sure to power OFF and power ON the system for these settings to take effect.

Slot 3	• Gen1 • Gen2 • **Gen3** (Default)	Set the PCIe slot as Generation 1, 2 or 3. This slot numbering appears only when M.2 data adapter is installed at left wing. **Note:** Some adapters may not operate correctly in Gen2 or Gen3. Make sure to power OFF and power ON the system for these settings to take effect.
Slot 4	• Gen1 • Gen2 • **Gen3** (Default)	Set the PCIe slot as Generation 1, 2 or 3. This slot numbering appears only when M.2 data adapter is installed at left wing. **Note:** Some adapters may not operate correctly in Gen2 or Gen3. Make sure to power OFF and power ON the system for these settings to take effect.
Slot 5	• Gen1 • Gen2 • **Gen3** (Default)	Set the PCIe slot as Generation 1, 2 or 3. This slot numbering appears only when M.2 data adapter is installed at left wing. **Note:** Some adapters may not operate correctly in Gen2 or Gen3. Make sure to power OFF and power ON the system for these settings to take effect.
Slot 6	• Gen1 • Gen2 • **Gen3** (Default)	Set the PCIe slot as Generation 1, 2 or 3. This slot numbering appears when M.2 data adapter is installed at right wing or PCIe Riser is installed **Note:** Some adapters may not operate correctly in Gen2 or Gen3. Make sure to power OFF and power ON the system for these settings to take effect.
Slot 7	• Gen1 • Gen2 • **Gen3** (Default)	Set the PCIe slot as Generation 1, 2 or 3. This slot numbering appears only when M.2 data adapter is installed at right wing. **Note:** Some adapters may not operate correctly in Gen2 or Gen3. Make sure to power OFF and power ON the system for these settings to take effect.

Slot 8	• Gen1 • Gen2 • **Gen3** (Default)	Set the PCIe slot as Generation 1, 2 or 3. This slot numbering appears only when M.2 data adapter is installed at right wing. **Note:** Some adapters may not operate correctly in Gen2 or Gen3. Make sure to power OFF and power ON the system for these settings to take effect.
Slot 9	• Gen1 • Gen2 • **Gen3** (Default)	Set the PCIe slot as Generation 1, 2 or 3. This slot numbering appears only when M.2 data adapter is installed at right wing. **Note:** Some adapters may not operate correctly in Gen2 or Gen3. Make sure to power OFF and power ON the system for these settings to take effect.

Console Redirection Settings

Item	Options	Description
COM Port 1	• **Enable** (Default) • Disable	Enable/disable COM1 device. If this item is set to **Disable**, the associated COM1 terminal settings will be hidden.
COM Port 2	• **Enable** (Default) • Disable	Enable/disable COM2 device. If this item is set to **Disable**, the associated COM2 terminal settings will be hidden.
Console Redirection	• Enable • Disable • **Auto** (Default)	Set remote console redirection preference to enable or disable console redirection. While **Auto** is set, console redirection will be enabled automatically if IPMI Serial over LAN status is active.
Serial Port Sharing	• Enable • **Disable** (Default)	Enable the System Baseboard Management Controller to allow access to the system serial port. • **Enable**: the BMC will be allowed to control the serial communication port as requested by remote control commands. • **Disable**: the serial port will be assigned to the BMC unless the Serial Port Access Mode is set to Disable.
Serial Port Access Mode	• Shared • Dedicated • **Disable** (Default)	Control the access the System Baseboard Management Controller has over the system serial port. • **Shared mode**: the serial port will be available for POST and operating system use; however the BMC will/can monitor the serial data for a takeover control sequence. • **Dedicated mode**: the BMC will have complete control of the serial port and POST and/or the operating system will not be able to use the serial port. • **Disable mode**: the BMC will not have any access to the serial port.

SP Redirection	• Enable • **Disable** (Default)	This item is only displayed while **Console Redirection**, **COM Port 1** and **COM Port 2** are all set to **Enable**. It allows you to choose which COM port to have the redirection. **Note:** This item will be only displayed when Console Redirection is set to Enable.
Legacy OS/Option ROM Display	• COM Port 2 • **COM Port 1** (Default)	Select a COM port to display redirection of Legacy OS and Legacy OPROM Messages.
COM1 Settings		Settings required for serial connections used for asynchronous start-stop communication.
COM1 Baud Rate	• **115200** (Default) • 57600 • 38400 • 19200 • 9600	Control the connection speed between the host and remote system.
COM1 Data Bits	• **8** (Default) • 7	Set the number of data bits in each character.
COM1 Parity	• **None** (Default) • Odd • Even	Select parity bit in each character to be None, Odd, or Even. **None** is the default setting and means that no parity bit is sent at all.
COM1 Stop Bits	• 2 • **1** (Default)	Set Stop Bits. Stop Bits sent at the end of every character allow the signal receiver to detect the end of a character and to resynchronize with the character stream.
COM1 Terminal Emulation	• VT100 • VT-UTF8 • **ANSI** (Default)	• **VT100**: select this item if the remote emulator does not support ANSI text graphics.
COM1 Active After Boot	• Enable • **Disable** (Default)	• **Enable**: Legacy Console Redirection is enabled for legacy OS. • **Disable**: Legacy Console Redirection is disabled before booting to legacy OS.
COM1 Flow Control	• **Disable** (Default) • Hardware	• **Disable**: the default setting. • **Hardware**: select this item only if the remote emulator support and is using hardware flow control.
COM2 Settings		Settings are required for serial connections which are used for asynchronous start-stop communication.
COM2 Baud Rate	• **115200** (Default) • 57600 • 38400 • 19200 • 9600	Control the connection speed between the host and remote system.

COM2 Data Bits	• **8** (Default) • 7	Set the number of data bits in each character.
COM2 Parity	• **None** (Default) • Odd • Even	Select parity bit in each character to be none, odd, or even. **None** is the default setting and means that no parity bit is sent at all.
COM2 Stop Bits	• 2 • **1** (Default)	Set Stop Bits. Stop Bits sent at the end of every character allow the signal receiver to detect the end of a character and to resynchronize with the character stream.
COM2 Terminal Emulation	• VT100 • VT-UTF8 • **ANSI** (Default)	• **VT100**: select this item if the remote emulator does not support ANSI text graphics.
COM2 Active After Boot	• Enable • **Disable** (Default)	• **Enable**: Legacy Console Redirection is enabled for legacy OS. • **Disable**: Legacy Console Redirection is disabled before booting to legacy OS.
COM2 Flow Control	• **Disable** (Default) • Hardware	• **Hardware**: select this item only if the remote emulator support and is using hardware flow control.

USB Configuration

Item	Options	Description
USB Mass Storage Driver Support	• **Enable** • Disable	Enable/Disable USB Mass Storage Driver Support. This setting only takes effect in post time.
USB Front Port 1	• **Enable** • Disable	Disable USB individual ports.
USB Front Port 2	• **Enable** • Disable	Disable USB individual ports.
USB Rear Port 1/2	• **Enable** • Disable	Disable USB individual ports.

Intel® VMD technology

Item	Options	Description
Intel® VMDTechnology	N/A	Press Enter to pop up the Intel® VMD for Volume Management Device Configuration menu.
Enable/Disable Intel® VMD	• Enabled • **Disabled**	Enable/Disable Intel® Volume Management Device Technology. **Disabled** is the default setting.

Driver health

This menu displays the health of the controllers in the system, which is reported by their corresponding drivers.

Note: According to your system configuration (e.g. which riser is installed), this menu may be different.

Table 5. Driver health details

Item	Options	Description
The platform is:	• Healthy • Repair Required • Configuration Required • Operation Failed • Reconnect Required • Reboot Required • Shutdown Required • No Operation Required	The health of the controllers in the system will be displayed here.
Driver/Controller Status		

Table 5. Driver health details (continued)

Controller Name - Status	• Healthy • Repair Required • Configuration Required • Operation Failed • Reconnect Required • Reboot Required • Shutdown Required • No Operation Required	
POST Attempts Driver	• Healthy • Repair Required • Configuration Required • Operation Failed • Reconnect Required • Reboot Required • Shutdown Required • No Operation Required	
Partition Driver (MBR/GPT/El Torito)	• Healthy • Repair Required • Configuration Required • Operation Failed • Reconnect Required • Reboot Required • Shutdown Required • No Operation Required	

Foreign Devices

This menu displays which foreign device(s) is or are installed.

Notes:

- Depending on your system configuration (for example, which device is installed), this page might be different.

- SAS/SATA drives or NVMe drives connected to a storage controller will be displayed in the storage controller submenu: **System settings → Storage → Storage controller xxxx**.
- NVMe drives connected to the system without raid controller (sometimes using a retimer) will be displayed in one of the following pages:
  - **System settings → Foreign Devices**
  - **System settings → Storage**

Table 6. Foreign Devices

Item	Description
Non devices (Unclassified devices)	Display the unclassified device.
Video device	Display the video device.
Input device	Display the input device.
Onboard device	Display the on board device.
Other device	Display the other device.

Legacy BIOS

Use this menu to configure system UEFI firmware execution environment preferences for supporting legacy OS and legacy Option ROM.

Note: When Secure Boot is enabled, the following message will be displayed in this menu:
`Legacy BIOS is disabled due to secure boot is enabled.`

Table 7. Legacy BIOS details

Item	Options	Description
Legacy BIOS	• **Enable** (Default) • Disable	Enable/Disable the system UEFI firmware execution environment for supporting legacy OS and legacy Option ROM.
Rehook INT 19h	• Enable • **Disable** (Default)	When this item is enabled, it prevents devices from taking control of the boot process.

Memory

This menu displays and provides options to change the memory setting.

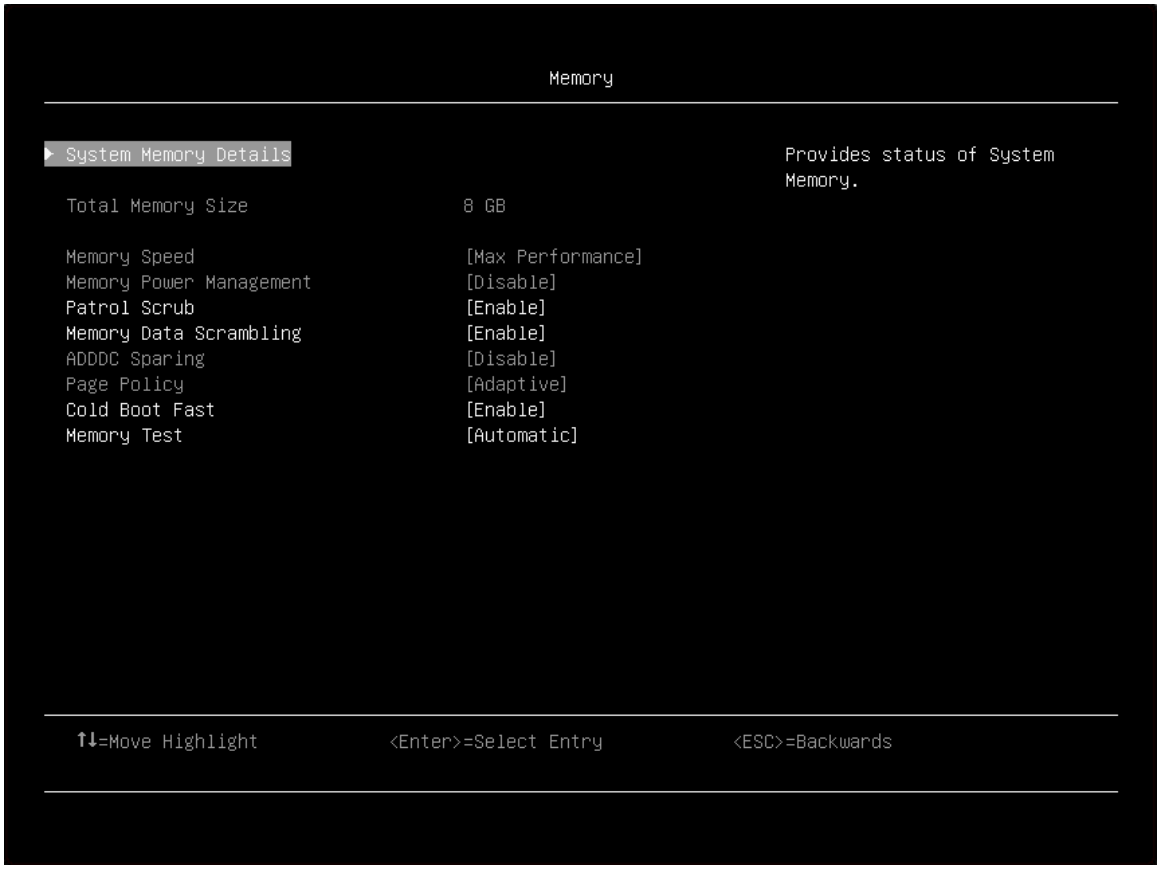


Table 8. Memory details

Item	Options	Description
"System Memory Details" **on page 23**		View the status of system memory.
Total Memory Size	yyyy GB	This item is hardware dependent.

Table 8. Memory details (continued)

Memory Speed	• Minimal Power • Balanced • **Max Performance** (Default)	Select the desired memory speed. • **Minimal power**: maximizes power savings. • **Balanced**: offers a balance between performance and power. • **Max Performance**: maximizes performance. When a preset mode is selected, the low-level setting are not changeable and will be grayed out. To change the settings, select **Choose Operating Mode → Custom Mode**.
Memory Power Management	• Automatic • **Disable** (Default)	• **Automatic**: suitable for most applications. • **Disable**: provides maximum performance but minimum power savings. When a preset mode is selected, the low-level setting are not changeable and will be grayed out. To change the settings, select **Choose Operating Mode → Custom Mode**.
Patrol Scrub	• **Enable** (Default) • Disable	Enable this item to proactively searches and repairs correctable errors in the system memory.
Memory Data Scrambling	• **Enable** (Default) • Disable	Enable/Disable memory data scrambling.
ADDDC Sparing	• Enable • **Disable** (Default)	Enable/Disable ADDDC Sparing. This setting is disabled and grayed out when Page policy is Adaptive. Enabling ADDDC may cause reduced reliability of memory error correction in virtual lockstep under rare conditions.
Page Policy	• **Adaptive** (Default) • Closed	• **Adaptive page policy**: improves performance for applications with a highly localized memory access pattern. • **Closed page policy**: benefits applications that access memory more randomly. **Note:** This item will be set to Closed and grayed out when ADDDC Sparing is set to Enable.
Cold Boot Fast	• **Enable** (Default) • Disable	Enable/Disable Cold Boot Fast.
Memory Test	• **Automatic** (Default) • Disable • Enable	• **Automatic**: skips the memory test by default unless memory configuration is changed or the last time the test has been run is more than 90 days ago. • **Disable**: disables this feature. • **Enable**: enables the memory test during normal boot.

Table 8. Memory details (continued)

2x Refresh Rate	• **Disabled** (Default) • Auto	• **Disabled**: sets system with 1x refresh rate. • **Auto**: sets 2x refresh rate if system supports. Choose refresh rate 2x to mitigate rowhammer issue which may cause side effect on performance. When the system has 16Gb 3DS LRDIMM/RDIMM or 16Gb Quad Rank LRDIMMS, 2x refresh rate is not supported.
Refresh Watermarks	• **Auto** (Default) • Low WM	• **Low WM**: mitigates power delivery issues with 128 GB or larger DIMM, and mitigates failures caused by rowhammer traffic patterns. • **Auto**: uses Low Watermarks for 16 Gb DIMM, and use High Watermarks for other DIMM configurations.

System Memory Details

System Memory Details

Item	Description
DIMM Details For Processor X	View the status of DIMMs. See **DIMM Details** below for more details.

DIMM Details

Note: The items in this menu is hardware-dependent.

Item	Description
DIMM 1	When DIMM has DBE, the item will turn from string description to Enable/Disable option, and it will be Enabled by default.
DIMM 2	
DIMM 3	
DIMM 4	

Network

This menu displays network devices and network related setting.

Note: The items in this menu are configuration dependent.

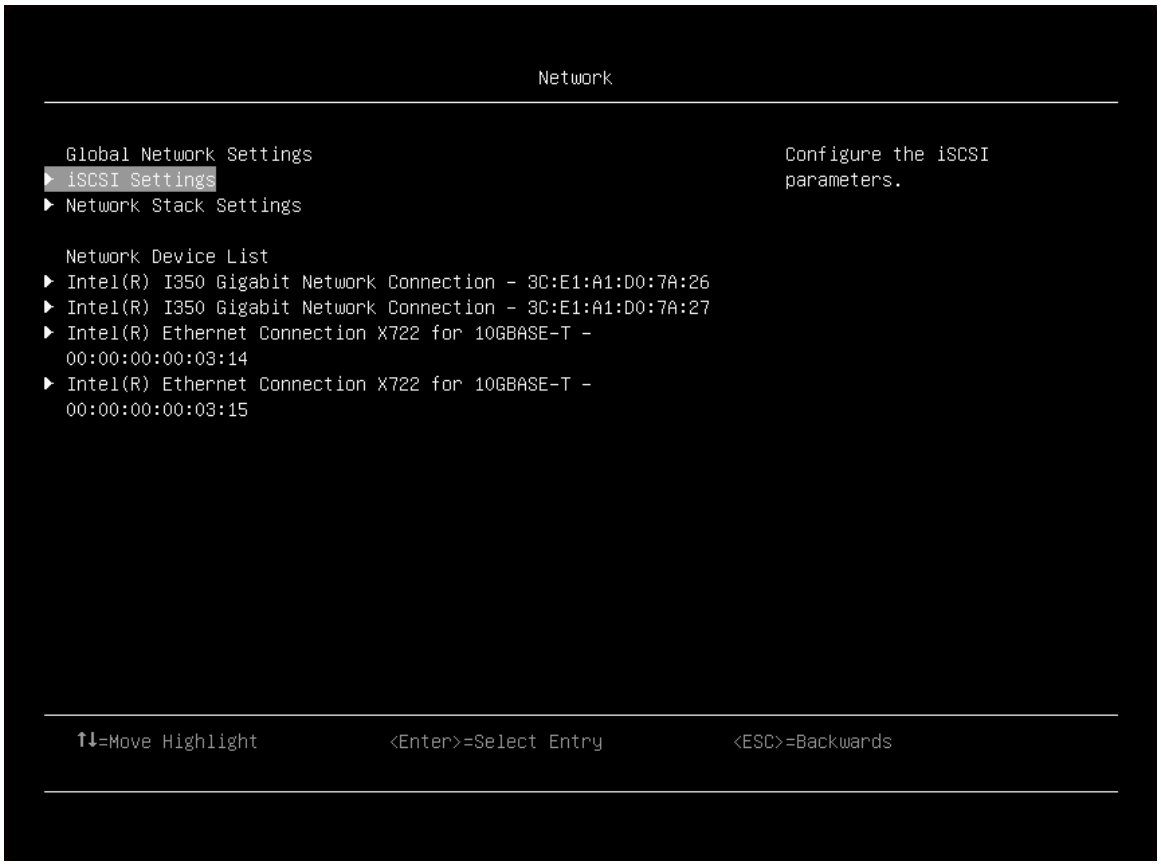


Table 9. Network details

Item	Description
Global Network Settings	View global network settings.
"iSCSI Configuration" on page 24	Configure the iSCSI parameters.
"Network Stack Settings" on page 28	Change network stack settings.
Network Device List	View network device list below. The information of the on-board card or add-on card will be displayed here, for example, the title of the card, the MAC address, or PFA.

iSCSI Configuration

Item	Options	Description
iSCSI Initiator Name	Iqn.1986-03.com.example	The worldwide unique name of iSCSI Initiator. Only IQN format is accepted. Range is from 4 to 233.
"Add an Attempt" on page 25		Add an attempt.
List of Attempts Selecting any item in the list will lead to "Attempt Configuration" on page 25.		After added, the attempt will be listed here. The values of each attempt will be displayed as follows: MAC: XX:XX:XX:XX:XX:XX, PFA: Bus XX | Dev XX | Func XX, "iSCSI Mode": [the option name], "Internet Protocol": [the setting name]. Exact value will be different depends on the attempt settings.

“Delete Attempts” on page 28		Delete one or more attempts.
“Change Attempt Order” on page 28		Change the order of Attempts using +/- keys. Use arrow keys to select the attempt then press +/- to move the attempt up/down in the attempt order list.

Add an Attempt

Table 10. MAC Selection

Item	Description
List of NICs in the system (e. g. MAC XX:XX:XX:XX:XX:XX)	Select the item that you want to add. The format of the attempt are as follows: PFA: Bus XX | Dev XX | Func XX

Attempt Configuration

Item	Options	Description
iSCSI Attempt Name		View the human name which is defined for this attempt. Maximum length of each name is up to 96 characters.
iSCSI Mode	• **Disable** (Default) • Enable • Enable for MPIO	Enable/Disable iSCSI mode, or enable iSCSI mode for MPIO. **Note:** Make sure all necessary items (e.g. initiator IP, target IP and authentication settings) are set appropriately before you enable this item. Otherwise, this attempt may be lost after reboot.
Internet Protocol	• **IPv4** (Default) • IPv6 • Autoconfigure	• **IPv4**: the default setting. • **IPv6**: initiator IP address is system assigned. • **Autoconfigure**: iSCSI driver will attempt to connect iSCSI target via IPv4 stack. If failed, then it will attempt to connect via IPv6 stack.
Connection Retry Count	**0** (Default)	The minimum value is 0 and the maximum is 16. 0 means no retry.
Connection Establishing Timeout	**1000** (Default)	The timeout value is in milliseconds. The minimum value is 100 milliseconds and the maximum is 20 seconds.
OUI-format ISID		OUI-format ISID is in 6 bytes. The format will be like as the following: 3CD30AC68EF8. Default values are derived from MAC address. Only the last 3 bytes are configurable. These values are taken from **Configure ISID** control.
Configure ISID		OUI-format ISID is in 6 bytes. The format will be like as the following: C68EF8. Default values are derived from MAC address. Only the last 3 bytes are configurable. For example: Update 0ABBCCDDEEFF to 0ABBCCF07901 by inputting F07901.
Enable DHCP	• **Empty** (Default) • X	Check the option to enable DHCP.

<table>
<tr><td>Initiator IP Address

Note: The items will be displayed when Enable DHCP is not enabled.</td><td>0.0.0.0</td><td>Enter IP address in dotted-decimal notation.</td></tr>
<tr><td>Initiator Subnet Mask

Note: The items will be displayed when Enable DHCP is not enabled.</td><td>0.0.0.0</td><td>Enter IP address in dotted-decimal notation.</td></tr>
<tr><td>Gateway

Note: The items will be displayed when Enable DHCP is not enabled.</td><td>0.0.0.0</td><td>Enter IP address in dotted-decimal notation.</td></tr>
<tr><td>Initiator IP: 0.0.0.0

Note: The item will be displayed when Enable DHCP is enabled.</td><td></td><td></td></tr>
<tr><td>Get target info via DHCP
Note: The item will be displayed when Enable DHCP is enabled.</td><td>• Empty (Default)
• X</td><td>Check the option if the target info will be gotten via DHCP.</td></tr>
<tr><td>Target Name

Note: The item will NOT be displayed when Get target info via DHCP is Enabled.</td><td></td><td>The worldwide unique name of the target. Only iqn. Format is accepted.</td></tr>
<tr><td>Target Address

Note: The item will NOT be displayed when Get target info via DHCP is Enabled.</td><td>0.0.0.0</td><td>Enter IP address in dotted-decimal notation.</td></tr>
<tr><td>Target Port

Note: The item will NOT be displayed when Get target info via DHCP is Enabled.</td><td>3260</td><td></td></tr>
<tr><td>Boot LUN

Note: The item will NOT be displayed when Get target info via DHCP is Enabled.</td><td>0</td><td>Hexadecimal representation of the LUN number. For example: 4751-3A4F-6b7e-2F99, 6734-9-156f-127, 4186-9.
Note:
<table><tr><th>Message box</th><th>What it means</th></tr><tr><td>ISCSI Message
Invalid LUN string!
Ok</td><td>The Boot LUN input is invalid.</td></tr></table></td></tr>
<tr><td>Authentication Type</td><td>• CHAP
• None (Default)</td><td>View the Authentication method is CHAP or None.</td></tr>
<tr><td>CHAP Type

Note: The items will be displayed when Authentication Type is CHAP.</td><td>• One way
• Mutual (Default)</td><td>View the CHAP Type is One way or Mutual.</td></tr>
</table>

<table>
<tr><td>CHAP Name

Note: The items will be displayed when Authentication Type is CHAP.</td><td></td><td></td></tr>
<tr><td>CHAP Secret

Note: The items will be displayed when Authentication Type is CHAP.</td><td></td><td>The minimum length is 12 bytes, and the maximum length is 16 bytes. To set CHAP secret, create a new password and confirm it by entering it again. When the CHAP Secret is successfully set, CHAP Status will be “Installed.”

Note:<table><tr><th>Message box</th><th>What it means</th></tr><tr><td>ERROR
Invalid Password
Ok</td><td>The two passwords that you entered do not match with each other.</td></tr><tr><td>ERROR
Invalid Input Range
Ok</td><td>The password contains insufficient characters.</td></tr></table></td></tr>
<tr><td>CHAP Status

Note: The items will be displayed when Authentication Type is CHAP.</td><td>• Not Installed (Default)
• Installed</td><td>• Not Installed: CHAP Name and CHAP Secret are not set.
• Installed: CHAP Name and CHAP Secret are set.</td></tr>
<tr><td>Reverse CHAP Name

Note: The items will be displayed when CHAP Type is Mutual.</td><td></td><td></td></tr>
<tr><td>Reverse CHAP Secret

Note: The items will be displayed when CHAP Type is Mutual.</td><td></td><td>The minimum length is 12 bytes, and the maximum length is 16 bytes. Create a new password and confirm it by entering it again. When Reverse CHAP Secret is successfully set, Reverse CHAP Status will be “Installed.”

Note:<table><tr><th>Message box</th><th>What it means</th></tr><tr><td>ERROR
Invalid Password
Ok</td><td>The two passwords that you entered do not match with each other.</td></tr><tr><td>ERROR
Invalid Input Range
Ok</td><td>The password contains insufficient characters.</td></tr></table></td></tr>
<tr><td>Reverse CHAP Status</td><td>• Not Installed
• Installed</td><td>• Not Installed: Reverse CHAP Name and Reverse CHAP Secret are not set.
• Installed: Reverse CHAP Name and Reverse CHAP Secret are set.</td></tr>
</table>

Save Changes		Reboot System manually for changes to take effect.
Back to Previous Page		Go back to the previous page.

Delete Attempts

Item	Options	Description
List of Attempts e.g. Attempt 1, Attempt 2	• **Empty** (Default) • X	Check the option to delete the attempt. The values of each attempt will be displayed as below: MAC: XX:XX:XX:XX:XX:XX, PFA: Bus XX | Dev XX | Func XX, “iSCSI Mode”: [%s1], “Internet Protocol”: [%s2] Exact value will be different depends on the attempt settings. • %s1: the option name for iSCSI Mode. • %s2: the setting name for Internet Protocol.
Commit Changes and Exit		Save changes and exit.
Discard Changes and Exit		Discard changes and exit.

Change Attempt Order

Item	Options	Description
Change Attempt Order **Note:** Existing attempts will be listed here.	• Attempt 1 • Attempt 2	Change the order of the attempts by using +/- keys. Use arrow keys to select the attempt, and then press +/- to move the attempt up/down in the order list.
Commit Changes and Exit		Save changes and exit.
Discard Changes and Exit		Discard changes and exit.

Network Stack Settings

Item	Options	Description
Network Stack	• **Enable** (Default) • Disable	Enable/Disable UEFI Network Stack.
IPv4 PXE Support	• **Enable** (Default) • Disable	Enable IPv4 PXE Boot Support. If this item is disabled, IPv4 PXE boot option will not be created.
IPv4 HTTP Support	• Enable • **Disable** (Default)	Enable IPv4 HTTP Boot Support. If this item is disabled, IPv4 HTTP boot option will not be created.
IPv6 PXE Support	• **Enable** (Default) • Disable	Enable IPv6 PXE Boot Support. If this item is disabled, IPv6 PXE boot option will not be created.
IPv6 HTTP Support	• Enable • **Disable** (Default)	Enable IPv6 HTTP Boot Support. If this item is disabled, IPv6 HTTP boot option will not be created.
IPSEC Certificate	• **Enable** (Default) • Disable	It is supported to enable/disable IPSEC certificate for Ikev.

<table>
<tr><td>PXE boot wait time</td><td>0 (Default)</td><td>Set the wait time for you to press ESC key to abort the PXE boot. Use either +/- or numeric keys to set the value, which is counted in seconds.

Note:
<table><tr><th>Message box</th><th>What it means</th></tr><tr><td>ERROR
Invalid Input Range
Ok</td><td>An invalid value is input.</td></tr></table></td></tr>
<tr><td>Media detect count</td><td>1 (Default)</td><td>Number of times presence of media will be checked. Use either +/- or numeric keys to set the value.

Note:
<table><tr><th>Message box</th><th>What it means</th></tr><tr><td>ERROR
Invalid Input Range
Ok</td><td>An invalid value is input.</td></tr></table></td></tr>
</table>

Operating modes

Select the operating mode based on your preference.

Table 11. Operating modes details

Item	Options	Description
Choose Operating Mode	• Minimal Power • Efficiency – Favor Power • **Efficiency – Favor Performance** (Default) • Custom Mode • Maximum Performance	Select the operating mode based on your preference. The efficiency of power saving and the system performance are highly dependent on your hardware and software environment. • **Custom Mode**: select this mode if you are going to configure the following items: – Memory speed – Memory Power Management – CPU P-state control – Turbo mode – Energy Efficient Turbo – C-States – Power/Performance Bias – Platform Controlled Type – MONITOR/MWAIT
Memory Speed	• Minimal Power • Balanced • **Max Performance** (Default)	Select your desired memory speed. • **Minimal power mode**: maximizes power savings. • **Balanced mode**: offers a balance between performance and power efficiency. • **Maximum performance**: maximizes the performance. When a preset mode is selected, the low-level setting are not changeable and will be grayed out. To change the settings, select **Choose Operating Mode → Custom Mode**.
Memory Power Management	• Automatic • **Disabled** (Default)	• **Automatic**: suitable for most applications. • **Disabled**: provides maximum performance but minimum power savings. When a preset mode is selected, the low-level setting are not changeable and will be grayed out. To change the settings, select **Choose Operating Mode → Custom Mode**.

Table 11. Operating modes details (continued)

CPU P-state Control	• None • Legacy • **Autonomous** (Default) • Cooperative	Select the method to control CPU P-states (performance states). • **None**: disables all P-states and the CPUs run at either their rated frequency or in turbo mode (if turbo is enabled). • **Legacy**: the CPU P-states will be presented to the operating system (OS) and the OS power management (OSPM) will directly control which P-state is selected. • **Autonomous**: the P-states are controlled fully by system hardware. No P-state support is required in the OS or VM. • **Cooperative**: a combination of Legacy and Autonomous. The P-states are still controlled in hardware but the OS can provide hints to the hardware for P-state limits and the desired setting. When a preset mode is selected, the low-level setting are not changeable and will be grayed out. To change the settings, select **Choose Operating Mode → Custom Mode**.
Turbo Mode	• **Enable** (Default) • Disable	Enabling turbo mode can boost the overall CPU performance when all CPU cores are not being fully utilized. A CPU core can run above its rated frequency for a short period of time when it is in turbo mode. When a preset mode is selected, the low-level setting are not changeable and will be grayed out. To change the settings, select **Choose Operating Mode → Custom Mode**.
Energy Efficient Turbo	• **Enable** (Default) • Disable	When energy efficient turbo is enabled, the CPU's optimal turbo frequency will be tuned dynamically based on CPU utilization. This item is also related to the setting of **Power/Performance Bias**. When a preset mode is selected, the low-level setting are not changeable and will be grayed out. To change the settings: 1. Select **System Settings → Operating Modes → Choose Operating Mode → Custom Mode**. 2. Select **System Settings → Operating Modes → Turbo Mode → Enable**

Table 11. Operating modes details (continued)

C-States	• Legacy • **Autonomous** (Default) • Disable	C-states reduce CPU idle power. • **Legacy**: When it is selected, the operating system initiates the C-state transitions. For E5/E7 CPUs, ACPI C1/C2/C3 map to Intel C1/C3/C6. For 6500/7500 CPUs, ACPI C1/C3 map to Intel C1/C3 (ACPI C2 is not available). Some OS SW may defeat the ACPI mapping (e.g. intel_idle driver). • **Autonomous**: When it is selected, HALT and C1 request get converted to C6 requests in hardware. When a preset mode is selected, the low-level setting are not changeable and will be grayed out. To change the settings, select **Choose Operating Mode → Custom Mode**.
Power/Performance Bias	• **Platform Controlled** (Default) • OS Controlled	Power/Performance bias determines how aggressively the CPU will be power managed and placed into turbo. • **Platform Controlled**: the system controls the setting. **Platform Controlled** is the default setting. • **OS Controlled**: allows the operating system to control it. Not all OSes support this feature. When a preset mode is selected, the low-level setting are not changeable and will be grayed out. To change the settings, select **Choose Operating Mode → Custom Mode**.
Platform Controlled Type	• Maximum Performance • **Efficiency - Favor Performance** (Default) • Minimal Power	• **Maximum Performance**: allows the most aggressive use of turbo and power management functions are disabled, thereby increasing power consumption. • **Efficiency - Favor Performance**: the default setting. • **Minimal Power**: disables turbo and maximizes the use of power management features. When a preset mode is selected, the low-level setting are not changeable and will be grayed out. To change the settings, select **Choose Operating Mode → Custom Mode**.
ADDDC Sparing	• Enable • **Disable** (Default)	Enable/Disable ADDDC Sparing. This setting is disabled and grayed out when **Page Policy** is Adaptive. Enabling ADDDC may cause reduced reliability of memory error correction in virtual lockstep under rare conditions.

Table 11. Operating modes details (continued)

Page Policy	• **Adaptive** (Default) • Closed	• **Adaptive page policy**: improves performance for applications with a highly localized memory access pattern. • **Closed page policy**: benefits applications that access memory more randomly. **Note:** This item will be set to Closed and grayed out when **ADDDC Sparing** is set to Enable.
MONITOR/MWAIT	• **Enable** (Default) • Disable	MONITOR/MWAIT instructions are used to engage C-states. Some operating systems will re-enable C-states even when they are disabled in setup. To prevent this, you also need to disable this item, and then change the following settings: 1. **Operating Modes → Choose Operating Mode → Custom Mode**. 2. **Operating Modes → C-States → Disable**

Power

Use this menu to configure power scheme options.

Table 12. Power details

Item	Options	Description
Power/Performance Bias	• **Platform Controlled** (Default) • OS Controlled	Power/Performance bias determines how aggressively the CPU will be power managed and placed into turbo. Not all OSes support this feature. • **Platform Controlled**: The system controls the setting. • **OS Controlled**: The operating system is allowed to control it. When a preset mode is selected, the low-level setting are not changeable and will be grayed out. To change the settings, select **Choose Operating Mode → Custom Mode**.
Platform Controlled Type	• Maximum Performance • **Efficiency - Favor Performance** (Default) • Efficiency - Favor Power • Minimal Power	• **Maximum Performance**: allows the most aggressive use of turbo and power management functions are disabled, thereby increasing power consumption. • **Minimal Power**: disables turbo and maximizes the use of power management features. When a preset mode is selected, the low-level setting are not changeable and will be grayed out. To change the settings, select **Choose Operating Mode → Custom Mode**.
Workload Configuration	• **Balanced** (Default) • I/O sensitive	• **I/O sensitive**: this option should be used with expansion cards that require high I/O bandwidth when the CPU cores are idle and allow enough frequency for the workload.
ACPI Fixed Power Button	• **Enable** (Default) • Disable	When the setting is disabled, manually pressing the power button which is located in front of the system won't execute the Operating System's Power Button Policy such as shutdown, turn off monitor, etc. In addition, "Shut down OS and ..." options under the iMM Server Power Actions feature will be disabled.

Processors

This menu displays and provides options to change the processor settings.

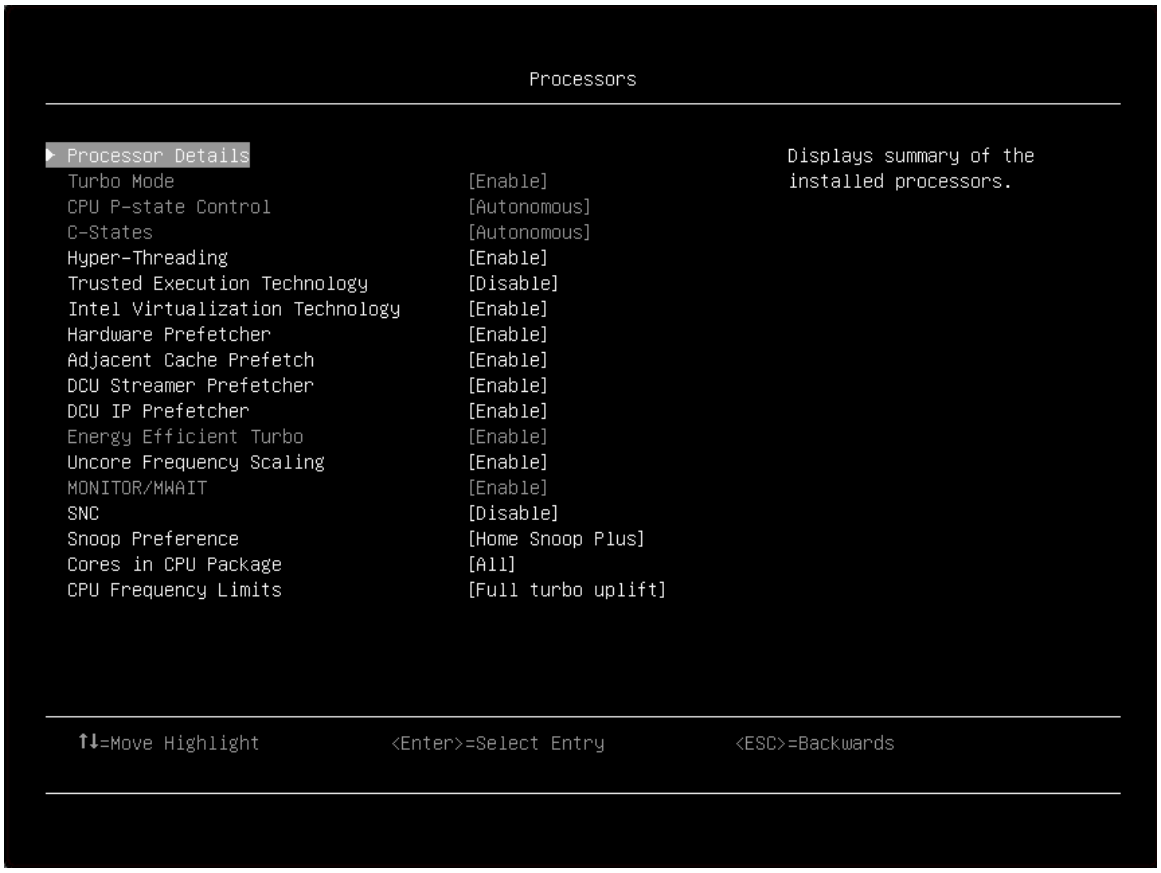


Table 13. Processors details

Item	Options	Description
"Processor details" on page 38		View the summary of the installed processors.
Turbo Mode **Note:** If the CPU doesn't support the feature, this item will not be displayed.	• **Enable** (Default) • Disable	Enabling turbo mode can boost the overall CPU performance when all CPU cores are not being fully utilized. A CPU core can run above its rated frequency for a short period of time when it is in turbo mode. When a preset mode is selected, the low-level setting are not changeable and will be grayed out. To change the settings, select **Choose Operating Mode → Custom Mode**.

Table 13. Processors details (continued)

CPU P-state Control	• None • Legacy • **Autonomous** (Default) • Cooperative	Select a method to control CPU P-states (performance states). • **None**: disables all P-states and the CPUs run at either their rated frequency or in turbo mode (if turbo is enabled). • **Legacy**: the CPU P-states will be presented to the operating system (OS) and the OS power management (OSPM) will directly control which P-state is selected. • **Autonomous**: the P-states are controlled fully by system hardware. No P-state support is required in the OS or VM. • **Cooperative**: a combination of Legacy and Autonomous. The P-states are still controlled in hardware but the OS can provide hints to the hardware for P-state limits and the desired setting. When a preset mode is selected, the low-level setting are not changeable and will be grayed out. To change the settings, select **Choose Operating Mode → Custom Mode**.
C-States	• Legacy • **Autonomous** (Default) • Disable	C-states reduce CPU idle power. • **Legacy**: the operating system initiates the C-state transitions. For E5/E7 CPUs, ACPI C1/C2/C3 map to Intel C1/C3/C6. For 6500/7500 CPUs, ACPI C1/C3 map to Intel C1/C3 (ACPI C2 is not available). Some OS SW may defeat the ACPI mapping (e.g. intel_idle driver). • **Autonomous**: HALT and C1 request get converted to C6 requests in hardware. When a preset mode is selected, the low-level setting are not changeable and will be grayed out. To change the settings, select **Choose Operating Mode → Custom Mode**.
C1 Enhanced Mode **Note:** This item is displayed only when C-state is not Autonomous.	• **Enable** (Default) • Disable	Enabling C1E (C1 Enhanced) state saves power by halting CPU cores that are idle. An operating system that supports C1E state must be installed to take advantage of this feature. Setting changes will be taken effect after the next reboot. When a preset mode is selected, the low-level settings are not changeable and will be grayed out. If you would like to change the settings, please follow these steps below: 1. **System Settings → Operating Modes → Choose Operating Mode → Custom Mode**. 2. **System Settings → Processor → C-States → Legacy** or **Disable**.
Hyper-Threading **Note:** If the CPU doesn't support the feature, this item will not be displayed.	• **Enable** (Default) • Disable	Enable Hyper Threading, a software method to enable/ disable Logical Processor threads. **Note:** It requires a reboot for the change to take effect.

Table 13. Processors details (continued)

Trusted Execution Technology	• Enable • **Disable** (Default)	Enable Intel Trusted Execution Technology (Intel TXT).
Intel Virtualization Technology	• **Enable** (Default) • Disable	Enable the Virtualization Technology.
Hardware Prefetcher	• **Enable** (Default) • Disable	Lightly threaded applications and some benchmarks can benefit from having the hardware prefetcher enabled.
Adjacent Cache Prefetch	• **Enable** (Default) • Disable	Lightly threaded applications and some benchmarks can benefit from having the adjacent cache line prefetch enabled.
DCU Streamer Prefetcher	• **Enable** (Default) • Disable	Lightly threaded applications and some benchmarks can benefit from having the DCU streamer prefetcher enabled.
DCU IP Prefetcher	• **Enable** (Default) • Disable	It is recommended that DCU IP prefetcher is set as **Enable** for most environments. However, some environments may benefit from having it set as **Disable**, e.g. Java.
Energy Efficient Turbo	• **Enable** (Default) • Disable	• **Enable**: the CPU's optimal turbo frequency will be tuned dynamically based on CPU utilization. The **power/performance bias** setting also influences energy efficient turbo. When a preset mode is selected, the low-level settings are not changeable and will be grayed out. To change the settings: 1. Select **System Settings → Operating Modes → Choose Operating Mode → Custom Mode**. 2. Select **System Settings → Processors → Turbo Mode → Enable**
Uncore Frequency Scaling	• **Enable** (Default) • Disable	• **Enable**: the CPU uncore will dynamically change speed based on the workload. All miscellaneous logic inside the CPU package is considered to be the uncore.
MONITOR/MWAIT	• **Enable** (Default) • Disable	MONITOR/MWAIT instructions are used to engage C-states. Some operating systems will re-enable C-states even when they are disabled in setup. To prevent this, disable MONNITOR/MWAIT: 1. **System Settings → Operating Modes → Choose Operating Mode → Custom Mode**. 2. **System Settings → Processor → C-States → Disable**.
SNC	• Enable • **Disable** (Default)	SNC (sub NUMA cluster) partitions the cores and the last level cache into clusters with each cluster bound to a set of memory controllers in the system. SNC improves average latency to the last level cache.

Table 13. Processors details (continued)

Snoop Preference	• **Home Snoop Plus** (Default) • Home Snoop	Select the appropriate snoop mode based on the workload. However, the snoop mode preference may be changed if the current hardware configuration does not support the desired mode. Also not that SNC has priority over the snoop mode.
Cores in CPU Package	• **All** (Default) • 1 • . • . • . • n-1	Select the amount of cores enabled within each CPU Package. The options will be the maximum number of cores that the installed processor supports. For example, if 6 cores are supported, there will be All, 1, 2, 3 4, and 5.
CPU Frequency Limits **Note:** This item can be only available when **Turbo Mode** is enabled.	• **Full turbo uplift** (Default) • Restrict maximum frequency	The maximum frequency (turbo, AVX, and non turbo) can be restricted to a frequency that is between the maximum turbo frequency for the CPU installed and 1.2GHz. This can be useful for synchronizing CPU tasks. **Note:** The max frequency for N+1 cores cannot be higher than N cores. If an illegal frequency is entered, it will automatically be limited to a legal value. If the CPU frequency limits are being controlled through application software, leave this item at the default (**Full turbo uplift**) and change the settings by following these steps below: 1. **System Settings → Operating Modes → Choose Operating Mode → Custom Mode**. 2. **System Settings → Processor → Turbo Mode → Enable**
"CPU Frequency Limits" **on page 39**		The maximum frequency (turbo, AVX, and non turbo) can be restricted to a frequency that is between the maximum turbo frequency for the CPU installed and 1.2GHz. This can be useful for synchronizing CPU tasks. **Note:** The max frequency for N+1 cores cannot be higher than N cores. If an illegal frequency is entered, it will automatically be limited to a legal value. If the CPU frequency limits are being controlled through application software, leave this item at the default (**Full turbo uplift**) and change the settings by following these steps below: 1. **System Settings → Operating Modes → Choose Operating Mode → Custom Mode**. 2. **System Settings → Processor → Turbo Mode → Enable**

Processor details

Item	Description
Processor ID	Tag for the Processor ID.
Processor Frequency	Value for the Processor Frequency.

Processor Revision	Value for the Microcode Revision.
L1 Cache RAM	Amount of L1 Cache RAM.
L2 Cache RAM	Amount of L2 Cache RAM.
L3 Cache RAM	Amount of L3 Cache RAM.
Cores Per Socket (Supported/Enabled):	Number of supported and enabled processor cores per processor socket.
Threads Per Socket (Supported/ Enabled):	Number of supported and enabled processor threads per processor socket.
Processor Version	Version of Processor 1.

CPU Frequency Limits

Item	Options	Description
Processors X to X cores active	• **Max turbo frequency –1 bin** (Default) • Max turbo frequency –2 bins • Max turbo frequency –3 bins	The maximum frequency (turbo, AVX, and non turbo) can be restricted to a frequency that is between the maximum turbo frequency for the CPU installed and 1.2GHz. This can be useful for synchronizing CPU tasks. **Note:** The max frequency for N+1 cores cannot be higher than N cores. If an illegal frequency is entered, it will automatically be limited to a legal value. If the CPU frequency limits are being controlled through application software, leave this item at the default (**Full turbo uplift**).

Recovery and RAS

Use this menu to configure recovery policies and advanced reliability, availability, and serviceability settings.

Table 14. Recovery and RAS

Item	Description
"Advanced RAS" **on page 40**	Choose whether to enable various advanced RAS options.
"System Recovery" **on page 40**	Configure system recovery settings.

Advanced RAS

Item	Options	Description
Machine Check Recovery	• Enabled • **Disabled** (Default)	Enable software layers (OS, VMM, DBMS, Application) to assist in system recovery from hardware uncorrectable errors.
PCI Error Recovery	• Enable • **Disable** (Default)	• **Enable**: the system will be able to recover from an uncorrectable PCIe fault. The faulting PCIe device will be disabled for error containment, and the OS will be notified to rescan the PCIe buses. • **Disable**: an uncorrectable PCIe fault will result in an NMI.

System Recovery

Item	Options	Description
POST Watchdog Timer	• Enable • **Disable** (Default)	Enable/Disable POST Watchdog Timer.

POST Watchdog Timer Value	[5]	Enter POST loader Watchdog timer value in minutes from the specified range (5-20).
Reboot System On NMI	• **Enable** (Default) • Disable	Enable/Disable reboot of the system during non-maskable interrupt.

Security

Use this menu to configure system security settings.

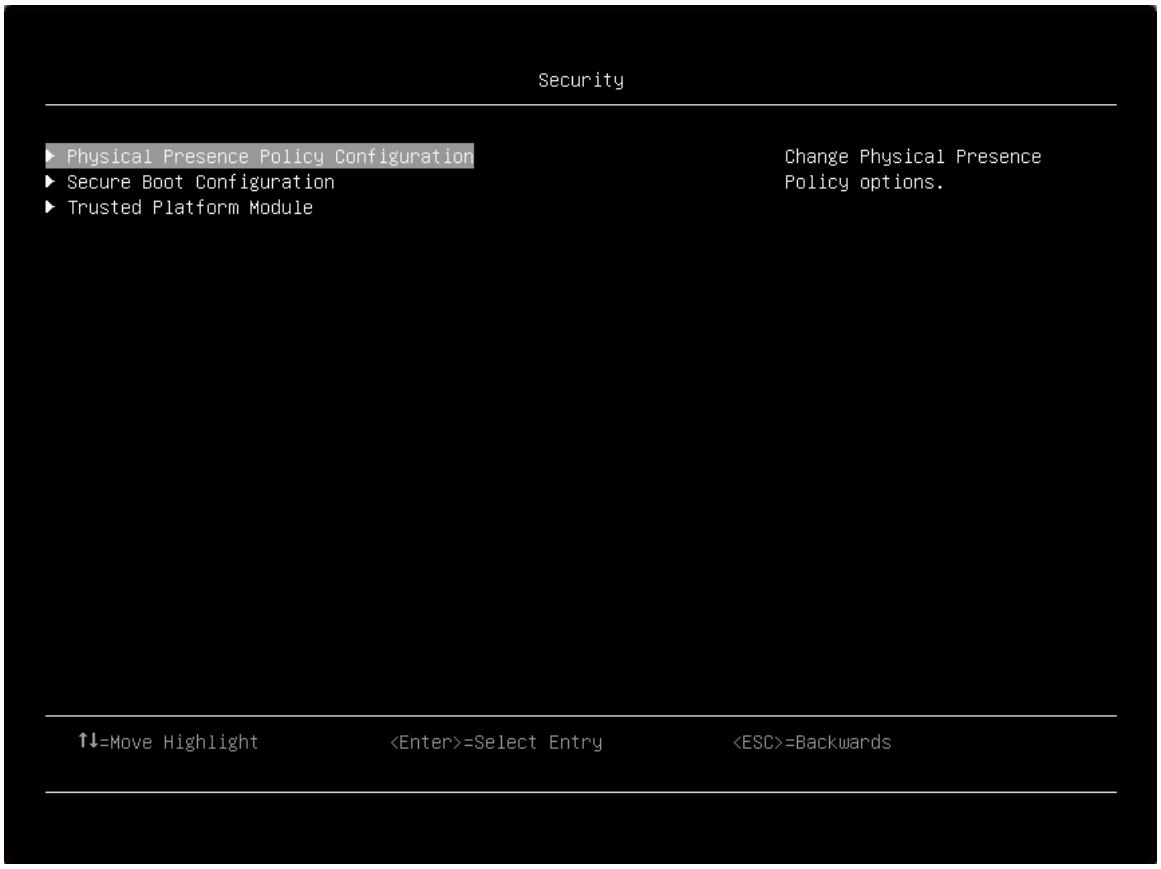


Table 15. Security

Item	Description
“Physical Presence Policy Configuration” on page 42	Change Physical Presence Policy options.
“Secure Boot Configuration” on page 42	Configure Secure Boot options.
“Trusted Platform Module (TPM 2.0)” on page 47	Configure the TPM Setup options.

Physical Presence Policy Configuration

Item	Options	Description
Physical Presence Policy	• **Enable** (Default) • Disable	Enable/Disable Remote Physical Presence policy. The option is modifiable when the Physical Presence State is asserted. • **Enable**: This option allows Remote Physical Presence to be asserted without the need for Hardware Physical Presence. When the item is enabled, a time-out value is used to assert the policy for a specified number of minutes. • **Disable**: If this item is disabled, this will require hardware physical presence to re-enable this policy.
Minutes To Assert	**30** (Default)	Number of minutes (range 1-100) to have Remote Physical Presence asserted. Physical Presence Policy must be enabled and a value set to have Remote Physical Presence asserted. **Note:** This is not a count-down value.
Physical Presence State	• Hardware Physical Presence Asserted • Remote Physical Presence Asserted • Hardware and Remote Physical Presence are Asserted • **De-asserted** (Default)	• **Hardware Physical Presence Asserted**: if Hardware Physical Presence Jumper is Asserted, the only way to de-assert Physical Presence is to change the jumper on the planar. • **Remote Physical Presence Asserted**: asserting allows Physical Presence to be set for a duration listed in minutes even if Hardware Physical Presence Jumper is not asserted. Asserting does not require a reboot. **Note:** Assertion does not require a reboot. • **Hardware and Remote Physical Presence are Asserted**: both the Hardware Physical Presence Jumper on the planar and the Remote Physical Presence are Asserted. • **De-asserted**: the default setting. De-asserting turns off Physical Presence (unless the HW Physical Presence Jumper is asserted). **Note:** De-assertion does not require a reboot.
Toggle Remote Physical Presence Assert		Switch the Remote Physical Presence between Assertion and De-assertion when Physical Presence Policy is enabled. The option is NOT modifiable when Physical Presence Policy is disabled.

Secure Boot Configuration

Item	Options	Description
Physical Presence	• Asserted • De-asserted	View the current Physical Presence status. Physical Presence is a form of authorization to perform certain security functions. **Asserted** means being authorized. When Physical Presence is asserted, **Secure Boot Setting** and **Secure Boot Policy** will be modifiable. When Physical Presence is De-asserted, the whole page will be grayed.

<table>
<tr><td>Secure Boot Status</td><td>Disabled
Enabled</td><td>View the current secure boot status.</td></tr>
<tr><td>Secure Boot Mode</td><td>Setup Mode
User Mode</td><td>When this item is in User Mode, and Secure Boot is enabled, the system will do secure boot authentication.</td></tr>
<tr><td>Secure Boot Setting</td><td>Enable
Disable (Default)</td><td>Enable/Disable Secure Boot. This setting is modifiable when Physical Presence is asserted and cannot be loaded to default in Setup Utility.

Note:<table><tr><th>Message box</th><th>What it means</th></tr><tr><td>WARNING: Legacy BIOS will be enabled when secure boot is ena</td><td>You attempt to enable secure boot while CSM is also enabled</td></tr><tr><td>Please verify physical presence and retry.</td><td>The change is failed. Please double-check.</td></tr></table></td></tr>
<tr><td>Secure Boot Policy</td><td>Factory Policy (Default)
Custom Policy
Delete All Keys
Delete PK
Reset All Keys to Default</td><td>This item is modifiable when Physical Presence is asserted and cannot be loaded to default in Setup Utility.
Factory Policy: Factory default keys will be used after reboot.
Custom Policy: Customized keys will be used after reboot.
Delete All Keys: PK, KEK, DB and DBX will be deleted after reboot.
Delete PK: PK will be deleted after reboot. After the PK is deleted, Secure Boot Mode will be in Setup Mode, and Secure Boot Policy will be Custom Policy.
Reset All Keys to Default: all the keys will be set to factory default and Secure Boot Policy will be Factory Policy after reboot.
Note:<table><tr><th>Message box</th><th>What it means</th></tr><tr><td>Please verify physical presence and retry.</td><td>The change is failed. Please double-check.</td></tr></table></td></tr>
<tr><td>“View Secure Boot Keys” on page 44</td><td></td><td>View the details of:
PK (Platform Key)
KEK (Key Exchange Key)
DB (Authorized Signature Database)
DBX (Forbidden Signature Database)</td></tr>
<tr><td>“Secure Boot Custom Policy” on page 44</td><td></td><td>Customize PK, KEK, DB or DBX.</td></tr>
</table>

View Secure Boot Keys

Secure Boot variable	Size	Keys#	Key Source	Description
PK	Number of bytes	Number of certificates (integer)	• **Factory Default** (Default) • No Key • Customized	View the Certificate in PK (Platform Key). **Note:** There will be only one PK in the system.
KEK	Number of bytes	Number of certificates (integer)	• **Factory Default** (Default) • No Key • Customized	View all Certificates in KEK (Key Exchange Key).
DB	Number of bytes	Number of certificates (integer)	• **Factory Default** (Default) • No Key • Customized	View all Certificates in DB (Authorized Signature Database).
DBX	Number of bytes	Number of certificates (integer)	• **Factory Default** (Default) • No Key • Customized	View all Certificates in DBX (Forbidden Signature Database).

To view the information about each secure boot variable above, You can press **Enter** on each item. The following message box will be then displayed:

PK / KEK / DB / DBX					
List	**Sig.Type**	**Count**	**Size**	**Owner GUID**	**Certificate Legend**
The key information of each section above will be listed here.					

Secure Boot Custom Policy

Item	Description
Enroll Efi Image	Enroll the SHA256 hash of the selected EFI image binary into the Authorized Signature Database (DB). **To Enroll:** 1. Select the file system that you are going to enroll. 2. If this change is confirmed, select Yes. Select No to cancel it. 3. You can check if the change is successful or not from the pop-up message box.

Note: A message box will pop up when booting from an unsigned shell.efi or OS when secure boot is enabled:

```
Secure Boot Violation
An unauthorized EFI image is detected. To use this image, please enroll this EFI image or disable secure boot at
"Secure Boot Configuration" in Setup Utility.
Ok
```

When selecting each Secure Boot variable, you will be able to add/delete it or view the details of it.

Secure Boot variable	Size	Keys#	Key Source	Description
PK	Number of bytes	Number of certificates (integer)	• **Factory Default** (Default) • No Key • Customized	Enroll a PK (from a Public Key Certificate file format) or delete the existing PK. **Note:** There will be only one PK in the system. If a PK already exists, it will not be available for you to add another unless the exiting one is removed.
KEK	Number of bytes	Number of certificates (integer)	• **Factory Default** (Default) • No Key • Customized	Enroll a KEK entry (from a Public Key Certificate file format), or delete an existing entry from the KEK.
DB	Number of bytes	Number of certificates (integer)	• **Factory Default** (Default) • No Key • Customized	Enroll a DB entry (from a Public Key Certificate file format or an EFI image file), or delete an existing entry from the DB.
DBX	Number of bytes	Number of certificates (integer)	• **Factory Default** (Default) • No Key • Customized	Enroll a DBX entry (from a Public Key Certificate file format or an EFI image file), or delete an existing entry from the DBX.

Add or Delete Secure Boot Variables

The following steps provide the information about the steps of adding/deleting the key items.

Table 16. PK

Add a PK

1. Select **Add**. Available file systems will be then displayed for you to select.
2.

Message box	What it means

`Input File Format`
`Public Key Certificate`
`Authenticated Variable`
	Select the file format.

3. If this change is confirmed, select Yes. Select No to cancel it.
4. You can check if the change is successful or not from the pop-up message box.

Delete a PK

1. Select **Delete**. A warning message will be then displayed
   ```
   Delete PK
   WARNING: Removing PK will change “Secure Boot
   Mode” to [Setup Mode].
   Ok
   ```
2. If the deletion is confirmed, select Yes. Select No to cancel it.
3. You can check if the change is successful or not from the pop-up message box.

Table 17. KEK

Add a KEK	Delete a KEK
1. Select **Add**. Available file systems will be then displayed for you to select. 2. 3. If this change is confirmed, select Yes. Select No to cancel it. 4. You can check if the change is successful or not from the pop-up message box.	1. Select **Delete**. 2. If the deletion is confirmed, select Yes. Select No to cancel it. 3. You can check if the change is successful or not from the pop-up message box.

Message box	What it means
`Input File Format Public Key Certificate Authenticated Variable`	Select the file format.

Table 18. DB

Add a DB	Delete a DB
1. Select **Add**. Available file systems will be then displayed for you to select. 2. 3. If this change is confirmed, select Yes. Select No to cancel it. 4. You can check if the change is successful or not from the pop-up message box.	1. Select **Delete**. 2. If the deletion is confirmed, select Yes. Select No to cancel it. 3. You can check if the change is successful or not from the pop-up message box.

Message box	What it means
`Input File Format Public Key Certificate Authenticated Variable EFI PE/COFF image`	Select the file format.

Table 19. DBX

Add a DBX	Delete a DBX
1. Select **Add**. Available file systems will be then displayed for you to select. 2. 3. If this change is confirmed, select Yes. Select No to cancel it. 4. You can check if the change is successful or not from the pop-up message box.	1. Select **Delete**. 2. If the deletion is confirmed, select Yes. Select No to cancel it. 3. You can check if the change is successful or not from the pop-up message box.

Message box	What it means
`Input File Format Public Key Certificate Authenticated Variable EFI PE/COFF image`	Select the file format.

Details of the Key

When selecting **Details** while viewing a key item, the detail of it will be then displayed:

PK / KEK / DB / DBX					
List	**Sig.Type**	**Count**	**Size**	**Owner GUID**	**Certificate Legend**
The key information of each section above will be listed here.					

Trusted Platform Module (TPM 2.0)

Item	Description
TPM 2.0	Configure the TPM 2.0 Setup options.

Table 20. TPM2.0 Setup options

Item	Options	Description
TPM Status		
TPM Vendor		View the TPM vendor.
TPM Firmware Version		View the current firmware version of the TPM device.
TPM Physical Presence	• Asserted • Not Asserted	View the current state of the TPM physical presence. This must be asserted for TPM commands to succeed.
TPM Settings		
TPM2 Operation	• **No Action** (Default) • Clear • TPM2.0 Device has been cleared. **Note:** The last option string will appear after the data has been successfully cleared and the system has been rebooted.	**WARNING**: This will erase the contents of the TPM. This command requires the TPM Physical Presence to be asserted. System reboot is required. To clear TPM data, select **Clear** and follow the message box on the screen.

Storage

The device list is based on your system configuration and system setting. The contents in this page are dynamically generated by installed storage vendor's HII utilities.

This menu allows you to manage storage adapter options. For systems that use planar devices, these options can be configured under **Devices and I/O ports**.

Item	Description
Intel(R) Virtual RAID on CPU	This formset allows you to manage Intel(R) Virtual RAID on CPU.

Notes:

- The device list is based on your system configuration and system setting. Contents of this page are dynamically generated by the storage vendor's HII utilities.
- SAS/SATA drives or NVMe drives connected to a storage controller will be displayed in the storage controller submenu: **System settings → Storage → Storage controller xxxx**.
- NVMe drives connected to the system without raid controller (sometimes using a retimer) will be displayed in one of the following pages:
  - **System settings → Foreign Devices**
  - **System settings → Storage**

Date and time

Use this menu to set the local date and time of the system.

Table 21. Date and time details

Item	Format	Description
System Date	MM/DD/YYYY	Use the +/- or the numeric keys to set the month, day and year (2000 – 2099). The date is saved as it is set.
System Time	HH:MM:SS	Use the +/- or the numeric keys to set the hour, minutes, and seconds. Use a 24 hour format. For example, 15:00 for 3pm.

Start options

Use this menu to boot the desired item from the primary boot sequence which is specified in **Boot Manager**.

Note: The following menu displays default boot order. The contents may be different on your device if different boot order has been set.

Table 22. Start options details

Item	Description
CD/DVD Rom	Device Path: VenHw(B2AD3248-4F72-4950-A966-CFE5062DB83A,02000000)
Hard Disk	Device Path: VenHw(B2AD3248-4F72-4950-A966-CFE5062DB83A,01000000)
Network	Device Path: VenHw(B2AD3248-4F72-4950-A966-CFE5062DB83A,05000000)

Boot manager

Use this menu to choose boot order, boot parameters, and boot from a file.

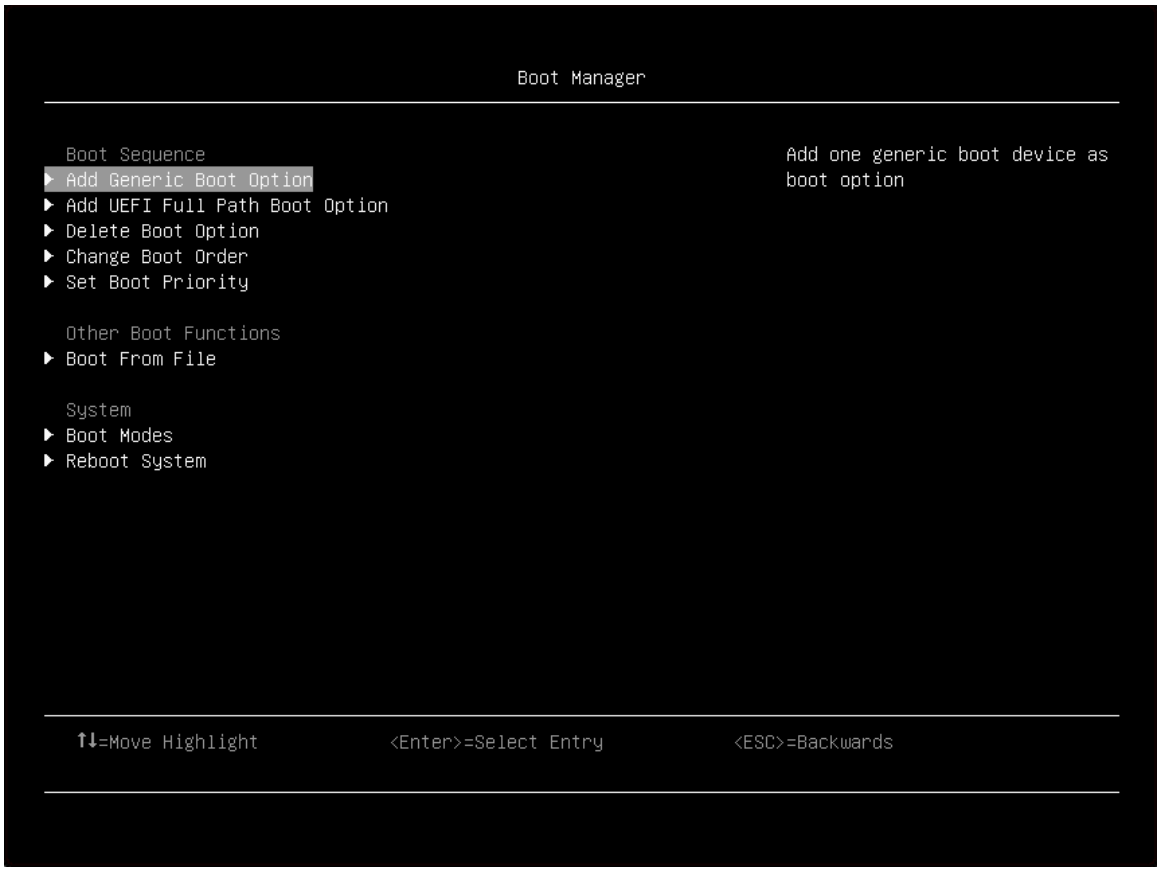


Table 23. Boot manager details

Item	Options	Description
Boot Sequence		
"Add Generic Boot Option" on page 52		Add one generic boot device as boot option.
"Add UEFI Full Path Boot Option" on page 52		Add one EFI application or one removable file systems as boot option.
"Delete Boot Option" on page 52		Remove boot option(s) from the Boot Order.
"Change Boot Order" on page 53		Modify the ordering of selections within the Boot Order.
"Set Boot Priority" on page 53		Set boot priority for the devices in a device group.
Other Boot Functions		
Boot From File	Xxxx {xxxx-xxx-xxx…}	Boot the system from a specific file or a device. The following message boxes will be displayed to guide you through the process.
System		

Table 23. Boot manager details (continued)

“Boot Mode” on page 53		Change between UEFI boot mode and legacy boot mode.

Reboot System		Reboot the system. When you select this item, the following message box will be displayed for you to confirm the action:
		`Reboot System`
		`Do you want to reboot system immediately?`
		`<Y> Reboot system immediately.`
		`<ESC> Return to System Setup`
		If **Y** is pressed, all setup changes will be lost and the system will reboot.

Add Generic Boot Option

Item	Options	Description
USB Storage	N/A	VenHw(B2AD3248-4F72-4950-A966-CFE5062DB83A,04000000)

Add UEFI Full Path Boot Option

Item	Options	Description
Boot option File Path		The file path for newly created boot option.

Input the Description		Specify the name for the new boot option.
		Note:
		Message box / **What it means**
		`ERROR`
		`Invalid Input Range`
		`Ok` — **The input is invalid.**

Select Device Path Option	Xxxx {xxxx-xxx-xxx…}	Select a file system from the available ones to boot.
		Note:
		Message box / **What it means**
		`No Valid File System`
		`No Valid File System Available`
		`Ok` — **No valid file system is present.**
		`No Valid File`
		`No Valid File Available in the Selected File System`
		`Ok` — **No valid file in a file system.**

Commit Changes and Exit		Save changes and exit.

Delete Boot Option

Item	Options	Description
CD/DVD Rom	[X]	VenHw(B2AD3248-4F72-4950-A966-CFE5062DB83A,02000000)

Hard Disk	[X]	VenHw(B2AD3248-4F72-4950-A966-CFE5062DB83A,01000000)
Network	[X]	VenHw(B2AD3248-4F72-4950-A966-CFE5062DB83A,05000000)
Commit Changes and Exit		Save changes and exit.

Note: The items in this menu is according to your system configuration.

Change Boot Order

Item	Options	Description
Change the Order	• CD/DVD Rom • Hard Disk • Network	Change the boot order. The boot options will be displayed in **Start Options**.
Commit Changes and Exit		Save changes and exit.

Set Boot Priority

This menu is hardware-depedent. Only the device group in **Boot Order** will be displayed here. The default of this menu includes CD/DVD, Hard Disk, and Network priorities. USB Priority will appear when it is added to Boot Order.

Note: Once a boot option is removed, it will not be displayed here.

Item	Description
CD/DVD Priority	Set boot priority in the CD/DVD group if multiple devices exist in the system.
Hard Disk Priority	Set boot priority in the Hard Disk group if multiple devices exist in the system.
Network Priority	Set boot priority in the Network group if multiple devices exist in the system.
USB Priority	Set boot priority in the USB group if multiple devices exist in the system.

Boot Mode

Item	Options	Description
System Boot Mode	• **UEFI Mode** (Default) • Legacy Mode	Drivers, option ROMs and OS loaders that **Boot Manager** attempts to boot. • **UEFI Mode**: Run UEFI drivers and boot a UEFI OS loader. UEFI mode is the default setting. • **Legacy Mode**: Run option ROMs and boot a legacy OS.

BMC settings

Use this menu to configure the management controller.

Table 24. BMC settings

Item	Options	Description
Power Restore Policy	• Always Off • **Restore** (Default) • Always On	Determine the mode of operation after loss of power. It will take a few minutes for the changes to take effect. • **Always Off**: the system remains off upon power restore. • **Restore**: the default setting; the system restores to the state it was before power failure. • **Always On**: the system turns on upon power restore. **Note:** This item is hardware-dependent, and it cannot be changed to the default value by using setup load default.
Ethernet over USB interface	• **Enable** (Default) • Disable	• **Enable**: for using the xClarity Essentials in-band update utility. • **Disable**: prevent xClarity Essentials and other applications that are running on the server from requesting the BMC to perform tasks.
"Network Settings" **on page 55**		Configure the network of the management controller.

Table 24. BMC settings (continued)

Reset Factory Defaults Setting		Restore all management controller settings to factory defaults, including network configuration and credentials. The management controller will be restarted automatically.

Restart BMC		Restart the BMC.
		
		When selecting this item, a following message box will then appear:
		`BMC restart (to defaults) command has been sent successfully.`
		`BMC will now be inaccessible for several minutes. During this time, please do not attempt to make any further changes to any BMC settings.`

Network Settings

Item	Options	Description
Network Interface Port	• **Dedicated** (Default) • Shared	Select the System Management Network Interface Port. **Note:** This item is hardware-dependent. Please refer to your hardware specifications.
Burned-in MAC Address	XX-XX-XX-XX-XX-XX	
Hostname	XCC-XXXX-XXXXXXXXXX	Change the host name. The new name should be within 1 to 63 characters.
DHCP Control	• Static IP • DHCP Enabled • **DHCP with Fallback** (Default)	Configure DHCP Control or manually configure a static IP address. • **Static IP**: enter IPv4 address manually. • **DHCP with Fallback**: use static IP address if DHCP fails.
IP Address	x.x.x.x	Enter IP address in dotted-decimal notation. **Note:** **Message box:** `ERROR Invalid Input Range Ok` **What it means:** **An invalid IP address is input.**
Subnet Mask	x.x.x.x	Enter subnet mask in dotted-decimal notation. **Note:** **Message box:** `ERROR Invalid Input Range Ok` **What it means:** **An invalid IP address is input.**

<table>
<tr><td>Default Gateway</td><td>x.x.x.x</td><td>Enter default gateway in dotted-decimal notation.

Note:
<table><tr><th>Message box</th><th>What it means</th></tr><tr><td>ERROR
Invalid Input Range
Ok</td><td>An invalid IP address is input.</td></tr></table></td></tr>
<tr><td>IPv6</td><td>• Enable (Default)
• Disable</td><td>Enable/Disable IPv6 support on management port.</td></tr>
<tr><td>Local Link Address</td><td>Unknown</td><td></td></tr>
<tr><td>VLAN Support</td><td>• Enable
• Disable (Default)</td><td>Enable VLAN support to specify the 802.1q VLAN ID on the management port network device.</td></tr>
<tr><td>VLAN ID</td><td>1</td><td>VLAN ID Range is from 1-4094
Note: This item is displayed only when VLAN Support is enabled.</td></tr>
<tr><td>“Advanced Settings for BMC Ethernet” on page 56</td><td></td><td></td></tr>
<tr><td>Save Network Settings</td><td></td><td>Commit the changes to BMC. Wait for a few minutes for the changes to take effect.</td></tr>
</table>

Advanced Settings for BMC Ethernet

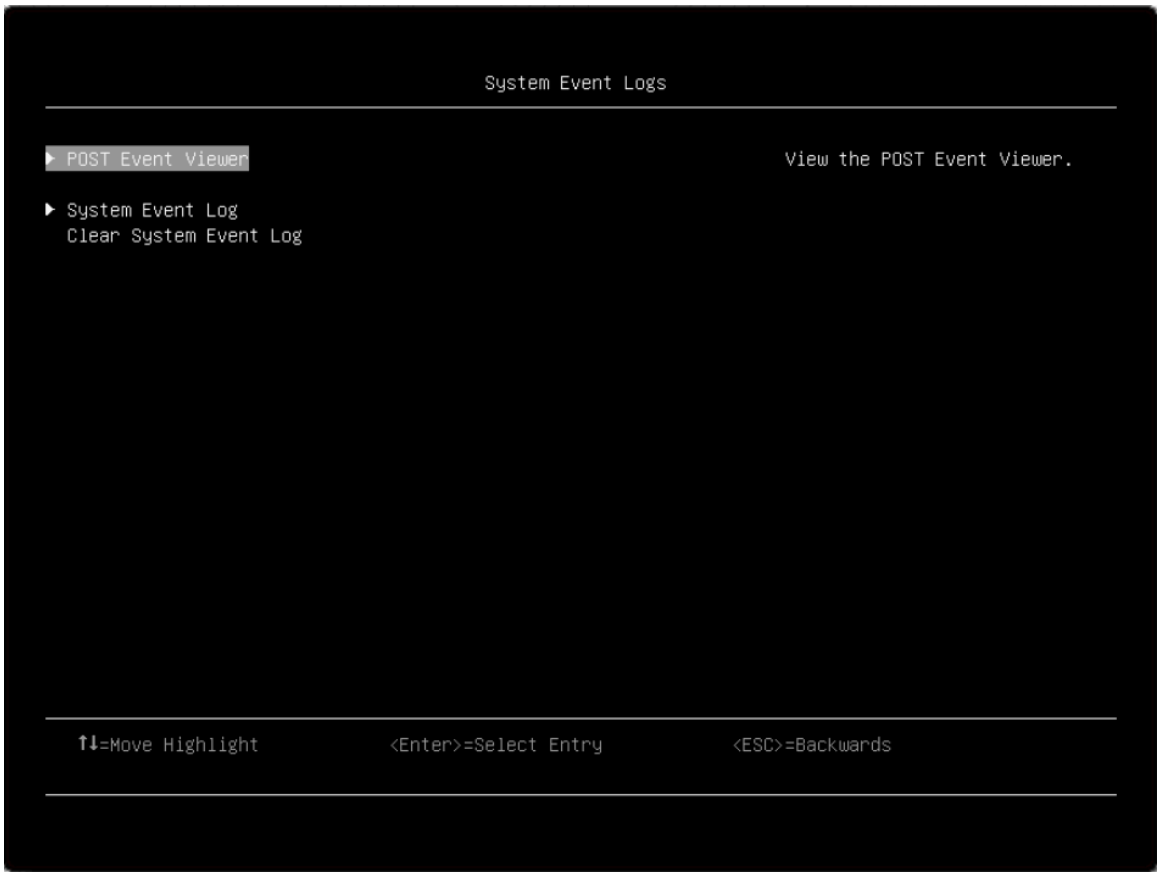
Note: Changes will be valid after saving network settings in previous page.

Item	Options	Description
Autonegotiation	• No • **Yes** (Default)	Set whether the data rate and duplex network settings are configurable or not.
Data rate	If Autonegotiation is set to **Yes**, the option will be: • **Auto** (Default) If Autonegotiation is set to **No**, the options will be: • 100 Mb (Ethernet) • 10 Mb (Ethernet)	Configure the amount of data to be transferred per second over LAN connection.

Duplex	If Autonegotiation is set to **Yes**, the option will be: • **Auto** (Default) If Autonegotiation is set to **No**, the options will be: • Half • Full	Configure the type of communication channel which will be used in your network. • **Half**: Allow data to be transferred in either one direction or the other, instead of both at the same time. • **Full**: Allow data to be transferred in both directions at once.
Maximum Transmission Unit	**1500** (Default)	Specify the maximum size of a packet (in bytes) for the network interface. The valid range is 68 – 1500.

System event logs

Use this menu to view or clear the system event log.



Item	Description
Post Event Viewer	View the post event viewer.
System Event Log	View the system event log.
Clear System Event Log	Clear the system event log.

Post Event Viewer

Item	Description
Entry [n]:	Information

System Event Log

Item	Description
Total SEL entries	Total number of system event logs retrieved from the BMC. Associated extended logs are not included.
Entry [n]:	Information

User security

Use this menu to set or change the passwords of power-on and administrator. There will be message boxes instructing you to finish the process.

Password rules:

- The following characters are allowed: A-Z, a-z, 0-9, ~`!@#$%^&*()-+={}[]|:;"'<>,?/._
- The password contains at least one letter/one number.
- The password contains at least one of these combinations: one upper case letter and one lower case letter/one upper case letter and one special character/one lower case letter and one special character.
- The password contains at least eight characters.
- No more than two consecutive occurrences of the same character.
- No white-space character is allowed.

Note: You can change the minimum number of characters with other values in **User Security → Password Rule and Policy → Minimum password length**.

Table 25. User security details

Item	Description
“Password Rule and Policy” **on page 60**	
Set Power-On Password	Follow the message boxes on the screen to complete password setting. Make sure your password meets the rules and policies. **Note:** **Message box** / **What it means** `Passwords operation have unknown issues Press <Enter> to Continue` / **This message box appears when IPMI command has no response.**
Clear Power-On Password	Follow the message boxes on the screen to complete password clearing.

Table 25. User security details (continued)

Set Administrator Password	Follow the message boxes on the screen to complete password setting. Make sure your password meets the rules and policies. **Note:** **Message box**: `Passwords operation have unknown problem Press <Enter> to Continue` **What it means**: **This message box appears when IPMI command has no response.**
Clear Administrator Password	Follow the message boxes on the screen to complete password clearing.

Password Rule and Policy

Item	Options	Function
Minimum password length	**8** (Default)	Input a value between 8 and 20. This value indicates minimum number of characters, which is part of the rules to specify a valid password.
Password expiration period	**0** (Default)	Input a value between 0 and 365. This value indicates the number of days that a password is expired and needs to be changed. If it is set to 0, the password will never expire.
Password expiration warning period	**0** (Default)	Input a value between 0 and 365. This value indicates the number of days that you will receive a warning about the expiration of the password. If it is set to 0, you will never receive the warning.
Minimum password change interval	**0** (Default)	Input a value between 0 and 240. This value indicates the number of hours that must elapse before a password is changed. The value specified for this setting cannot exceed the value specified for the **Password expiration period**. If it is set to 0, the password can be changed immediately.
Minimum password reuse cycle	**0** (Default)	Input a value between 0 and 10. This value indicates the minimum number of times a unique password must be set before reusing a previous password. If it is set to 0, the password can be reused immediately.

Maximum number of login failures	**5** (Default)	Input a value between 0 and 100. This value indicates the number of login attempts that can be made with an incorrect password before the user account is locked out. The account is locked out for the time specified in **Lockout period after maximum login failures**. If it is set to 0, accounts will never be locked. The failed login counter is reset to zero after a successful login.
Lockout period after maximum login failures	**2** (Default)	Input a value between 0 and 2880. This value indicates the number of minutes that a locked-user must wait to attempt to login. Entering a valid password cannot even unlock the account during the lockout period. If it is set to 0, accounts will not be locked out even if the **Maximum number of login failures** is exceeded.

F12 One Time Boot Device

Use this menu to manage boot devices in the system.

Note: The items in this menu are hardware dependent. The menu on your device may be different from the list here.

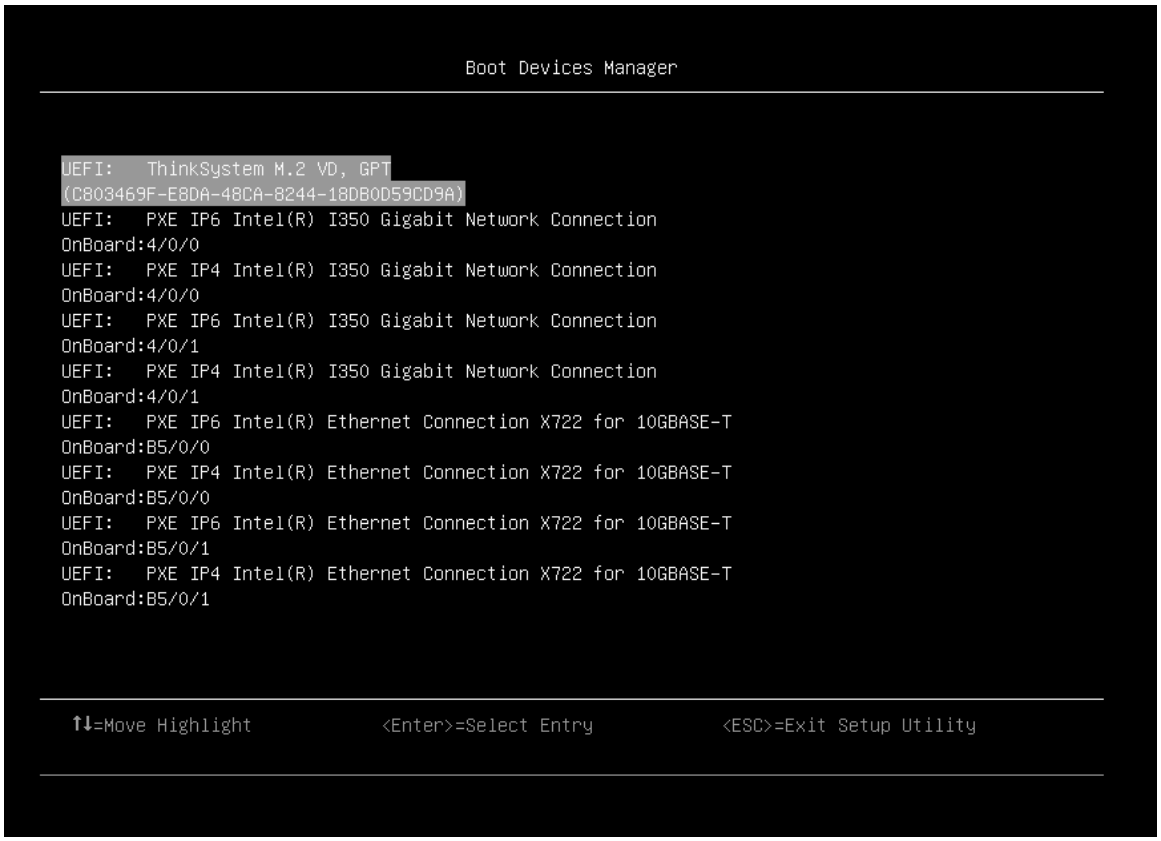


Table 26. Boot Devices Manager details

Item	Description
List of UEFI Boot Options	The list of UEFI Boot Options will be displayed here and will be changed according to the system configurations.

Appendix A. Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area.

Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service.

Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document is not an offer and does not provide a license under any patents or patent applications. You can send inquiries in writing to the following:

Lenovo (United States), Inc.
8001 Development Drive
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing

LENOVO PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary.

Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk.

Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Trademarks

LENOVO and LENOVO logo are trademarks of Lenovo.


Lenovo