Lenovo

ThinkEdge Server V2 with Intel Xeon D UEFI Manual

Server Models: SE350 V2, SE360 V2

Second Edition (November 2023)

Contents

Chapter 1. UEFI Overview

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

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

- SE350 V2
- SE360 V2

The following table details the main menu:

Table 1. Main menu

Item	Options	Description
Chapter 3 "System configuration and boot management" **on page 5**	N/A	Main menu
Select Language		Selects the display language.
Launch Graphical System Setup	N/A	Starts the graphical user interface for system setup, provisioning manager, and RAID configuration. There is no screen output to console in Graphical System Setup. Use VGA monitor for Graphical System Setup.
"System Information" **on page 5**	N/A	Displays basic details of the system.
"System Settings" **on page 6**	N/A	Displays or modifies system settings. Changes might not take effect immediately. Save changes and reboot the system.
"Date and Time" **on page 47**	N/A	Sets date and time of the system.
"Start Options" **on page 48**	N/A	Boots a desired selection from the primary boot sequence in the Boot Manager menu.
"Boot Manager" **on page 48**	N/A	Changes boot order, boot parameters, and boot from a file.
"BMC Settings" **on page 52**	N/A	Configures Baseboard Management Controller (BMC).
"System Event Logs" **on page 55**	N/A	Clears or views the system event log.

Table 1. Main menu (continued)

Item	Options	Description
“User Security” **on page 56**	N/A	Sets or changes Power-On and Administrator passwords.
Save Settings	N/A	Saves changed settings.
Discard Settings	N/A	Discards changes.
Load Default Settings	N/A	Loads default values for system settings.
Exit Setup Utility	N/A	Exits Setup.

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 system setup utility.

System Information

This menu displays the system information.

Table 2. System Information

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

System Summary

Table 3. System Summary

Item	Format	Description
System Identification Data		
Machine Type/Model	ASCII string of 10 or 8 characters	Displays System Machine Type and Model.
Serial Number	ASCII string of 10 or 8 characters	Displays tag for Serial Number.
UUID Number	16-byte Hexadecimal String of 32 characters	Displays tag for UUID.
Asset Tag Number	ASCII string of 32 characters	Displays Asset Tag Number.
Processor		
Installed CPU packages	ASCII string of 1 character	Displays number of Installed CPU packages.
Processor Speed	y.yyy **GHz**	Displays Processor Speed.
Memory		
Memory Speed	yyyy **MHz**	Displays speed of the installed memory.
Total Usable Memory Capacity	yyyy **GB**	Displays amount of the usable memory capacity minus the overhead required by mirroring mode, reserved capacity, bad blocks and other factors.

Product Data

Table 4. Product Data

Item	Format	Description
Host Firmware		
Build ID	ASCII string of 7 characters	Displays build ID of the host firmware.
Version	String format: **1.xx**	Displays version of the host firmware.
Build Date	Character string format: MM/DD/YYYY	Displays build date of the host firmware.
BMC Firmware		
Build ID	ASCII string	Displays build ID of the Baseboard Management Controller (BMC) firmware.
Version	ASCII string	Displays version of the BMC firmware.
Build Date	Character string format: MM/DD/YYYY	Displays build date of the BMC firmware.

Open Source License

This page lists open-source software acknowledgements and required copyright notices.

System Settings

This menu displays the system settings.

Table 5. System Settings

Item	Options	Description
<F1> Start Control	• **Auto** (Default) • Tool Suite • Text Setup	Controls the tools that are started using the F1 key or equivalent IPMI command. • [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” on page 7	N/A	Displays onboard devices and I/O port options.
“Driver Health” on page 13	N/A	Displays health status of the drivers.
“Foreign Devices” on page 14	N/A	Displays a list of foreign devices.
“Legacy BIOS” on page 15	N/A	Sets UEFI firmware execution environment preferences for supporting legacy OS and legacy Option ROM.
“Memory” on page 15	N/A	Displays and modifies options to change the memory settings.

Table 5. System Settings (continued)

Item	Options	Description
“Network” on page 17	N/A	Display network devices and network related settings.
“Operating Modes” on page 26	N/A	Selects operating mode based on the preference. **Note:** Power savings and performance are also highly dependent on hardware configuration and the software running on the system.
“Power” on page 29	N/A	Configures power plan options.
“Processors” on page 31	N/A	Displays and modifies options to change the processor settings.
“Recovery and RAS” on page 39	N/A	Configures recovery policies and advanced reliability, availability, and serviceability settings.
“Security” on page 41	N/A	Configures system security settings.
“Storage” on page 45	N/A	Manages storage adapter options. Some systems may use planar devices and can be configured in the Devices and I/O Ports menu.

Devices and I/O Ports

Table 6. Devices and I/O Ports

Item	Options	Description
Onboard SATA Mode	• **AHCI** (Default) • RAID	Configures SATA as AHCI or RAID.
Active Video	• **Onboard Device** (Default) • Add-in Device	This feature is available only when the server has an add-in video adapter. When option ROM is set to [Legacy] for both onboard and add-in video adapters, the setting controls which single adapter displays the System Setup utility. Regardless of this setting, the system boot early video is displayed at the onboard video only, and the management controller remote console shows the onboard video only. This setting does not affect how the operating system (OS) displays its graphical desktop.
PCI 64-Bit Resource Allocation	• Enabled • Disabled • **Auto** (Default)	Enables or disables allocation of 64-bit resources for PCI devices. [Auto]: Allocates some resources below 4GB for legacy compatibility.
SRIOV	• **Enabled** (Default) • Disabled	Enables or disables support of resource allocation for Single Root I/O Virtualization (SR-IOV) virtual functions during system boot.
Intel® VT for Direct I/O (VT-d)	• **Enabled** (Default) • Disabled	Enables or disables Intel® Virtualization Technology for Directed I/O (VT-d) by reporting the I/O device assignment to VMM (Virtual Machine Monitor) through DMAR (DMA Remapping) ACPI (Advance Configuration Power Interface) tables.

Table 6. Devices and I/O Ports (continued)

Item	Options	Description
DMA Control Opt-In Flag	• Enabled • **Disabled** (Default)	Enables or disables DMA_CTRL_PLATFORM_OPT_IN_ FLAG in DMAR ACPI table. This feature is not compatible with Direct Device Assignment (DDA). **Note:** This feature is grayed out when VT-d is set to [Disabled].
"Enable/Disable Onboard Device (s)" **on page 8**	N/A	Enables or disables onboard devices or slots.
"Enable/Disable Adapter Option ROM Support" **on page 9**	N/A	Controls Legacy and UEFI-compliant adapter support. Disabling UEFI/Legacy support may adversely affect pre-boot/boot functions.
"Set Option ROM Execution Order" **on page 10**	N/A	Sets load order for Legacy Option ROMs.
"PCIe Gen Speed Selection" **on page 10**	N/A	Chooses generation speed for available PCIe slots.
"Override Slot Bifurcation" **on page 10**	N/A	Overrides bifurcation of the physical x16 slot to support the adapter with multiple devices.
"Console Redirection Settings" **on page 11**	N/A	Configures console redirection and COM port settings.
"USB Configuration" **on page 12**	N/A	Enables or disables USB storage devices or individual ports.
"Intel® VMD technology" **on page 13**	N/A	Enables or disables Intel® Volume Management Device (VMD) Technology.

Note: Most of the features in Devices and I/O Ports are platform dependent.

Enable/Disable Onboard Device(s)

Table 7. Enable/Disable Onboard Device(s)

Item	Options	Description
Onboard Video	• Disabled • **Enabled** (Default)	Disabling an entry prevents the associated device from being enumerated during the subsequent boot.
Onboard SATA (for ODD)	• Disabled • **Enabled** (Default)	Disabling an entry prevents the associated device from being enumerated during the subsequent boot.
Onboard LAN	• **Enabled** (Default) • Disabled	Disabling an entry prevents the associated device from being enumerated during the subsequent boot.
M.2 (for M.2 SATA mode.)	• **Enabled** (Default) • Disabled	Disabling an entry prevents the associated device from being enumerated during the subsequent boot.

Table 7. Enable/Disable Onboard Device(s) (continued)

Item	Options	Description
Slot (n...) ("n" varies with the riser card which is installed.)	• Disabled • **Enabled** (Default) or • Disabled • **Enabled**(Default) • Auto	Disabling an entry prevents the associated device from being enumerated during the subsequent boot. [Auto] removes the port if there is no device or error on the device.
NVMe Bay (n...)	• Disabled • **Enabled** (Default) or • Disabled • **Enabled**(Default) • Auto	Disabling an entry prevents the associated device from being enumerated during the subsequent boot. [Auto] removes the port if there is no device or error on the device.

Enable/Disable Adapter Option ROM Support

Table 8. Enable/Disable Adapter Option ROM Support

Item	Options	Description
Network	• Do not launch • **UEFI** (Default) • Legacy	Controls the execution of UEFI and Legacy Network OpROM. [Legacy] will not appear when legacy BIOS is disabled.
Storage	• Do not launch • **UEFI** (Default) • Legacy	Controls the execution of UEFI and Legacy Storage OpROM. [Legacy] will not appear when legacy BIOS is disabled.
Video	• Do not launch • **UEFI** (Default) • Legacy	Controls the execution of UEFI and Legacy Video OpROM. [Legacy] will not appear when legacy BIOS is disabled.
Other PCI devices	• Do not launch • **UEFI** (Default) • Legacy	Determines OpROM execution policy for devices other than Network, Storage, or Video. [Legacy] will not appear when legacy BIOS is disabled.

Set Option ROM Execution Order

Table 9. Set Option ROM Execution Order

Item	Options	Description
Set Option ROM Execution Order	• Onboard Video • Onboard SATA • Slot 1 • Slot 2 • Slot (n...) • Onboard LAN Port 1 • Onboard LAN (n...) • NVMe Bay 0 • NVMe Bay n	Selects load order for legacy PCI option ROM(s). Press **+** to execute the selected devices ROM sooner or press **-** to execute later. **Notes:** • The order may be overridden for devices controlled by UEFI thunk drivers. • [Onboard LAN Port (n...)] varies depending on whether PHY card is installed or not. • [Slot (n...)] varies depending on which riser card is installed.

PCIe Gen Speed Selection

Note: SR250 V3, ST50 V3 and ST250 V3 do not support some functions in this section.

Table 10. PCIe Gen Speed Selection

Item	Options	Description
Slot 1 (appears depending on which riser card is installed)	• **Auto** (Default) • Gen1 • Gen2 • Gen3 • Gen4	Sets the maximum speed supported by individual PCIe slot.
Slot 2 (appears depending on which riser card is installed)	• **Auto** (Default) • Gen1 • Gen2 • Gen3 • Gen4	Sets the maximum speed supported by individual PCIe slot.
Slot (n...) ("n" varies with the riser card which is installed.)	• **Auto** (Default) • Gen1 • Gen2 • Gen3 • Gen4	Sets the maximum speed supported by individual PCIe slot.
NVMe (n...) ("n" varies with the riser card which is installed.)	• **Auto** (Default) • Gen1 • Gen2 • Gen3 • Gen4	Sets the maximum speed supported by individual PCIe slot. **Note:** This function is only applicable for SR250 V3, ST50 V3 and ST250 V3.

Override Slot Bifurcation

Note: SR250 V3, ST50 V3 and ST250 V3 do not support this function.

This page allows you to override the bifurcation settings.

Console Redirection Settings

Table 11. Console Redirection Settings

Item	Options	Description
COM Port 1	• **Enabled** (Default) • Disabled	Enables or disables COM 1 device. When [Disabled] is selected, the associated COM 1 terminal settings are hidden.
Virtual COM Port 2	• **Enabled** (Default) • Disabled	Enables or disables Virtual COM Port 2 device. When [Disabled] is selected, SSH connection is disabled.
Console Redirection	• Enabled • Disabled • **Auto** (Default)	Sets remote console redirection preference to enable or disable console redirection. When [Auto] is selected, Console Redirection is enabled automatically if IPMI Serial over LAN status is active.
Serial Port Sharing	• Enabled • **Disabled** (Default)	Enables system BMC to allow access to the system serial port. When [Enabled] is selected, BMC is allowed to control the serial communication port as requested by remote control commands. When [Disabled] is selected, the serial port is assigned to BMC unless Serial Port Access Mode is set to [Disabled].
Serial Port Access Mode	• Shared • Dedicated • **Disabled** (Default)	Controls access to the system BMC over the system serial port. • [Shared]: Serial port is available for both of POST and operating system. However, BMC can monitor the serial data for a takeover control sequence. • [Dedicated]: BMC has complete control of the serial port for POST and/or OS use. • [Disabled]: BMC has no access to the serial port.
SP Redirection	• Enabled • **Disabled** (Default)	Serial Over LAN (SOL) or SSH redirection enables a system administrator to use BMC as a serial terminal server. It allows you to choose which mode to have the redirection. When [Disabled] is selected, it is configured with SOL. A server serial port can be accessed from SSH connection (Virtual COM 2) when SP Redirection is set to [Enabled]. **Note:** This feature appears only when Console Redirection is set to [Enabled].
Legacy OS/Option ROM Display	• Virtual COM Port 2 • **COM Port 1** (Default)	Selects a COM port to display the redirection of Legacy OS and Legacy OPROM (Option ROM) Messages.

Table 11. Console Redirection Settings (continued)

Item	Options	Description
COM Port Active After Boot	• Enabled • **Disabled** (Default)	When [Disabled] is selected, Legacy Console Redirection is disabled before booting to legacy OS. When [Enabled] is selected, Legacy Console Redirection is enabled for legacy OS.
COM1 Settings		
COM1 Baud Rate	• **115200** (Default) • 57600 • 38400 • 19200 • 9600	Controls connection speed between the host and the remote system.
COM1 Data Bits	• **8** (Default) • 7	Sets number of data bits in each character.
COM1 Parity	• **None** (Default) • Odd • Even	Sets the parity bit in each character to be [None], [Odd], or [Even]. [None] means that no parity bit is transmitted.
COM1 Stop Bits	• 2 • **1** (Default)	Sets Stop Bits. Stop Bits which follow at the end of each character allow the signal receiver to detect the end of a character and to resynchronize with the character stream.
COM1 Terminal Emulation	• VT100 • VT100Plus • VT-UTF8 • **ANSI** (Default)	Select [VT100] only if the remote emulator does not support ANSI text graphics. **Note:** If needed, change the character encoding setting in the remote emulator to ensure the characters show correctly.
COM1 Flow Control	• **Disabled** (Default) • Hardware	Select [Hardware] only if the remote emulator supports and is using hardware flow control.

USB Configuration

Table 12. USB Configuration

Item	Options	Description
USB Mass Storage Driver Support	• **Enabled** (Default) • Disabled	Enables or disables USB Mass Storage Driver Support. This feature only takes effect during the POST process.
USB Front Port 1	• **Enabled** (Default) • Disabled	Enables or disables USB individual ports.

Table 12. USB Configuration (continued)

Item	Options	Description
USB Front Port 2	• **Enabled** (Default) • Disabled	Enables or disables USB individual ports.
USB Rear Port 3	• **Enabled** (Default) • Disabled	Enables or disables USB individual ports.

Intel® VMD technology

Table 13. Intel® VMD Technology

Item	Options	Description
Enable/Disable Intel® VMD	• Enabled • **Disabled** (Default)	Enables or disables Intel® VMD (Volume Management Device) Technology.
Enable VMD Only on Boot Drives	• Enabled • **Disabled** (Default)	Enable this setting for certain application which requires to enable VMD on boot drive and leave other drives excluding from VMD controller. **Note:** This feature appears only when Enable/Disable Intel® VMD is set to [Enabled].

Driver Health

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

Table 14. Driver Health

Item	Options	Description
The platform is:	• **Healthy** • Repair Required • Configuration Required • Operation Failed • Reconnect Required • Reboot Required • Shutdown Required • No Operation Required	Displays health statuses of the drivers.
Driver/Controller Status		

Table 14. Driver Health (continued)

Item	Options	Description
Controller Name - Status	• **Healthy** • Repair Required • Configuration Required • Operation Failed • Reconnect Required • Reboot Required • Shutdown Required • No Operation Required	Displays health status of the controller.
POST Attempts Driver	• **Healthy** • Repair Required • Configuration Required • Operation Failed • Reconnect Required • Reboot Required • Shutdown Required • No Operation Required	Displays health status of the POST Attempts Driver.
Partition Driver (MBR/GPT/El Torito)	• **Healthy** • Repair Required • Configuration Required • Operation Failed • Reconnect Required • Reboot Required • Shutdown Required • No Operation Required	Displays health status of the Partition Driver.

Foreign Devices

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

Table 15. Foreign Devices

Item	Description
Unclassified devices:	Displays unclassified device.
Video devices:	Displays video devices.
Input devices:	Displays input devices.
Onboard devices:	Displays onboard devices.
Other devices:	Displays other devices.

Legacy BIOS

Table 16. Legacy BIOS

Item	Options	Description
Legacy BIOS	• **Enabled** (Default) • Disabled	Enables or disables UEFI firmware execution environment for supporting legacy OS and legacy Option ROM.
Rehook INT 19h	• Enabled • **Disabled** (Default)	[Enabled] prevents devices from taking control of the boot process.
Non-Onboard PXE	• **Enabled** (Default) • Disabled	Enables or disables legacy PXE boot for the installed network adapters.
Legacy BIOS is disabled due to secure boot is enabled. **Note:** This feature appears only when the Secure Boot is enabled.		

Memory

This menu offers options to change the memory settings.

Table 17. Memory

Item	Options	Description
"System Memory Details" on page 17	N/A	Displays status of the system memory.
Total Usable Memory Capacity	yyyy **GB**	Displays Total Usable Memory Capacity.

Table 17. Memory (continued)

Item	Options	Description
Memory Speed	• Minimal Power • Balanced • **Max Performance** (Default)	Selects the desired memory speed. [Maximum Performance] maximizes performance. [Balanced] offers a balance between performance and power. [Minimal power] maximizes power savings. 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**.
Memory Power Management	• Automatic • **Disabled** (Default)	[Disabled] maximizes performance and minimizes power savings. [Automatic] is suitable for most applications. 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**.
Socket Interleave	• **NUMA** (Default) • Non-NUMA	Sets Socket Interleave to NUMA(Non Unified Memory Architecture) or Non-NUMA. [NUMA] means that memory is not interleaved across processors. [Non-NUMA] means that memory is interleaved across processors. **Note:** Setting change requires a Power Good reset to take effect.
Patrol Scrub	• **Enabled** (Default) • Disabled	Enables or disables Patrol Scrub which proactively searches the system memory to repair correctable errors. When [Enabled] is selected, Patrol Scrub takes effect at the end of POST.
Memory Data Scrambling	• **Enabled** (Default) • Disabled	Enables or disables Memory Data Scrambling.
ADDDC Sparing	• Disabled • **Enabled** (Default)	Enables or disables ADDDC Sparing. ADDDC Sparing is not supported when the server has x8 DIMM, 9x4 value DIMM or memory is set to [Mirror mode] (Full or Partial).
Page Policy	• **Adaptive** (Default) • Closed	[Adaptive] can improve performance for applications with a highly localized memory access pattern. [Closed] can benefit applications that access memory more randomly.

Table 17. Memory (continued)

Item	Options	Description
Cold Boot Fast	• **Enabled** (Default) • Disabled	Enables or disables Cold Boot Fast.
AC Boot Fast	• Enabled • **Disabled** (Default)	Enables or disables AC Boot Fast which is for AC boot only.
Memory Test	• Disabled • **Enabled** (Default)	Enables or disables Memory Test during normal boot.
2x Refresh Rate	• **Disabled** (Default) • Auto	[Disabled] sets the system with 1x refresh rate. [Auto] sets the system with 2x refresh rate if it is supported by the system. Setting it to [Auto] can mitigate Rowhammer issue, but that might have a performance impact. 2x refresh rate is not supported by system that has 16Gb 3DS with 4 Die DIMM.

System Memory Details

System Memory Details

Table 18. System Memory Details

Item	Description
DIMM Details For Processor X	Displays DIMM status.

DIMM Details

If a double bit error (DBE) occurs on the DIMM, the [Enabled] and [Disabled] options will be available. For current generation, [Enabled] is the default setting.

Network

This menu displays the network devices and network-related settings.

Note: The information and title of on-board or add-on card will show the title of the card, MAC address or PFA.

Table 19. Network

Item	Description
Global Network Settings	
“iSCSI Settings” on page 18	Configures iSCSI parameters.
“Network Stack Settings” on page 22	Specifies network stack settings.
“Network Boot Settings” on page 23	Configures network boot parameters.
“HTTP Boot Configuration” on page 24	Configures HTTP Boot parameters.

Table 19. Network (continued)

Item	Description
"Tls Auth Configuration" on page 25	You can press **Enter** to select Tls Auth Configuration.
Network Device	

iSCSI Settings

Table 20. Host iSCSI Configuration

Item	Description
iSCSI Initiator Name	Displays the worldwide unique name of iSCSI Initiator. Only the IQN format which contains a maximum of 223 characters.
"Add an attempt" on page 18	Adds an attempt.
List of Attempts Selecting any item in the list will lead to "Attempt Settings" on page 19	MAC: XX:XX:XX:XX:XX:XX, PFA: Bus XX | Dev XX | Func XX, "iSCSI Mode": [%s1], "Internet Protocol": [%s2] **Notes:** • 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" on page 22	Deletes one or more attempts.
"Change Attempt Order" on page 22	You can change attempt order by using **+/-** keys, and use arrow keys to select an attempt and press **+/-** to move the attempt up/down in the attempt order list.

Add an attempt

Table 21. MAC Selection

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

Attempt Settings

Table 22. Attempt Settings

Item	Options	Description
iSCSI Attempt Name	N/A	Defines the name for this attempt. The maximum length is up to 96 characters.
iSCSI Mode	• **Disabled** (Default) • Enabled • Enable for MPIO	Enables or disables iSCSI mode, or enables iSCSI mode for MPIO. **Note:** Make sure all necessary items (e.g. initiator IP, target IP and authentication settings) are set appropriately before you enable this feature. Otherwise, this attempt may be lost after reboot.
Internet Protocol	• **IPv4** (Default) • IPv6 • Autoconfigure	[IPv6]: Initiator IP address is assigned by the system. [Autoconfigure]: iSCSI driver attempts to connect iSCSI target via IPv4 stack. If it fails, it will attempt to connect via IPv6 stack.
Connection Retry Count	0	The minimum value is 0 and the maximum value is 16. 0 means that you do not want to retry.
Connection Establishing Timeout	1000	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 is 6 bytes. The default values is derived from MAC address. Only the last 3 bytes are configurable. These values are taken from Configure ISID control.
Configure ISID	e. g., C68EF8	OUI-format ISID is 6 bytes, the default values is derived from MAC address. Only the last 3 bytes are configurable. Example: Update 0ABBCCDDEEFF to 0ABBCCF07901 by inputting F07901.
Enable DHCP	• **Empty** (Default) • X	Enables DHCP.
Initiator IP Address	0.0.0.0	Sets initiator IP address in dotted-decimal notation. **Note:** This feature appears only when Enable DHCP is not enabled.

Table 22. Attempt Settings (continued)

Item	Options	Description
Initiator Subnet Mask	0.0.0.0	Sets initiator subnet mask IP address in dotted-decimal notation. **Note:** This feature appears only when Enable DHCP is not enabled.
Gateway	0.0.0.0	Sets initiator gateway IP address in dotted-decimal notation. **Note:** This feature appears only when Enable DHCP is not enabled.
Initiator IP: 0.0.0.0	N/A	**Note:** This feature appears only when Enable DHCP is enabled.
Get target info via DHCP	• **Empty** (Default) • X	Gets target info via DHCP. **Note:** This feature appears only when Enable DHCP is enabled.
Target Name	N/A	Indicates the worldwide unique name of the target. Only IQN format is accepted. **Note:** This feature does not appear when Get target info via DHCP is enabled.
Target IP Address	0.0.0.0	Sets target IP address in dotted-decimal notation. **Note:** This feature does not appear when Get target info via DHCP is enabled.
Target Port	3260	Target Port **Note:** This feature does not appear when Get target info via DHCP is enabled.
Boot LUN	0	Sets hexadecimal representation of the LUN number. Examples: 4751-3A4F-6b7e-2F99, 6734-9-156f-127, 4186-9 **Note:** This feature does not appear when Get target info via DHCP is enabled.
Authentication Type	• CHAP • **None** (Default)	Defines authentication type.
CHAP Type	• One way • **Mutual** (Default)	Sets CHAP type. **Note:** This feature appears only when Authentication Type is set to [CHAP].

Table 22. Attempt Settings (continued)

Item	Options	Description
CHAP Name	N/A	Sets CHAP Name. **Note:** This feature appears only when Authentication Type is set to [CHAP].
CHAP Secret	N/A	The CHAP secret length must be between 12 and 16 bytes. **Note:** This feature appears only when Authentication Type is set to [CHAP].
CHAP Status	• **Not Installed** (Default) • Installed	[Not Installed]: CHAP Name and CHAP Secret are not set. [Installed]: CHAP Name and CHAP Secret are set. **Note:** This feature appears only when Authentication Type is set to [CHAP].
Reverse CHAP Name	N/A	Reverses CHAP Name. **Note:** This feature appears only when CHAP Type is set to [Mutual].
Reverse CHAP Secret	N/A	The reverse CHAP secret length must be between 12 and 16 bytes. **Note:** This feature appears only when CHAP Type is set to [Mutual].
Reverse CHAP Status	• **Not Installed** (Default) • Installed	[Not Installed]: Reverse CHAP Name and Reverse CHAP Secret are not set. [Installed]: Reverse CHAP Name and Reverse CHAP Secret are set. **Note:** This feature appears only when CHAP Type is set to [Mutual].
Save Changes	N/A	Rebooting the system manually is required for changes to take effect.
Back to Previous Page	N/A	Goes back to the previous page.

Delete Attempts

Table 23. Delete Attempts

Item	Options	Description
List of Attempts e.g., Attempt 1	• **Empty** (Default) • X	You can check the option to delete the attempt. The values of each attempt will be displayed as follows: MAC: XX:XX:XX:XX:XX:XX, PFA: Bus XX | Dev XX | Func XX, “iSCSI Mode”: [%s1], “Internet Protocol”: [%s2] Exact value are different depending on the attempt settings. • %s1: the option name for iSCSI Mode. • %s2: the setting name for Internet Protocol.
Commit Changes and Exit	N/A	Saves changes and exits.
Discard Changes and Exit	N/A	Discards changes and exits.

Change Attempt Order

Table 24. Change Attempt Order

Item	Options	Description
Change Attempt Order **Note:** Existing attempts are listed here.	• e.g. • Attempt 1 • Attempt 2	You can use **+/-** keys to change attempt order, and 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	Saves changes and exits.
Discard Changes and Exit	N/A	Discards changes and exits.

Network Stack Settings

Table 25. Network Stack Settings

Item	Options	Description
Network Stack	• **Enabled** (Default) • Disabled	Enables or disables UEFI Network Stack.
IPv4 PXE Support	• **Enabled** (Default) • Disabled	Enables or disables IPv4 PXE Boot Support. If this feature is disabled, IPv4 PXE boot option will not be created.
IPv4 HTTP Support	• Enabled • **Disabled** (Default)	Enables or disables IPv4 HTTP Boot Support. If this feature is disabled, IPv4 HTTP boot option will not be created.
IPv6 PXE Support	• **Enabled** (Default) • Disabled	Enables or disables IPv6 PXE Boot Support. If this feature is disabled, IPv6 PXE boot option will not be created.

Table 25. Network Stack Settings (continued)

Item	Options	Description
IPv6 HTTP Support	• Enabled • **Disabled** (Default)	Enables or disables IPv6 HTTP Boot Support. If this feature is disabled, IPv6 HTTP boot option will not be created.
PXE boot wait time	**0**	You can use either **+/-** or numeric keys to set a specific wait time before you can press **Esc** to abort the PXE boot.
Media detect count	**1**	You can use either **+/-** or numeric keys to set the number of times to detect media.

Network Boot Settings

Network Boot Settings

Table 26. Network Boot Settings

Item	Description
MAC:XX:XX:XX:XX:XX:XX SlotXXX PFA XXXX:XX:XX.X or **MAC:XX:XX:XX:XX:XX:XX SlotXXX PFA XX:X:X**	Sets boot configuration parameters on MAC XX:XX:XX:XX:XX:XX PCI Function Address: XXXX:XX:XX.X or Sets boot configuration parameters on MAC XX:XX:XX:XX:XX:XX PCI Function Address: Bus XX:Dev XX:Func: XX
VLAN Configuration List: VLAN Configuration (MAC: XXXXXXXXXXXX)	VLAN Configuration: (MAC:XXXXXXXXXXXX)
IPv4 Configuration List: MAC:XXXXXXXXXXXX-IPv4 Network Configuration	Configures network parameters. (MAC:XXXXXXXXXXXX)
IPv6 Configuration List: MAC:XXXXXXXXXXXX-IPv6 Network Configuration	Configures IPv6 network parameters. (MAC:XXXXXXXXXXXX)

MAC: Onboard PFA 1:0:0

Table 27. MAC: Onboard PFA 1:0:0

Item	Options	Description
UEFI PXE Mode	• **Enabled** (Default) • Disabled	Enables or disables NIC to include or skip boot attempt during generic PXE Network boot. For Legacy mode, enable or disable Option ROM in the Devices and I/O Ports menu. Network Driver in “Network Device List” may also require configuration. System Boot Mode may further impact PXE.
Legacy PXE Mode	• **Enabled** (Default) • Disabled	Enables or disables NIC to include or skip boot attempt during generic PXE Network boot. For Legacy mode, enable or disable Option ROM from Devices and I/O Ports menu. Network Driver in “Network Device List” may also require configuration. System Boot Mode may further impact PXE.

HTTP Boot Configuration

Note: SR250 V3, ST50 V3 and ST250 V3 do not support this function.

HTTP Boot Configuration

Notes:

- When you enable **Network** -> **Network Stack Setting** -> **IPv4 HTTP Support** or **IPv6 HTTP support**, **HTTP Boot Configuration** is 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.

Table 28. HTTP Boot Configuration

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

MAC:xxxxxxxxxxxx-HTTP Boot Configuration

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.

Table 29. MAC:xxxxxxxxxxxx-HTTP Boot Configuration

Item	Options	Description
Input the description	N/A	Default value is UEFI HTTP.
Internet Protocol	• IPv4 • IPv6	Selects version of the Internet Protocol.
Boot URI	N/A	A new Boot Option will be created according to the Boot URI.

Tls Auth Configuration

Note: SR250 V3, ST50 V3 and ST250 V3 do not support this function.

Note: When you enable **Network** -> **Network Stack Setting** -> **IPv4 HTTP Support** or **IPv6 HTTP support**, **Tls Auth Configuration** is displayed in Network page.

Table 30. Tls Auth Configuration

Item	Description
"Server CA Configuration" on page 25	You can press **Enter** to configure Server CA.
Client Cert Configuration	Client Cert configuration is unsupported currently.

Server CA Configuration

Table 31. Server CA Configuration

Item	Description
"Enroll Cert" on page 25	You can press **Enter** to enroll cert.
"Delete Cert" on page 25	You can press **Enter** to delete cert.

Enroll Cert

Table 32. Enroll Cert

Item	Description
Enroll Cert Using File	Enrolls Cert Using File.
Cert GUID	You can enter Cert GUID in the following format: 11111111-2222-3333-4444-1234567890ab.
Commit Changes and Exit	Saves changes and exits.
Discard Changes and Exit	Discards changes and exits.

Delete Cert

Table 33. Delete Cert

Item	Options	Description
xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx	• **Empty** • X	GUID for Cert. **Note:** If there's no cert file, the default value is [Empty].

Operating Modes

Select the operating mode based on your preference.

Table 34. Operating Modes

Item	Options	Description
Choose Operating Mode	• Minimal Power • Efficiency – Favor Power • **Efficiency – Favor Performance** (Default) • Custom Mode • Maximum Performance	You can select the operating mode based on your preference. Power savings and performance are heavily dependent on the hardware and the software running on the system.
Acoustic Mode	• **Disabled** (Default) • Mode 1 • Mode 2	Acoustic modes reduce system acoustics by limiting fan speeds. [Mode 2] attempts to reduce acoustics more aggressively than [Mode 1]. When the acoustic mode is set to Disabled, no system fan speed limits are applied. Throttling may momentarily occur when the acoustic mode is set to Mode 1 or Mode 2. To maintain system operation during fan failures, high ambient temperatures or component over temperature conditions, acoustic mode fan limits will be overridden to ensure adequate system airflow. For the high ambient temperature threshold for a specific system, refer to the system documentation.
Memory Speed	• Minimal Power • Balanced • **Max Performance** (Default)	You can select the desired memory speed. [Maximum performance] maximizes the performance. [Balanced] offers a balance between performance and power. [Minimal power] maximizes power savings. 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**.

Table 34. Operating Modes (continued)

Item	Options	Description
CPU P-state Control	• None • Legacy • **Autonomous** (Default) • Cooperative without Legacy • Cooperative with Legacy	You can select to control CPU P-states (performance states). [None]: Disables all P-states and processors work either at rated frequency or in Turbo Mode (if Turbo Mode is enabled). [Legacy]: CPU P-states will be presented to the OS and the OS power management (OSPM) will directly control which P-state is selected. [Autonomous]: P-states are fully controlled by system hardware. No P-state support is required in the OS or VM. [Cooperative] is a combination of [Legacy] and [Autonomous]. P-states are still controlled by hardware but the OS can provide hints to the hardware for P-state limits, indicating the desired setting. 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**.
C1 Enhanced Mode	• **Enabled** (Default) • Disabled	[Enabled]: Saves power by halting processor cores that are idle. Using this feature requires an operating system that supports C1E state. Changes take effect after the system rebooted. 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** > **C-States** > **[Legacy]/[Disabled]** . **Note:** C1E status is changeable only when C-states is not set to [Autonomous].
Turbo Mode	• **Enabled** (Default) • Disabled	[Enabled] improves the overall processor performance when all processor cores are not being fully utilized. A processor core can run above its rated frequency for a short period of time when it is in turbo mode. When a preset mode is selected, the low-level settings are not changeable and will be grayed out. To change the settings, choose **System Settings** > **Operating Modes** > **Choose Operating Mode** > **Custom Mode**.

Table 34. Operating Modes (continued)

Item	Options	Description
UPI Link Disable	• **Enabled All Links** (Default) • Disabled 1 Link	Disabling one of the UPI links can save power. To achieve optimal performance, all UPI links should be enabled. 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**. **Note:** UPI is available only when two or more processors are installed.
UPI Link Frequency	• Minimal Power • Balanced • **Maximum Performance** (Default)	You can select the desired UPI link frequency. [Maximum performance] maximizes the performance. [Balanced] offers a balance between performance and power. [Minimal power] maximizes power savings. 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**. **Note:** UPI is available only when two or more processors are installed.
Energy Efficient Turbo	• **Enabled** (Default) • Disabled	[Enabled]: The optimal turbo frequency of processors can be adjusted dynamically based on processor utilization. This feature is also influenced by **Power/Performance Bias**. 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** > **Turbo Mode** > **[Enabled]**
C-States	• **Legacy** (Default) • Disabled	C-states reduces power consumption during the idle time. [Legacy]: The operating system initiates the C-state transitions. For E5/E7 processors, ACPI C1/C2/C3 map to Intel C1/C3/C6. For 6500/7500 processors, ACPI C1/C3 map to Intel C1/C3 (ACPI C2 is not available). Some OS may defeat the ACPI mapping (e.g., Intel idle driver). 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**.

Table 34. Operating Modes (continued)

Item	Options	Description
Power/Performance Bias	• **Platform Controlled** (Default) • OS Controlled	Power/Performance Bias determines how the power management of the processor is controlled. [Platform Controlled]: The system controls the setting. [OS Controlled]: The operating system controls the setting. Not all operating systems support this feature. 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**.
Platform Controlled Type	• Maximum Performance • **Efficiency - Favor Performance** (Default) • Efficiency - Favor Power • Minimal Power	[Maximum Performance] allows the most aggressive use of turbo and power management functions are disabled, thereby increasing power consumption. Turbo mode can be engaged opportunistically before it is requested and uncore power management features (Memory, UPI, C-state demotion, I/O bandwidth limit and UFS) are aggressively disabled [Minimal Power] disables turbo and maximizes the use of power management features. 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**.
Page Policy	• **Adaptive** (Default) • Closed	[Adaptive] improves the performance of applications with a highly localized memory access pattern. [Closed] benefits applications that access memory more randomly.
MONITOR/MWAIT	• **Enabled** (Default) • Disabled	MONITOR/MWAIT instructions are used to engage C-states. Some operating systems re-enable C-states even when they are disabled in setup. To prevent this, do the following: 1. Disable MONNITOR/MWAIT. 2. a. Choose **System Settings** > **Operating Modes** > **Choose Operating Mode** > **Custom Mode**. b. Choose **System Settings** > **C-States** > **Disabled**.

Power

This menu allows you to configure power scheme options.

Table 35. Power

Item	Options	Description
Power/Performance Bias	• **Platform Controlled** (Default) • OS Controlled	Power/Performance Bias determines how the power management of the processor is controlled. [Platform Controlled]: The system controls the setting. [OS Controlled]: The operating system controls the setting. Not all operating systems support this feature. 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**.
Platform Controlled Type	• Maximum Performance • **Efficiency - Favor Performance** (Default) • Efficiency - Favor Power • Minimal Power	[Maximum Performance] allows the most aggressive use of turbo and power management functions are disabled, thereby increasing power consumption. [Minimal Power] disables turbo and maximizes the use of power management features. When a preset mode is selected, the low-level settings are not changeable and will be grayed out. To change the settings, choose **System Settings** > **Operating Modes** > **Choose Operating Mode** > **Custom Mode**.
Workload Configuration	• **Balanced** (Default) • I/O sensitive	[I/O sensitive] is recommended for expansion cards that require the high bandwidth I/O when the processor cores are idle to allow enough frequency for the workload.
ACPI Fixed Power Button	• **Enabled** (Default) • Disabled	Enables or disables ACPI Fixed Power Button. When [Disabled] is selected, pressing the power button on front of the system does not execute the power button policy in operating system, 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.
PCIe Power Brake	• Reactive • **Proactive** (Default) • Disabled	PCIe Power Brake quickly reduces the power consumption and performance of high-power 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. **Note:** This feature is platform dependent.
ASPM	• **Auto** (Default) • Disabled	[Auto] enables ASPM on PCIe endpoint adapters that support it. [Disabled] disables ASPM for all PCIe endpoints. **Note:** This feature is platform dependent.

Processors

This menu offers options to change the processor settings.

Table 36. Processors

Item	Options	Description
"Processor Details" on page 36	N/A	Displays summary of the installed processors.
Turbo Mode	• **Enabled** (Default) • Disabled	[Enabled] improves the overall processor performance when all processor cores are not being fully utilized. A processor core can run above its rated frequency for a short period of time when it is in turbo mode. When a preset mode is selected, the low-level settings are not changeable and will be grayed out. To change the settings, choose **System Settings** > **Operating Modes** > **Choose Operating Mode** > **Custom Mode**. **Note:** This feature only appears when supported by processor.
CPU P-state Control	• None • Legacy • **Autonomous** (Default) • Cooperative without Legacy • Cooperative with Legacy	You can select to controls CPU P-states (performance states). [None]: Disables all P-states and processors work either at rated frequency or in Turbo Mode (if Turbo Mode is enabled). [Legacy]: CPU P-states will be presented to the OS. The OS power management (OSPM) controls which P-state is selected. [Autonomous]: The P-states are fully controlled by system hardware. No P-state support is required in the OS or VM. [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. 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**.
C-States	• **Legacy** (Default) • Disabled	C-states reduces power consumption during the idle time. [Legacy]: The operating system initiates the C-state transitions. For E5/E7 processors, ACPI C1/C2/C3 map to Intel C1/C3/C6. For 6500/7500 processors, ACPI C1/C3 map to Intel C1/C3 (ACPI C2 is not available). Some OS may defeat the ACPI mapping (e.g., Intel idle driver).

Table 36. Processors (continued)

Item	Options	Description
C1 Enhanced Mode	• **Enabled** (Default) • Disabled	[Enabled]: Saves power by halting processor cores that are idle. Using this feature requires an operating system supporting C1E state. Changes take effect after the system rebooted. 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** > **C-States** > **[Legacy]/[Disabled]** . **Note:** C1E status is changeable only when C-states is not set to [Autonomous].
Hyper-Threading	• **Enabled** (Default) • Disabled	Enables or disables logical processor cores on processors **Notes:** • Changing this setting requires a Power Good reset to take effect. • This feature only appears when supported by processor.
Trusted Execution Technology	• Enabled • **Disabled** (Default)	Enables or disables Intel® Trusted Execution Technology (Intel® TXT).
Intel Virtualization Technology	• **Enabled** (Default) • Disabled	Enables or disables Intel® Virtualization Technology.
Hardware Prefetcher	• **Enabled** (Default) • Disabled	Lightly-threaded applications and some benchmarks can take advantage of this feature when it is enabled.
Adjacent Cache Prefetch	• **Enabled** (Default) • Disabled	Lightly-threaded applications and some benchmarks can take advantage of this feature when it is enabled.
DCU Streamer Prefetcher	• **Enabled** (Default) • Disabled	Lightly-threaded applications and some benchmarks can take advantage of this feature when it is enabled.
DCU IP Prefetcher	• **Enabled** (Default) • Disabled	It is recommended that the Data Cache Unit (DCU) IP Prefetcher is set to [Enabled] for the most environments. However, some environments may benefit from having it set to [Disabled], e.g. Java.
Energy Efficient Turbo	• **Enabled** (Default) • Disabled	[Enabled]: The optimal turbo frequency of processors can be adjusted dynamically based on processor utilization. This feature is also influenced by Power/Performance Bias. 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** > **Turbo Mode** > **[Enabled]**

Table 36. Processors (continued)

Item	Options	Description
Uncore Frequency Scaling	• **Enabled** (Default) • Disabled	When [Enabled] is selected, the processor uncore (all miscellaneous logic inside the processor package) dynamically changes the speed based on the workload.
MONITOR/MWAIT	• **Enabled** (Default) • Disabled	MONITOR/MWAIT instructions are used to engage C-states. Some operating systems re-enable C-states even when they are disabled in setup. To prevent this, do the following: 1. Disable MONNITOR/MWAIT. 2. a. Choose **System Settings** > **Operating Modes** > **Choose Operating Mode** > **Custom Mode**. b. Choose **System Settings** > **C-States** > **Disabled**.
Limit CPU PA to 46 bits	• **Enabled** (Default) • Disabled	Limit CPU physical address to 46 bits to support older Hyper-v.
Total Memory Encryption	• **Disabled** (Default) • Enabled	Enables or disables Total Memory Encryption (TME).
Multikey Total Memory Encryption	• **Disabled** (Default) • Enabled	Enables or disables Multikey Total Memory Encryption (MK-TME). **Note:** This feature appears only when Total Memory Encryption is set to [Enabled].
Max MKTME Keys	0x0 **Note:** when MKTME is enabled, this value will change with system configuration. (Information only, not editable)	Displays Max MKTME (Multi-Key Total Memory Encryption) Keys.
SGX Factory Reset	• **Disabled** (Default) • Enabled	Enables or disables SGX Factory Reset. When [Enabled] is selected, it erases all registration data on subsequent boot, and additionally forces an Initial Platform Establishment flow when SGX is enabled. **Notes:** This feature appears only when the system supports NUMA or TME. In addition, before enabling this option, do the following: 1. Enable Total Memory Encryption. 2. Disable Patrol Scrub and Mirror Mode before enabling SGX.

Table 36. Processors (continued)

Item	Options	Description
SW Guard Extensions	• **Disabled** (Default) • Enabled	Enables or disables Software Guard Extensions (SGX). **Notes:** This feature appears only when the system supports NUMA or TME. In addition, before enabling this option, do the following: 1. Enable Total Memory Encryption. 2. Disable Patrol Scrub and Mirror Mode before enabling SGX.
SGX Package Info In-Band Access	• **Disabled** (Default) • Enabled	Enables or disables Software Guard Extensions (SGX) Package Info In-Band Access. **Notes:** This feature appears only when the system supports NUMA or TME. In addition, before enabling this option, do the following: 1. Enable Total Memory Encryption. 2. Disable Patrol Scrub and Mirror Mode before enabling SGX.
PRMRR Size	• 1G • **2G** (Default) • 4G • 8G • 16G • 32G • 128G **Note:** The default value and option changes with different system memory configurations.	Setting the PRMRR Size. **Note:** This feature will be grayed out if SW Guard Extensions is set to [Disabled].
Snoop Preference	• **Home Snoop Plus** (Default) • Home Snoop	You can select the appropriate snoop mode based on the workload. Setting the snoop mode preference does not always guarantee that it will be selected. The mode will be changed if the current hardware configuration does not support the desired mode
LLC Prefectch	• Disabled • **Enabled**(Default)	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.
PECI Is Trusted	• Disabled • **Enabled**(Default)	Enables/disables trust for the system's PECI interface. **[Disable]** (PECI not trusted) can be used for a higher level of security but some functions such as memory and I/O utilization reporting may not work.

Table 36. Processors (continued)

Item	Options	Description
Cores in CPU Package	• **All** (Default) • 1 • . • . • . • n-1	Selects number of cores enabled within each CPU package. The number "n" is the maximum core count supported by the installed processor.
"CPU Frequency Limits" on page 36	• **Full turbo uplift** (Default) • Restrict maximum frequency	The maximum frequency (turbo, AVX, and non turbo) can be restricted to a frequency that is between the maximum turbo frequency for the installed processor and 1.2GHz. The max frequency for N+1 cores can not be higher than N cores. If an unsupported frequency is entered, it will automatically be limited to a supported value. If the CPU Frequency Limits are being controlled through application software, leave this feature at the default [Full turbo uplift] and change the settings by choosing **System Settings** > **Operating Modes** > **Choose Operating Mode** > **Custom Mode** > **Turbo Mode** > **Enabled**. **Notes:** • This feature appears only when Turbo Mode is enabled. • This sub-menu item appears only when CPU Frequency Limits is set to [Restrict maximum frequency].
TCC Mode	• **Disabled** (Default) • Enabled	TCC mode will automatically change low-level settings including power management parameters. Experimentation in customer pre-production environment is recommended. The TCC affected UEFI settings will not roll back to <default> when TCC Mode toggles from enable to disable. **Note:** If CPU doesn't support this feature, it will be grayed out.
Software SRAM	• **Disabled** (Default) • Enabled	Enable or Disable Software SRAM. Enable will allocate 1 way of LLC; if Cache Configuration subregion is available, it will allocate based on the subregion. **Note:** If CPU doesn't support this feature, it will be grayed out.
Data Streams Optimizer	• **Disabled** (Default) • Enabled	Enable or Disable Data Streams Optimizer (DSO). Enable will utilize DSO Subregion to tune system. DSO settings supercede Intel(R) TCC Mode settings that overlap between the two. **Note:** If CPU doesn't support this feature, it will be greyed out.

Table 36. Processors (continued)

Item	Options	Description
Intel(R) TCC Authentication	• Disabled • **OEM Enrolled Key**(Default) • Non-OEM Enrolled Key	Intel(R) TCC Authentication determines the key to be used. • OEM Enrolled Key is built in by OEM. • Non-OEM Enrolled Key can be add by user. **Note:** If CPU doesn't support this feature, it will be greyed out.
"Non-OEM Intel(R) TCC AuthKey Menu" **on page 37**	N/A	Non-OEM Intel(R) Time Coordinated Computing AuthKey Menu Options. **Note:** This submenu is only available when " Intel(R) TCC Authentication " set to [Non-OEM Enrolled Key].
"Intel(R) TCC Mode Affected Settings" **on page 38**	N/A	Intel(R) TCC Mode Affected Settings. **Note:** If CPU doesn't support this feature, it will be grayed out.

Processor Details

Table 37. Processor Details

Item	Format	Description
Processor ID	ASCII string	Displays tag for the processor ID.
Processor Frequency	ASCII string	Displays value for the processor frequency.
Processor Revision	ASCII string	Displays value for the microcode revision.
L1 Cache RAM	ASCII string	Displays amount of L1 Cache RAM.
L2 Cache RAM	ASCII string	Displays amount of L2 Cache RAM.
L3 Cache RAM	ASCII string	Displays 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 Version	ASCII string	Displays version of processor 1.
Processor n Version	ASCII string	Displays version of processor n.

CPU Frequency Limits

Note: SR250 V3, ST50 V3 and ST250 V3 do not support this function.

Table 38. CPU Frequency Limits

Item	Options	Description
CPU Frequency Limits		
Processors X to X cores active **Note:** This feature is dynamic text, depending on the current processor state.	• **Max turbo frequency bin** (Default) • Max turbo frequency –1 bins • Max turbo frequency –2 bins • ... • Base frequency +1 bins	The maximum frequency (turbo, AVX, and non turbo) can be restricted to a frequency that is between the maximum turbo frequency for the installed processor and 1.2GHz. The max frequency for N+1 cores can not be higher than N cores. If an unsupported frequency is entered, it will automatically be limited to a supported value. If the CPU Frequency Limits are being controlled through application software, leave this feature at the default [Full turbo uplift].

Non-OEM Intel(R) TCC AuthKey Menu

Table 39. Non-OEM Intel(R) TCC AuthKey Menu

Item	Options	Description
“Enroll AuthKey Menu” **on page 39**	N/A	Enroll Authkey options
“Delete Authkey Menu” **on page 39**	N/A	Delete Authkey options

Intel(R) TCC Mode Affected Settings

Table 40. Intel(R) TCC Mode Affected Settings

Item	Options	Description
Enable Monitor MWAIT	ASCII string	Allows Monitor and MWAIT instructions.
CPU P-state Control	ASCII string	You can select to controls CPU P-states (performance states). [None]: Disables all P-states and processors work either at rated frequency or in Turbo Mode (if Turbo Mode is enabled). [Legacy]: CPU P-states will be presented to the OS. The OS power management (OSPM) controls which P-state is selected. [Autonomous]: The P-states are fully controlled by system hardware. No P-state support is required in the OS or VM. [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. 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**.
Hardware P-states	ASCII string	[Disable]: Hardware chooses a P-state based on OS Request (Legacy P-States)\n [Native Mode]: Hardware chooses a P-state based on OS guidance\n [Out of Band Mode]: Hardware autonomously chooses a P-state (no OS guidance)
SpeedStep (Pstates)	ASCII string	Enable/Disable EIST (P-States)
Hyper-Threading [ALL]	ASCII string	Enables Hyper Threading (Software Method to Enable/ Disable Logical Processor threads.
Page Policy	ASCII string	Select Page Policy
DRAM RAPL	ASCII string	Enable\Disable DRAM Rapl
DRAM RAPL Extended Range	ASCII string	Select DRAM RAPL Extended Range
CKE Throttling	ASCII string	Configures CKE Throttling
APD	ASCII string	APD On/Off
PPD	ASCII string	PPD On/Off
PCI-E ASPM Support (Global)	ASCII string	This option can disable ASPM support in all PCIe root ports.
PCI-E ASPM Support	ASCII string	This option can disable ASPM support in PCIe root ports.
Rlink ASPM Enable	ASCII string	Enable L1 ASPM for Rlink

Table 40. Intel(R) TCC Mode Affected Settings (continued)

Item	Options	Description
Legacy IO Low Latency	ASCII string	Set to enable low latency of legacy IO.
PCI Express Root Port 1 - 12	N/A	PCI Express Root Port 1 - 12
ASPM	ASCII string	PCI Express Active State Power Management settings.
L1 Substates	ASCII string	PCI Express L1 Substates settings.
PTM	ASCII string	Enable/Disable Precision Time Measurement
Multi Virtual Channel	ASCII string	Enable/Disable Multi Virtual Channel

Enroll AuthKey Menu

Table 41. Enroll Authkey Menu

Item	Options	Description
Enroll Authkey from file	N/A	Read the hash of public key from file.
Signature GUID		Input digit character in 11111111-2222-3333-4444-1234567890ab format.
Commit Changes and Exit	N/A	Commit Changes and Exit
Discard Changes and Exit	N/A	Discard Changes and Exit

Delete Authkey Menu

Table 42. Delete Authkey Menu

Item	Options	Description
Commit Changes and Exit	N/A	Commit Changes and Exit
Discard Changes and Exit	N/A	Discard Changes and Exit

Recovery and RAS

Note: SR250 V3, ST50 V3 and ST250 V3 do not support some functions in this section.

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

Table 43. Recovery and RAS

Item	Description
“POST Attempts” on page 40	Configures number of attempts to POST before the recovery mechanisms is invoked.
“Advanced RAS” on page 40	Chooses whether to enable various advanced RAS options or not.

Table 43. Recovery and RAS (continued)

Item	Description
"Disk GPT Recovery" on page 40	Displays Disk GPT (GUID Partition Table) Recovery Options.
"System Recovery" on page 41	Configures system recovery settings.

POST Attempts

Note: SR250 V3, ST50 V3 and ST250 V3 do not support this function.

Table 44. POST Attempts

Item	Options	Description
Post Attempt Limit	• Disabled • 9 • 6 • **3** (Default)	Configures number of attempts to POST before the recovery mechanism is invoked. When the number of consecutive failed POST attempts reaches the limit, the system will reboot with the factory default settings.

Advanced RAS

Note: SR250 V3, ST50 V3 and ST250 V3 do not support this function.

Table 45. Advanced RAS

Item	Options	Description
Machine Check Recovery	• **Enabled** (Default) • Disabled	Allows the software layer (OS, VMM, DBMS, Application) to enable recovery from uncorrectable hardware errors.
PCI Error Recovery	• **Enabled**(Default) • Disabled	When [Enabled] is selected, it allows the system to recover from an uncorrectable PCIe error. The corresponding PCIe device will be disabled to prevent the error from damaging the system, and the operating system will rescan the PCIe buses. When [Disabled] is selected, an uncorrectable PCIe error results in an NMI.

Disk GPT Recovery

Note: SR250 V3, ST50 V3 and ST250 V3 do not support this function.

Table 46. Disk GPT Recovery

Item	Options	Description
Disk GPT Recovery	• Automatic • **Manual** (Default) • None	[Automatic]: UEFI recovers corrupt GUID Partition Table (GPT) automatically. [Manual]: UEFI recovers corrupt GPT based on the input in a dialog box. [None]: UEFI does not recover corrupt GPT. Check system event log for the recovery result.

System Recovery

Table 47. System Recovery

Item	Options	Description
POST Watchdog Timer	• Enabled • **Disabled** (Default)	Enables or disables POST Watchdog Timer.
POST Watchdog Timer Value	[5]	Sets POST Watchdog Timer Value in minutes in the specified range (5-20).
Reboot System On NMI	• **Enabled** (Default) • Disabled	Enables or disables system reboot with non-maskable interrupt (NMI).

Security

This menu allows you to configure system security settings.

Table 48. Security

Item	Description
"Secure Boot Configuration" on page 41	Configures secure boot options.
"Trusted Platform Module (TPM1.2) or (TPM2.0)" on page 43	Configures TPM setup options.

Secure Boot Configuration

Table 49. Secure Boot Configuration

Item	Options	Description
Secure Boot Status	• Disabled • Enabled	Checks Secure Boot Status.
Secure Boot Mode	• Setup Mode • User Mode • Audit Mode • Deploy Mode	System performs secure boot authentication when this feature is set to [User Mode] and secure boot is enabled.
Secure Boot Setting	• Enabled • **Disabled** (Default)	Secure Boot feature is Active when this feature is set to [Enabled], Platform Key (PK) is enrolled, and the system is in user mode. To change the mode, resetting the platform is required. **Note:** A warning will appear when you attempt to enable secure boot while CSM is enabled. WARNING: Legacy BIOS will be disabled when secure boot is enabled.

Table 49. Secure Boot Configuration (continued)

Item	Options	Description
Secure Boot Policy	• **Factory Policy** (Default) • Custom Policy • Delete All Keys • Delete PK • Reset All Keys to Default	Secure Boot policy options: [Factory Policy]: Factory default keys will be used after reboot. [Custom Policy]: Customized keys will be used after reboot. [Delete All Keys]: PK (Platform Key), KEK (Key Exchange Key), DB (Authorized Signature Database), and DBX (Forbidden Signature Database) will be deleted after reboot. [Delete PK]: PK will be deleted after reboot. After the PK is deleted, Secure Boot Mode will be in [Setup Mode], and Secure Boot Policy will be in [Custom Policy]. [Reset All Keys to Default]: All keys will be set to factory defaults and Secure Boot Policy will be set to [Factory Policy] after reboot.
"View Secure Boot Keys" on page 42	N/A	Views the details of PK, KEK, DB, and DBX.
"Secure Boot Custom Policy" on page 43	N/A	Customizes PK, KEK, DB, and DBX. **Note:** This feature appears only when Secure Boot Policy is set to [Custom Policy].

View Secure Boot Keys

Table 50. View Secure Boot Keys

Item	Description
Secure Boot variable	Displays PK (Platform Keys), KEK (Key Exchange Keys), DB (Authorized Signature Database), and DBX (Forbidden Signature Database).
Size	Displays number of key bytes.
Keys	Displays number of certificates.
Key Source	Displays certificate sources. The sources can be **Factory Default**, **No Keys**, **Mixed**, or **Customized**.
PK	Displays Certificate in PK. **Note:** There is only one PK in the system.
KEK	Displays all Certificates in KEK.
DB	Displays all Certificates in DB.
DBX	Displays all Certificates in DBX.

Secure Boot Custom Policy

Table 51. Secure Boot Custom Policy

Item	Description
Enroll Efi Image	Enrolls SHA256 hash of the selected EFI image binary into the DB (Authorized Signature Database).
Secure Boot variable	Displays PK (Platform Keys), KEK (Key Exchange Keys), DB (Authorized Signature Database), and DBX (Forbidden Signature Database).
Size	Displays number of key bytes.
Keys	Displays number of certificates.
Key Source	Displays certificate sources. The sources can be **Factory Default**, **No Keys**, **Mixed**, or **Customized**.
PK	Enrolls the PK or delete the existing PK. **Note:** There is only one PK in the system.
KEK	Enrolls a KEK entry or delete the existing entry from the KEK.
DB	Enrolls a DB entry or delete the existing entry from the DB.
DBX	Enrolls a DBX entry or delete the existing entry from the DBX.

Trusted Platform Module (TPM1.2) or (TPM2.0)

For updating the TPM firmware from 2.0 to 1.2:

Table 52. Trusted Platform Module

Item	Description
TPM 2.0	Configures TPM 2.0 Setup options.
TPM Versoin	
Update to TPM1.2 compliant	**CAUTION:** **Change will be effective after the system reboots. You can only switch TPM firmware 128 times.**

For TPM 2.0 firmware:

Table 53. Trusted Platform Module (TPM2.0)

Item	Options	Description
TPM Status		
TPM Vendor		
TPM Firmware Version		
[TPM Settings]		

Table 53. Trusted Platform Module (TPM2.0) (continued)

Item	Options	Description
TPM2 Operation	• **No Action** (Default) • Clear • TPM Device has been cleared.	**Attention:** This will erase the contents of the TPM. System reboot is required. You can select [Clear] to clear TPM data.
SHA-1 PCR Bank	• Enabled • **Disabled**(Default)	Enables or disables SHA-1 PCR Bank.
Hide TPM from OS	• Yes • **No**(Default)	Hide TPM from OS, TPM device object will not be present in the ACPI namespace.

For upgrading the TPM firmware from 1.2 to 2.0:

Table 54. Trusted Platform Module

Item	Description
TPM 1.2	Configures TPM 1.2 Setup options.
TPM Version	
Update to TPM2.0 compliant	**Attention:** When updating the TPM version to TPM2.0 compliant, do not boot a legacy OS due to security consideration. Change will be effective after the system reboots. You can only switch TPM firmware 128 times

For updating the TPM 2.0 firmware:

Table 55. Trusted Platform Module (TPM 2.0)

Item	Options	Description
TPM Status		
TPM Vendor		
TPM Firmware Version		
TPM Device Sate		
TPM Ownership		
[TPM Settings]		
TPM Device	• **Enabled** (Default) • Disabled	Enables or disables TPM Device.

Table 55. Trusted Platform Module (TPM 2.0) (continued)

Item	Options	Description
TPM State	• **Activate** (Default) • Deactivate	Activates or deactivates TPM State.
TPM Operation	• **No Action** (Default) • Clear • TPM1.2 Device has been cleared	**Attention:** This will erase the contents of the TPM. System reboot is required. You can select [Clear] to clear TPM data.

For TPM 1.2 firmware:

Note: This page appears only when the system supports TPM 1.2 firmware.

Table 56. Trusted Platform Module (TPM 1.2)

Item	Options	Description
TPM Status		
TPM Vendor		
TPM Firmware Version		
TPM Device Sate		
TPM Ownership		
[TPM Settings]		
TPM Device	• **Enabled** (Default) • Disabled	Enables or disables TPM Device.
TPM State	• **Activate** (Default) • Deactivate	Activates or deactivates TPM State.
TPM Operation	• **No Action** (Default) • Clear • TPM1.2 Device has been cleared	**Attention:** This will erase the contents of the TPM. System reboot is required. You can select [Clear] to clear TPM data.

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**.

Table 57. Storage

Item	Description
"NVMe" on page 46	Displays NVMe device list.
Intel® Virtual RAID on CPU	Allows to manage Intel® Virtual RAID on CPU.
"RAM Disk Configuration" on page 47	Press <Enter> to add/remove RAM disks.

NVMe

Table 58. NVMe

Item	Description
Bay X: NVMe Bus-Dev-Fun (X is bay number)	Bus-Dev-Fun is PCI address value.

Table 59. NVMe Detail Information

Item	Format	Description
Model Name	ASCII string	Displays Model Name.
Serial Number	ASCII string	Displays Serial Number.
Firmware Revision	ASCII string	Displays Firmware Revision.
Vendor ID	0xXXXX (XXX is hex number)	Displays Vendor ID.
Device ID	0xXXXX (XXX is hex number)	Displays Device ID.
Subsystem Vendor ID	0xXXXX (XXX is hex number)	Displays Subsystem Vendor ID.
Subsystem ID	0xXXXX (XXX is hex number)	Displays Subsystem ID.
Maximum Link Speed	Gen N (N is number)	Displays Maximum Link Speed.
Maximum Link Width	xN (N is number)	Displays Maximum Link Width.
Negotiated Link Speed	Gen N (N is number)	Displays Negotiated Link Speed.
Negotiated Link Width	xN (N is number)	Displays Negotiated Link Width.
Number of Namespaces	N (N is number)	Displays Number of Namespaces.

Table 59. NVMe Detail Information (continued)

Item	Format	Description
Total Size	X.XX TB (Unit can be GB or MB, depending on the size)	Displays total size.
Device driver data link:		
Device HII Title	N/A	Displays description of device HII.

RAM Disk Configuration

Table 60. RAM Disk Configuration

Item	Options	Description
Disk Memory Type	• **Boot Service Data** (Default) • Reserved	Specifies type of the memory to use from available memory pool in the system to create a disk.
"Create Raw" **on page 47**	N/A	Creates a raw RAM disk.
Create from file	N/A	Creates a RAM disk from a given file.
Created RAM disk list		
Remove selected RAM disk(s)	N/A	Removes the selected RAM disk(s).

Create Raw

Table 61. Create Raw

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

Date and Time

This menu allows you to set the local date and time of the system.

Table 62. Date and Time

Item	Format	Description
System Date	MM/DD/YYYY	You can use the **+/-** or the numeric keys to set the date of the server.
System Time	HH:MM:SS	You can use the **+/-** or the numeric keys to set the time of the server.

Start Options

This menu allows you to boot as desired from the primary boot sequence.

Table 63. Start Options

Item	Description
CD/DVD Rom	Device Path: VenHw(B2AD3248-4F72-4950-A966-CFE5062DB83A,02000000)
Hard Disk	Device Path: VenHw(B2AD3248-4F72-4950-A966-CFE5062DB83A,01000000)
Network	Device Path: VenHw(B2AD3248-4F72-4950-A966-CFE5062DB83A,05000000)
USB Storage	Device Path: VenHw(B2AD3248-4F72-4950-A966-CFE5062DB83A,04000000)

Boot Manager

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

Table 64. Boot Manager

Item	Options	Description
Boot Sequence		
“Add Generic Boot Option” on page 49	N/A	Adds one generic boot device as the boot option.
“Add UEFI Full Path Boot Option” on page 49	N/A	Adds one EFI application or one removable file system as the boot option.
“Delete Boot Option” on page 49	N/A	Removes boot option(s) from the boot order.
“Change Boot Order” on page 50	N/A	Modifies ordering of selections within the Boot Order.
“Set Boot Priority” on page 50	N/A	Sets boot priority of the devices in a device group.
Other Boot Functions		
“Boot From File” on page 51	Xxxx {xxxx-xxx-xxx…}	Boots the system from a specific file or a device.
“Select Next One-Time Boot Option” on page 51	N/A	Selects one-time boot option for the next boot.

Table 64. Boot Manager (continued)

Item	Options	Description
System		
“Boot Modes” **on page 51**	N/A	Changes between the UEFI boot mode and the legacy boot mode.
“Reboot System” **on page 52**	N/A	Reboots the system. If **<Y>** is pressed, any setup changes will be lost and the system will reboot.

Add Generic Boot Option

Use this page to add one generic boot device as boot option.

Add UEFI Full Path Boot Option

Table 65. Add UEFI Full Path Boot Option

Item	Options	Description
Boot option File Path	N/A	Specifies file path for the boot option.
Input the Description	N/A	Specifies name for the new boot option.
Select Device Path Option	Xxxx {xxxx-xxx-xxx…}	Selects device path option.
Commit Changes and Exit	N/A	Saves changes and exits.

Delete Boot Option

Table 66. Delete Boot Option

Item	Options	Description
CD/DVD Rom	[X]	Device Path: VenHw(B2AD3248-4F72-4950-A966-CFE5062DB83A,02000000)
Hard Disk	[X]	Device Path: VenHw(B2AD3248-4F72-4950-A966-CFE5062DB83A,01000000)
Network	[X]	Device Path: VenHw(B2AD3248-4F72-4950-A966-CFE5062DB83A,05000000)
USB Storage	[X]	Device Path: VenHw(B2AD3248-4F72-4950-A966-CFE5062DB83A,04000000)
Commit Changes and Exit	N/A	Saves changes and exits.

Note: The options may change according to your system configuration.

Change Boot Order

Table 67. Change Boot Order

Item	Options	Description
Change the Order	• CD/DVD Rom • Hard Disk • Network • USB Storage	Changes boot order.
Commit Changes and Exit	N/A	Saves changes and exits.

Set Boot Priority

Table 68. Set Boot Priority

Item	Description
“CD/DVD Priority” on page 50	Sets boot priority for CD/DVD if multiple devices exist in the system.
“Hard Disk Priority” on page 50	Sets boot priority for Hard Disk if multiple devices exist in the system.
“Network Priority” on page 50	Sets boot priority for Network if multiple devices exist in the system.
“USB Priority” on page 51	Sets boot priority for USB if multiple devices exist in the system.

CD/DVD Priority

Table 69. CD/DVD Priority

Item	Description
Boot Priority	Changes boot priority for the CD/DVD devices.
Commit Changes and Exit	Saves changes and exits.

Hard Disk Priority

Table 70. Hard Disk Priority

Item	Description
Boot Priority	Changes boot priority for the hard disk devices.
Commit Changes and Exit	Saves changes and exits.

Network Priority

Table 71. Network Priority

Item	Description
Boot Priority	Changes boot priority for the network devices.
Commit Changes and Exit	Saves changes and exits.

USB Priority

Table 72. USB Priority

Item	Description
Boot Priority	Changes the boot priority for the USB devices.
Commit Changes and Exit	Saves changes and exits.

Boot From File

Use this page to boot the system from a specific file or device..

Select Next One-Time Boot Option

Use this page to select the one-time boot option for the next boot.

Table 73. Select Next One-Time Boot Option

Item	Options	Description
Boot Option	• CD/DVD Rom • Hard Disk • Network • USB Storage • System Setup • **NONE** (Default)	Selects one-time boot option for the next boot.

Boot Modes

Table 74. Boot Modes

Item	Options	Description
System Boot Mode	• **UEFI Mode** (Default) • Legacy Mode	Drivers, option ROMs and OS loaders the Boot Manager attempts to boot. [UEFI Mode] runs UEFI drivers and boot the OS in UEFI Mode. [Legacy Mode] runs option ROMs and boot the OS in Legacy Mode. **Note:** This feature is set to [UEFI Mode] when Legacy BIOS is disabled.
Infinite Boot Retry	• Enabled • **Disabled** (Default)	The system continuously attempts the Boot Order. Make sure that a bootable device is specified in Boot Order.
Prevent OS Changes To Boot Order	• Enabled • **Disabled** (Default)	When [Enabled] is selected, UEFI removes the boot option which is created by OS or OS Installer from the boot order list.

Reboot System

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

BMC Settings

This menu allows you to configure the management controller.

Note: All settings under BMC page are unable to reset to default with **Load Default Settings**. Use **Reset Factory Defaults Setting** to reset to default setting in this page.

Table 75. BMC Settings

Item	Options	Description
Power Restore Policy	• Always Off • Restore • Always On	Determines operation mode after a power loss. [Always Off]: The system remains off even when power is restored. [Restore]: The system returns to the state before power was lost. [Always On]: The system turns on when power is restored. **Note:** This feature is platform dependent. This feature is unable to reset to default value by using the load default in Setup.
Power Restore Random Delay	• Enabled • Disabled	Provides a random delay of 1 to 15 seconds for Power On. If the server status is on before a power failure occurs, the power-on will be delayed once power is restored. **Note:** This feature is platform dependent. This feature is unable to reset to default value by using the load default in Setup. This feature does not appear when Power Restore Policy is set to [Always Off].
Ethernet over USB interface	• Enabled • Disabled	[Enabled] makes the xClarity Essentials in-band update utility available. [Disabled] prevents xClarity Essentials and other applications running on the server from requesting the BMC to perform tasks.
“Network Settings” **on page 53**	N/A	Configures network of the management controller.
Reset Factory Defaults Setting	N/A	Restores all management controller settings to factory defaults, including network configuration and credentials. The management controller will be restarted automatically.

Table 75. BMC Settings (continued)

Item	Options	Description
Restart BMC	N/A	Restarts the BMC.

Network Settings

Attention: Clicking “Save Network Settings” at the bottom of this page is required to save changes on this page and subpage.

Table 76. Network Settings

Item	Options	Description
Network Interface Port	• Dedicated • Shared	Selects System Management Network Interface Port.
Shared NIC on	OCP Card	Selects shared NIC port. **Note:** This feature is platform dependent and appears only when Network Interface Port is set to [Shared].
Fail-Over Rule	• None • Failover to shared (Optional Card ML2) • Failover to shared (Optional Card PHY) • Failover to shared (Onboard Port)	Controls fail-over types allowed. **Note:** This feature is platform dependent and appears only when Network Interface Port is set to [Dedicated].
Network Setting	• Synchronization • Independence	The feature is selectable only when Fail-Over Rule is enabled to onboard port or optional card.
Burned-in MAC Address	N/A	Displays MAC addresses from the network interface controller.
Hostname	N/A	Changes host name. The length must be within 1 to 63 characters.
DHCP Control	• Static IP • DHCP Enabled • DHCP with Fallback	Configures DHCP Control or configure a staic IP address manually. Fallback uses static IP address if DHCP fails. Select [Static IP] to enter IPV4 address manually.
IP Address	x.x.x.x	Enters IP Address in dotted-decimal notation.
Subnet Mask	x.x.x.x	Enters Subnet Mask in dotted-decimal notation.
Default Gateway	x.x.x.x	Enters Default Gateway in dotted-decimal notation.

Table 76. Network Settings (continued)

Item	Options	Description
IPv6	• Enabled • Disabled	Enables or disables IPv6 support on management port. **Note:** This feature is platform dependent. This feature is unable to reset to default value by using the load default in Setup.
Local Link Address	N/A	Displays local link address.
VLAN Support	• Enabled • Disabled	Enables or disables VLAN Support to specify the 802.1q VLAN ID on the management port network device. **Note:** This feature is platform dependent. This feature is unable to reset to default value by using the load default in Setup.
VLAN ID	1	VLAN ID Range is 1 to 4094. **Note:** This feature appears only when VLAN Support is enabled.
"Advanced Settings for BMC Ethernet" **on page 54**	N/A	Provides advanced settings for BMC Ethernet.
Save Network Settings	N/A	Saves changes in BMC.

Advanced Settings for BMC Ethernet

Table 77. Advanced Settings for BMC Ethernet

Item	Options	Description
Autonegotiation	• No • Yes	[No]: You can choose the Data rate and Duplex mode. [Yes]: Manual configuration is not needed. **Notes:** • This feature is platform dependent. • This feature is unable to reset to default value by using the load default in Setup.
Data rate	When **Autonegotiation** is set to [Yes]: **Auto** When **Autonegotiation** is set to [No]: • 100 Mb (Ethernet) • 10 Mb (Ethernet)	Configures amount of data to be transferred per second over LAN connection. **Notes:** • This feature is platform dependent. • This feature appears only when Autonegotiation is set to [No]. • This feature is unable to reset to default value by using the load default in Setup.

Table 77. Advanced Settings for BMC Ethernet (continued)

Item	Options	Description
Duplex	When **Autonegotiation** is set to [Yes]: **Auto** When **Autonegotiation** is set to [No]: • Half • Full	Sets type of communication channel used in the network. [Full] allows the data to be transferred in both directions simultaneously. [Half] allows the data to be transferred in one direction at a time. **Notes:** • This feature is platform dependent. • This feature appears only when Autonegotiation is set to [No]. • This feature is unable to reset to default value by using the load default in Setup.
Maximum Transmission Unit	1500	Specifies the maximum size of a packet (in bytes) for the network interface. For IPv4 networks, the MTU range is from 68-1500 bytes For IPv6 networks, the MTU range is from 1280-1500 bytes.
Note: Changes will be affective after saving network settings in the previous page.		

System Event Logs

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

Table 78. System Event Logs

Item	Description
"POST Event Viewer" on page 55	Displays POST Event Viewer.
"System Event Log" on page 56	Displays System Event Log.
Clear System Event Log	Clears System Event Log.

POST Event Viewer

Table 79. POST Event Viewer

Item	Description
Entry [N]:	Information.

System Event Log

Table 80. System Event Log

Item	Description
Total SEL entries	Displays total number of the system event logs (SEL) retrieved from the BMC. Associated extended logs are not included.
Previous Page	Displays system event logs in the previous page.
Entry [N]:	Information.
Next Page	Displays system event logs in the next page.

User Security

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

Table 81. User security

Item	Description
"Password Rule and Policy" on page 57	Sets password rule and policy.
Set Power-On Password	Sets Power-On Password. The password can only contain the following characters (excluding white-space characters): A-Z, a-z, 0-9, ~`!@#$%^&*()-+={}[]|:;"'<>,?/._ Must contain at least one letter. Must contain at least one number. Must contain at least 2 of the following: • At least one upper-case letter • At least one lower-case letter • At least one special character No more than 2 consecutive occurrences of the same character Must be at least *x* characters set in Minimum password length, or 8 characters if Minimum password length is not set.
Clear Power-On Password	Clears Power-On password.

Table 81. User security (continued)

Item	Description
Set Administrator Password	Sets Administrator Password. The password can only contain the following characters (excluding white-space characters): A-Z, a-z, 0-9, ~`!@#$%^&*()-+={}[]|:;"'<>,?/._ Must contain at least one letter. Must contain at least one number. Must contain at least 2 of the following: • At least one upper-case letter • At least one lower-case letter • At least one special character No more than 2 consecutive occurrences of the same character Must be at least *x* characters set in Minimum password length, or 8 characters if Minimum password length is not set.
Clear Administrator Password	Clears Administrator password.

Password Rule and Policy

Table 82. Password Rule and Policy

Item	Options	Function
Minimum password length	8-20	You can set a value between 8 and 20. This value indicates the minimum number of characters, which is part of the rules to specify a valid password. Changes take effect right after the value is set. Click “Save Setting” on Main Menu if you would like to keep the setting after the system reboot.
Password expiration period	0-365	You can set passwords to expire after a number of days between 0 and 365, or you can specify that passwords never expire by setting the value to 0.
Password expiration warning period	0-365	You can set a number of days between 0 and 365 before a password expiration to receive a password expiration warning. If you set the value to 0, there is no password expiration warning.
Minimum password change interval	0-240	You can set a value between 0 and 240. This feature allows you to set the minimum interval (in hours) at which users can change the passwords. The value specified for this feature can not exceed the value specified for Password expiration period. If you set the value to 0, users can change the password immediately.

Table 82. Password Rule and Policy (continued)

Item	Options	Function
Minimum password reuse cycle	0-10	You can set a value between 0 and 10. This feature allows you to determine the number of unique new passwords that must be set before an old password can be reused. If you set the value to 0, an old password can be reused immediately. Changes take effect right after the value is set. Click "Save Setting" on Main Menu if you would like to keep the setting after the system reboot.
Maximum number of login failures	0-100	You can set a value between 0 and 100. This feature allows you to set a maximum number of times users attempt to login with an incorrect password before user account is locked out. The lockout duration depends on the value of the Lockout period after maximum login failures. If you set the value to 0, the account will never be locked out.
Lockout period after maximum login failures	0-2880	You can set a value between 0 and 2880. This feature allows you to set the number of minutes to lock out an account when the maximum number of failed login attempts is reached. The account is locked even the correct password is entered during the lockout period. If you set the value to 0, the account will never be locked out even the number of Lockout period after maximum login failures is exceeded.

F12 One Time Boot Device

Table 83. Boot Devices Manager

Item	Options	Description
Legacy Mode	• [ ] • [X]	Overrides System Boot Mode in the Boot Mode menu. Setting Option ROM Execution Order in the Devices and I/O Ports menu may still affect the boot ordering. It is needed to have PCI 64-Bit Resource Allocation in the Device and I/O Ports menu set to [Disabled] for some network cards' legacy PXE boot option. **Notes:** When selecting this feature, the page is refreshed to show legacy group: • CD/DVD Rom • Hard Disk • Network • USB Storage
List of UEFI Boot Options	N/A	The list of UEFI Boot Options are displayed here and will be changed according to the system configurations.

Appendix A. Notices

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

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

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

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

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

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

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

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

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

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

Trademarks

LENOVO and LENOVO logo are trademarks of Lenovo.