

Lenovo

ThinkSystem Server with Intel Xeon SP (3rd Gen) UEFI Manual



Server Models: ST650 V2, SN550 V2, SD630 V2, SD650 V2, SD650-N V2, SR630 V2, SR650 V2, SR670 V2, SR850 V2, SR860 V2, ST250 V2, SR250 V2, SE450, MX3330, MX3331, MX3530, MX3531, MX450 IS

Twelfth Edition (April 2024)

© Copyright Lenovo 2020, 2024.

LIMITED AND RESTRICTED RIGHTS NOTICE: If data or software is delivered pursuant to a General Services Administration (GSA) contract, use, reproduction, or disclosure is subject to restrictions set forth in Contract No. GS-35F-05925.

Contents

Contents	i	Operating Modes	33
Chapter 1. UEFI overview	1	Power	38
Chapter 2. Get started.	3	Processors	40
Chapter 3. System configuration and boot management	5	Recovery and RAS	49
System information	5	Security	50
System settings	6	Storage	54
Device and I/O Ports	8	Date and Time	55
Driver Health	16	Start Options	56
Foreign Devices	18	Boot Manager	57
Intel Optane PMEMs	19	BMC Settings	60
Legacy BIOS	21	System Event Logs	64
Memory	21	User Security	65
Network	26	Appendix A. Notices.	71
		Trademarks	72

Chapter 1. UEFI overview

This chapter provides general introduction to the Unified Extensible Firmware Interface (UEFI) Setup utility.

UEFI Setup is a utility 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 models:

- ST650 V2
- SN550 V2
- SD630 V2
- SD650 V2
- SD650-N V2
- SR630 V2
- SR650 V2
- SR670 V2
- SR850 V2
- SR860 V2
- ST250 V2
- SR250 V2
- SE450
- MX3330
- MX3331
- MX3530
- MX3531
- MX450 IS

Note: SR250 V2 and ST250 V2 only support specific functions among the listed ones. See the specific function descriptions for details.

Below table details the main menu.

Note: If the Serial Over LAN (SOL) utility window is displayed incorrectly, change the window buffer size to ROW(100) x Column (31).

Table 1. Main menu details


Item	Options	Description
System Configuration and Boot Management	N/A	Main menu
Select Language		Change the language for the current system.

Table 1. Main menu details (continued)

Launch Graphical System Setup	N/A	Enter the graphical user interface for System Setup, provisioning manager, and RAID configuration. There will be no screen output to console in Graphical System Setup. Use VGA monitor for setup.
System Information	N/A	Display the basic information of the system.
System Settings	N/A	Display or modify system settings. Changes may not take effect immediately. Save any changed settings and reboot the system.
Date and Time	N/A	Set the local Date and Time of the system.
Start Options	N/A	Boot a desired selection from the primary boot sequence as specified under Boot Manager .
Boot Manager	N/A	Change the boot order and boot parameters.
BMC Settings	N/A	Configure the management controller.
System Event Logs	N/A	Clear or view the System Event Log.
User Security	N/A	Set or change Power-On and Administrator passwords.
Save Settings	N/A	Save changes and commit them to BMC.
Discard Settings	N/A	Discard any changes.
Load Default Settings	N/A	Load the default values for system settings.
Exit Setup Utility	N/A	Exit the Setup utility.

Note: The UEFI Utility interfaces and settings in this guide are for reference only, and may vary depending on the server model and configuration.

Chapter 2. Get started

This chapter describes how to get started with the UEFI Setup utility.

First launch

Perform the following steps to first launch the UEFI Setup utility.

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.

Wait for about 90s. The setup utility window is displayed.

Switch between graphic/text modes

The setup utility can be launched in graphic mode (default) or in text mode. You can switch between the two modes by referring to sections below.

- **Graphic mode to text mode**

Perform the following steps to switch from graphic mode to text mode:

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.

Wait for about 90s. The setup utility window is displayed in text mode.

- **Text mode to graphic mode**

Perform the following steps to switch from text mode to graphic mode:

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.

Wait for about 90s. The setup utility window is displayed in graphic mode.

Chapter 3. System configuration and boot management

This chapter details the System Setup utility.

System information

Select **System Information**, and then the following window is displayed:



Table 2. System information details

Item	Description
System Summary	Display basic information of the system.
Product Data	Display system firmware information.
Open Source License	Display open-source license.

System Summary

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

UUID Number	Specify the UUID.
Asset Tag Number	Specify a customer-assigned system asset tag number.
Processor	
Installed CPU Packages	Specify the number of installed CPU packages.
Processor Speed	Specify the processor speed.
UPI Link Speed	Specify the UPI link speed. Note: The UPI function works only if two or more processors are installed.
Memory	
Memory Mode	Specify the memory mode.
Memory Speed	Specify the speed of installed memory.
Total Memory Detected	Display the total capacity of all DIMMs installed.
Total Usable Memory Capacity	Display the amount of usable memory capacity after deduction of the overhead caused by mirroring mode, reserved or bad blocks, and so on.
Volatile Memory Capacity	Display the usable volatile memory capacity, which is seen as standard RAM by the operating system (OS).
Non-volatile Memory Capacity*	Display the usable non-volatile memory capacity, which can be partitioned and used by the OS as persistent RAM or persistent storage.

Product Data

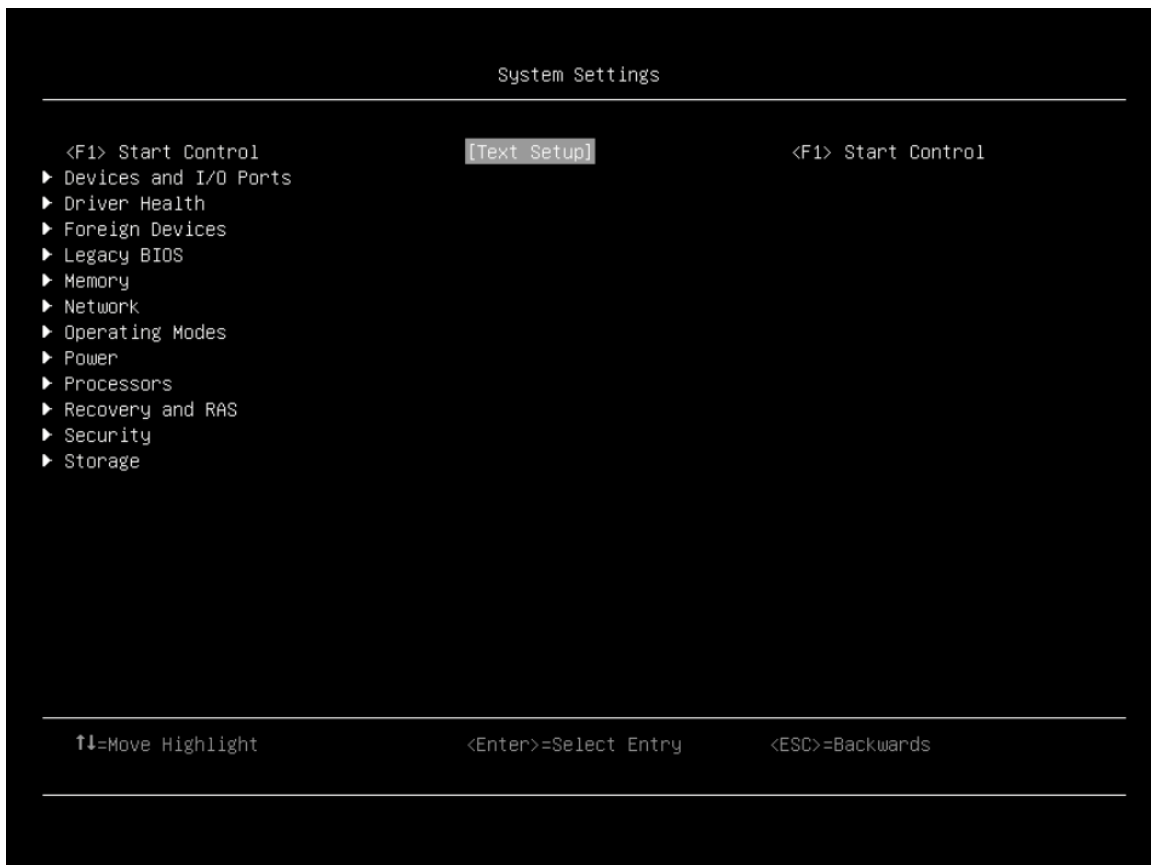
Item	Description
Host Firmware	
Build ID	Display the build ID of the host firmware.
Version	Display the version of the host firmware.
Build Date	Display the build date of the host firmware.
BMC Firmware	
Build ID	Display the build ID of the Baseboard Management Controller (BMC) firmware.
Version	Display the version of the BMC firmware.
Build Date	Display the build date of the BMC firmware.

Open Source License

This page lists open-source software acknowledgements and required copyright notices. The content of license varies with the platform.

System settings

Select **System Settings** and press Enter, and then the following window is displayed:



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 setting details

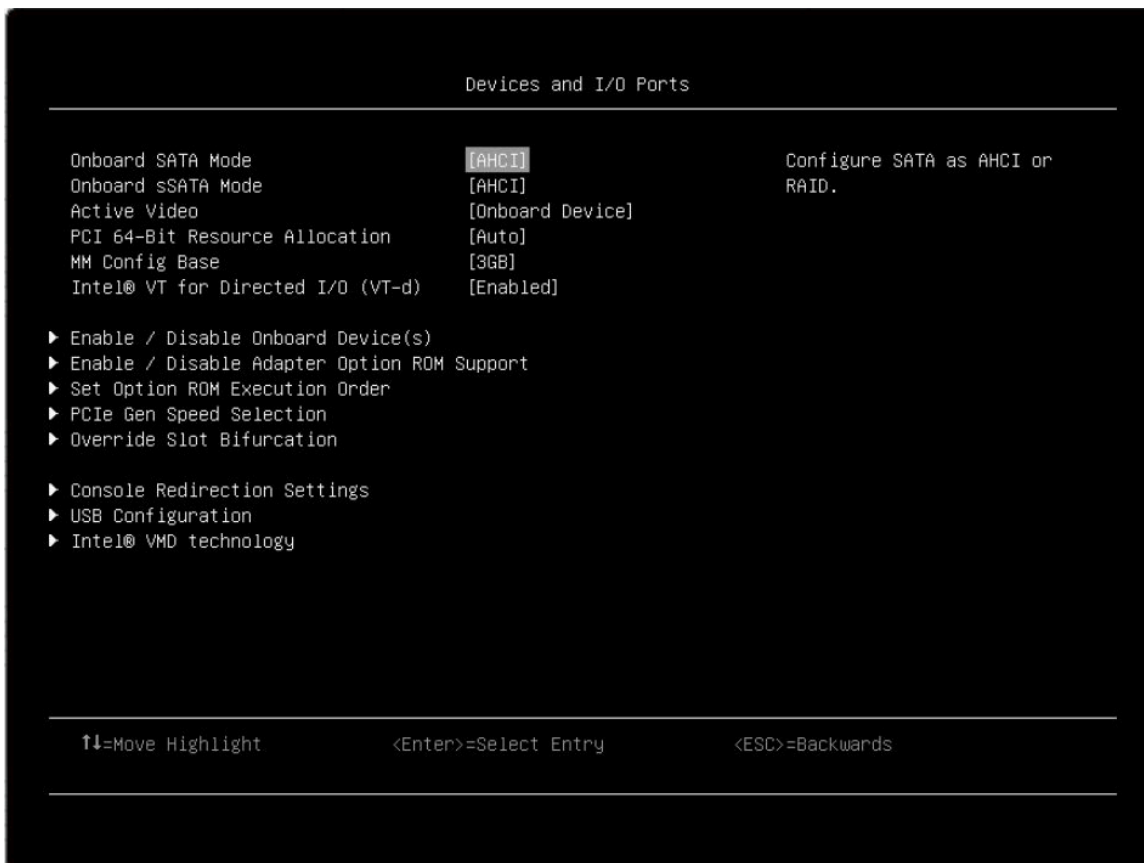
Item	Options	Description
Start Control	<ul style="list-style-type: none"> • Auto • Tool Suite • Text Setup 	Controls the tools that are started using the F1 key or equivalent IPMI command. <ul style="list-style-type: none"> • [Tool Suite] starts a graphical suite of tools which support System Information, UEFI setup, Platform Update, Raid Setup, OS installation and Diagnostics functions. • [Text Setup] starts a text mode UEFI setup utility. • [Auto] starts text mode UEFI setup if Serial Over Lan (SOL) or “Console Redirection” are enabled or SOL is configured to [Auto] and an active session is detected. Otherwise, [Auto] starts the graphical [Tool Suite].
Devices and I/O Ports	N/A	Display onboard devices and I/O port options.
Driver Health	N/A	View the health of controllers in the system as reported by their corresponding drivers.

Table 3. System setting details (continued)

Foreign Devices	N/A	View a list of foreign devices, including unclassified devices, video devices, input devices, onboard devices, and other devices.
Intel Optane DCPMMs*	N/A	View and configure Intel Optane DCPMMs. Note: This item is only available for special system configurations.
Legacy BIOS	N/A	Configure system UEFI firmware execution environment preferences for supporting legacy OS and legacy Option ROM.
Memory	N/A	Provide options to change the memory settings.
Network	N/A	Display network devices and network-related settings.
Operating Modes	N/A	Select the operating mode based on your preference. Note: Power savings and performance are also highly dependent on hardware configuration and software running on the system.
Power	N/A	Configure power scheme options.
Processors	N/A	Display and provide options to change the processor settings.
Recovery and RAS	N/A	Configure recovery policies and advanced reliability, availability, and serviceability settings.
Security	N/A	Configure system security settings.
Storage	N/A	Manage storage adapter options. Some systems may use planar devices and can be configured under "Devices and I/O Ports".

Device and I/O Ports

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



Note: Settings in this menu vary with models and configurations.

Table 4. Device and I/O ports details

Item	Options	Description
Onboard SATA Mode	<ul style="list-style-type: none"> • AHCI • RAID 	Configure SATA as AHCI or RAID. Note: This item is platform-dependent.
Onboard sSATA Mode	<ul style="list-style-type: none"> • AHCI • RAID 	Configure sSATA as AHCI or RAID. Note: This item is platform-dependent.
Active Video	<ul style="list-style-type: none"> • Onboard Device • Add-in Device 	This item is available only 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. Onboard Device is the default setting. Regardless of this setting, the system boot early video is displayed at the onboard video only, and the management controller remote console shows the onboard video only. This setting does not affect how the OS displays its graphical desktop.
PCI 64-Bit Resource Allocation	<ul style="list-style-type: none"> • Enabled • Disabled • Auto 	Enable/Disable the allocation of 64-bit resources for PCI. Auto is the default setting. [Auto] mode allocates some resources below 4 GB for legacy compatibility.

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

MM Config Base	<ul style="list-style-type: none"> • 3GB • 2GB • 1GB 	Recommend the default setting: 3GB . A greater value increases memory available to the OS (below 4 GB) and reduces the memory mapped I/O (MMIO) resource available to PCI adapters. Values smaller than 3 GB increases MMIO resources but reduces memory available to OS (below 4 GB). Revert to your previous selection if new issues occur with setting change.
Intel® VT for Direct I/O (VT-d)	<ul style="list-style-type: none"> • Enabled • Disabled 	Enable/Disable Intel® Virtualization Technology for Directed I/O (VT-d) by reporting the I/O device assignment to VMM through DMAR (DMA Remapping) ACPI Tables. Enabled is the default setting.
DMA Control Opt-In Flag	<ul style="list-style-type: none"> • Enabled • Disabled 	Enable/Disable DMA_CTRL_PLATFORM_OPT_IN_FLAG in DMAR (DMA Remapping) ACPI Table. Notes: <ul style="list-style-type: none"> • This item is not compatible with Direct Device Assignment (DDA). • This item is only supported on ICX platform.
SRIOV	<ul style="list-style-type: none"> • Enabled • Disabled 	Enable or Disable the support of resource allocation for virtual functions of Single Root I/O Virtualization(SRIOV) during boot.
Enable/Disable Onboard Device(s)	N/A	Enable/Disable onboard devices or slots.
Enable/Disable Adapter Option ROM Support	N/A	Control Legacy and UEFI-compliant adapter support. Disabling UEFI/Legacy support may adversely affect pre-boot/boot functions.
Set Option ROM Execution Order	N/A	Control legacy ROM load order.
PCIe Gen Speed Selection	N/A	Choose the generation speed for available PCIe slots.
Override Slot Bifurcation	N/A	Override the slot bifurcation setting of the physical x16 slot to support the adapter with multiple devices.
Console Redirection Settings	N/A	Provide settings for console redirection and COM port settings.
USB Configuration	N/A	Enable/Disable USB storage devices or individual ports.
Intel® VMD technology	N/A	Press Enter to pop up the Intel® VMD for Volume Management Device Configuration menu.

Enable/Disable Onboard Device(s)

Item	Options	Description
Onboard Video	<ul style="list-style-type: none"> • Enabled • Disabled 	Disabling an entry will prevent the associated device from being enumerated during subsequent boots. Enabled is the default setting.
Onboard SATA (for ODD)	<ul style="list-style-type: none"> • Enabled • Disabled 	Disabling an entry will prevent the associated device from being enumerated during subsequent boots. Enabled is the default setting.

Onboard sSATA (for M.2 SATA mode)	<ul style="list-style-type: none"> • Enabled • Disabled 	Disabling an entry will prevent the associated device from being enumerated during subsequent boots. Enabled is the default setting.
Onboard LAN (Displayed when a PHY card is installed)	<ul style="list-style-type: none"> • Enabled • Disabled 	Disabling an entry will prevent the associated device from being enumerated during subsequent boots. Enabled is the default setting.
Onboard LAN Port (x) ("x" varies with the PHY card.)	<ul style="list-style-type: none"> • Enabled • Disabled 	Disabling an entry will prevent the associated device from being enumerated during boot. This item is grayed out when "Onboard LAN" is [Disabled], and is hidden when this port is not present. Enabled is the default setting.
Slot (x) ("x" varies with the slot on which riser card is installed.)	<ul style="list-style-type: none"> • Enabled • Disabled 	Disabling an entry will prevent the associated device from being enumerated during subsequent boots. Enabled is the default setting.
NVMe Bay (x) ("x" varies with the PHY card.)	<ul style="list-style-type: none"> • Enabled • Disabled 	Disabling an entry will prevent the associated device from being enumerated during subsequent boots. Enabled is the default setting.

Enable/Disable Adapter Option ROM Support

Item	Options	Description
Onboard SATA (for HDD)	<ul style="list-style-type: none"> • Auto • Disabled • UEFI • Legacy 	<p>Select whether UEFI or legacy option ROM of this device will be executed.</p> <p>[Disabled] means neither UEFI nor legacy option ROM will be executed.</p>
Onboard sSATA (for M.2 SATA mode)	<ul style="list-style-type: none"> • Auto • Disabled • UEFI • Legacy 	<p>[UEFI] means only UEFI option ROM will be executed.</p> <p>[Legacy] means only legacy option ROM will be executed.</p> <p>[Auto] means which option ROM will be executed depends on "System Boot Mode".</p>
Onboard Video	<ul style="list-style-type: none"> • Auto • Disabled • UEFI • Legacy 	<p>When [Legacy] is selected, "Onboard Video" will be changed to [Legacy] automatically and cannot be changed to other options.</p> <p>Option in bold is the default setting.</p>
Onboard LAN Port x ("x" varies with the PHY card.)	<ul style="list-style-type: none"> • Auto • Disabled • UEFI • Legacy 	
Slot x ("x" depends the slot on which riser card is installed.)	<ul style="list-style-type: none"> • Auto • Disabled • UEFI • Legacy 	<p>When a card is installed:</p> <p>Select whether UEFI or legacy option ROM of this device will be executed.</p> <p>[Disabled] means neither UEFI nor legacy option ROM will be executed.</p> <p>[UEFI] means only UEFI option ROM will be executed.</p> <p>[Legacy] means only legacy option ROM will be executed.</p> <p>[Auto] means which option ROM will be executed depends on "System Boot Mode".</p> <p>When [Legacy] is selected, "Onboard Video" will be changed to [Legacy] automatically and cannot be changed to other options.</p> <p>When there is <i>no</i> card installed, this item is empty.</p> <p>Auto is the default setting.</p>

Set Option ROM Execution Order

Item	Options	Description
Set Option ROM Execution Order	<ul style="list-style-type: none"> Onboard Video Onboard SATA Onboard sSATA Onboard LAN Slot x 	<p>Select the load order for legacy PCI option ROM. Use the + key to execute the selected devices ROM sooner or – key to execute later.</p> <p>Notes:</p> <ul style="list-style-type: none"> Onboard LAN Port x depends on whether PHY card is installed or not. The displayed slots x (1–8) may vary depending on which riser card is installed.

PCIe Gen Speed Selection

Item	Options	Description
Slot x ("x" varies depending on which riser card is installed.)	<ul style="list-style-type: none"> Auto Gen1 Gen2 Gen3 	<p>Set the maximum speed supported by individual PCIe slot.</p> <p>Note: Some adapters may not operate correctly in Gen2 or Gen3. The settings will take effect after the system is rebooted.</p>

Note: The slot numbers listed here may vary with platforms. This is just a generic example on how all other slot-related settings are.

Override Slot Bifurcation

This page is platform-dependent. Refer to the platform document for details.

Console Redirection Settings

Item	Options	Description
COM Port 1	<ul style="list-style-type: none"> Enabled Disabled 	<p>Enable/Disable COM 1 device. If [Disabled] is selected, the associated COM1 terminal settings will be hidden. Enabled is the default setting.</p>
COM Port 2	<ul style="list-style-type: none"> Enabled Disabled 	<p>Enable/Disable COM 2 device. If [Disabled] is selected, the associated COM 2 terminal settings will be hidden. Enabled is the default setting.</p>
Console Redirection	<ul style="list-style-type: none"> Enabled Disabled Auto 	<p>Set remote console redirection preference to enable or disable console redirection.</p> <p>When [Auto] is selected, console redirection will be enabled automatically if IPMI Serial over LAN status is active. Auto is the default setting.</p>
Serial Port Sharing	<ul style="list-style-type: none"> Enabled Disabled 	<p>Enable the system BMC to allow access to the system serial port.</p> <p>If [Enabled], BMC will be allowed to control the serial communication port as requested by remote control commands.</p> <p>If [Disabled], the serial port will be assigned to BMC unless the "Serial Port Access Mode" is set to [Disabled].</p> <p>Disabled is the default setting.</p>

Serial Port Access Mode	<ul style="list-style-type: none"> • Shared • Dedicated • Disabled 	<p>Control the access to the system BMC over the system serial port.</p> <ul style="list-style-type: none"> • [Shared]: The serial port will be available for both POST and OS use; however, BMC can monitor the serial data for a takeover control sequence. • [Dedicated]: BMC will have complete control of the serial port for POST and/or OS use. • [Disabled]: BMC will not have any access to the serial port. <p>Disabled is the default setting.</p>
SP Redirection	<ul style="list-style-type: none"> • Enabled • Disabled 	<p>Choose which COM port to do the redirection.</p> <p>Note: This option is available only when "Console Redirection", "COM Port 1" and "COM Port 2" are set to [Enabled].</p> <p>Disabled is the default setting.</p>
Legacy OS/Option ROM Display	<ul style="list-style-type: none"> • COM Port 1 • COM Port 2 	<p>Select a COM port to display redirection of Legacy OS and Legacy OPRM Messages.</p> <p>COM Port 1 is the default setting.</p>
COM Port Active After Boot	<ul style="list-style-type: none"> • Enabled • Disabled 	<p>When [Disabled], Legacy Console Redirection is disabled before booting to Legacy OS.</p> <p>When [Enabled], Legacy Console Redirection is enabled for Legacy OS.</p> <p>Disabled is the default setting.</p>
COM1 Settings	N/A	Set serial connections for "asynchronous start-stop" communication.
COM1 Baud Rate	<ul style="list-style-type: none"> • 115200 • 57600 • 38400 • 19200 • 9600 	Control the connection speed between the host and remote system. 115200 is the default setting.
COM1 Data Bits	<ul style="list-style-type: none"> • 8 • 7 	Set the number of data bits in each character.
COM1 Parity	<ul style="list-style-type: none"> • None • Odd • Even 	<p>Set the parity bit in each character to be [None], [Odd], or [Even].</p> <p>[None] means that no parity bit is sent. None is the default setting.</p>
COM1 Stop Bits	<ul style="list-style-type: none"> • 2 • 1 	Set the number of stop bits. Stop bits at the end of each character allow the signal receiver to detect the end of a character and resynchronize with the character stream.

COM1 Terminal Emulation	<ul style="list-style-type: none"> • VT100 • VT-UTF8 • ANSI 	<p>Set the type of terminal emulation.</p> <p>Select [VT100] only when the remote emulator does not support ANSI text graphics. Refer to the emulator documentation for more information. ANSI is the default setting.</p> <p>Note: If needed, change the character encoding setting in the remote emulator to ensure the characters show correctly.</p>
COM1 Flow Control	<ul style="list-style-type: none"> • Disabled • Hardware 	<p>Select [Hardware] only when the remote emulator supports and is using hardware flow control. Refer to the emulator documentation for more information. Disabled is the default setting.</p>
COM2 Settings	N/A	Set serial connections for "asynchronous start-stop" communication.
COM2 Baud Rate	<ul style="list-style-type: none"> • 115200 • 57600 • 38400 • 19200 • 9600 	Control the connection speed between the host and remote system. 115200 is the default setting.
COM2 Data Bits	<ul style="list-style-type: none"> • 8 • 7 	Set the number of data bits in each character.
COM2 Parity	<ul style="list-style-type: none"> • None • Odd • Even 	Set parity bit in each character to be [None], [Odd], or [Even]. [None] means that no parity bit is sent. None is the default setting.
COM2 Stop Bits	<ul style="list-style-type: none"> • 2 • 1 	Set the number of stop bits. Stop bits 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	<ul style="list-style-type: none"> • VT100 • VT-UTF8 • ANSI 	<p>Set the type of terminal emulation.</p> <p>Select [VT100] only when the remote emulator does not support ANSI text graphics. Refer to the emulator documentation for more information. ANSI is the default setting.</p>
COM2 Flow Control	<ul style="list-style-type: none"> • Disabled • Hardware 	<p>Select [Hardware] only when the remote emulator support and is using hardware flow control. Refer to the emulator documentation for more information. Disabled is the default setting.</p>

USB Configuration

Item	Options	Description
USB Mass Storage Driver Support	<ul style="list-style-type: none"> • Enabled • Disabled 	<p>Enable/Disable USB Mass Storage Driver Support.</p> <p>The setting only takes effect in post time. Enabled is the default setting.</p> <p>Notes: If this item is [Disabled],</p> <ul style="list-style-type: none"> • The GUI tool for UEFI Setup utility is disabled. In this case, the UEFI Setup utility can only be launched in text mode. • Some other features relying on the USB Mass Storage Driver Support might be disabled as well.
USB Front Port 1	<ul style="list-style-type: none"> • Enabled • Disabled 	<p>Enable/Disable USB individual ports. Enabled is the default setting.</p>
USB Front Port 2		
USB Rear Port 1		
USB Rear Port 2		

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	<ul style="list-style-type: none"> • Enabled • Disabled 	Enable/Disable Intel® Volume Management Device Technology. Disabled is the default setting.

Driver Health

This menu displays the health statuses of controllers in the system as reported by their corresponding drivers.

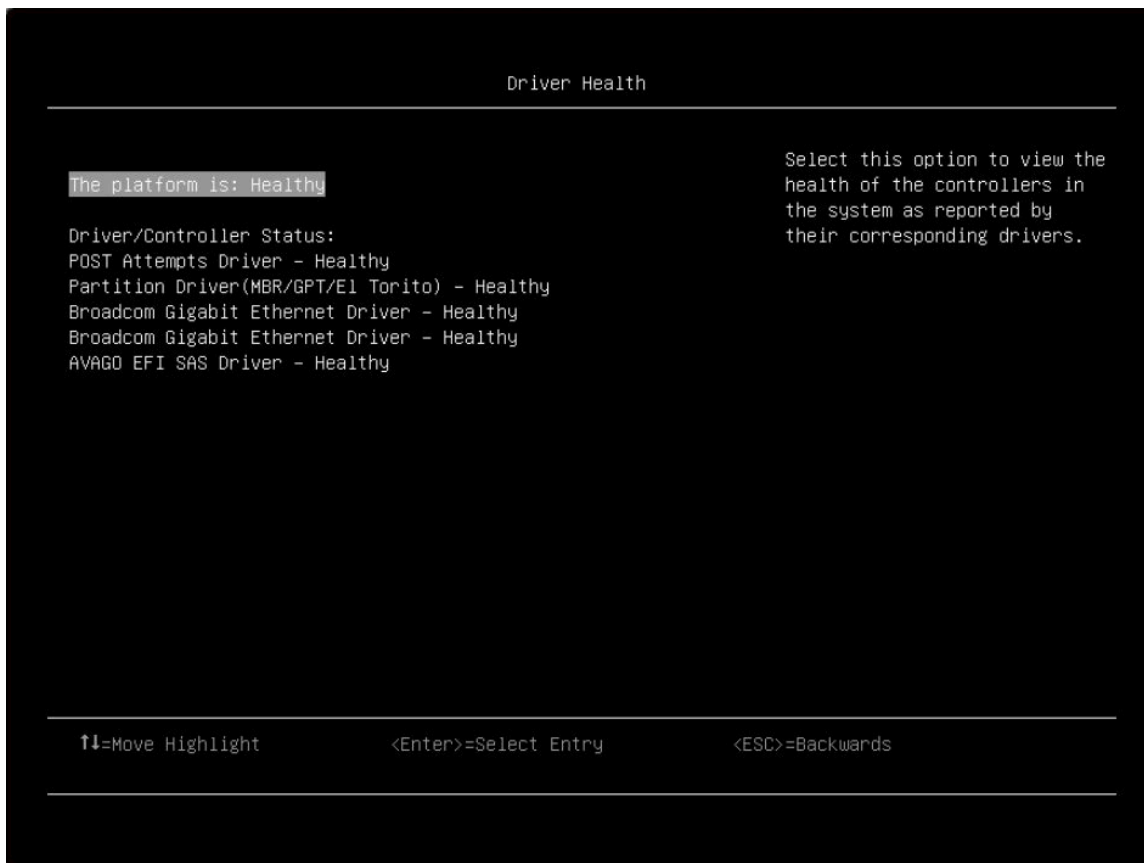


Table 5. Driver health details

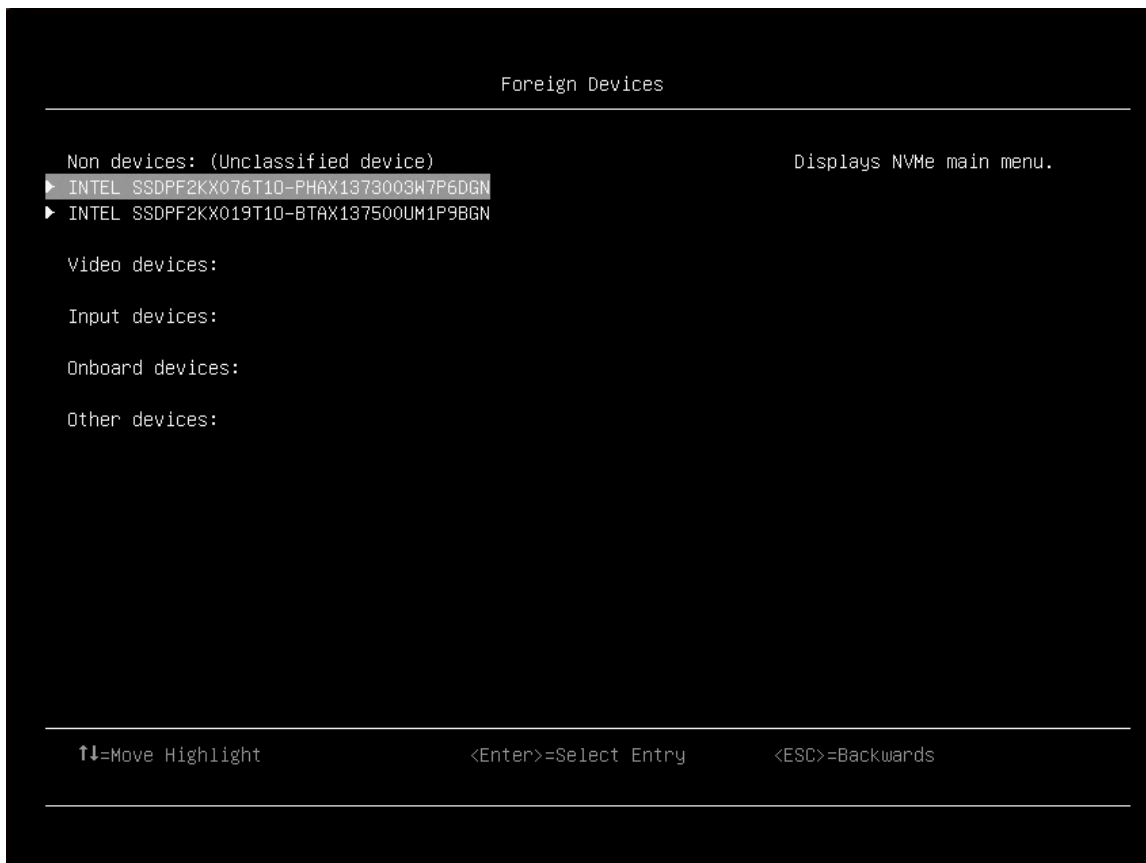
Item	Options	Description
The platform is:	<ul style="list-style-type: none"> • Healthy • Repair Required • Configuration Required • Operation Failed • Reconnect Required • Reboot Required • Shutdown Required • No Operation Required 	Display the health statuses of controllers in the system as reported by their corresponding drivers.
Driver/Controller Status		

Table 5. Driver health details (continued)

<p>Controller Name - Status</p>	<ul style="list-style-type: none"> • Healthy • Repair Required • Configuration Required • Operation Failed • Reconnect Required • Reboot Required • Shutdown Required • No Operation Required 	<p>Display the health of controller.</p> <p>Notes:</p> <ul style="list-style-type: none"> • This item is displayed dynamically and is based on a card that supports the driver healthy function. • The following "POST Attempts Driver" and "Partition Driver (xxx)" are example formats.
<p>POST Attempts Driver</p>	<ul style="list-style-type: none"> • Healthy • Repair Required • Configuration Required • Operation Failed • Reconnect Required • Reboot Required • Shutdown Required • No Operation Required 	<p>Display the health of POST Attempts Driver.</p>
<p>Partition Driver (MBR/GPT/EFI Torito)</p>	<ul style="list-style-type: none"> • Healthy • Repair Required • Configuration Required • Operation Failed • Reconnect Required • Reboot Required • Shutdown Required • No Operation Required 	<p>Display the health of Partition Driver.</p>

Foreign Devices

This menu displays a list of foreign devices, including unclassified devices, video devices, input devices, onboard devices, and other devices.



Notes:

- Depending on your system configuration (for example, which device is installed), this page might look slightly different from the image.

Table 6. Foreign device details

Item	Options	Description
Non devices (Unclassified devices)	N/A	Display installed device information dynamically.
Video device	N/A	
Input device	N/A	
Onboard device	N/A	
Other device	N/A	

Intel Optane PMEMs

This menu displays the settings of Intel Optane PMEMs.

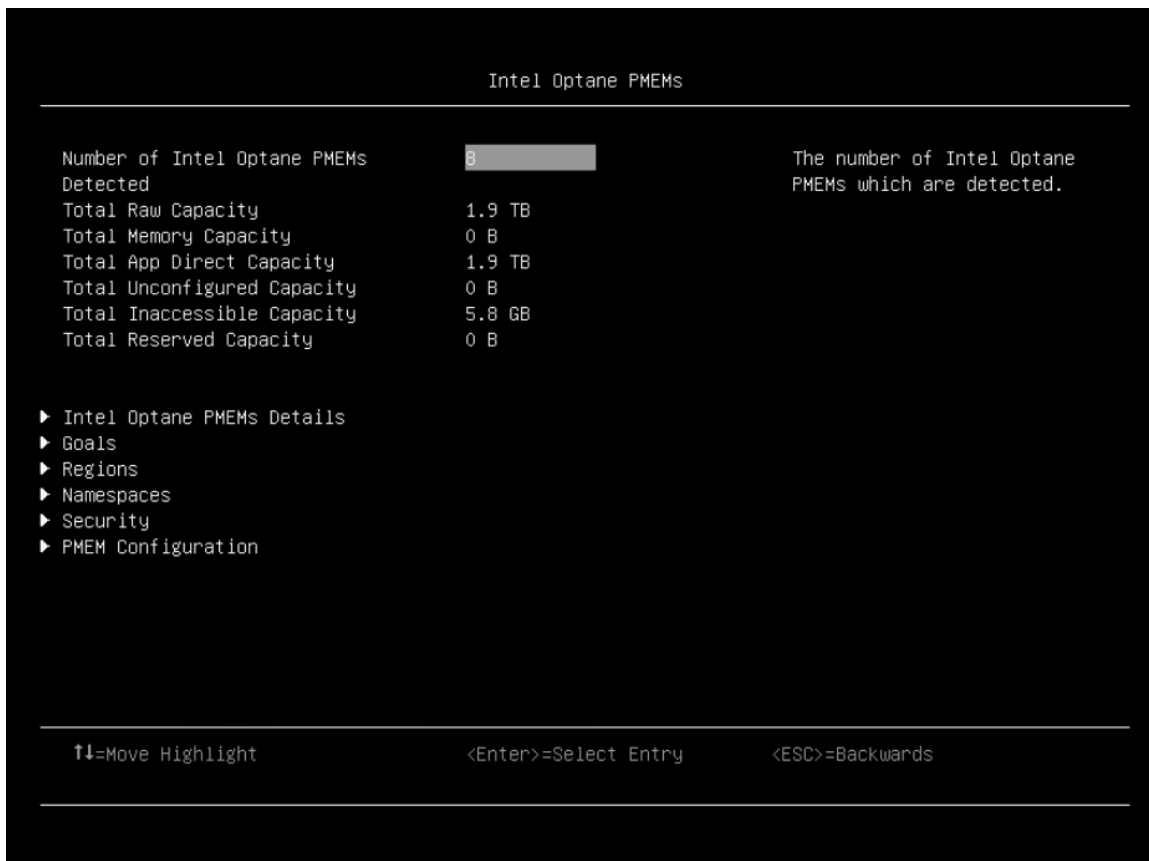


Table 7. Intel Optane PMEMs details

Item	Options	Description
Number of Intel Optane PMEMs Detected	N/A	Number of detected Intel Optane PMEMs.
Total Raw Capacity	N/A	Total raw capacity of all detected Intel Optane PMEMs.
Total Memory Capacity	N/A	Total memory mode capacity of all detected Intel Optane PMEMs.
Total App Direct Capacity	N/A	Total App Direct capacity of all detected Intel Optane PMEMs.
Total Unconfigured Capacity	N/A	Total unconfigured capacity of all detected Intel Optane PMEMs.
Total Inaccessible Capacity	N/A	Total inaccessible capacity of all detected Intel Optane PMEMs.
Total Reserved Capacity	N/A	Total reserved capacity of all detected Intel Optane PMEMs.
Intel Optane PMEMs Details	N/A	Details of each detected Intel Optane PMEM.
Goals	N/A	Create or delete memory allocation goals.
Regions		Display the info of each region.
Namespaces	N/A	Create, delete, and view namespaces.

Table 7. Intel Optane PMEMs details (continued)

Security	N/A	Configure the security state of each Intel Optane PMEM.
PMEM Configuration	N/A	PMEM configuration.

Legacy BIOS

This menu configures system UEFI firmware execution environment preferences for supporting legacy OS and legacy Option ROM.



Table 8. Legacy BIOS details

Item	Options	Description
Legacy BIOS	<ul style="list-style-type: none"> • Enabled • Disabled 	Enable/Disable the system UEFI firmware execution environment for supporting legacy OS and legacy Option ROM. Enabled is the default setting.
Rehook INT 19h	<ul style="list-style-type: none"> • Enabled • Disabled 	[Enabled] prevents devices from taking control of the boot process. Disabled is the default setting.
Non-Onboard PXE	<ul style="list-style-type: none"> • Enabled • Disabled 	Enable/Disable legacy PXE boot for installed network adapters. Enabled is the default setting.

Memory

This menu offers options to change the memory setting.



Table 9. Memory

Item	Options	Description
System Memory Details	N/A	Provide status of System Memory.
Total Usable Memory Capacity	(in GB)	Display the total usable memory capacity.
Memory Speed	<ul style="list-style-type: none"> • Minimal Power • Balanced • Max Performance 	<p>Select the desired memory speed.</p> <p>[Maximum Performance] mode maximizes performance. [Balanced] mode offers a balance between performance and power. [Minimal power] mode maximizes power savings.</p> <p>When a preset mode is selected, the low-level settings are not changeable and will be grayed out. To change the settings, choose System Settings > Operating Modes > Choose Operating Mode > Custom Mode.</p> <p>Max Performance is the default setting.</p>

Table 9. Memory (continued)

Memory Power Management	<ul style="list-style-type: none"> • Automatic • Disabled 	<p>[Disabled] provides maximum performance but minimum power savings. [Automatic] is suitable for most applications.</p> <p>When a preset mode is selected, the low-level settings are not changeable and will be grayed out. To change the settings, choose System Settings > Operating Modes > Choose Operating Mode > Custom Mode.</p> <p>Disabled is the default setting.</p>
Socket Interleave	<ul style="list-style-type: none"> • NUMA • Non-NUMA 	<p>Set the socket interleave mode. [NUMA]: Memory is not interleaved across processors. [Non-NUMA]: Memory is interleaved across processors.</p> <p>Note: Setting change requires a Power Good reset to take effect.</p>
Patrol Scrub	<ul style="list-style-type: none"> • Enabled • Disabled 	<p>Enable/Disable "Patrol Scrub" which proactively searches the system memory to repair correctable errors. Enabled is the default setting.</p>
Memory Data Scrambling	<ul style="list-style-type: none"> • Enabled • Disabled 	<p>Enable/Disable memory data scrambling. Enabled is the default setting.</p>
ADDDC Sparing	<ul style="list-style-type: none"> • Disabled • Enabled 	<p>Enable/Disable ADDDC Sparing. Enabling ADDDC Sparing may reduce the reliability of memory error correction in virtual lockstep under rare conditions. Enabled is the default setting.</p> <p>Note: For Cooper Lake processor-based servers, this item is [Disabled] and grayed out when Page Policy is [Adaptive].</p>
Page Policy	<ul style="list-style-type: none"> • Adaptive • Closed 	<p>[Adaptive] can improve performance for applications with a highly localized memory access pattern; [Closed] can benefit applications that access memory more randomly. Adaptive is the default setting.</p> <p>Note: For Cooper Lake processor-based servers, this item is [Closed] and grayed out when "ADDDC Sparing" is [Enabled].</p>
Cold Boot Fast	<ul style="list-style-type: none"> • Enabled • Disabled 	<p>Enable/Disable "Cold Boot Fast". Enabled is the default setting.</p>
AC Boot Fast	<ul style="list-style-type: none"> • Enabled • Disabled 	<p>Enable/Disable "AC Boot Fast" for AC boot only. Enabled is the default setting.</p>
Memory Test	<ul style="list-style-type: none"> • Enabled • Disabled 	<p>Enable/Disable memory test during normal boot. Enabled is the default setting.</p>

Table 9. Memory (continued)

2x Refresh Rate	<ul style="list-style-type: none"> • Disabled • Auto 	<ul style="list-style-type: none"> • Disabled: the memory refresh rate of the system is 1x. • Auto: the memory refresh rate is 2x if the system supports. <p>Choose a memory refresh rate of 2x to mitigate the rowhammer issue that may have a performance side effect.</p> <p>Notes:</p> <ul style="list-style-type: none"> • For the system with an ICX (Ice Lake) processor, when the system has 16Gb 3DS with 4 Die DIMM, 2x refresh rate is not supported. • For the system with a CPX (Cooper Lake) processor, when the system has 16Gb 3DS LRDIMM/RDIMM or 16Gb Quad Rank LRDIMMS, 2x refresh rate is not supported.
Mirror Configuration	N/A	<p>Display and configure memory mirror state.</p> <p>Note: Mirror Configuration can be configured only when ADDDC Sparing is disabled and memory population meets requirements.</p>
RAM Disk Configuration	N/A	Create or remove RAM disks.

System Memory Details

Item	Options	Description
DIMM Details For Processor X	N/A	Provides status of DIMMs.

DIMM Details

The DIMM population list is platform dependent. When DIMM has DBE, the DIMM item will turn from string description to enable/disable option. In this generation the enable/disable option will set **Enable** as default.

Mirror Configuration

Item	Options	Description
Configuration Made From OS	N/A	Show the memory mirror configuration state that was defined from OS utility. When a definition is found, you can use Delete Configuration Made From OS to clear it.
Mirror Below 4GB	N/A	Display the mirroring configuration of memory below 4 GB. Note: This option may be TRUE or FALSE after the OS has configured Mirror .
Partial Mirror Ratio In Basis Points	N/A	Display the memory mirror ratio for the memory above 4 GB in basis points value. The valid range is 1 – 5000, meaning 0.01% to 50%. For example, to mirror 12.75% of memory, input the value 1275. Note: After the OS is configured Mirror, this option may display a range of 1 – 5000.

Delete OS Configuration	<ul style="list-style-type: none"> • No • Yes 	Remove the memory mirror configuration that was made from OS utility. System reboot is required to take effect. Notes: <ul style="list-style-type: none"> • This item only exists if the OS is configured Mirror. • If you select Yes to delete the item, it will be hidden.
Configuration Made From UEFI	N/A	Show the memory mirror configuration state that was defined from UEFI system utility. In case of conflicting configuration values from OS and UEFI, the values from OS take precedence.
Full Mirror	<ul style="list-style-type: none"> • Disable • Enable 	Full mirroring reduces the available system memory by half of the total installed memory.
Partial Mirror	<ul style="list-style-type: none"> • Disable • Enable 	Partial mirroring reduces the available system memory by percentage of up to 50% per processor. The percentage is set by Partial Mirror Ratio In Basis Points . Note: Partial Memory Mirroring is a sub-function of memory mirroring. It requires to follow the memory population for memory mirroring.
Mirror Below 4GB	<ul style="list-style-type: none"> • Disable • Enable 	Mirrors all available system memory below the 4GB address limit when enabled; typically 1 to 3 GB. Note: Note: This item is only displayed when “Partial Mirror” is set to Enabled.
Partial Mirror Ratio In Basis Points	200	Configure the memory mirror ratio for the memory above 4 GB in basis points value. The valid range is 1 – 5000, meaning 0.01% to 50%. For example, to mirror 12.75% of memory, input the value 1275. Note: This item is only displayed when “Partial Mirror” is set to Enabled.

RAM Disk Configuration

Item	Options	Description
Disk Memory Type	<ul style="list-style-type: none"> • Boot Service Data • Reserved 	Specify type of memory to use from available memory pool in system to create a disk. Boot Service Data is the default setting.
Create raw	N/A	Create a raw RAM disk.
Create from file	N/A	Create a RAM disk from a given file.
Create RAM disk list	N/A	Specify RAM disk list.
Remove selected RAM disk(s)	N/A	Remove selected RAM disk(s).

Create raw

Item	Options	Description
Size (Hex)	1000	Specify the RAM disk size. The value should be multiples of the RAM disk block size.
Create & Exit	N/A	Create a raw RAM disk with the given starting and ending addresses.
Discard & Exit	N/A	Discard and exit.

Network

This menu displays network devices and network-related settings.



Table 10. Network

Item	Options	Description
Global Network Settings	N/A	Specify global network settings.
iSCSI Settings	N/A	Configure the iSCSI parameters.
Network Stack Settings	N/A	Specify network stack settings.
Network Boot Settings	N/A	Configure the network boot parameters.
HTTP Boot Configuration	N/A	Configure HTTP Boot parameters.
Tls Auth Configuration	N/A	Press Enter to select Tls Auth Configuration. Note: This item is only available for special system configurations.
Network Device	N/A	Display the network device list.

Note: The information and title of on-board or add-on card will show card's title, MAC address or PFA. These formats depend on card's driver, please contact with card vender for the format.

iSCSI Settings

Item	Options	Description
iSCSI Initiator Name	lqn.1986-03.com. example	The worldwide unique name of iSCSI Initiator. Only the IQN format is accepted. Range is from 4 to 233.
Add an Attempt	N/A	Add an attempt.
List of Attempts Note: Only appears when attempts exist.	N/A	MAC: XX:XX:XX:XX:XX:XX, PFA: Bus XX Dev XX Func XX, "iSCSI Mode": [%s1], "Internet Protocol": [%s2] The values vary with the attempt settings. %s1 is the option name for iSCSI Mode. %s2 is the setting name for Internet Protocol.
Delete Attempts	N/A	Delete one or more attempts.
Change Attempt Order	N/A	Change the order of attempts using +/- keys. Use arrow keys to select an attempt then press +/- to move the attempt up/down in the attempt order list.

Add an attempt

Item	Options	Description
List of NICs in the system e.g. MAC XX:XX:XX:XX:XX:XX	N/A	PFA: Bus XX Dev XX Func XX

MAC XX:XX:XX:XX:XX:XX

Item	Options	Description
iSCSI Attempt Name	N/A	Attempt Name is assigned automatically and not changeable.
iSCSI Mode	<ul style="list-style-type: none"> • Disabled • Enabled • Enable for MPIO 	Note: Please make sure that all necessary items (e.g., initiator IP, target IP and authentication settings) have been set properly before enabling this item. Otherwise, this attempt may lose after reboot.
Internet Protocol	<ul style="list-style-type: none"> • IPv4 • IPv6 • Autoconfigure 	Initiator IP address is system assigned in [IPv6] mode. In [Autoconfigure] mode, iSCSI driver will attempt to connect iSCSI target via IPv4 stack, if failed then via IPv6 stack.
Connection Retry Count	0	The minimum value is 0 and the maximum is 16. 0 means no retry.
Connection Establishing Timeout	1000	The timeout value is in milliseconds. The minimum value is 100 milliseconds and the maximum is 20 seconds.

OUI-format ISID	e. g., 3CD30AC68EF8	OUI-format ISID comes with 6 bytes. The default values are derived from MAC address. Only last 3 bytes are configurable. These values are taken from "Configure ISID" control.
Configure ISID	e. g., C68EF8	OUI-format ISID in 6 bytes, default value are derived from MAC address. Only last 3 bytes are configurable. Example: Update 0ABBCCDDEEFF to 0ABBCCF07901 by inputting F07901.
Enable DHCP	<ul style="list-style-type: none"> • Empty • X 	Enable DHCP
Initiator IP Address Note: This item appears when Enable DHCP is not enabled.	0.0.0.0	Enter IP address in dotted-decimal notation. Notes: When the IP address input is invalid, the following pop-up messages will show up: <ul style="list-style-type: none"> • ISCSI Message • Invalid IP address! • Ok
Initiator Subnet Mask Note: This item appears when Enable DHCP is not enabled.	0.0.0.0	Enter IP address in dotted-decimal notation. Notes: When the Subnet Mask input is invalid, the following pop-up messages will show up: <ul style="list-style-type: none"> • ISCSI Message • Invalid Subnet Mask! • Ok
Gateway Note: This item appears when Enable DHCP is not enabled.	0.0.0.0	Enter IP address in dotted-decimal notation. Notes: When the Gateway input is invalid, the following pop-up messages will show up: <ul style="list-style-type: none"> • ISCSI Message • Invalid Gateway! • Ok
Get target info via DHCP Note: This item appears when Enable DHCP is enabled.	<ul style="list-style-type: none"> • Empty • X 	Get target info via DHCP
Target Name Note: This item will not appear when Get target info via DHCP is enabled.	N/A	It indicates the worldwide unique name of the target. Only iqn. format is accepted. Notes: When the Target Name input is invalid, the following pop-up messages will show up: <ul style="list-style-type: none"> • ISCSI Message • Invalid iSCSI Name! • Ok

Target Address Note: This item will not appear when Get target info via DHCP is enabled.	0.0.0.0	Enter Target address in IPv4, IPv6 or URL format. You need to configure DNS server address in advance if input a URL string. Notes: When the IP address input is invalid, the following pop-up messages will show up: <ul style="list-style-type: none"> • ISCSI Message • Invalid IP address! • Ok
Target Port Note: This item will not appear when Get target info via DHCP is enabled.	3260	Target Port
Boot LUN Note: This item will not appear when Get target info via DHCP is enabled.	0	Hexadecimal representation of the LUN number. Examples are: 4751-3A4F-6b7e-2F99, 6734-9-156f-127, 4186-9 Notes: When the Boot LUN input is invalid, the following pop-up messages will show up: <ul style="list-style-type: none"> • ISCSI Message • Invalid LUN string! • Ok
Authentication Type	<ul style="list-style-type: none"> • CHAP • None 	Authentication method: [CHAP] or [None]
CHAP Type Note: This item appears when Authentication Type is CHAP.	<ul style="list-style-type: none"> • One way • Mutual 	[One way] or [Mutual]
CHAP Name Note: This item appears when Authentication Type is CHAP.	N/A	CHAP Name
CHAP Secret Note: This item appears when Authentication Type is CHAP.	N/A	The minimum length is in 12 bytes and the maximum length is in 16 bytes.
CHAP Status Note: This item appears when Authentication Type is CHAP.	<ul style="list-style-type: none"> • Not Installed • Installed 	<ul style="list-style-type: none"> • [Not Installed] if “CHAP Name” and “CHAP Secret” are not set. • [Installed] if “CHAP Name” and “CHAP Secret” are set.
Reverse CHAP Name Note: This item appears when CHAP Type is Mutual.		Reverse CHAP Name
Reverse CHAP Secret Note: This item appears when CHAP Type is Mutual.		The minimum length is in 12 bytes and the maximum length is in 16 bytes.

Reverse CHAP Status Note: This item appears when CHAP Type is Mutual.	<ul style="list-style-type: none"> • Not Installed • Installed 	<ul style="list-style-type: none"> • [Not Installed] if “Reverse CHAP Name” and “Reverse CHAP Secret” are not set. • [Installed] if “Reverse CHAP Name” and “Reverse CHAP Secret” are set.
Save Changes	N/A	Must reboot System manually for changes to take place.
Back to Previous Page	N/A	Back to previous page

Delete Attempts

Item	Options	Description
List of Attempts e.g., Attempt 1	<ul style="list-style-type: none"> • Empty • X 	MAC: XX:XX:XX:XX:XX:XX, PFA: Bus XX Dev XX Func XX, “iSCSI Mode”: [%s1], “Internet Protocol”: [%s2]
Commit Changes and Exit	N/A	Save changes and exit.
Discard Changes and Exit	N/A	Discard changes and exit.

Change Attempt Order

Item	Options	Description
Change Attempt Order Note: Options will list existing Attempts.	e.g. Attempt 1 Attempt 2	Change the order of Attempts using +/- keys. Use arrow keys to select the attempt and then press +/- to move the attempt up/down in the attempt order list.
Commit Changes and Exit	N/A	Save changes and exit.
Discard Changes and Exit	N/A	Discard changes and exit.

Network Stack Settings

Item	Options	Description
Network Stack	<ul style="list-style-type: none"> • Enabled • Disabled 	Enable/Disable UEFI Network Stack. Enabled is the default setting.
IPv4 PXE Support	<ul style="list-style-type: none"> • Enabled • Disabled 	Enable/Disable IPv4 PXE Boot Support. If disabled, IPv4 PXE boot option will not be created. Enabled is the default setting.
IPv4 HTTP Support	<ul style="list-style-type: none"> • Enabled • Disabled 	Enable/Disable IPv4 HTTP Boot Support. If disabled, IPv4 HTTP boot option will not be created. Disabled is the default setting.
IPv6 PXE Support	<ul style="list-style-type: none"> • Enabled • Disabled 	Enable/Disable IPv6 PXE Boot Support. If disabled, IPv6 PXE boot option will not be created. Enabled is the default setting.
IPv6 HTTP Support	<ul style="list-style-type: none"> • Enabled • Disabled 	Enable/Disable IPv6 HTTP Boot Support. If disabled, IPv6 HTTP boot option will not be created. Disabled is the default setting.

PXE boot wait time	0	<p>Wait time (in seconds) to press Esc to abort the PXE boot. Use either +/- or numeric keys to set the value.</p> <p>Notes: When an invalid value is input, the following popup message is displayed:</p> <ul style="list-style-type: none"> • ERROR • Invalid Input Range • Ok
Media detect count	1	<p>Number of times to detect media. Use either +/- or numeric keys to set the value.</p> <p>Notes: When an invalid value is input, the following popup message is displayed:</p> <ul style="list-style-type: none"> • ERROR • Invalid Input Range • Ok

Network Boot Settings

Item	Options	Description
MAC:XX:XX:XX:XX:XX:XX SlotXXX PFA XX:X:X	N/A	<p>Set the boot configuration parameters on MAC XX:XX:XX:XX:XX:XX</p> <p>PCI Function Address: Bus XX:Dev XX:Func: XX</p>
VLAN Configuration List: VLAN Configuration (MAC:XXXXXXXXXXXX)	N/A	<p>VLAN Configuration (MAC:XXXXXXXXXXXX)</p>
IPv4 Configuration List: MAC:XXXXXXXXXXXX-IPv4 Network Configuration	N/A	<p>Configure network parameters. (MAC:XXXXXXXXXXXX)</p>
IPv6 Configuration List: MAC:XXXXXXXXXXXX-IPv6 Network Configuration	N/A	<p>Configure IPv6 network parameters. (MAC:XXXXXXXXXXXX)</p>

MAC: Onboard PFA 1:0:0

Item	Options	Description
UEFI PXE Mode	<ul style="list-style-type: none"> • Enabled • Disabled 	<p>Enable/Disable NIC to include or skip boot attempt during generic PXE Network boot. For Legacy mode, Enable/Disable Option Rom from “Devices and I/O Ports” menu.</p> <p>Network Driver in “Network Device List” may also require configuration. “System Boot Mode” may further impact PXE.</p>
Legacy PXE Mode	<ul style="list-style-type: none"> • Enabled • Disabled 	<p>Enable/Disable NIC to include or skip boot attempt during generic PXE Network boot. For Legacy mode, Enable/Disable Option Rom from “Devices and I/O Ports” menu.</p> <p>Network Driver in “Network Device List” may also require configuration. “System Boot Mode” may further impact PXE.</p>

HTTP Boot Configuration

Note: When you enable Network->Network Stack Setting->IPv4 HTTP Support-or IPv6 HTTP support, HTTP Boot Configuration will be displayed in Network page.

When the network adapter is installed in the system, you will see the submenu, or nothing will be displayed in HTTP Boot Configuration form.

Item	Options	Description
List of NICs in the system e. g. MAC:XX:XX:XX:XX:XX:XX HTTP Boot Configuration	N/A	Configure HTTP Boot parameters. (MAC: XXXXXXXXXXXXX)

MAC:xxxxxxxxxx-HTTP Boot Configuration

Item	Options	Description
Input the description	N/A	Default value is UEFI HTTP.
Internet Protocol	<ul style="list-style-type: none"> • IPv4 • IPv6 	Select the version of Internet Protocol.
Boot URI	N/A	A new Boot Option will be created according to this Boot URI.

Note: After you input some information to create the new http boot option, you need to save it from the front-page System Configuration and Boot Management ->Save Settings, then you will see the boot option in Start Options.

Tls Auth Configuration

Note: These forms are from AMI/Intel CRB. When you enable Network->Network Stack Setting->IPv4 HTTP Support or IPv6 HTTP support, Tls Auth Configuration will be displayed in Network page.

Item	Options	Description
Server CA Configuration	N/A	Press <Enter> to configure Server CA.
Client Cert Configuration	N/A	Client cert configuration is unsupported currently.

Server CA Configuration

Item	Options	Description
Enroll Cert	N/A	Press <Enter> to enroll cert.
Delete Cert	N/A	Press <Enter> to delete cert.

Enroll Cert

Item	Options	Description
Enroll Cert Using File	N/A	Enroll Cert Using File. Note: Select the storage device from the popup message box and then select the file.
Cert GUID	N/A	Input digit character in 11111111-2222-3333-4444-1234567890ab format. Note: Pop up message box to input Cert GUID.
Commit Changes and Exit	N/A	Commit Changes and Exit
Discard Changes and Exit	N/A	Discard Changes and Exit

Delete Cert

Item	Options	Description
XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX	<ul style="list-style-type: none">• Empty• X	GUID for Cert. Note: If there's no cert file, the default is empty.

Operating Modes

Select the operating mode based on your preference.

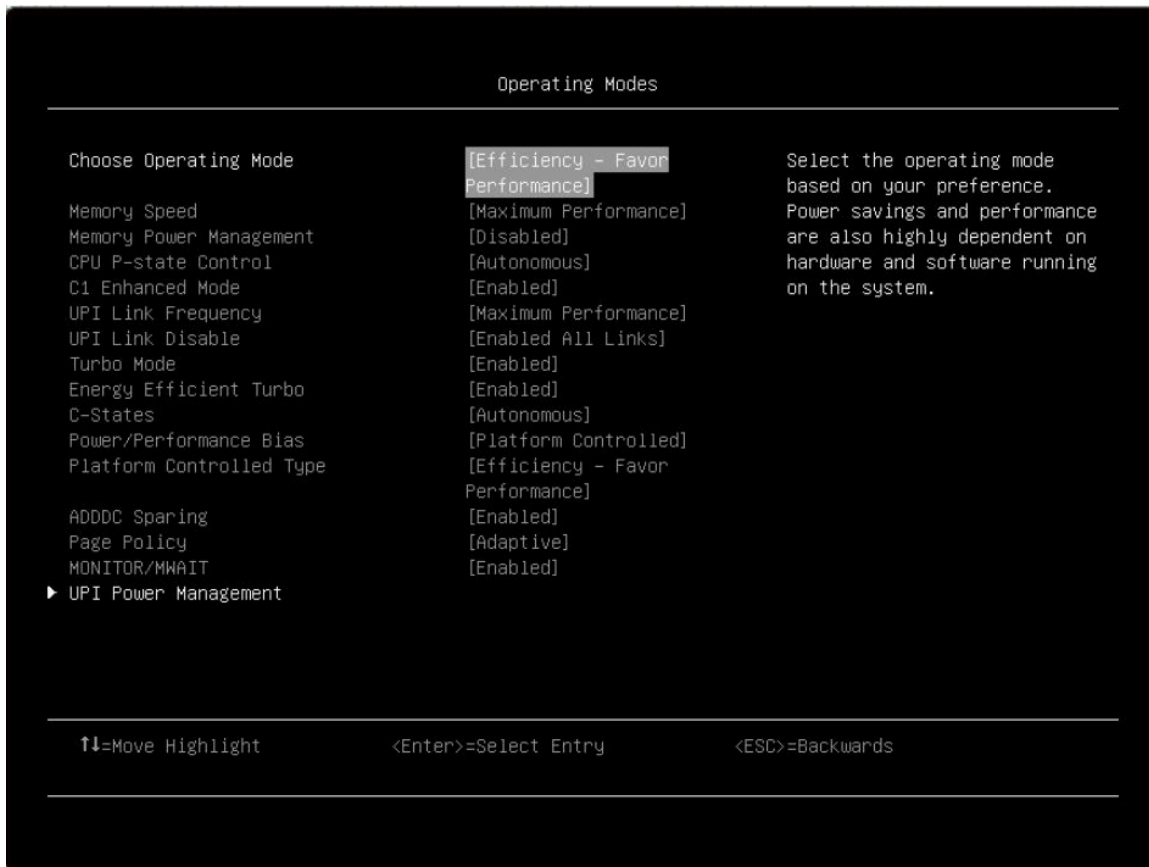


Table 11. Operating modes details

Item	Options	Description
Choose Operating Mode	<ul style="list-style-type: none"> Minimal Power Efficiency – Favor Power Efficiency – Favor Performance Custom Mode Maximum Performance 	<p>Select the operating mode based on your preference.</p> <p>Power savings and performance are highly dependent on hardware and software running on the system.</p> <p>Efficiency – Favor Performance is the default setting.</p>
Memory Speed	<ul style="list-style-type: none"> Minimal Power Balanced Max Performance 	<p>Select the desired memory speed mode.</p> <p>[Maximum performance] mode maximizes performance. [Balanced] mode offers a balance between performance and power. [Minimal power] mode maximizes power savings.</p> <p>When a preset mode is selected, the low-level settings are not changeable and will be grayed out. To change the settings, choose [Custom Mode] for "Choose Operating Mode" in "Operating Modes" located under "System Setting" submenu.</p> <p>Max Performance is the default setting.</p>

Table 11. Operating modes details (continued)

<p>Memory Power Management</p>	<ul style="list-style-type: none"> • Automatic • Disabled 	<p>[Disabled] provides maximum performance but minimum power savings. [Automatic] is suitable for most applications.</p> <p>When a preset mode is selected, the low-level settings are not changeable and will be grayed out. To change the settings, choose System Settings > Operating Modes > Choose Operating Mode > Custom Mode.</p> <p>Disabled is the default setting.</p>
<p>CPU P-state Control</p>	<ul style="list-style-type: none"> • None • Legacy • Autonomous • Cooperative without Legacy • Cooperative with Legacy 	<p>Select the method to control CPU P-states (performance states).</p> <p>[None] disables all P-states and the CPUs run at either their rated frequency or in turbo mode (if "Turbo Mode" is enabled).</p> <p>[Legacy]: The CPU P-states will be presented to the OS and the OS power management (OSPM) will directly control which P-state is selected.</p> <p>[Autonomous]: The P-states are controlled fully by system hardware. No P-state support is required in the OS or VM.</p> <p>[Cooperative] is a combination of [Legacy] and [Autonomous]. The P-states are still controlled by hardware but the OS can provide hints to the hardware for P-state limits, indicating the desired setting.</p> <p>When a preset mode is selected, the low-level settings are not changeable and will be grayed out. To change the settings, choose System Settings > Operating Modes > Choose Operating Mode > Custom Mode.</p> <p>Autonomous is the default setting.</p>
<p>C1 Enhanced Mode</p>	<ul style="list-style-type: none"> • Enabled • Disabled 	<p>[Enabled]: Save power by halting idle CPU cores. To use this feature, an OS that supports C1E state must be installed. Setting change takes effect after the next reboot.</p> <p>When a preset mode is selected, the low-level settings are not changeable and will be grayed out. To change the settings, choose [Custom Mode] for "Choose Operating Mode" in "Operating Modes" and [Legacy]/[Disabled] in "C-States" located under "System Setting" submenu.</p> <p>C1E status is changeable only when "C-states" is not [Autonomous].</p> <p>Enabled is the default setting.</p>

Table 11. Operating modes details (continued)

<p>UPI Link Frequency</p>	<ul style="list-style-type: none"> • Minimal Power • Balanced • Max Performance 	<p>Select the desired CPU UPI link frequency.</p> <p>[Maximum Performance] mode maximizes performance. [Balanced] mode offers a balance between performance and power. [Minimal Power] mode maximizes power savings.</p> <p>When a preset mode is selected, the low-level settings are not changeable and will be grayed out. To change the settings, choose System Settings > Operating Modes > Choose Operating Mode > Custom Mode.</p> <p>Max Performance is the default setting.</p> <p>Note: The UPI function works only if two or more processors are installed.</p>
<p>UPI Link Disable</p>	<ul style="list-style-type: none"> • Enabled All Links • Disabled 1 Link 	<p>Disabling one of the CPU UPI links can save power. To achieve the maximum performance, all UPI links should be enabled.</p> <p>When a preset mode is selected, the low-level settings are not changeable and will be grayed out. To change the settings, choose System Settings > Operating Modes > Choose Operating Mode > Custom Mode.</p> <p>Enabled All Links is the default setting.</p> <p>Note: The UPI function works only if two or more processors are installed.</p>
<p>Turbo Mode</p>	<ul style="list-style-type: none"> • Enabled • Disabled 	<p>[Enabled] 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.</p> <p>When a preset mode is selected, the low-level settings are not changeable and will be grayed out. To change the settings, choose System Settings > Operating Modes > Choose Operating Mode > Custom Mode.</p> <p>Enabled is the default setting.</p>
<p>Energy Efficient Turbo</p>	<ul style="list-style-type: none"> • Enabled • Disabled 	<p>[Enabled]: The CPU's optimal turbo frequency will be tuned dynamically based on CPU utilization. This item is also influenced by "Power/Performance Bias".</p> <p>When a preset mode is selected, the low-level settings are not changeable and will be grayed out. To change the settings, choose [Custom Mode] for "Choose Operating Mode" in "Operating Modes" and [Enabled] in "Turbo Mode" located under "System Setting" submenu.</p> <p>Enabled is the default setting.</p>

Table 11. Operating modes details (continued)

<p>C-States</p>	<ul style="list-style-type: none"> • Legacy • Autonomous • Disabled 	<p>C-states reduce CPU idle power.</p> <p>[Legacy]: The OS initiates the C-state transitions. ACPI C1/C2/C3 map to Intel C1/C3/C6.</p> <p>[Autonomous]: HALT and C1 request get converted to C6 requests in hardware.</p> <p>When a preset mode is selected, the low-level settings are not changeable and will be grayed out. To change the settings, choose System Settings > Operating Modes > Choose Operating Mode > Custom Mode.</p> <p>Autonomous is the default setting.</p>
<p>Power/Performance Bias</p>	<ul style="list-style-type: none"> • Platform Controlled • OS Controlled 	<p>Power/Performance Bias determines how aggressively the CPU will be power managed and placed into turbo.</p> <p>[Platform Controlled]: The system controls the setting.</p> <p>[OS Controlled] allows the OS to control it. Not all OSs support this feature.</p> <p>When a preset mode is selected, the low-level settings are not changeable and will be grayed out. To change the settings, choose System Settings > Operating Modes > Choose Operating Mode > Custom Mode.</p> <p>Platform Controlled is the default setting.</p>
<p>Platform Controlled Type</p>	<ul style="list-style-type: none"> • Maximum Performance • Efficiency - Favor Performance • Minimal Power 	<p>[Maximum Performance] allows the most aggressive use of turbo and power management functions are disabled, thereby increasing power consumption.</p> <p>[Minimal Power] disables turbo and maximizes the use of power management features.</p> <p>When a preset mode is selected, the low-level settings are not changeable and will be grayed out. To change the settings, choose System Settings > Operating Modes > Choose Operating Mode > Custom Mode.</p> <p>Efficiency - Favor Performance is the default setting.</p>
<p>ADDDC Sparing</p>	<ul style="list-style-type: none"> • Enabled • Disabled 	<p>Enable/Disable ADDDC Sparing.</p> <p>Additional note for CPX platform: This item is [Disabled] and grayed out when "Page Policy" is [Adaptive].</p> <p>Note: Displayed help messages vary with platforms.</p>
<p>Page Policy</p>	<ul style="list-style-type: none"> • Adaptive • Closed 	<p>[Adaptive] improves the performance of applications with a highly localized memory access pattern; [Closed] benefits applications that access memory more randomly.</p> <p>Closed is the default setting.</p>

Table 11. Operating modes details (continued)

<p>MONITOR/MWAIT</p>	<ul style="list-style-type: none"> • Enabled • Disabled 	<p>MONITOR/MWAIT instructions are used to engage C-states. Some OSs re-enable C-states even when they are disabled in setup. To prevent this, do the following:</p> <ol style="list-style-type: none"> 1. Disable "MONNITOR/MWAIT". 2. Choose System Settings > Operating Modes > Choose Operating Mode > Custom Mode. 3. Choose System Settings > C-States > Disabled. <p>Enabled is the default setting.</p>
<p>UPI Power Management</p>	<p>N/A</p>	<p>Set the desired power management level for the CPU UPI interface. L1 saves the most power but has longer latency compared to L0p or Disabled.</p> <p>When a preset mode is selected, the low-level settings are not changeable and will be grayed out. To change the settings, choose System Settings > Operating Modes > Choose Operating Mode > Custom Mode.</p> <p>Note: The UPI function works only if two or more processors are installed.</p>

Power

This menu allows you to configure power scheme options.



Table 12. Power details

Item	Options	Description
Power/Performance Bias	<ul style="list-style-type: none"> • Platform Controlled • OS Controlled 	<p>Power/Performance Bias determines how aggressively the CPU will be power managed and placed into turbo.</p> <p>[Platform Controlled]: The system controls the setting.</p> <p>[OS Controlled]: The OS controls the setting. Not all OSs support this feature.</p> <p>When a preset mode is selected, the low-level settings are not changeable and will be grayed out. To change the settings, choose System Settings > Operating Modes > Choose Operating Mode > Custom Mode.</p> <p>Platform Controlled is the default setting.</p>
Platform Controlled Type	<ul style="list-style-type: none"> • Maximum Performance • Efficiency - Favor Performance • Efficiency - Favor Power • Minimal Power 	<p>[Maximum Performance] allows the most aggressive use of turbo and power management functions are disabled, thereby increasing power consumption.</p> <p>[Minimal Power] disables turbo and maximizes the use of power management features.</p> <p>When a preset mode is selected, the low-level settings are not changeable and will be grayed out. To change the settings, choose System Settings > Operating Modes > Choose Operating Mode > Custom Mode.</p> <p>Efficiency - Favor Performance is the default setting.</p>
Workload Configuration	<ul style="list-style-type: none"> • Balanced • I/O sensitive 	<p>[I/O sensitive] is recommended for expansion cards that require high I/O bandwidth when the CPU cores are idle to allow enough frequency for the workload.</p> <p>Balanced is the default setting.</p>
ACPI Fixed Power Button	<ul style="list-style-type: none"> • Enabled • Disabled 	<p>Enable/Disable ACPI Fixed Power Button.</p> <p>When disabled, physically pressing the power button on front of the system will not execute the OS's Power Button Policy such as shutdown and turn off monitor. In addition, the "Shut down OS and ..." options under the IMM Server Power Actions feature will be disabled.</p> <p>Enabled is the default setting.</p>
PCIe Power Brake Note: This item is platform-dependent. Confirm with platform design guide for details.	<ul style="list-style-type: none"> • Reactive • Proactive • Disabled 	<p>PCIe Power Brake quickly reduces the power consumption and performance of high powered PCIe devices. Performances of low-power PCIe devices are not impacted by this setting. A high-power PCIe device refers to the one with a rated power of 75 W TDP or greater.</p>
ASPM Note: This item is platform-dependent. Confirm with platform design guide for details.	<ul style="list-style-type: none"> • Auto • Disabled 	<p>[Auto] will enable ASPM on PCIe endpoint adapters that support it. [Disabled] will disable ASPM for all PCIe endpoints. Disabled is the default setting.</p>

Processors

This menu offers options to change the processor settings.

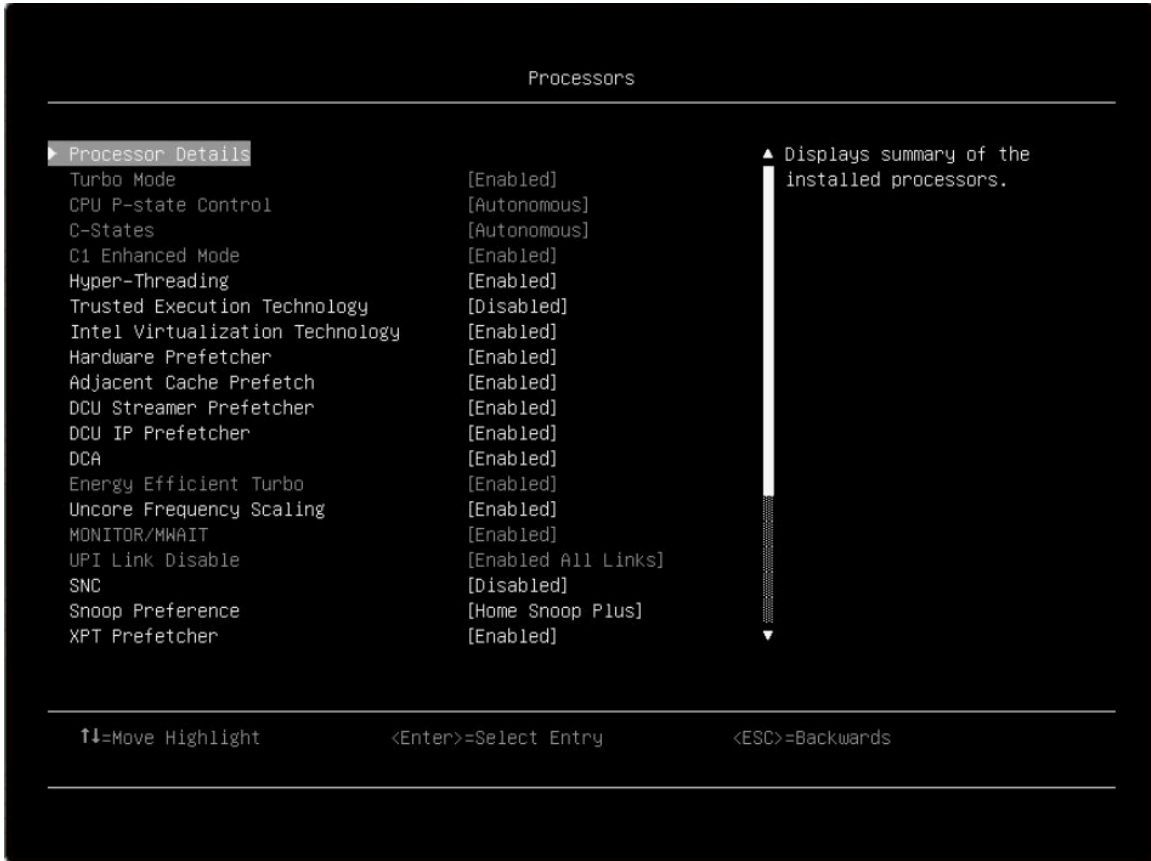


Table 13. Processors details

Item	Options	Description
Processor Details	N/A	Display summary of the installed processors.
Turbo Mode	<ul style="list-style-type: none"> • Enabled • Disabled 	<p>[Enabled] 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.</p> <p>When a preset mode is selected, the low-level settings are not changeable and will be grayed out. To change the settings, choose System Settings > Operating Modes > Choose Operating Mode > Custom Mode.</p> <p>Enabled is the default setting.</p> <p>Note: If a CPU does not support the feature, it will not be displayed.</p>

Table 13. Processors details (continued)

<p>CPU P-state Control</p>	<ul style="list-style-type: none"> • None • Legacy • Autonomous • Cooperative without Legacy • Cooperative with Legacy 	<p>Control the CPU P-states (performance states).</p> <p>[None]: All P-states are disabled and the CPUs run at either their rated frequency or in turbo mode (if turbo mode is enabled).</p> <p>[Legacy]: CPU P-states will be presented to the OS. The OS power management (OSPM) controls which P-state is selected.</p> <p>[Autonomous]: The P-states are fully controlled by system hardware. No P-state support is required in the OS or VM.</p> <p>[Cooperative] is a combination of [Legacy] and [Autonomous]. The P-states are still controlled by hardware but the OS can provide hints to the hardware for P-state limits, indicating the desired setting.</p> <p>When a preset mode is selected, the low-level settings are not changeable and will be grayed out. To change the settings, choose System Settings > Operating Modes > Choose Operating Mode > Custom Mode.</p> <p>Autonomous is the default setting.</p>
<p>C-States</p>	<ul style="list-style-type: none"> • Legacy • Autonomous • Disabled 	<p>C-states reduce CPU idle power.</p> <p>[Legacy]: The OS initiates the C-state transitions. ACPI C1/C2/C3 map to Intel C1/C3/C6.</p> <p>[Autonomous]: HALT and C1 request get converted to C6 requests in hardware.</p> <p>When a preset mode is selected, the low-level settings are not changeable and will be grayed out. To change the settings, choose System Settings > Operating Modes > Choose Operating Mode > Custom Mode.</p> <p>Autonomous is the default setting.</p>
<p>C1 Enhanced Mode</p>	<ul style="list-style-type: none"> • Enabled • Disabled 	<p>[Enabled]: Save power by halting idle CPU cores. To use this feature, an OS that supports C1E state must be installed. Setting change takes effect after the next reboot.</p> <p>When a preset mode is selected, the low-level settings are not changeable and will be grayed out. To change the settings, choose [Custom Mode] in "Choose Operating Mode" and [Legacy]/[Disabled] in "C-States" under the "System Setting" submenu.</p> <p>Enabled is the default setting.</p> <p>Note: C1E status is changeable only when "C-states" is not set to [Autonomous].</p>

Table 13. Processors details (continued)

Hyper-Threading	<ul style="list-style-type: none"> • Enabled • Disabled 	<p>Enable/Disable Hyper Threading, which is a software method to enable/disable Logical Processor threads.</p> <p>Enabled is the default setting.</p> <p>Notes:</p> <ul style="list-style-type: none"> • Changing this setting requires a Power Good reset to take effect. • If a CPU does not support the feature, it will not be displayed.
Trusted Execution Technology	<ul style="list-style-type: none"> • Enabled • Disabled 	<p>Enable/Disable the Intel Trusted Execution Technology (Intel TXT). Disabled is the default setting.</p>
Intel Virtualization Technology	<ul style="list-style-type: none"> • Enabled • Disabled 	<p>Enable/Disable the Intel Virtualization Technology. Enabled is the default setting.</p>
Hardware Prefetcher	<ul style="list-style-type: none"> • Enabled • Disabled 	<p>Lightly threaded applications and some benchmarks can benefit from having the hardware prefetcher enabled. Enabled is the default setting.</p>
Adjacent Cache Prefetch	<ul style="list-style-type: none"> • Enabled • Disabled 	<p>[Enabled] can benefit lightly threaded applications and some benchmarks. Enabled is the default setting.</p>
DCU Streamer Prefetcher	<ul style="list-style-type: none"> • Enabled • Disabled 	<p>[Enabled] can benefit lightly threaded applications and some benchmarks. Enabled is the default setting.</p>
DCU IP Prefetcher	<ul style="list-style-type: none"> • Enabled • Disabled 	<p>This item is typically best left enabled for most environments. Enabled is the default setting.</p>
DCA	<ul style="list-style-type: none"> • Enabled • Disabled 	<p>When enabled, DCA capable I/O devices such as network controllers can place data directly into the CPU cache, shortening response time. Enabled is the default setting.</p>
Energy Efficient Turbo	<ul style="list-style-type: none"> • Enabled • Disabled 	<p>When enabled, the CPU optimal turbo frequency will be tuned dynamically based on CPU utilization. This item is also influenced by "Power/Performance Bias".</p> <p>When a preset mode is selected, the low-level settings are not changeable and will be grayed out. To change the settings, choose [Custom Mode] for "Choose Operating Mode" in "Operating Modes" and [Enabled] in "Turbo Mode" located under "System Setting" submenu.</p> <p>Enabled is the default setting.</p>
Uncore Frequency Scaling	<ul style="list-style-type: none"> • Enabled • Disabled 	<p>When [Enabled], the CPU uncore (all miscellaneous logic inside the CPU package) will dynamically change the speed based on the workload. Enabled is the default setting.</p>

Table 13. Processors details (continued)

MONITOR/MWAIT	<ul style="list-style-type: none"> • Enabled • Disabled 	<p>MONITOR/MWAIT instructions are used to engage C-states. Some OSs will re-enable C-states even when they are disabled in setup. To prevent this, do the following:</p> <ol style="list-style-type: none"> 1. Disable MONNITOR/MWAIT. 2. Choose System Settings > Operating Modes > Choose Operating Mode > Custom Mode. 3. Choose System Settings > C-States > Disabled. <p>Enabled is the default setting.</p>
UPI Link Disable	<ul style="list-style-type: none"> • Enabled All Links • Disabled 1 Link 	<p>Disabling one of the CPU UPI links can save power. To achieve the maximum performance, all UPI links should be enabled.</p> <p>When a preset mode is selected, the low-level settings are not changeable and will be grayed out. To change the settings, choose System Settings > Operating Modes > Choose Operating Mode > Custom Mode.</p> <p>Enabled All Links is the default setting.</p> <p>Note: The UPI function works only if two or more processors are installed.</p>
SNC	<ul style="list-style-type: none"> • Enabled • Disabled 	<p>SNC (sub NUMA cluster) partitions the cores and 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.</p> <p>Disabled is the default setting.</p>
Snoop Preference	<ul style="list-style-type: none"> • Home Snoop Plus • Home Snoop 	<p>Select the appropriate snoop mode based on the workload.</p> <p>You cannot select a snoop mode once and for all. The mode will be changed if the current hardware configuration does not support the desired mode. Also not that SNC has priority over the snoop mode.</p> <p>Home Snoop Plus is the default setting.</p>
XPT Prefetcher	<ul style="list-style-type: none"> • Enabled • Disabled 	<p>XPT prefetch is a mechanism that enables a read request that is being sent to the last level cache to speculatively issue a copy of that read to the memory controller prefetching.</p> <p>Enabled is the default setting.</p>
UPI Prefetcher	<ul style="list-style-type: none"> • Enabled • Disabled 	<p>UPI prefetch is a mechanism to get the memory read started early on DDR bus.</p> <p>The UPI receive path will spawn a memory read to the memory controller prefetcher. Enabled is the default setting.</p> <p>Note: The UPI function works only if two or more processors are installed.</p>
Total Memory Encryption	<ul style="list-style-type: none"> • Enabled • Disabled 	<p>Enable/Disable Total Memory Encryption (TME). Disabled is the default setting.</p>

Table 13. Processors details (continued)

Multikey Total Memory Encryption	<ul style="list-style-type: none"> • Enabled • Disabled 	Enable/Disable Multikey Total Memory Encryption (MK-TME). Disabled is the default setting. Note: This option is only available when "Total Memory Encryption" is [Enabled].
Max MKTME Keys (for Ice Lake processor only)	N/A	
SW Guard Extensions (for Ice Lake processor only)	<ul style="list-style-type: none"> • Enabled • Disabled 	Enable/Disable Software Guard Extensions (SGX). Disabled is the default setting. Notes: This option is only available with some conditions. Before enabling this option, you need to: <ul style="list-style-type: none"> • Disable UMA-Based Clustering and enable Total Memory Encryption in System Setup; otherwise, this item is not available and not configurable. • Disable Mirror Mode; otherwise, this item may not work well. For more details about enabling SGX, go to: https://lenovopress.com/lp1471
SGX Factory Reset (for Ice Lake processor only)	<ul style="list-style-type: none"> • Enabled • Disabled 	Enable/Disable SGX Factory Reset. When enabled, it will erase all registration data on subsequent boot, and will additionally force an Initial Platform Establishment flow when SGX is enabled. Disabled is the default setting. Note: This item is only available with some conditions, same as SW Guard Extensions . Refer to the SGX document for details.
SGX Package Info In-Band Access (for Ice Lake processor only)	<ul style="list-style-type: none"> • Enabled • Disabled 	Enable/Disable SGX Package Info In-Band Access. Disabled is the default setting. Note: This option is only available with some conditions, same as SW Guard Extensions . Refer to the SGX document for details.
UMA-Based Clustering (for Ice Lake processor only)	<ul style="list-style-type: none"> • Disabled • Hemisphere • Quadrant 	Options for this item include: <ul style="list-style-type: none"> • [Disabled] (ALL2ALL) • [Hemisphere] (2 clusters) • [Quadrant] (4 clusters, not supported on ICX) Note: These option are only valid when SNC is disabled. If SNC is enabled, UMA-Based Clustering is automatically disabled by BIOS. Hemisphere is the default setting.

Table 13. Processors details (continued)

<p>Intel Speed Select (for Ice Lake processor and Bona only)</p>	<ul style="list-style-type: none"> • Base • Auto • Config1 • Config2 • SST-PP V2 	<p>If a CPU is installed that doesn't support SST, the Base option will be used regardless of the setting selected</p> <p>[Auto]: The level of SST enablement is controlled automatically based on the number of CPU cores enabled in UEFI. Auto is the default setting.</p> <p>[Base]: Effectively disabled SST.</p> <p>[Config1]/[Config2]: Force the SST cores limits based on the config option selected.</p> <p>[SST-PP V2]: Enable dynamic SST-PP mode. With SST-PP V2, the mode can be dynamically changed at runtime via Linux OS.</p> <p>Note: [Config1]/[Config2] may override the option that enables the number CPU cores in UEFI.</p>
<p>LLC Prefetch</p>	<ul style="list-style-type: none"> • Disabled • Enabled 	<p>F1 LLC prefetcher is an additional prefetch mechanism on top of the existing prefetchers that prefetch data into the core DCU and MLC. Enabling LLC prefetch gives the core prefetcher the ability to prefetch data directly into the LLC without necessarily filling into the MLC.</p>
<p>L2 RFO Prefetcher</p>	<ul style="list-style-type: none"> • Auto • Disabled 	<p>One of 4 variables (IRQThreshold, StaleAtoS, CRQoSConfiguration, L2RFOPrefetchDisable) used to optimize performance for SAP HANA on servers with 2-hop memory configurations such as 4-socket ring, 6-socket and 8-socket configurations. The Auto option makes the L2 prefetcher less aggressive and lowers NT write bandwidth. The Disabled menu option limits burstiness and reduces snooping.</p>
<p>PECI Is Trusted</p>	<ul style="list-style-type: none"> • Enabled • Disabled 	<p>Enable/Disable trust for the system's Peci (Platform Environment Control Interface).</p> <p>Select [Disabled] if a higher level of security is required. When [Disabled], some functions such as memory and I/O utilization reporting may not work. Enabled is the default setting.</p>
<p>Cores in CPU Package</p>	<ul style="list-style-type: none"> • All • 1 • . • . • . • . • n-1 	<p>Select the number of cores enabled within each CPU package.</p> <p>All is the default setting.</p> <p>The number "n" is the maximum core count supported by the installed processor. For example, if the installed processor supports 6 cores, the options will show All, 1, 2, 3, 4, and 5.</p>

Table 13. Processors details (continued)

<p>UPI Link Frequency</p>	<ul style="list-style-type: none"> • Minimal Power • Balanced • Maximum Performance 	<p>Select the desired CPU UPI link frequency.</p> <p>[Maximum Performance] mode maximizes performance.</p> <p>[Balanced] mode offers a balance between performance and power.</p> <p>[Minimal Power] mode maximizes power savings.</p> <p>When a preset mode is selected, the low-level settings are not changeable and will be grayed out. To change the settings, choose System Settings > Operating Modes > Choose Operating Mode > Custom Mode.</p> <p>Maximum Performance is the default setting.</p> <p>Note: The UPI function works only if two or more processors are installed.</p>
<p>CPU Frequency Limits</p>	<ul style="list-style-type: none"> • Full turbo uplift • Restrict maximum frequency 	<p>Note: This option is only available when "Turbo Mode" is enabled.</p> <p>Full turbo uplift is the default setting.</p>
<p>UPI Power Management</p>	<p>N/A</p>	<p>Set the desired power management level for the CPU UPI interface.</p> <p>[L1] is the most power-efficient but has longer latency compared to [L0p] or [Disabled].</p> <p>When a preset mode is selected, the low-level settings are not changeable and will be grayed out. To change the settings, choose System Settings > Operating Modes > Choose Operating Mode > Custom Mode.</p> <p>Note: The UPI function works only if two or more processors are installed.</p>
<p>CPU Frequency Limits</p>	<p>N/A</p>	<p>Note: This submenu is only available when "CPU Frequency Limits" is set to Restrict maximum frequency.</p> <p>The maximum frequency (turbo, AVX, and non turbo) can be restricted to a frequency between the maximum turbo frequency for the CPU installed and 1.2 GHz. This can be useful for synchronizing CPU tasks.</p> <p>Note: The maximum frequency does not change with the core count. 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.</p> <p>If the CPU frequency limits are being controlled through application software, leave this menu item at the default ([Full turbo uplift]), choose [Custom Mode] for "Choose Operating Mode" in "Operating Modes" and [Enabled] in "Turbo Mode" located under "System Setting" submenu.</p>

Processor Details

Item	Options	Description
Processor Socket	<ul style="list-style-type: none"> • Socket 1 • Socket n 	Processor Socket Table.
Processor ID	ASCII string	Tag for the Processor ID.
Processor Frequency	ASCII string	Value for the Processor Frequency.
Processor Revision	ASCII string	Value for the Microcode Revision.
L1 Cache RAM	ASCII string	Amount of L1 Cache RAM.
L2 Cache RAM	ASCII string	Amount of L2 Cache RAM.
L3 Cache RAM	ASCII string	Amount of L3 Cache RAM.
Cores Per Socket (Supported/ Enabled)	ASCII string	Number of supported and enabled processor cores per processor socket.
Threads Per Socket (Supported/ Enabled)	ASCII string	Number of supported and enabled processor threads per processor socket.
Processor 1 Version	ASCII string	Version of Processor 1. Note: The string might be read as generic string format. If any concern, you might check with Intel dear customer letter (DCL) for more detail. Such as the “Brand String” field in the document.
Processor n Version	ASCII string	Version of Processor n.

UPI Power Management

Item	Options	Description
L1	<ul style="list-style-type: none"> • Enabled • Disabled 	<p>Select the desired power management level for the CPU UPI interface. L1 saves the most power but has longer latency compared to L0p or Disabled. When a preset mode is selected, the low-level settings are not changeable and will be grayed out. If user would like to change the settings, please choose [Custom Mode] in “Operating Mode” located under “System Setting” submenu.</p> <p>Note: The UPI function works only if 2 or more processors installed.</p>
L0p	<ul style="list-style-type: none"> • Enabled • Disabled 	<p>Select the desired power management level for the CPU UPI interface. L1 saves the most power but has longer latency compared to L0p or Disabled. When a preset mode is selected, the low-level settings are not changeable and will be grayed out. If user would like to change the settings, please choose [Custom Mode] in “Operating Mode” located under “System Setting” submenu.</p> <p>Note: The UPI function works only if 2 or more processors installed.</p>

CPU Frequency Limits

Item	Options	Description
CPU Frequency Limits		
<p>Processors X to X cores active Note: This item is dynamic text, depending on the current processor state.</p>	<ul style="list-style-type: none"> • Max turbo frequency –1 bin • Max turbo frequency –2 bins • Max turbo frequency –3 bins 	<p>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.</p> <p>Note: The max frequency for N+1 cores cannot be higher than N cores.</p> <p>If an illegal frequency is entered, it will automatically be limited to a legal value.</p> <p>If the CPU frequency limits are being controlled through application software, leave this menu item at the default ([Full turbo uplift]).</p>

Recovery and RAS

This menu allows you to configure recovery policies and advanced reliability, availability, and serviceability settings.



POST Attempts

Item	Options	Description
Post Attempt Limit	<ul style="list-style-type: none"> • Disabled • 9 • 6 • 3 	<p>Configure the number of attempts to POST before the recovery mechanism is invoked.</p> <p>When the number of consecutive failed POST attempts reaches the limit, the system will reboot with the factory default settings. 3 is the default setting.</p>

Note: You may encounter some message boxes during POST attempts. Follow the message for setup.

Advanced RAS

Item	Options	Description
Machine Check Recovery	<ul style="list-style-type: none"> • Enabled • Disabled 	<p>Enable software layers (OS, VMM, DBMS, Application) to assist in system recovery from hardware uncorrectable error. Enabled is the default setting.</p>

PCI Error Recovery	<ul style="list-style-type: none"> • Enabled • Disabled 	<p>Allow the system to recover from an uncorrectable PCIe fault when enabled. The faulting PCIe device will be disabled for error containment and the OS will be notified to rescan the PCIe buses.</p> <p>Enabled is the default setting. An uncorrectable PCIe fault will result in an NMI (non-maskable interrupt) when disabled.</p>
PCIe Endpoint Reset on Fatal Error	<ul style="list-style-type: none"> • Enabled • Disabled 	<p>When enabled, the system will perform a PCIe Endpoint Reset after a fatal error. Disabled is the default setting.</p>

Disk GPT Recovery

Item	Options	Description
Disk GPT Recovery	<ul style="list-style-type: none"> • Automatic • Manual • None 	<p>[Automatic] means that system UEFI will automatically repair the corrupt GUID Partition Table (GPT).</p> <p>[Manual] means that system UEFI will only repair the corrupt GPT based on user input to a message box.</p> <p>[None] means that system UEFI will not repair the corrupted GPT. Recovery result can be retrieved from the system event log.</p> <p>None is the default setting.</p>

System Recovery

Item	Options	Description
POST Watchdog Timer	<ul style="list-style-type: none"> • Enabled • Disabled 	<p>Enable/Disable POST Watchdog Timer. Disabled is the default setting.</p>
POST Watchdog Timer Value	[5]	<p>Set a POST loader watchdog timer value in minutes from the specified range (5–20).</p>
Reboot System On NMI	<ul style="list-style-type: none"> • Enabled • Disabled 	<p>Enable/Disable system reboot on an NMI. Enabled is the default setting.</p> <p>Notes:</p> <ul style="list-style-type: none"> • If NMI is triggered by NMI button as diagnostic interrupt, XCC will only drive NMI without reboot action. • If NMI is triggered by XCC WebUI/IPMIcmd as software NMI, XCC will perform action based on setting. The default reboot timeout is 60 seconds.

Security

This menu allows you to configure system security settings.



Secure Boot Configuration

Item	Options	Description
Secure Boot Status	<ul style="list-style-type: none"> • Disabled • Enabled 	Display the current secure boot status. Disabled is the default setting.
Secure Boot Mode	<ul style="list-style-type: none"> • Setup Mode • User Mode 	The system will do secure boot authentication when this item is set to [User Mode] and secure boot is enabled. User Mode is the default setting.
Secure Boot Setting	<ul style="list-style-type: none"> • Enabled • Disabled 	<p>When enabled, the Secure Boot feature is Active, Platform Key (PK) is enrolled, and the system is in user mode.</p> <p>The mode change requires platform reset. Disabled is the default setting.</p> <p>Note: When you attempt to enable secure boot while CSM is enabled, there is a prompt:</p> <p>WARNING: Legacy BIOS will be disabled when secure boot is enabled.</p>

Secure Boot Policy	<ul style="list-style-type: none"> • Factory Policy • Custom Policy • Delete All Keys • Delete PK • Reset All Keys to Default 	<p>Secure Boot policy options:</p> <p>[Factory Policy]: Factory default keys will be used after reboot.</p> <p>[Custom Policy]: Customized keys will be used after reboot.</p> <p>[Delete All Keys]: PK, KEK, DB, and DBX will be deleted after reboot.</p> <p>[Delete PK]: PK will be deleted after reboot.</p> <p>[Reset All Keys to Default]: All keys will be set to factory defaults and "Secure Boot Policy" will be [Factory Policy] after reboot.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. "Secure Boot Mode" will be [Setup Mode] and "Secure Boot Policy" will be [Custom Policy] after PK is deleted. 2. The options cannot be loaded to default in Setup Utility.
View Secure Boot Keys	N/A	View the details of PK (Platform Key), KEK (Key Exchange Key), DB (Authorized Signature Database) and DBX (Forbidden Signature Database).
Secure Boot Custom Policy	N/A	<p>Customize PK, KEK, DB, and DBX.</p> <p>This page is available when "Secure Boot Policy" is [Custom Policy].</p>

View Secure Boot Keys

Item	Options	Description
PK	N/A	View Certificate in PK (Platform Key). Note: The system can only have one PK.
KEK	N/A	View all Certificates in KEK (Key Exchange Key).
DB	N/A	View all Certificates in DB (Authorized Signature Database).
DBX	N/A	View all Certificates in DBX (Forbidden Signature Database).

Secure Boot Custom Policy

Item	Options	Description
Enroll Efi Image	N/A	Enroll the SHA256 hash of the selected EFI image binary into the Authorized Signature Database (DB).

Trusted Platform Module (TPM 2.0)

Item	Options	Description
TPM 2.0	N/A	Configure the TPM 2.0 Setup options.
Update to TPM 2.0 firmware version 7.2.2.0	N/A	<p>Note: The latest TPM toggling configuration only supports TPM 2.0 firmware update from version 7.2.1.0 to version 7.2.2.0; therefore, this setting is not available for other TPM versions.</p> <p>When you are trying to degrade to TPM 1.2 or an earlier version of TPM 2.0, the following message will be displayed:</p> <p>Note: This action is irreversible, you won't be able to change to TPM 1.2 or an earlier firmware version of TPM 2.0. The updated firmware will be effective after system reboot.</p>

For TPM 2.0:

Item	Options	Description
TPM Status	N/A	
TPM Vendor	N/A	Display the TPM Vendor.
TPM Firmware Version	N/A	Display the current firmware version of the TPM device.
TPM Settings	N/A	
TPM2 Operation	<ul style="list-style-type: none"> • No Action • Clear 	Select [Clear] to clear TPM data. This will erase the contents of the TPM. System reboot is required.
SHA-1 PCR Bank	<p>For Ice Lake processor:</p> <ul style="list-style-type: none"> • Enabled • Disabled <p>For CPX platform:</p> <ul style="list-style-type: none"> • Enabled • Disabled 	Enable/Disable SHA-1 PCR Bank.

Update TPM Firmware from TPM 2.0 to TPM 1.2

Item	Options	Description
TPM 1.2		Configure the TPM 1.2 Setup options.
TPM Version	N/A	
Update to TPM2.0 compliant		<p>Notes:</p> <ul style="list-style-type: none"> • When update TPM version to TPM2.0 compliant, do not boot a legacy OS due to security consideration. • Change is effective after system reboot. • You can only switch TPM firmware 128 times.

In latest TPM toggling configuration, only support updating TPM 2.0 firmware version 7.2.1.0 to 7.2.2.0, so this setting will disappear with other TPM version.

Table 14. Trusted Platform Module (TPM 1.2)

Item	Options	Description
TPM Status	N/A	
TPM Vendor		Display TPM Vendor.
TPM Firmware Version		Display the current firmware version of the TPM device.
TPM Device State	Dynamic String depend on current TPM status.	Display the current state of the TPM Device.
TPM Ownership	Dynamic String depend on current TPM status.	Display the current status of ownership.
TPM Device	<ul style="list-style-type: none"> • Enabled • Disabled 	Enable/Disable the TPM device.
TPM State	<ul style="list-style-type: none"> • Activate • Deactivate 	Activate/Deactivate the TPM device.
TPM Operation	<ul style="list-style-type: none"> • No Action • Clear 	Select [Clear] to clear TPM data. WARNING: This will erase the contents of the TPM. System reboot required.

Storage

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
NVMe	NVMe Devices list.
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.
- All onboard NVMe drives connected to the system will be only displayed in the page: **System settings → Storage → NVMe.**
- Onboard NVMe devices will not list when VMD is enabled.

Date and Time

This menu allows you to set the local Date and Time of the system.



Table 15. 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 numeric keys to set the hour, minutes, and seconds. Use a 24-hour format for entering hours. Example: 15:00 for 3pm.

Start Options

This menu allows you to boot as desired from the primary boot sequence as specified under **Boot Manager**.

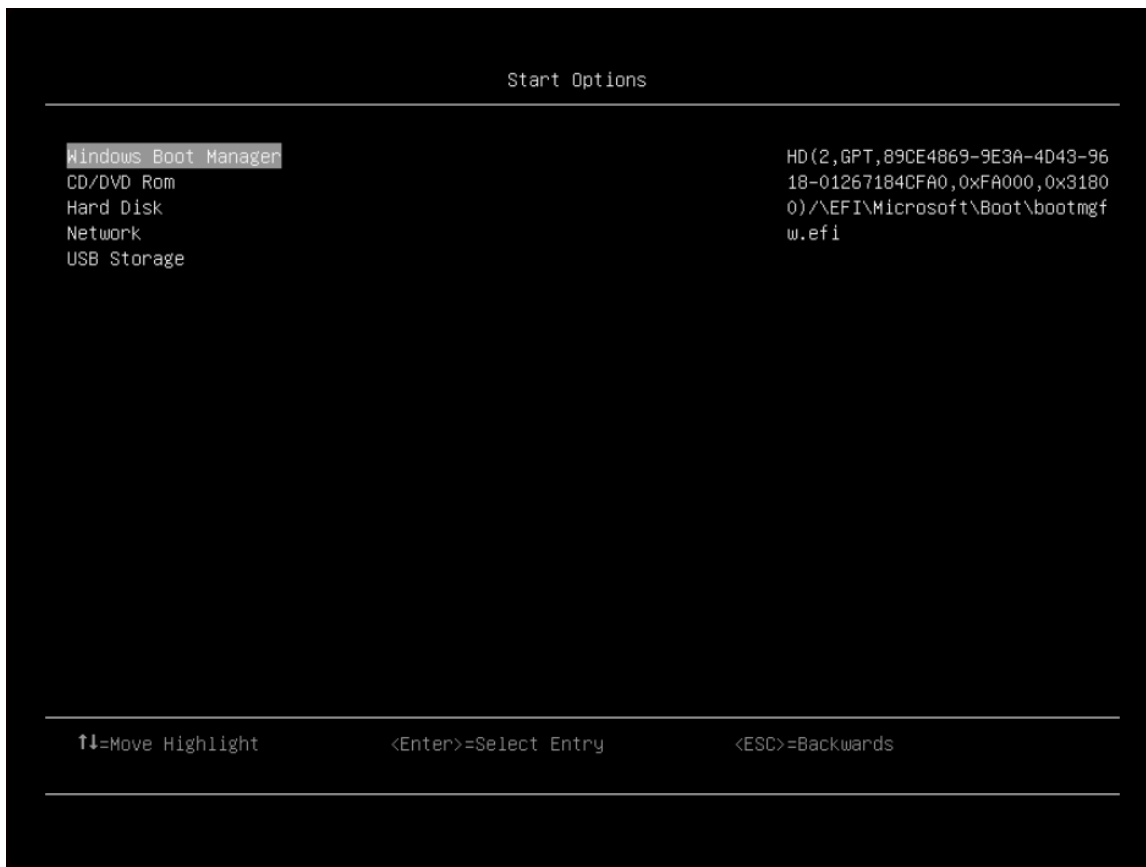


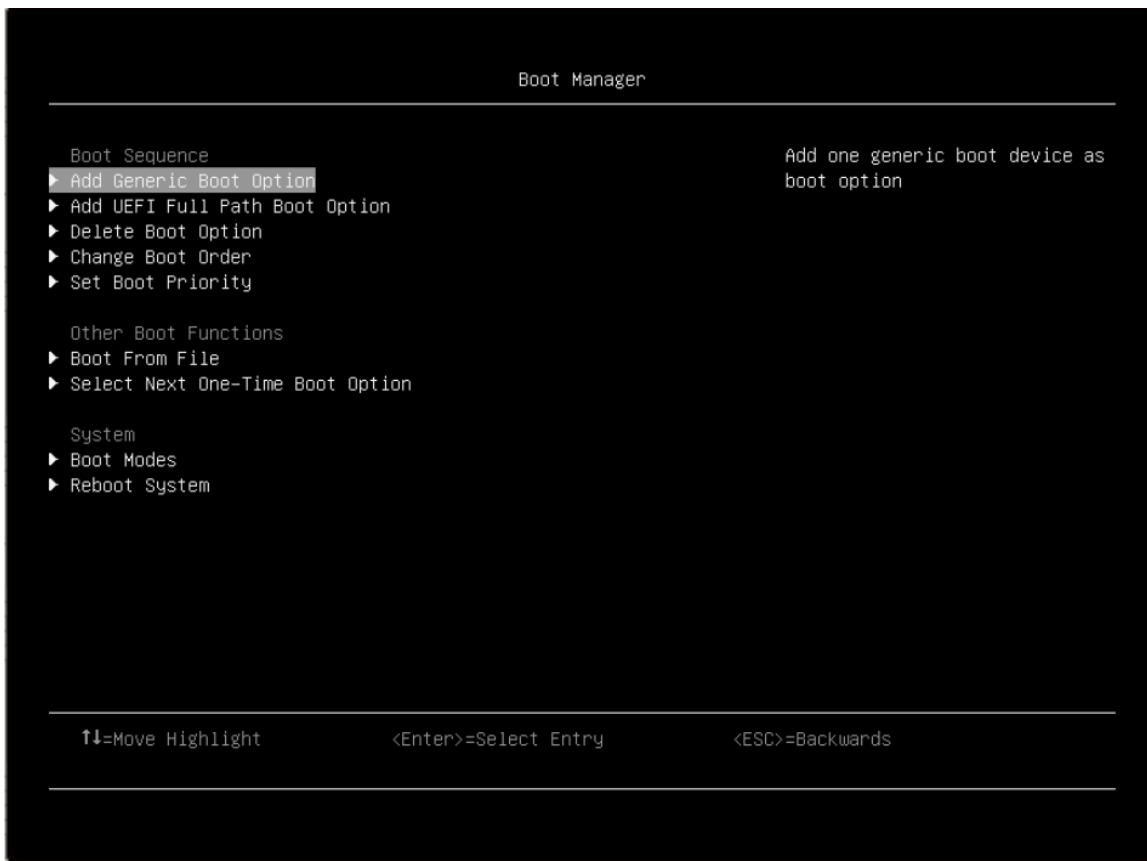
Table 16. Start options details

Item	Description
CD/DVD Rom	Select the hexadecimal device address and the server will boot from this device next time.
Hard Disk	
Network	
USB Storage	

Note: This page will list current boot order. The above table is for default boot order. Contents will be different if system has different boot order.

Boot Manager

This menu allows you to choose boot order, boot parameters, and boot from a file.



Add Generic Boot Option

Add one generic boot device as boot option.

Add UEFI Full Path Boot Option

Add one UEFI application or one removable file system as boot option.

Item	Options	Description
Boot option File Path	N/A	Specify the file path for newly created boot option.
Input the Description	N/A	Specify name for the new boot option.
Select Device Path Option	Xxxx {xxxx-xxx-xxx...}	Select device path option.
Commit Changes and Exit	N/A	Save changes and exit.

Delete Boot Option

Remove boot option(s) from "Boot Order".

Item	Options	Description
CD/DVD Rom	<ul style="list-style-type: none"> • [] • [X] 	Example: VenHw(B2AD3248-4F72-4950-A966-CFE5062DB83A,02000000)
Hard Disk		Example: VenHw(B2AD3248-4F72-4950-A966-CFE5062DB83A,01000000)

Network		Example: VenHw(B2AD3248-4F72-4950-A966-CFE5062DB83A,05000000)
USB Storage		Example: VenHw(B2AD3248-4F72-4950-A966-CFE5062DB83A,04000000)
Commit Changes and Exit	N/A	Save changes and exit.

This page may be changed according to your system configuration.

Change Boot Order

Modify the ordering of selections within "Boot Order".

Item	Options	Description
Change the Order	<ul style="list-style-type: none"> • CD/DVD Rom • Hard Disk • Network • USB Storage 	<p>Change the order.</p> <p>It will display the boot options under [Start Options].</p>
Commit Changes and Exit	N/A	Save changes and exit.

Set Boot Priority

Set boot priority of the devices in a device group.

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

This page may be changed according to your system configuration. Only device group in Boot Order will appear in this page. For default, this page will contain CD/DVD, Hard Disk, and Network priorities. USB Priority will appear once added to boot order. Removed option will not appear in this page.

Boot From File

Boot the system from a specific file or device.

Select Next One-Time Boot Option

Select the one-time boot option for the next boot.

Item	Options	Description
Boot Option	<ul style="list-style-type: none"> • CD/DVD Rom • Hard Disk • Network • USB Storage 	Select the one-time boot option for the next boot. NONE is the default setting.

Boot Modes

Switch between UEFI boot mode and legacy boot mode.

Item	Options	Description
System Boot Mode	<ul style="list-style-type: none"> • UEFI Mode • Legacy Mode 	<p>Drivers, option ROMs and OS loaders the "Boot Manager" attempts to boot.</p> <p>[UEFI Mode]: Run UEFI drivers and boot a UEFI OS loader. [Legacy Mode]: Run option ROMs and boot a legacy OS.</p> <p>UEFI Mode is the default setting.</p> <p>Note: This setting will be forced to [UEFI Mode] when Legacy BIOS is disabled under System Settings > Legacy BIOS > Legacy BIOS.</p>
Infinite Boot Retry	<ul style="list-style-type: none"> • Enabled • Disabled 	Continuously retry the Boot Order. Ensure a bootable device is specified in "Boot Order". Disabled is the default setting.
Prevent OS Changes To Boot Order	<ul style="list-style-type: none"> • Enabled • Disabled 	When set to "Enable", UEFI will remove the boot option which is created by OS or OS Installer from Boot Order List.

Reboot System

Prompt to reboot the system. If Y is pressed, any setup changes will be lost and the system will reboot.

BMC Settings

This menu allows you to configure the management controller.

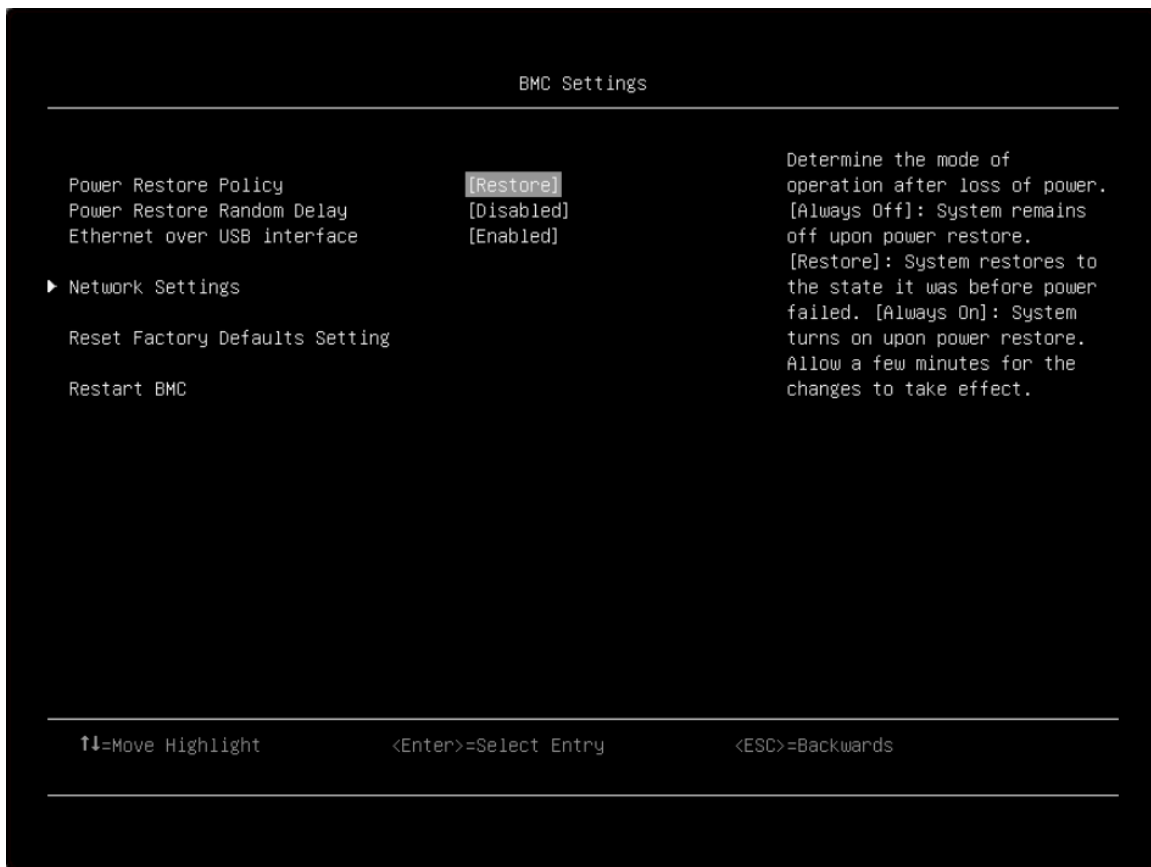


Table 17. BMC settings

Item	Options	Description
Power Restore Policy	<ul style="list-style-type: none"> • Always Off • Restore • Always On 	<p>Determine the mode of operation after loss of power.</p> <p>[Always Off]: System remains off upon power restore. [Restore]: System restores to the state it was before power failed. [Always On]: System turns on upon power restore. Allow a few minutes for the changes to take effect.</p> <p>Note: This option is configuration-dependent, and this item cannot restore to default value by using the "load default" option in Setup.</p>
Power Restore Random Delay	<ul style="list-style-type: none"> • Enabled • Disabled 	<p>Provide a random delay of 1 to 15 seconds for Power On. If system state was on before power failed, the system will delay Power On once power is restored.</p> <p>Notes:</p> <ul style="list-style-type: none"> • This option is platform-dependent, and this item cannot restore to default value by using the "load default" option in Setup. • When "Power Restore Policy" is [Always Off], the item is not shown.

Table 17. BMC settings (continued)

Ethernet over USB interface	<ul style="list-style-type: none"> • Enabled • Disabled 	<p>[Enabled] will make the xClarity Essentials in-band update utility available.</p> <p>[Disabled] will prevent xClarity Essentials and other applications running on the server from requesting the BMC to perform tasks.</p> <p>Note: After you modify related settings of Ethernet over USB interface, the new settings do not take effect immediately but after a while.</p>
Network Settings	N/A	Configure the network of the management controller.
Reset Factory Defaults Setting	N/A	Restore all management controller settings to factory defaults, including network configuration and credentials. The management controller will be restarted automatically.
Restart BMC	N/A	Restart the BMC.

Note: All settings under BMC page could not reset to default with **Load Default Settings**. Please use **Reset Factory Defaults Setting** to reset to default setting in this page.

Network settings

Item	Options	Description
Network Interface Port	<ul style="list-style-type: none"> • Dedicated • Shared 	<p>Select the System Management Network Interface Port.</p> <p>Note: This option is configuration-dependent.</p>
Shared NIC on	Dedicated	<p>Select the shared NIC port.</p> <p>Note: This item is only on when "Network Interface Port" is [Shared], and this option is configuration-dependent.</p>
Fail-Over Rule	<ul style="list-style-type: none"> • None • Failover to shared (Optional Card ML2) • Failover to shared (Optional Card PHY) • Failover to shared (Onboard Port) 	<p>Control fail-over types allowed.</p> <p>Note: This item is only on when "Network Interface Port" is [Dedicated], and this option is configuration-dependent.</p>
Network Setting	<ul style="list-style-type: none"> • Dedicated • Shared 	The item is selectable when Fail-Over Rule is enabled to onboard port or optional card.
Burned-in MAC Address	N/A	
Hostname	N/A	Change the host name. The new name should be within 1 to 63 characters.
DHCP Control	<ul style="list-style-type: none"> • Static IP • DHCP Enabled • DHCP with Fallback 	Configure DHCP Control or manually configure a static IP address. Fallback will use static IP address if DHCP fails. Select Static IP to enter IPV4 address manually.

IP Address	x.x.x.x	Enter an IP address in dotted-decimal notation. When an invalid IP address is input, the following popup message is displayed: <ul style="list-style-type: none"> • ERROR • Invalid Input Range • Ok
Subnet Mask	x.x.x.x	Enter the subnet mask in dotted-decimal notation. When an invalid IP address is input, the following popup message is displayed: <ul style="list-style-type: none"> • ERROR • Invalid Input Range • Ok
Default Gateway	x.x.x.x	Enter the default gateway in dotted-decimal notation. When an invalid IP address is input, the following popup message is displayed: <ul style="list-style-type: none"> • ERROR • Invalid Input Range • Ok
IPv6	<ul style="list-style-type: none"> • Enabled • Disabled 	Enable/Disable IPv6 support on management port.
Local Link Address	N/A	
VLAN Support	<ul style="list-style-type: none"> • Enabled • Disabled 	Enable/Disable VLAN Support to specify the 802.1q VLAN ID on the management port network device.
VLAN ID	1	VLAN ID Range is 1-4094. Note: This item only on VLAN Support is enabled. Note: Enter an invalid VLAN ID, the following popup message will display: ERROR Invalid Input Range Ok
Advanced Setting for BMC Ethernet	N/A	Provide advanced settings for BMC Ethernet.

Note: UEFI Setup does not cache the previous shared NIC settings, so after changing "Network Interface Port" to [Dedicated] and enabling "Failover to Shared NIC" with "Independence" mode, you need to change "Network Interface Port" back to [Shared] and configure the network settings for failover to shared NIC.

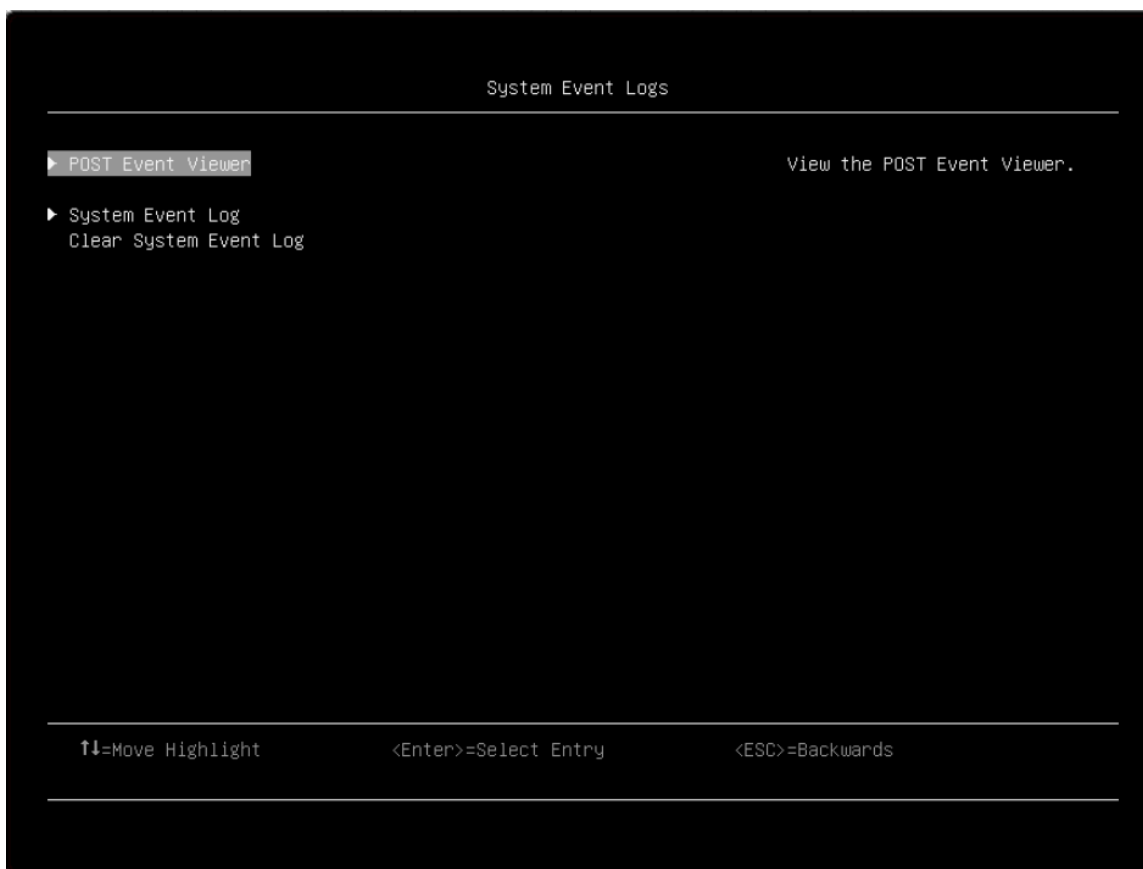
Advanced Settings for BMC Ethernet

Item	Options	Description
Autonegotiation	<ul style="list-style-type: none"> No Yes 	<p>[No]: Can manually choose the Data rate and Duplex mode.</p> <p>[Yes]: There is no manual configuration needed.</p> <p>Notes:</p> <ul style="list-style-type: none"> This item is configuration-dependent. This item cannot restore to default value by using the "load default" option in Setup.
<p>Data rate</p> <p>Note: This item is only displayed when Autonegotiation is No.</p>	<ul style="list-style-type: none"> 100 Mb (Ethernet) 10 Mb (Ethernet) 	<p>Set the amount of data to be transferred per second over LAN connection.</p> <p>Notes:</p> <ul style="list-style-type: none"> This item is configuration-dependent. This item cannot restore to default value by using the "load default" option in Setup.
<p>Duplex</p> <p>Note: This item is only displayed when Autonegotiation is No.</p>	<ul style="list-style-type: none"> Half Full 	<p>Set the type of communication channel used in the network.</p> <p>[Full]: Allow data to be transferred in both directions at once.</p> <p>[Half]: Allow data to be transferred in either one direction or the other, but not both at the same time.</p> <p>Notes:</p> <ul style="list-style-type: none"> This item is configuration-dependent. This item cannot restore to default value by using the "load default" option in Setup.
Maximum Transmission Unit	1500	Specify the maximum size of a packet (in bytes) for the network interface. The valid range is 68–1500.

Note: Changes will take effect after network settings in previous page are saved.

System Event Logs

This menu allows you to clear or view the System Event Log.



POST Event Viewer

View the POST event logs in POST Event Viewer.

System Event Log

View the System Event Log.

Item	Options	Description
Total SEL entries	N/A	Total number of system event logs retrieved from the BMC. This does not include any associated extended logs.
Previous Page	N/A	View system event logs in the previous page.
Next Page	N/A	View system event logs in the next page.

User Security

This menu allows you to set or change Power-On and Administrator passwords.

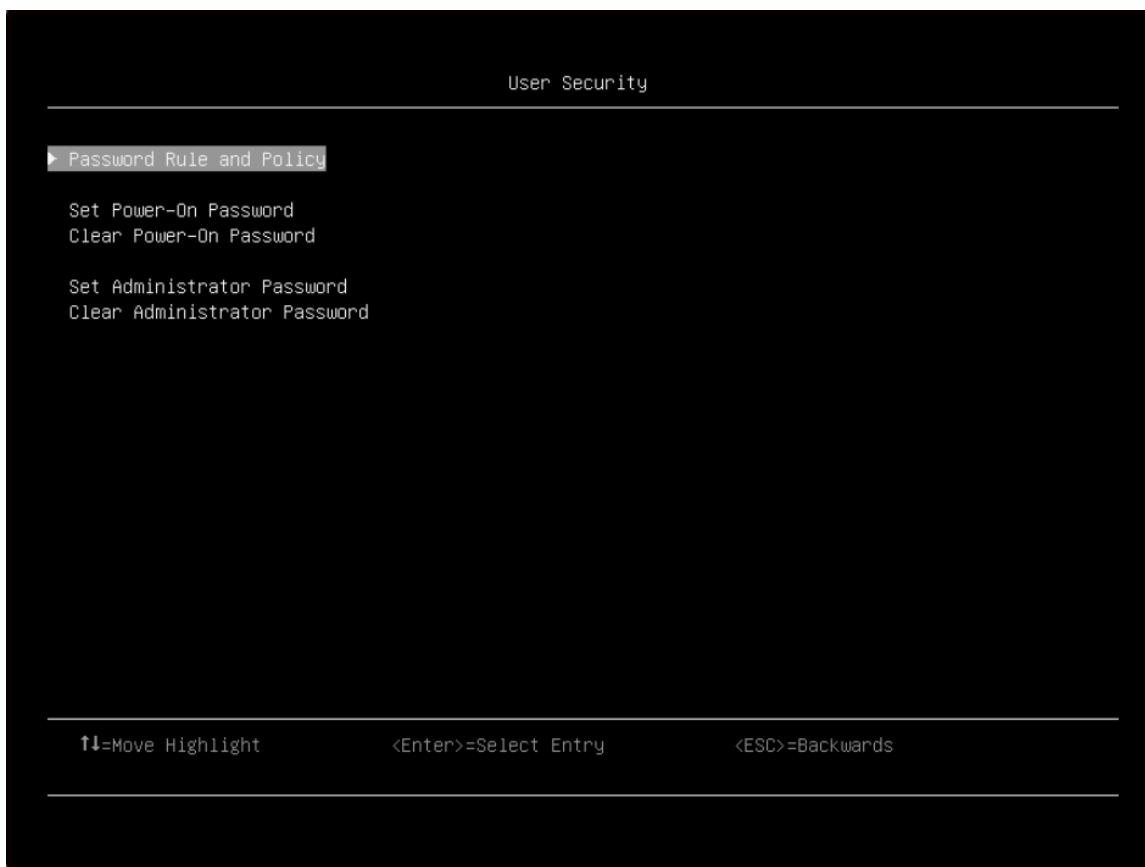


Table 18. User security details

Item	Options	Description
Password Rule and Policy	N/A	Set the password rule and policy.

Table 18. User security details (continued)

<p>Set Power-On Password</p>	<p>N/A</p>	<p>Set the power-on password.</p> <p>The password can only contain the following characters (excluding white-space characters): A-Z, a-z, 0-9, ~!@#\$%^&*()-+={}[];:"'<>,?/_</p> <p>Must contain at least one letter.</p> <p>Must contain at least one number.</p> <p>Must contain at least 2 of the following:</p> <ul style="list-style-type: none"> • At least one upper-case letter • At least one lower-case letter • At least one special character <p>No more than 2 consecutive occurrences of the same character</p> <p>Must be at least x characters set in "Minimum password length", or 8 characters if "Minimum password length" is not set.</p> <p>Notes: Click the button, a pop-up message box will show up.</p> <ul style="list-style-type: none"> • Please type in your password • Please type in your new password • Please confirm your new password • Power-On Password has been set successfully • The password failed to meet the "Minimum password reuse cycle" requirements. • Please enter enough characters <p>Press Enter to continue</p> <ul style="list-style-type: none"> • The password cannot be changed because the "Minimum password change interval" time is not exceeded. • The password does not meet the minimum password complexity requirements. <p>Please check the help for "Set Power-On Password" or "Set Administrator Password" settings.</p> <ul style="list-style-type: none"> • Passwords are not the same <p>Press Enter to Continue</p> <ul style="list-style-type: none"> • Incorrect Password <p>Press Enter to Continue</p> <ul style="list-style-type: none"> • Passwords operation has unknown problems. <p>Press Enter to Continue</p> <p>When IPMI command has no response, then pop out this message.</p>
-------------------------------------	------------	---

Table 18. User security details (continued)

<p>Clear Power-On Password</p>	<p>N/A</p>	<p>Clear the Power-On password.</p> <p>Note: Click the button, a pop-up message box will show up.</p> <ul style="list-style-type: none"> • Power-On Password is not set <p>Press Enter to Continue</p> <ul style="list-style-type: none"> • An existing Power-On Password will be deleted. <ENTER> Continue. <ESC> Return to Setup Utility • Power-On Password has been cleared successfully <p>Press Enter to Continue</p>
<p>Set Administrator Password</p>	<p>N/A</p>	<p>Set the Administrator password.</p> <p>The password can only contain the following characters (no white-space characters allowed): A-Z, a-z, 0-9, ~!@#\$%^&*()-+={}[];:"'<>?/._</p> <p>Must contain at least one letter</p> <p>Must contain at least one number</p> <p>Must contain at least 2 of the following:</p> <ul style="list-style-type: none"> • At least one upper-case letter • At least one lower-case letter • At least one special character <p>No more than 2 consecutive occurrences of the same character</p> <p>Must be at least x characters set in "Minimum password length", or 8 characters if "Minimum password length" is not set.</p> <p>Notes: Click the button, a pop-up message box will show up.</p> <ul style="list-style-type: none"> • Please type in your password • Please type in your new password • Please confirm your new password • Administrative Password has been set successfully • The password failed to meet the "Minimum password reuse cycle" requirements. • The password can't be changed because the "Minimum password change interval" time is not exceeded. • The password does not meet the minimum password complexity requirements. <p>Please check the help for "Set Power-On Password" or "Set Administrator Password" settings.</p> <ul style="list-style-type: none"> • Please enter enough characters <p>Press Enter to Continue</p>

Table 18. User security details (continued)

		<ul style="list-style-type: none"> • Passwords are not the same <p>Press Enter to Continue</p> <ul style="list-style-type: none"> • Incorrect Password <p>Press Enter to Continue</p> <ul style="list-style-type: none"> • Passwords operation has unknown problems. <p>Press Enter to Continue</p> <p>When IPMI command has no response then pop out this message.</p>
Clear Administrator Password	N/A	<p>Clear the Administrator password.</p> <p>Clicking the button, pop-up message box will show up.</p> <ul style="list-style-type: none"> • An existing Administrative Password will be deleted <ENTER> Continue. <ESC> Return to Setup Utility • Administrative Password has been cleared successfully <p>Press Enter to Continue</p> <ul style="list-style-type: none"> • Administrative Password is not set <p>Press Enter to Continue</p>

Password Rule and Policy

Item	Options	Function
Minimum password length	8–20	<p>Input a value from 8 to 20.</p> <p>It indicates the minimum number of characters of a valid password.</p> <p>The length value will take affect right after the value get changed. Please “Save Setting” from Main Menu if would like to keep setting after system reboot.</p>
Password expiration period	0–365	<p>Input a value from 0 to 365. The number of days a password may be used before it must be changed. If set to 0, the passwords never expire.</p>
Password expiration warning period	0–365	<p>Input a value from 0 to 365. The number of days before receiving a warning about the expiration of the password. If set to 0, the passwords will never be warned.</p>
Minimum password change interval	0–240	<p>Input a value from 0 to 240. The number of hours that must elapse before changing a password. The value specified for this setting cannot exceed the value specified for "Password expiration period". If set to 0, the passwords can be changed immediately.</p>

Minimum password reuse cycle	0–10	<p>Input a value from 0 to 10. The minimum number of times a unique password must be set before reusing a previous password. If set to 0, the passwords can be reused immediately.</p> <p>The reuse cycle value will take affect right after the value get changed. Please “Save Setting” from Main Menu if would like to keep setting after system reboot.</p>
Maximum number of login failures	0–100	<p>Input a value from 0 to 100. The number of login attempts that can be made with an incorrect password before the user account is locked out. If set to 0, the account will never be locked. The login failure counter is reset to zero after a successful login.</p>
Lockout period after maximum login failures	0–2880	<p>Input a value from 0 to 2880. The number of minutes that must pass before a locked out user account can attempt to login.</p> <p>Entering a valid password does not unlock the account during the lockout period. If set to 0, the account will not be locked out even if the "Maximum number of login failures" is exceeded.</p>

F12 One Time Boot Device

Item	Options	Description
Legacy Mode	<ul style="list-style-type: none"> • <input type="checkbox"/> • <input checked="" type="checkbox"/> 	<p>Override the “System Boot Mode” specified in the “Boot Mode” menu. “Set Option ROM Execution Order” setting under the “Devices and I/O Ports” menu may still affect boot ordering.</p> <p>Some network cards' legacy PXE boot option need have "PCI 64-Bit Resource Allocation" as "Disable" in the "Device and I/O Ports" menu.</p> <p>Notes: When select this item, the page will be refreshed to show legacy group:</p> <ul style="list-style-type: none"> • CD/DVD Rom • Hard Disk • Network • USB Storage
List of UEFI Boot Options	N/A	Enter in specified Boot Device.

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.

All other trademarks are the property of their respective owners. © 2024 Lenovo

Lenovo