Lenovo

UEFI Manual for Lenovo ThinkEdge Server with Intel Core Ultra Series 2 Processors

Server Models: SE100

First Edition (May 2025)

Contents

Contents i

Chapter 1. UEFI Introduction 1

Chapter 2. Get Started 3

Chapter 3. UEFI Setup Utility Overview 5

Chapter 4. System Configuration and Boot Management. 7

System Information 7
- System Summary 7
- Product Data 7

System Settings 8
- Devices and I/O Ports 9
- Driver Health 14
- Foreign Devices 15
- Memory 15
- Network 16
- Operating Modes 25
- Power 26
- Processors 27
- Recovery and RAS 30
- Security 31
- Storage 35

Date and Time 37

Start Options 37

Boot Manager 37
- Add Generic Boot Option 38
- Add UEFI Full Path Boot Option 38
- Delete Boot Option. 38
- Change Boot Order 39
- Set Boot Priority 39
- Boot From File 40
- Select Next One-Time Boot Option 40
- Boot Modes 41
- Reboot System 41

BMC Settings 41
- Network Settings 42

System Event Logs 45
- POST Event Viewer 45
- System Event Log 45

User Security 45
- Password Rule and Policy 47

F12 One Time Boot Device 48

Appendix A. Notices. 49

Trademarks 50

Chapter 1. UEFI Introduction

Unified Extensible Firmware Interface (UEFI) defines the architecture of the platform firmware used for booting the system hardware and interacting with the operating system. UEFI is an interface packed with various features, including but not limited to:

- System information and settings
- Boot and runtime services
- BMC settings
- System event logs
- User security

This guide applies to the following server models:

- SE100

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 Web UI).
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 the 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. Save the setting.
4. 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. Save the setting.
4. Restart the server and press F1.

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

Keyboard navigation tip:

Here are some useful keys for you to navigate items through the UEFI Setup in text mode using a keyboard:

- Enter: Select an item.
- +: Increase the value.
- –: Decrease the value.
- Esc: Return to the previous interface.
- F1: Display the help information.

Chapter 3. UEFI Setup Utility Overview

This topic provides a general introduction to the UEFI Setup utility.

Notes:

- **Server platform variation**: UEFI system configuration options vary by server platform. Some menus or options described in this document might be slightly different from those on your specific server platform.
- **Default settings**: The default settings are already optimized for you. Use the default value for any item you are not familiar with. Do not change the value of unfamiliar items to avoid unexpected problems. If you consider changing the server configuration, proceed with extreme caution. Setting the configuration incorrectly might cause unexpected results.
- **System boot for settings to take effect**: For settings that require a system reboot to take effect, use one of the following methods:
  - After changing the settings, click **Save Settings → Exit Setup Utility** on the main menu.
  - After changing the settings, press Esc and select **<Y> Save and Exit the Setup Utility** on the main menu.

    If you are in a nested submenu, press Esc repeatedly to return to the main menu.

The following table details the main menu of the UEFI Setup utility:

Table 1. System Configuration and Boot Management

Item	Description
Chapter 4 "System Configuration and Boot Management**" on page 7**	Main menu
Launch Graphical System Setup	Start the graphical user interface for system setup. You can view or change UEFI settings on the **UEFI Setup** page. **Note:** When navigating in the graphical System Setup, there will be no screen output through text-based console redirection. Please use a VGA monitor or the XCC Remote Console web viewer for graphical system setup screen output.
"System Information**" on page 7**	View basic details of the system.
"System Settings**" on page 8**	View or modify system settings. Changes might not take effect immediately. For settings that require a system reboot to take effect, save changes and reboot the system.
"Date and Time**" on page 37**	Set the local date and time of the system.
"Start Options**" on page 37**	Boot a desired selection from the primary boot sequence in the Boot Manager menu.
"Boot Manager**" on page 37**	Change the boot order, boot parameters, and boot from a file.
"BMC Settings**" on page 41**	Configure the baseboard management controller (BMC).
"System Event Logs**" on page 45**	Clear or view the system event log.
"User Security**" on page 45**	Set or change the power-on password and administrator password.
Save Settings	Save the changed settings and commit them to BMC.
Discard Settings	Discard the changes.

Table 1. System Configuration and Boot Management (continued)

Item	Description
Load Default Settings	Load the default values for system settings.
Exit Setup Utility	Exit the UEFI Setup utility.

Chapter 4. System Configuration and Boot Management

This chapter details the system UEFI Setup utility.

System Information

This section provides information about the system's configuration, firmware, and product data.

Table 2. System Information

Item	Description
“System Summary” on page 7	A summary of detailed system information
“Product Data” on page 7	System firmware information
Open Source License	Display open-source software acknowledgements and required copyright notices.

System Summary

This topic provides a summary of system information.

Table 3. System Summary

Item	Format	Description
System Identification Data		
Machine Type/Model	ASCII string of 10 or 8 characters	System machine type and model
Serial Number	ASCII string of 10 or 8 characters	Serial number
UUID Number	16-byte Hexadecimal String of 32 characters	Universally Unique Identifier (UUID)
Asset Tag Number	ASCII string of 32 characters	A customer-assigned system asset tag number
Processor		
Installed CPU Packages	ASCII string of 1 character	Number of installed CPU packages
Processor Speed	y.yyy **GHz**	Processor speed
Memory		
Memory Speed	yyyy **MHz**	Speed of the installed memory
Total Memory Detected	yyyy **GB**	Total capacity of all installed DIMMs
Total Usable Memory Capacity	yyyy **GB**	Amount of usable memory after deducting the overhead caused by mirroring mode, reserved or bad blocks, and other factors

Product Data

The topic provides essential information regarding the firmware of both the host system and the baseboard management controller (BMC).

Table 4. Product Data

Item	Format	Description
Host Firmware		
Build ID	ASCII string of 7 characters	Build ID of the host firmware
Version	String format: **X.YY** (where *X* is the major revision and *YY* is the minor revision)	Version of the host firmware
Build Date	Character string format: MM/DD/YYYY	Build date of the host firmware
BMC Firmware		
Build ID	ASCII string	Build ID of the baseboard management controller (BMC) firmware
Version	ASCII string	Version of the BMC firmware
Build Date	Character string format: MM/DD/YYYY	Build date of the BMC firmware

System Settings

This section provides an overview of configurable options within the Unified Extensible Firmware Interface (UEFI).

Table 5. System Settings

Item	Option	Description
"Devices and I/O Ports" on page 9	N/A	View and configure onboard devices and I/O port options.
"Driver Health" on page 14	N/A	View the health status of the drivers.
"Foreign Devices" on page 15	N/A	View the foreign devices if installed.
"Memory" on page 15	N/A	View and configure the memory settings.
"Network" on page 16	N/A	View and configure network devices and network-related settings.
"Operating Modes" on page 25	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 26	N/A	Configure power plan options.
"Processors" on page 27	N/A	View and configure the processor settings.
"Recovery and RAS" on page 30	N/A	Configure recovery policies and advanced reliability, availability, and serviceability (RAS) settings.
"Security" on page 31	N/A	Configure system security settings.
"Storage" on page 35	N/A	Manage storage adapter options. Some systems may use planar devices and can be configured under the **Devices and I/O Ports** menu.

Devices and I/O Ports

The settings available can vary based on the specific hardware installed, such as the type of riser card used. Items on this menu vary by server platform.

Table 6. Devices and I/O Ports

Item	Options	Description
Onboard SATA Mode	• **AHCI** (Default) • RAID	Configures SATA as AHCI or RAID.
PCI 64-Bit Resource Allocation	• **Enabled**(Default) • Disabled	Enables or disables allocation of 64-bit resources for PCI devices.
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.
“Enable/Disable Onboard Device (s)**” on page 9**	N/A	Enable or disable onboard devices or slots.
“Enable/Disable Adapter Option ROM Support**” on page 10**	N/A	Enable or disable UEFI-compliant adapter support. Disabling UEFI support may adversely affect pre-boot/ boot functions.
“PCIe Gen Speed Selection**” on page 11**	N/A	Choose the generation speed for the available PCIe slots.
“Console Redirection Settings**” on page 11**	N/A	Configure console redirection and COM port settings
“USB Configuration**” on page 13**	N/A	Enables or disables USB storage devices or individual ports.

Enable/Disable Onboard Device(s)

The settings available can vary based on the specific hardware installed, such as the type of riser card used. Items on this menu vary by server platform.

Table 7. Enable/Disable Onboard Device(s)

Item	Options	Description
Onboard Video	• **Enabled** (Default) • Disabled	Disabling an entry prevents the associated device from being enumerated during the subsequent boot. [Auto] is to disable this port if there is no device installed or there are errors detected on that device. **Note:** [Auto] is the setting for PCIe devices by CPU only.
Onboard SATA (For ODD)	• **Enabled** (Default) • Disabled	Disabling an entry prevents the associated device from being enumerated during the subsequent boot. [Auto] is to disable this port if there is no device installed or there are errors detected on that device. **Note:** [Auto] is the setting for PCIe devices by CPU only.
Slot (n...) (For M.2 SATA mode)	• **Enabled** (Default) • Disabled Or • Auto • **Enabled**(Default) • Disabled	Disabling an entry prevents the associated device from being enumerated during the subsequent boot. [Auto] is to disable this port if there is no device installed or there are errors detected on that device. **Note:** [Auto] is the setting for PCIe devices by CPU only.
NVMe (Display depending on which riser card is installed.)	• **Enabled** (Default) • Disabled or • Auto • **Enabled**(Default) • Disabled	Disabling an entry prevents the associated device from being enumerated during the subsequent boot. [Auto] is to disable this port if there is no device installed or there are errors detected on that device. **Note:** [Auto] is the setting for PCIe devices by CPU only.
Onboard LAN (Display depending on which riser card is installed.)	• Disable LOM • Disable Port 1 & 2 • Disable Port 2 • **Enable All Ports** (Default)	Disabling an entry prevents the associated device from being enumerated during the subsequent boot. [Auto] is to disable this port if there is no device installed or there are errors detected on that device. **Note:** [Auto] is the setting for PCIe devices by CPU only.

Enable/Disable Adapter Option ROM Support

The settings available can vary based on the specific hardware installed, such as the type of riser card used. Items on this menu vary by server platform.

Table 8. Enable/Disable Adapter Option ROM Support

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

PCIe Gen Speed Selection

The settings available can vary based on the specific hardware installed, such as the type of riser card used. Items on this menu vary by server platform.

Table 9. PCIe Gen Speed Selection

Item	Options	Description
Slot (n...) (Display depending on which riser card is installed.)	• **Auto** (Default) • Gen1 • Gen2 • Gen3 • Gen4 • Gen5	Sets the maximum speed supported by individual PCIe slot.
NVMe (n...) (Display depending on which riser card is installed.)	• **Auto** (Default) • Gen1 • Gen2 • Gen3 • Gen4	Sets the maximum speed supported by individual PCIe slot.

Console Redirection Settings

On this menu, you can configure how console output is managed, particularly for remote management and troubleshooting.

Table 10. Console Redirection Settings

Item	Options	Description
COM Port 1	• **Enabled** (Default) • Disabled	Enable or disable the COM 1 device. When [Disabled] is selected, the associated COM 1 terminal settings are hidden.
Virtual COM Port 2	• **Enabled** (Default) • Disabled	Enable or disable the Virtual COM Port 2 device. When [Disabled] is selected, SSH for console redirection is disabled.
Console Redirection	• Enabled • Disabled • **Auto**(Default)	Enable or disable console redirection. While [Auto] is selected, console redirection will be enabled automatically if IPMI Serial over LAN status is active.
Serial Port Sharing	• Enabled • **Disabled** (Default)	Enable the BMC to allow access to the system serial port. When [Enabled] is selected, the 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 the BMC unless **Serial Port Access Mode** is set to [Disabled].
Serial Port Access Mode	• Shared • Dedicated • **Disabled** (Default)	This option allows you to control the system BMC's access over the system serial port. • [Shared]: The serial port is available for POST and operating system use; however, the BMC will/can monitor the serial data for takeover control. • [Dedicated]: The BMC has complete control of the serial port. POST and/or OS will not be able to use the serial port. • [Disabled]: The BMC has no access to the serial port.
SP Redirection	• Enabled • **Disabled** (Default)	Serial over LAN (SOL) or Serial over SSH redirection enables a system administrator to use the BMC as a serial terminal server. This item allows you to choose which mode to have the redirection, SOL or SSH. • When [Disabled] is selected, it is configured with SOL redirection. • When [Enabled] is selected, a server serial port can be accessed from an SSH connection (Virtual COM 2). **Note:** This item is only displayed 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 10. 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	Set the connection speed between the host and the remote system.
COM1 Data Bits	• **8** (Default) • 7	Set the number of data bits in each character.
COM1 Parity	• **None** (Default) • Odd • Even	Set 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)	Set Stop Bits. Stop Bits, sent at the end of every character, allow the signal receiver to detect the end of a character and to resynchronize with the character stream.
COM1 Terminal Emulation	• VT100 • 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 11. 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 Rear Port (n...)	• **Enabled** (Default) • Disabled	Enables or disables USB individual ports.
USB Front Port (n...)	• **Enabled** (Default) • Disabled	Enables or disables USB individual ports.

Note:

Driver Health

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

Table 12. 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		
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.

Table 12. Driver Health (continued)

Item	Options	Description
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 13. 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.

Memory

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

Table 14. Memory

Item	Options	Description
“System Memory Details” on page 16	N/A	Displays status of the system memory.
Memory Speed	• Minimal Power • Balanced • **Maximum 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**.
In-Band ECC Support	• **Enabled** (Default) • Disabled	Enables or disables In-Band ECC. This feature will be enabled if memory has symmetric configuration.
DRAM Post Package Repair	• **Enabled** (Default) • Disabled	Enables or disables DRAM Post Package Repair.

System Memory Details

This section provides essential information of the DIMMs installed in the system.

System Memory Details

Table 15. System Memory Details

Item	Description
DIMM Details For Processor X	View the status of the installed DIMMs associated with a specific processor.

DIMM Details

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

Network

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

Table 16. Network

Item	Description
Global Network Settings	
“iSCSI Settings” on page 17	Configures iSCSI parameters.
“Network Stack Settings” on page 22	Specifies network stack settings.
“Network Boot Settings” on page 23	Configures network boot parameters.

Table 16. Network (continued)

Item	Description
“HTTP Boot Configuration” on page 23	Configures HTTP Boot parameters. **Note:** This item is available only when **Network** -> **Network Stack Setting** -> **IPv4 HTTP Support** or **IPv6 HTTP support** is enabled.
“Tls Auth Configuration” on page 24	You can press **Enter** to select Tls Auth Configuration. **Note:** This item is available only when **Network** -> **Network Stack Setting** -> **IPv4 HTTP Support** or **IPv6 HTTP support** is enabled.
Network Device List	View the network devices. The information of on-board cards or add-on cards will be displayed here, for example, the title of a card, the MAC address, or PFA.

iSCSI Settings

Table 17. iSCSI Settings

Item	Options	Description
“Host iSCSI Configuration” on page 17	N/A	Host iSCSI configuration.

Host iSCSI Configuration

On this menu, you can configure the iSCSI initiator, which allows a system to connect to iSCSI targets over a network.

Table 18. Host iSCSI Configuration

Item	Options	Description
iSCSI Initiator Name	Iqn.1986-03.com.example	Worldwide unique name of the iSCSI initiator Only the iSCSI Qualified Name (IQN) format is accepted. Range is from 4 to 233.
“Add an attempt” on page 18	N/A	Configure and add an attempt.
List of Attempts e.g. • Attempt 1 • Attempt 2 Selecting any item in the list will lead to “Attempt Settings” on page 18	N/A	After an attempt is added, the attempt will be listed here. The value 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”: [%s1]. **Notes:** • The exact value will be different, depending on the attempt settings. • %s1 is the option name for iSCSI Mode. • %s2 is the setting name for Internet Protocol.

Table 18. Host iSCSI Configuration (continued)

Item	Options	Description
“Delete Attempts” on page 21	N/A	Delete one or more attempts.
“Change Attempt Order” on page 22	N/A	You can change the attempt order by using the **+/-** keys. Use the arrow keys to select an attempt and press **+/-** to move the attempt up/down in the attempt order list.

Add an attempt

Table 19. MAC Selection

Item	Description
List of NICs in the system: Example: **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 20. 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.

Table 20. Attempt Settings (continued)

Item	Options	Description
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.
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.
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 Address	N/A	Enter an IPv4 or IPv6 address or a URL string. You need to configure the DNS server address in advance if input a URL string. **Note:** This item is not available 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.

Table 20. Attempt Settings (continued)

Item	Options	Description
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].
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].

Table 20. Attempt Settings (continued)

Item	Options	Description
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 21. Delete Attempts

Item	Options	Description
List of Attempts e.g., Attempt 1	Check box: • **Empty** (Default) • X	You can select an attempt to be deleted. The value 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] **Notes:** • The exact value will be different, depending on the attempt settings. • %s1 is the option name for iSCSI Mode. • %s2 is the setting name for Internet Protocol.
Commit Changes and Exit	N/A	Save changes and exit.
Discard Changes and Exit	N/A	Discard changes and exit.

Change Attempt Order

Table 22. Change Attempt Order

Item	Options	Description
Change Attempt Order	• e.g. • Attempt 1 • Attempt 2	Existing attempts are listed here. You can use the **+/-** keys to change the attempt order. Use the arrow keys to select the attempt and then press **+/-** to move the attempt up/down in the attempt order list.
Commit Changes and Exit	N/A	Save changes and exit.
Discard Changes and Exit	N/A	Discard changes and exit.

Network Stack Settings

On this menu, you can configure how a system interacts with network resources during the boot process, particularly for network-based booting methods such as Preboot Execution Environment (PXE) and HTTP boot.

Table 23. Network Stack Settings

Item	Options	Description
Network Stack	• **Enabled** (Default) • Disabled	Enable or disable the UEFI network stack.
IPv4 PXE Support	• **Enabled** (Default) • Disabled	Enable or disable IPv4 PXE Boot Support. If this item is disabled, the IPv4 PXE boot option will not be created.
IPv4 HTTP Support	• Enabled • **Disabled** (Default)	Enable or disable IPv4 HTTP Boot Support. If this item is disabled, the IPv4 HTTP boot option will not be created.
IPv6 PXE Support	• **Enabled** (Default) • Disabled	Enable or disable IPv6 PXE Boot Support. If this item is disabled, the IPv6 PXE boot option will not be created.
IPv6 HTTP Support	• Enabled • **Disabled** (Default)	Enable or disable IPv6 HTTP Boot Support. If this item is disabled, the IPv6 HTTP boot option will not be created.
PXE boot wait time	**0**	Wait time in seconds to press the ESC key to abort the PXE boot. Use either **+/-** or numeric keys to set the value.
Media detect count	**1**	Number of times the presence of media will be checked. Use either **+/-** or numeric keys to set the value.

Network Boot Settings

Table 24. Network Boot Settings

Item	Description
MAC:XX:XX:XX:XX:XX:XX **SlotXXX PCI X:XX:X:X**	Set boot configuration parameters on MAC XX:XX:XX:XX:XX:XX PCI function address: Bus XX:Dev XX:Func XX
VLAN Configuration List:	Configure VLAN parameters. (MAC:XXXXXXXXXXXX)
IPv4 Configuration List:	Configure IPv4 network parameters. (MAC:XXXXXXXXXXXX)
IPv6 Configuration List:	Configure IPv6 network parameters. (MAC:XXXXXXXXXXXX)

MAC:Onboard PCI

Table 25. MAC:Onboard PFA 1:0:0

Item	Options	Description
UEFI PXE Mode	• **Enabled** (Default) • Disabled	Enable or disable NIC to include or skip boot attempts during generic PXE network boot. Network Driver in “Network Device List” may also require configuration. System Boot Mode may further impact PXE.

HTTP Boot Configuration

On this menu, you can set up network booting using the HTTP protocol.

Notes:

- The **HTTP Boot Configuration** menu is displayed only when **IPv4 HTTP Support** or **IPv6 HTTP support** is enabled. To enable IPv4 HTTP support or IPv6 HTTP support, go to **Network → Network Stack Setting**.
- 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 26. 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	Configure HTTP Boot parameters. (MAC: XXXXXXXXXXXX)

Table 27. MAC:xxxxxxxxxxxx-HTTP Boot Configuration

Item	Options	Description
Input the description	N/A	Enter the boot description.
Internet Protocol	• IPv4 • IPv6	Select the Internet Protocol version.
Boot URI	N/A	A new boot option will be created according to the boot URI.

Tls Auth Configuration

Note: The **Tls Auth Configuration** menu is displayed only when **IPv4 HTTP Support** or **IPv6 HTTP support** is enabled. To enable IPv4 HTTP support or IPv6 HTTP support, go to **Network → Network Stack Setting**.

Table 28. Tls Auth Configuration

Item	Description
"Server CA Configuration" on page 24	You can press **Enter** to configure server Certificate Authority (CA).
Client Cert Configuration	Client certificate configuration is unsupported currently.

Server CA Configuration

Table 29. Server CA Configuration

Item	Description
"Enroll Cert" on page 24	You can press **Enter** to enroll the certificate.
"Delete Cert" on page 24	You can press **Enter** to delete the certificate.

Enroll Cert

Table 30. Enroll Cert

Item	Description
Enroll Cert Using File	Enroll the certificate using a certificate file.
Cert GUID	Enter the certificate GUID in the following format: 11111111-2222-3333-4444-1234567890ab.
Commit Changes and Exit	Save changes and exit.
Discard Changes and Exit	Discard changes and exit.

Delete Cert

Table 31. Delete Cert

Item	Options	Description
xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx	Check box: • **Empty** • X	List of certificate GUIDs. You can select the check box to delete the certificate. **Note:** If there is no security certificate file, no certificate GUID is displayed.

Operating Modes

Select the operating mode based on your preference.

Table 32. 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 highly dependent on the hardware and the software running on the system. According to the selected operating mode, related low-level settings will be automatically changed and can not be changed individually. To set low-level settings individually, select [Custom Mode]. [Efficiency – Favor Performance] is comparable to Intel's Optimized Power Mode (OPM). **Note:** For maximum performance on applications that don't utilize all CPU cores, it is best to select [Maximum Performance] first, then select [Custom] and enable C-states. Doing so will allow the active cores to achieve maximum turbo uplift. Alternatively, unused cores can be disabled under **System Settings** > **Processor** > **Active Performance-cores/Active Efficient-cores/Active SOC-North Efficient-cores**.
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 32. 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]** .
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**.

Power

On this menu, you can configure power scheme options.

Table 33. Power

Item	Options	Description
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. Also, when disabled, the following options under the BMC Server (Web) Power Actions feature will be disabled. 1. Power Off Server Normally. 2. Restart Server Normally.
PCIe Power Brake	• **Reactive**(Default) • Proactive • 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 75W TDP or greater.
ASPM	• Auto • **Disabled**(Default) **Note:** SR250 V3, ST50 V3 and ST250 V3 are set to Auto by default.	[Auto] enables ASPM on PCIe endpoint adapters that support it. [Disabled] disables ASPM for all PCIe endpoints.

Processors

This menu offers options to change the processor settings.

Table 34. Processors

Item	Options	Description
“Processor Details” on page 30	N/A	Summary of the installed processors
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. When [Legacy] is selected, the operating system initiates the C-state transitions. Some OS software may defeat the ACPI mapping (e.g. intel_idle driver). **Note:** When a preset workload profile is selected, this setting is not changeable and is grayed out. To change the setting, select **System Settings → Workload Profile → Custom** first. Then, you can change this setting.
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]** .
Trusted Execution Technology	• Enabled • **Disabled** (Default)	Enable or disable Intel Trusted Execution Technology (Intel TXT). Intel TXT is a set of hardware extensions to Intel processors and chipsets that enhance the digital office platform with security capabilities such as measured launch and protected execution.

Table 34. Processors (continued)

Item	Options	Description
Intel Virtualization Technology	• Disabled • **Enabled** (Default)	Enable or disable Intel Virtualization Technology. Intel Virtualization Technology abstracts hardware that allows multiple workloads to share a common set of resources. **Note:** When **Trusted Execution Technology** is set to [Enabled], this setting is not changeable and is grayed out.
Active Performace-cores	• **All**(Default) • . • . • 2 • 1	Select the number of P-Cores to be enabled in each processor package. **Note:** The number of P-Cores and E-Cores are looked at together. When both P-Cores and E-Cores are set to 0, Pcode will enable all cores.
Active Efficient-cores	• **All**(Default) • . • . • 3 • 2 • 1 • 0	Select the number of E-Cores to be enabled in each processor package. **Note:** The number of P-Cores and E-Cores are looked at together. When both P-Cores and E-Cores are set to 0, Pcode will enable all cores.
Active SOC-North Efficient-cores	• **All**(Default) • . • . • 1 • 0	Select the number of SOC-North Efficient-cores to be enabled in SOC North.
Package C State Limit	• C0/C1 • C2 • C3 • C6 • C7 • C7S • C8 • C9 • C10 • Cpu Default • **Auto**(Default)	Select the maximum Package C State Limit. [Cpu Default]: Leaves to factory default value. [Auto]: Initializes to deepest available Package C State Limit. **Note:** This feature appears only when **C-states** is not set to [Disabled].

Processor Details

Table 35. Processor Details

Item	Format	Description
Processor Socket	• Socket 1 • Socket n	Processor socket table
Processor ID	ASCII string	Tag of the processor ID
Processor Frequency	ASCII string	Value of the processor frequency
Processor Revision	ASCII string	Value of the microcode revision
L1 Cache RAM	ASCII string	Amount of L1 Cache RAM
L2 Cache RAM	ASCII string	Amount of L2 Cache RAM
L3 Cache RAM	ASCII string	Amount of L3 Cache RAM
Cores Per Socket (Supported/ Enabled)	ASCII string	Number of supported and enabled processor cores per processor socket
Threads Per Socket (Supported/ Enabled)	ASCII string	Number of supported and enabled processor threads per processor socket
Processor 1 Version	ASCII string	Version of processor 1
Processor n Version	ASCII string	Version of processor n

Recovery and RAS

On this menu, you can configure recovery policies and advanced reliability, availability, and serviceability settings.

Table 36. Recovery and RAS

Item	Description
“POST Attempts” on page 30	Configure number of attempts to POST before the recovery mechanisms is invoked.
“Disk GPT Recovery” on page 31	Configure Disk GUID Partition Table (GPT) Recovery options.
“System Recovery” on page 31	Configure system recovery settings.

POST Attempts

Table 37. POST Attempts

Item	Options	Description
Post Attempt Limit	• Disabled • 9 • 6 • **3** (Default)	Configure the 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.

Disk GPT Recovery

Table 38. Disk GPT Recovery

Item	Options	Description
Disk GPT Recovery	• Automatic • **Manual**(Default) • None	• [Automatic]: The system UEFI will automatically repair the corrupt GUID Partition Table (GPT). • [Manual]: The system UEFI will only repair the corrupt GPT based on user input. • [None]: The system UEFI will not repair the corrupted GPT. Recovery result can be retrieved from the system event log.

System Recovery

Table 39. System Recovery

Item	Options	Description
POST Watchdog Timer	• Enabled • **Disabled** (Default)	Enable or disable the POST Watchdog Timer.
POST Watchdog Timer Value	[5]	Enter the POST Watchdog Timer Value in minutes within the specified range (5-20).
Reboot System On NMI	• **Enabled** (Default) • Disabled	Specify whether to reboot the system during non-maskable interrupt (NMI).

Security

On this menu, you can configure system security settings.

Table 40. Security

Item	Description
“Secure Boot Configuration” **on page 31**	Configure secure boot options.
“Trusted Platform Module” **on page 33**	Configure TPM setup options.

Secure Boot Configuration

Secure Boot is a UEFI feature that prevents unauthorized firmware, operating systems, or drivers from loading. Secure Boot is essential for enhancing system security by ensuring that only trusted software is allowed to run during the boot process.

Table 41. Secure Boot Configuration

Item	Options	Description
Secure Boot Status	• Disabled • Enabled	Display the current secure boot status.
Secure Boot Mode	• User Mode • Setup Mode • Audit Mode • Deploy Mode	System performs secure boot authentication when this item is set to [User Mode] and secure boot is enabled.
Secure Boot Setting	• Enabled • **Disabled** (Default)	Enable or disable Secure Boot. A mode change requires a system reboot. The Secure Boot feature is Active only when Secure Boot is enabled, Platform Key (PK) is enrolled, and the system is in [User Mode] (**Secure Boot Mode**).
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 32	N/A	View the details of the PK, KEK, DB, and DBX.
"Secure Boot Custom Policy" on page 33	N/A	Customize the PK, KEK, DB, and DBX. **Note:** This menu is configurable only when **Secure Boot Policy** is set to [Custom Policy].

View Secure Boot Keys

Table 42. 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.

Table 42. View Secure Boot Keys (continued)

Item	Description
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 43. 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

The Trusted Platform Module (TPM) is a hardware-based security component that provides secure storage for cryptographic keys, digital certificates, and other sensitive data used to authenticate the system.

The menu below is for TPM 2.0:

Table 44. Trusted Platform Module

Item	Options	Description
"TPM 2.0" on page 34	N/A	Configure the TPM 2.0 Setup options.

The menu below is for TPM 1.2:

Table 45. Trusted Platform Module

Item	Options	Description
"TPM 1.2" on page 34	N/A	Configure the TPM 1.2 Setup options.

Trusted Platform Module (TPM 2.0)

Table 46. Trusted Platform Module (TPM 2.0)

Item	Options	Description
TPM Status		
TPM Vendor		
TPM Firmware Version		
[TPM Settings]		
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	• **Disabled**(Default) • Enabled	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.

Trusted Platform Module (TPM 1.2)

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

Table 47. 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

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

Table 48. Storage

Item	Description
“NVMe” on page 35	Displays NVMe device list.
“SATA Drives” on page 36	Displays SATA information.

NVMe

Table 49. NVMe

Item	Description
Bay X: NVMe Bus-Dev-Fun e.g. NVMe 64-0-0	This string is defined by platform. Each platform may display a different string. “X” is the bay number. “Bus-Dev-Fun” is the PCI address value.

NVMe Detail Information

Table 50. NVMe Detail Information

Item	Format	Description
Model Name	ASCII string	Model name of the NVMe device
Serial Number	ASCII string	Serial number of the NVMe device
Firmware Revision	ASCII string	Firmware revision of the NVMe device
Vendor ID	0xXXXX (XXX is hex number)	Vendor ID of the NVMe device
Device ID	0xXXXX (XXX is hex number)	Device ID of the NVMe device
Subsystem Vendor ID	0xXXXX (XXX is hex number)	Subsystem vendor ID of the NVMe device
Subsystem ID	0xXXXX (XXX is hex number)	Subsystem ID of the NVMe device
Maximum Link Speed	Gen N (N is number)	Maximum link speed
Maximum Link Width	xN (N is number)	Maximum link width
Negotiated Link Speed	Gen N (N is number)	Negotiated link speed

Table 50. NVMe Detail Information (continued)

Item	Format	Description
Negotiated Link Width	xN (N is number)	Negotiated link width
Number of Namespaces	N (N is number)	Number of namespaces
Total Size	X.XX TB (Unit can be GB or MB, depending on the size)	Total size
Device driver data link		
Device HII Title	N/A	Description of the device HII The title and description are generated by the installed storage vendor's HII utilities. If the device does not provide HII data, "N/A" will be displayed.

SATA Drives

Table 51. SATA Drives

Item	Description
Bay X Model Number	This string is defined by platform. Each platform may display a different string. "X" is the bay number. Display model number and serial number.

SATA Drive Information

Table 52. SATA Drive Information

Item	Format	Description
Location	Bay X	Location
Product Name	ASCII string	Product Name
Serial Number	ASCII string	Serial Number
FRU Number	ASCII string	FRU Number
Manufacturer	ASCII string	Manufacturer
Firmware Version	ASCII string	Firmware Version
Size	X.XX TB (Unit can be GB or MB, depending on the size)	Size

Date and Time

On this menu, you can set the local date and time of the system.

Table 53. Date and Time

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

Start Options

Below is a summary of the default boot order settings. Contents will be different if the system has a different boot order.

Table 54. 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

On this menu, you can manage various boot settings, including the boot order, options, modes, and system reboot functionalities.

Table 55. Boot Manager

Item	Options	Description
Boot Sequence		
“Add Generic Boot Option” on page 38	N/A	Adds one generic boot device as the boot option.
“Add UEFI Full Path Boot Option ” on page 38	N/A	Adds one UEFI application or one removable file system as the boot option.
“Delete Boot Option” on page 38	N/A	Removes boot option(s) from the boot order.

Table 55. Boot Manager (continued)

Item	Options	Description
“Change Boot Order” on page 39	N/A	Modifies ordering of selections within the boot order.
“Set Boot Priority” on page 39	N/A	Sets boot priority of the devices in a device group.
Other Boot Functions		
“Boot From File” on page 40	Xxxx {xxxx-xxx-xxx…}	Boots the system from a specific file or a device.
“Select Next One-Time Boot Option” on page 40	N/A	Selects one-time boot option for the next boot.
System		
“Boot Modes” on page 41	N/A	Changes between the UEFI boot mode and the legacy boot mode.
“Reboot System” on page 41	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 56. Add UEFI Full Path Boot Option

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

Delete Boot Option

Table 57. 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)

Table 57. Delete Boot Option (continued)

Item	Options	Description
USB Storage	[X]	Device Path: VenHw(B2AD3248-4F72-4950-A966-CFE5062DB83A,04000000)
Commit Changes and Exit	N/A	Saves changes and exits.

Change Boot Order

Table 58. 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 59. Set Boot Priority

Item	Description
“CD/DVD Priority” on page 39	Set the boot priority for the CD/DVD group if multiple devices exist in the system.
“Hard Disk Priority” on page 40	Set the boot priority for the hard disk group if multiple devices exist in the system.
“Network Priority” on page 40	Set the boot priority for the network device group if multiple devices exist in the system.
“USB Priority” on page 40	Set the boot priority for the USB device group if multiple devices exist in the system.

CD/DVD Priority

Table 60. 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 61. 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 62. Network Priority

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

USB Priority

Table 63. 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 menu to boot the system from a specific file or device. Message boxes will be displayed to guide you through the process.

Select Next One-Time Boot Option

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

Table 64. Select Next One-Time Boot Option

Item	Options	Description
Boot Option	• CD/DVD ROM • Hard Disk • Network • USB Storage • System Setup • **None** (Default) **Note:** This option list contains the boot options in the current boot order list, [System Setup], and [None]. The options will be different if the system has a different boot order.	Select the one-time boot option for the next boot.

Boot Modes

Table 65. Boot Modes

Item	Options	Description
System Boot Mode	• **UEFI Mode** (Default)	Drivers, option ROMs and OS loaders the Boot Manager attempts to boot. [UEFI Mode] runs UEFI drivers and boot an UEFI OS loader. Only the UEFI mode is supported.
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

Table 66. Reboot System

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

BMC Settings

On this menu, you can configure the baseboard management controller (BMC) settings.

Note: All settings under the BMC page cannot be reset to default values using **Load Default Settings**. Use **Reset Factory Defaults Setting** on this page to reset settings to default values.

Table 67. BMC Settings

Item	Options	Description
Power Restore Policy	• Always Off • Restore • Always On	Determines how the system reacts when the power is restored from a power loss. It will take a few minutes for the changes to take effect. • [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.
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 item is not available when **Power Restore Policy** is set to [Always Off].
Ethernet over USB interface	• Enabled • Disabled	Controls the Ethernet over USB interface used for in-band communication to the BMC. • [Enabled]: Enables in-band communication between the BMC and the xClarity Essentials in-band update utility running on the server. • [Disabled]: Prevents xClarity Essentials and other applications running on the server from requesting the BMC to perform tasks. **Note:** Change to the settings may keep stale for a while and do not take effect immediately.
“Network Settings” **on page 42**	N/A	Configure network settings of the BMC.
Reset Factory Defaults Setting	N/A	Restore all BMC settings to factory defaults, including network configuration and credentials. The BMC will be restarted automatically.
Restart BMC	N/A	Restart the BMC.

Network Settings

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

Table 68. Network Settings

Item	Options	Description
Network Interface Port	• Dedicated • Shared	Select the system management network port. **Note:** The options vary by platform.
Fail-Over Rule	• None • Failover to shared (Optional Card ML2) • Failover to shared (Optional Card PHY) • Failover to shared (Onboard Port)	This item controls the types of fail-over allowed. **Notes:** • This item is available only when **Network Interface Port** is set to [Dedicated]. • The options vary by platform.
Burned-in MAC Address	N/A	Burned-in MAC address of the network interface controller
Hostname	N/A	Host name of the BMC controller You can change the host name by entering up to a maximum of 63 characters in this field.
DHCP Control	• Static IP • DHCP Enabled • DHCP with Fallback	Configure DHCP Control or configure a static IP address manually. • [Static IP]: Enter an IP address manually. • [DHCP Enabled]: The IP address will be assigned automatically by the DHCP server. • [DHCP with Fallback]: The static IP address will be used if DHCP fails.
IP Address	x.x.x.x	Enter the IP address in dotted-decimal notation.
Subnet Mask	x.x.x.x	Enter the subnet mask address in dotted-decimal notation.
Default Gateway	x.x.x.x	Enter the default gateway address in dotted-decimal notation.
IPv6	• Enabled • Disabled	Enable or disable IPv6 support on the management port. **Note:** This item is unable to reset to the default value by using **Load Default Settings** on the main menu.
Local Link Address	N/A	Local link address
VLAN Support	• Enabled • Disabled	Enable or disable Virtual LAN (VLAN) support. When VLAN is enabled, you can specify an 802.1q VLAN ID for the management network port. **Note:** This item is unable to reset to the default value by using **Load Default Settings** on the main menu.
VLAN ID	1	Specify a VLAN ID. The value range is 1 to 4094. **Note:** This feature appears only when VLAN Support is enabled.

Table 68. Network Settings (continued)

Item	Options	Description
“Advanced Settings for BMC Ethernet” **on page 44**	N/A	Provides advanced settings for BMC Ethernet.
Save Network Settings	N/A	Save the network setting changes to the BMC. It takes a few minutes for the changes to take effect.

Advanced Settings for BMC Ethernet

Table 69. 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. **Note:** This item is unable to reset to the default value by using **Load Default Settings** on the main menu.
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 appears only when Autonegotiation is set to [No]. • This item is unable to reset to the default value by using **Load Default Settings** on the main menu.
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 appears only when Autonegotiation is set to [No]. • This item is unable to reset to the default value by using **Load Default Settings** on the main menu.
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.

System Event Logs

The System Event Logs (SEL) provide a record of significant events related to hardware and system operations. This menu provides options to manage these logs.

Table 70. System Event Logs

Item	Description
“POST Event Viewer” on page 45	Displays POST Event Viewer.
“System Event Log” on page 45	Displays System Event Log.
Clear System Event Log	Clears System Event Log.

POST Event Viewer

Table 71. POST Event Viewer

Item	Description
Entry [n]:	Information.

System Event Log

Table 72. 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

On this menu, you can set or change power-on and administrator passwords.

Table 73. User Security

Item	Description
“Password Rule and Policy” **on page 47**	Set the password rule and policy.
Set Power-On Password	Set the power-on password. The password can only contain the following characters (excluding white-space characters): A-Z, a-z, 0-9, ~`!@#$%^&*()-+={}[]|:;"'<>,?/._ Must contain at least one letter. Must contain at least one number. Must contain at least two of the following characters in combination: • At least one upper-case letter • At least one lower-case letter • At least one special character No more than two consecutive occurrences of the same character Must contain at least 8 characters if **Minimum password length** is not set.
Clear Power-On Password	Clear the power-on password.
Set Administrator Password	Set the administrator password. The password can only contain the following characters (excluding white-space characters): A-Z, a-z, 0-9, ~`!@#$%^&*()-+={}[]|:;"'<>,?/._ Must contain at least one letter. Must contain at least one number. Must contain at least two of the following characters in combination: • At least one upper-case letter • At least one lower-case letter • At least one special character No more than two consecutive occurrences of the same character Must contain at least 8 characters if **Minimum password length** is not set.
Clear Administrator Password	Clear the administrator password.

Password Rule and Policy

Table 74. 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.
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.

Table 74. Password Rule and Policy (continued)

Item	Options	Function
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 75. 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.