Lenovo ThinkEdge server V3 with AMD EPYC processors UEFI Manual

Server Models: SE455 V3, MX455 V3 IS

Second Edition (April 2024)

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 model:

- SE455 V3
- MX455 V3 IS

The following table details the main menu:

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

Table 1. Main menu

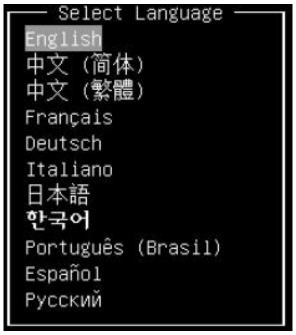
Item	Options	Description
Chapter 3 "System configuration and boot management" **on page 5**	N/A	Main menu
Select Language	 Select Language English 中文（简体） 中文（繁體） Français Deutsch Italiano 日本語 한국어 Português (Brasil) Español Русский	Change the language for the current system.
Launch Graphical System Setup	N/A	Start the graphical user interface for system setup, provisioning manager, and RAID configuration. When in Graphical System Setup, there will be no screen output to console, please use VGA monitor for Graphical System Setup.
"System Information" **on page 5**	N/A	Display the basic details of the system.
"System Settings" **on page 7**	N/A	Display or modify system settings. Changes may not take effect immediately. Save any changed settings and reboot the system.
"Date and Time" **on page 47**	N/A	Set the local Date and Time of the system.
"Start Options" **on page 47**	N/A	Boot a desired selection from the primary boot sequence as specified under **Boot Manager**.
"Boot Manager" **on page 48**	N/A	Change boot order, boot parameters, and boot from a file.

Table 1. Main menu (continued)

Item	Options	Description
“BMC Settings” **on page 52**	N/A	Configure the management controller.
“System Event Logs” **on page 55**	N/A	Clear or view the System Event Log.
“User Security” **on page 56**	N/A	Set or change Power-On and Administrator passwords.
Save Settings	N/A	Save the changes and commit them to BMC.
Discard Settings	N/A	Discard any changes.
Load Default Settings	N/A	Load the default values for system settings.
Exit Setup Utility	N/A	Exit Setup.

Chapter 2. Get started

First launch

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

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

Switch between graphic/text modes

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

Graphic mode to text mode

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

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

Text mode to graphic mode

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

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

Chapter 3. System configuration and boot management

This chapter details system setup utility.

System Information

This menu displays the system information.

Table 2. System Information

Item	Description
"System Summary" **on page 5**	Display the basic details of the system.
"Product Data" **on page 6**	Display system firmware information.
"Open Source License" **on page 7**	Open Source License

System Summary

Table 3. System Summary

Item	Format	Description
System Identification Data		
Machine Type/Model	10-character or 8-character ASCII string	The systems machine type and model.
Serial Number	10-character or 8-character ASCII string	Tag for the Serial Number.
UUID Number	32-character Hex string (16 bytes)	Tag for the UUID.
Asset Tag Number	32-character ASCII string	A customer assigned system Asset Tag Number.
Processor		
Installed CPU packages	1-character ASCII string	Number of installed CPU packages.
Processor Speed	y.yyy **GHz**	Processor Speed.
Memory		
Memory Mode	ASCII string	Memory Mode.
Memory Speed	yyyy **MHz**	The installed Memory Speed.
Total Memory Detected	yyyy **GB**	Total amount of memory from the sum of all DIMM installed.
Total Usable Memory Capacity	yyyy **GB**	Amount of usable memory after deducting the overhead caused by mirroring mode, reserved or bad blocks, etc.

Product Data

Table 4. Product Data

Item	Format
Host Firmware	
Build ID	7-character ASCII string
Version	4-character string format: **1.xx**
Build Date	Character string format: MM/DD/YYYY
BMC Firmware	
Build ID	ASCII string
Version	ASCII string
Build Date	Character string format: MM/DD/YYYY

Open Source License

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

When you enter this option, the initial position is always at the top.

System Settings

This menu displays the system settings.

Table 5. System Settings

Item	Options	Description
<F1> Start Control	- **Auto** - 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].
“Device and I/O ports” on page 8	N/A	Display onboard devices and I/O port options.
“Driver Health” on page 13	N/A	View the health of the controllers in the system as reported by their corresponding drivers.
“Foreign Devices” **on page 14**	N/A	Foreign other devices list.
“Legacy BIOS” on page 14	N/A	Configure system UEFI firmware execution environment preferences for supporting legacy OS and legacy Option ROM.
“Memory” on page 15	N/A	Display and provide options to change the memory settings.
“Network” on page 18	N/A	Display network devices and network related settings.
“Operating Modes” on page 24	N/A	Select the operating mode desired based on your preference. **Note:** Power savings and performance are also highly dependent on hardware configuration and the software running on the system.
“Power” on page 27	N/A	Configures power scheme options.
“Processors” on page 28	N/A	Display and provide options to change the processor settings.
“Recovery and RAS” on page 33	N/A	Configure recovery policies and advanced reliability, availability, and serviceability settings.
“Security” on page 36	N/A	Configure system security settings.
“Storage” on page 44	N/A	Manage storage adapter options. Some systems may use planar devices and can be configured under “Devices and I/O Ports”.

Devices and I/O Ports

Table 6. Devices and I/O ports

Item	Options	Description
Onboard SATA 1 Mode	- **AHCI** (Default) - RAID	Configure SATA 1 as AHCI or RAID.
Onboard SATA 2 Mode	- **AHCI** (Default) - RAID	Configure SATA 2 as AHCI or RAID.
Onboard SATA 3 Mode	- **AHCI** (Default) - RAID	Configure SATA 3 as AHCI or RAID.
Active Video	- **Onboard Device** (Default) - Add-in Device	This setting only applies if the server has an add-in video adapter. When the option ROM is set to Legacy for both onboard and add-in video adapters, the Active Video setting controls which single adapter will display the System Setup utility. Regardless of this setting, the system boot early video is displayed at the onboard video only, and the management controller remote console shows the onboard video only. This setting does not affect how the OS chooses to display its graphical desktop.
PCI 64-Bit Resource Allocation	- Enabled - Disabled - **Auto** (Default)	[Enabled] or [Disabled] the allocation of 64-bit resources for PCI. [Auto] would allocate some resources below 4GB for legacy compatibility.
IOMMU	- Disabled - **Enabled** (Default)	Enable/Disable IOMMU.
SRIOV	- **Enabled** (Default) - Disabled	[Enabled] or [Disabled] the support of resource allocation for Single Root I/O Virtualization (SR-IOV) virtual functions during boot.
PCIe ARI Forwarding	- **Disabled** (Default) - Enabled	ARI Forwarding Enable for each downstream port.
"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	Control Legacy and UEFI-compliant adapter support. Disabling UEFI/Legacy support may adversely affect pre-boot/boot functions.
"Set Option ROM Execution Order" on page 10	N/A	Control legacy ROM load order.
"PCIe Gen Speed Selection" on page 10	N/A	Choose the generation speed for available PCIe slots.
"Override Slot Bifurcation" **on page 11**	N/A	This is used to override the slot bifurcation setting of the physical x16 slot to support the adapter with multiple devices.

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

Item	Options	Description
"Console Redirection Settings" on page 11	N/A	Settings for console redirection and COM port settings.
"USB Configuration" on page 13	N/A	Disable USB storage devices or individual ports.

Enable/Disable Onboard Device(s)

Table 7. Enable/Disable Onboard Device(s)

Item	Operation	Description
Onboard Video	• Disabled • **Enabled** (Default)	Disabling an entry will prevent the associated device from being enumerated during subsequent boots. [Auto] is removing the port if there is no device or errors on that device. **Note:** [Auto] is the setting for PCIe devices by CPU only.
Onboard SATA (It's for ODD)	• Disabled • **Enabled** (Default)	Disabling an entry will prevent the associated device from being enumerated during subsequent boots. [Auto] is removing the port if there is no device or errors on that device. **Note:** [Auto] is the setting for PCIe devices by CPU only.
M.2 (It's for M.2 SATA mode)	• Disabled • **Enabled** (Default)	Disabling an entry will prevent the associated device from being enumerated during subsequent boots. [Auto] is removing the port if there is no device or errors on that device. **Note:** [Auto] is the setting for PCIe devices by CPU only.
Slot (n…)	• Disabled • **Enabled** (Default) Or • Disabled • **Enabled** (Default) • Auto	Disabling an entry will prevent the associated device from being enumerated during subsequent boots. [Auto] is removing the port if there is no device or errors on that device. **Note:** [Auto] is the setting for PCIe devices by CPU only.
NVMe Bay (n…)	• Disabled • **Enabled** (Default) Or • Disabled • **Enabled** (Default) • Auto	Disabling an entry will prevent the associated device from being enumerated during subsequent boots. [Auto] is removing the port if there is no device or errors on that device. **Note:** [Auto] is the setting for PCIe devices by CPU only.

Enable/Disable Adapter Option ROM Support

Table 8. Enable/Disable Adapter Option ROM Support

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

Set Option ROM Execution Order

Table 9. Set Option ROM Execution Order

Item	Options	Description
Set Option ROM Execution Order 1. "Onboard LAN Port x "depends on PHY card installed. 2. Slot 1~3 will display depending on which riser card is installed.	• Onboard Video • Onboard SATA • Slot 1 • Slot 2 • Slot n... • Onboard LAN Port 1 • Onboard LAN Port n... • NVMe Bay 0 • NVMe Bay n...	Select the load order for legacy PCI option ROM(s). Use the **+** key to execute the selected devices ROM sooner or **–** key to execute late.

PCIe Gen Speed Selection

Table 10. PCIe Gen Speed Selection

Item	Operation	Description
Slot 1	• **Auto** (Default) • Gen1 • Gen2 • Gen3 • Gen4	Set the maximum speed supported by individual PCIe slot.
Slot 2	• **Auto** (Default) • Gen1 • Gen2 • Gen3 • Gen4	Set the maximum speed supported by individual PCIe slot.
Slot (n...)	• **Auto** (Default) • Gen1 • Gen2 • Gen3 • Gen4	Set the maximum speed supported by individual PCIe slot.

Override Slot Bifurcation

This page allows you to override the slot bifurcation settings.

This page is platform dependent, refer to platform document for details.

Console Redirection Settings

Table 11. Console Redirection Settings

Item	Options	Description
COM Port 1	• **Enabled** (Default) • Disabled	Enable or disable COM 1 device. If [Disabled] is selected, the associated COM1 terminal settings will be hidden.
Virtual COM Port 2	• **Enabled** (Default) • Disabled	Enable or disable virtual COM 2 device. If [Disabled] is selected, the SSH connection will be disabled.
Console Redirection	• Enabled • Disabled • **Auto** (Default)	Set remote console redirection preference to 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 system Baseboard Management Controller to allow access to the system serial port. If this option is set to [Enabled], the BMC will be allowed to control the serial communication port as requested by remote control commands. If sharing is [Disabled], the serial port will be assigned to the BMC unless the “Serial Port Access Mode” is set to [Disabled].
Serial Port Access Mode	• Shared • Dedicated • **Disabled** (Default)	This option allows you to control the access the system Baseboard Management Controller has over the system serial port. • (a) Shared mode: By selecting [Shared], the serial port will be available for POST and operating system use; however the BMC will/can monitor the serial data for a takeover control sequence. • (b) Dedicated mode: By selecting [Dedicated], the BMC will have complete control of the serial port and POST and/or the operating system will not be able to use the serial port. • (c) Disable mode: By selecting [Disabled], the BMC will not have any access to the serial port.

Table 11. Console Redirection Settings (continued)

Item	Options	Description
SP Redirection	• Enabled • **Disabled** (Default)	Serial Over LAN (SOL) or SSH redirection enables a system administrator to use the BMC as a serial terminal server. It allows you to choose which mode to have the redirection. If this option is set to [Disabled], it will be configured with Serial over Lan (SOL). A server serial port can be accessed from SSH connection (Virtual COM 2) when SP Redirection is set to [Enabled].
Legacy OS/Option ROM Display	• Virtual COM Port 2 • **COM Port 1** (Default)	Select a COM port to display redirection of Legacy OS and Legacy OPROM Messages.
COM Port Active After Boot	• Enabled • **Disabled** (Default)	When [Disabled] is selected, then Legacy Console Redirection is disabled before booting to legacy OS. When [Enabled] is selected, then Legacy Console Redirection is enabled for legacy OS.
COM1 Settings Settings required for serial connections used for asynchronous start-stop communication.		
COM1 Baud Rate	• **115200** (Default) • 57600 • 38400 • 19200 • 9600	Control the connection speed between the host and remote system.
COM1 Data Bits	• **8** (Default) • 7	Set the number of Data Bits in each character.
COM1 Parity	• **None** (Default) • Odd • Even	Select parity bit in each character to be [None], [Odd], or [Even]. [None] means that no parity bit is sent at all.
COM1 Stop Bits	• 2 • **1** (Default)	Set Stop Bits. Stop Bits sent at the end of every character allow the signal receiver to detect the end of a character and to resynthesize 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. Consult the emulator documentation for more information.
COM1 Flow Control	• **Disabled** (Default) • Hardware	Select [Hardware] only if the remote emulator support and is using hardware flow control. Consult the emulator documentation for more information.

USB Configuration

Table 12. USB Configuration

Item	Options	Description
USB Mass Storage Driver Support	• **Enabled** (Default) • Disabled	Enable/Disable USB Mass Storage Driver Support. This setting only takes effect in post time.
USB Port 1	• **Enabled** (Default) • Disabled	Disabling USB individual ports.
USB Port 2	• **Enabled** (Default) • Disabled	Disabling USB individual ports.
USB Port 3	• **Enabled** (Default) • Disabled	Disabling USB individual ports.

Driver Health

Table 13. Driver Health

Item	Options	Description
The platform is:	The platform is: • **Healthy** (Default) • Repair Required • Configuration Required • Operation Failed • Reconnect Required • Reboot Required • Shutdown Required • No Operation Required	Select this option to view the health of the controllers in the system as reported by their corresponding drivers.
Driver/Controller Status:		
Controller Name - Status	• **Healthy** (Default) • Repair Required • Configuration Required • Operation Failed • Reconnect Required • Reboot Required • Shutdown Required • No Operation Required	

Table 13. Driver Health (continued)

Item	Options	Description
POST Attempts Driver	• **Healthy** (Default) • Repair Required • Configuration Required • Operation Failed • Reconnect Required • Reboot Required • Shutdown Required • No Operation Required	
Partition Driver (MBR/GPT/El Torito)	• **Healthy** (Default) • Repair Required • Configuration Required • Operation Failed • Reconnect Required • Reboot Required • Shutdown Required • No Operation Required	

Foreign Devices

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

Table 14. Foreign Devices

Item	Description
Unclassified device:	
Video devices:	
Input devices:	
Onboard devices:	
Other devices:	

Legacy BIOS

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

Table 15. Legacy BIOS

Item	Options	Description
Legacy BIOS	• **Enabled** (Default) • Disabled	Enable/Disable the system UEFI firmware execution environment for supporting legacy OS and legacy Option ROM.

Table 15. Legacy BIOS (continued)

Item	Options	Description
Rehook INT 19h	• Enabled • **Disabled** (Default)	[Enable] prevents devices from taking control of the boot process.
Non-Onboard PXE	• **Enabled** (Default) • Disabled	Enable/Disable legacy PXE boot for installed network adapters.
When security boot is enabled, the Legacy BIOS will be changed into: Legacy BIOS is disabled due to secure boot is enabled.		

Memory

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

Table 16. Memory

Item	Options	Description
"System Memory Details" on page 17	N/A	Provides status of System Memory.
Total Usable Memory Capacity	yyyy **GB**	
Memory Speed	• Maximum • xxxxMHz • Minimum	The option number of the memory speed is changed dynamically according to the combination of the installed CPU SKU, DIMM type, number of DIMMs per channel, and system motherboard support. The system operates at the rated speed of the slowest DIMM in the system when populated with different speed DIMMs. If DIMMs are installed with a rated speed below 3600, this will result in the memory speed getting set to the Minimum value.
Memory Power Down Enable	• **Enabled** (Default) • Disabled	Enables/disables low-power features for DIMMs.
NUMA Nodes per Socket	• NPS0 • **NPS1** (Default) • NPS2 • NPS4	Specify the number of desired NUMA nodes per CPU socket (for example, NPS1 means 1 NUMA per socket). NPS0 will attempt to interleave the two CPU sockets together into one NUMA node. This setting may degrade performance due to increased memory latency.

Table 16. Memory (continued)

Item	Options	Description
Chipselect Interleaving	• Disabled • **Auto** (Default)	This setting specifies if the system should use a DRAM rank also known as chipselect interleaving. This feature will spread memory accesses across the banks of memory within a channel and will increase memory block access performance. This setting requires that the populated DIMMs have the same bank size, type, and that the number of banks is a power of two. It is strongly recommended that DIMMs with the same part number be populated.
DRAM Post Package Repair	• **Enabled** (Default) • Disabled	Enable or disable DRAM Post Package Repair.
DDR Healing BIST	• **Disabled** (Default) • PMU Mem BIST • Self-Healing Mem BIST • PMU and Self-Healing Mem BIST	[Disabled]: Disable memory self-healing feature. [PMU Mem BIST]: Use vendor-provided physical layer management unit firmware (PMU) to test memory on all channels simultaneously. Failing memory will be repaired using soft (temporary) or hard (permanent) repair, depending on the post package repair (PPR) configuration. [Self-Healing Mem BIST]: Use JEDEC DRAM built-in self-test (BIST) to detect failure and attempt a hard repair (permanent) for the failing memory row. [PMU and Self-Healing Mem BIST]: Run PMU Mem BIST and then Self-Healing Mem BIST tests sequentially.
DRAM Scrub Time	• Disabled • 1 hour • 4 hours • 6 hours • 8 hours • 12 hours • 16 hours • **24 hours** (Default) • 48 hours	Sets the period of time between successive DRAM scrub events.
Memory Interleave	• **Enabled** (Default) • Disabled	Enable or disable memory interleaving. Note that the NUMA nodes per socket value will be honored regardless of this setting.
SubUrgRefLowerBound	[1]	Specify the stored refresh limit to required enter sub-urgent refresh mode. Constraint: SubUrgRefLowerBound <= UrgRefLimit Valid value: 6 ~ 1.

Table 16. Memory (continued)

Item	Options	Description
UrgRefLimit	[4]	Specify the stored refresh limit to required enter urgent refresh mode. Constraint: SubUrgRefLowerBound <= UrgRefLimit. Valid value: 6 ~ 1.
DRAM Refresh Rate	• **1x** (Default) • 2x	A refresh rate of 1x is recommended for better performance. Choose refresh rate 2x to mitigate rowhammer issue, this may have a performance side effect.
TSME	• **Disabled** (Default) • Enabled	Transparent SME: • AddrTweakEn = 1 • ForceEncrEn = 0 • DataEncrEn = 1
SME-MK	• Enabled • **Disabled** (Default)	SME-MK encryption mode. Enabling both SMEE and SME-MK is not supported.
SEV-ES ASID Space Limit	[1] Range: 1–1007	SEV VMs using ASIDs below the SEV-ES ASID Space Limit must enable the SEV-ES feature. ASIDs from SEV-ES ASID Space Limit to (SEV ASID Count + 1) can only be used with SEV VMs. If this field is set to (SEV ASID Count + 1), all ASIDs are forced to be SEV-ES ASIDs. Hence, the valid values for this field is 1 - (SEV ASID Count + 1).
SEV Control	• **Enabled**(Default) • Disabled	Can be used to disable SEV. To re-enable SEV, a POWER CYCLE is needed after selecting the **Enabled** option.
SMEE	• Enabled • **Disabled** (Default)	Control secure memory encryption enable.
1TB remap	• Do not remap • **Attempt to remap** (Default)	Attempt to remap DRAM out of the space just below the 1TB boundary. The ability to remap depends on DRAM configuration, NPS, and interleaving selection, and may not always be possible.

System Memory Details

Table 17. System Memory Details

Item	Description
DIMM Details For Processor X	Provides status of DIMMs.

DIMM Details

This menu displays DIMM population list.

The DIMM population list in this page is platform dependent.

When Dimm has DBE, the Dimm item will turn from string description to enable/disable option. In this generation the enable/disable option will set enable as default.

Note: These items according to your system configuration.

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 card's title, MAC address or PFA. These formats depend on card's driver, please contact with card vender for the format.

Table 18. Network

Item	Description
Global Network Settings	
"iSCSI Settings" on page 18	Configure the iSCSI parameters.
"Network Stack Settings" on page 22	Network Stack Settings
"Network Boot Settings" on page 23	Configure the network boot parameters.
"HTTP Boot Configuration" on page 23	Configure HTTP Boot parameters.
"Tls Auth Configuration" on page 23	Press **Enter** to select Tls Auth Configuration.

iSCSI Settings

Table 19. iSCSI Settings

Item	Description
"Host iSCSI Configuration" **on page 18**	Host iSCSI Configuration.

Host iSCSI Configuration

Table 20. Host iSCSI configuration

Item	Options	Description
iSCSI Initiator Name	Iqn.1986-03.com.example	The worldwide unique name of iSCSI Initiator. Only IQN format is accepted. Range is from 4 to 233.
"Add an Attempt" **on page 19**	N/A	Add an attempt.
List of Attempts For example, • Attempt 1 • Attempt 2 **Note:** Only appears when attempts exist. Selecting an item will lead to Attempt Configuration page in 2.1.9.1.1.1.1.	N/A	MAC: XX:XX:XX:XX:XX:XX, PFA: Bus XX | Dev XX | Func XX, "iSCSI Mode": [%s1], "Internet Protocol": [%s2] **Notes:** • Exact value will be different depends on the attempt settings. • %s1 will be option name for iSCSI Mode. • %s2 will be the setting name for Internet Protocol.
"Delete Attempts" **on page 22**	N/A	Delete one or more attempts.

Table 20. Host iSCSI configuration (continued)

Item	Options	Description
“Change Attempt Order” **on page 22**	N/A	Change the order of Attempts using +/- keys. Use arrow keys to select the attempt then press +/- to move the attempt up/ down in the attempt order list.

Add an Attempt

Table 21. MAC Selection

Item	Description
Example, “MAC XX:XX:XX:XX:XX:XX**” on page 19** **Note:** List of NICs in the system	PFA: Bus XX | Dev XX | Func XX

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

Table 22. Attempt Settings

Item	Options	Description
iSCSI Attempt Name	N/A	Attempt Name is assigned automatically and not changeable.
iSCSI Mode	• **Disabled** (Default) • Enabled • Enabled for MPIO	[Disabled], [Enabled], [Enabled for MPIO] Make sure all necessary items (for example, initiator IP, target IP and authentication settings) been set appropriately before enable this item. Otherwise, this attempt may be lost after reboot.
Internet Protocol	• **IPv4** (Default) • IPv6 • Autoconfigure	Initiator IP address is system assigned in [IPv6] mode. In [Autoconfigure] mode, iSCSI driver will attempt to connect iSCSI target via IPv4 stack, if failed then attempt IPv6 stack.
Connection Retry Count	[0]	The minimum value is 0 and the maximum is 16. 0 means no retry.
Connection Establishing Timeout	[1000]	The timeout value in milliseconds. The minimum value is 100 milliseconds and the maximum is 20 seconds.

Table 22. Attempt Settings (continued)

OUI-format ISID	Example, 3CD30AC68EF8	OUI-format ISID in 6 bytes, default value are derived from MAC address. Only last 3 bytes are configurable. These values are taken from “Configure ISID” control.
Configure ISID	Example, C68EF8	OUI-format ISID in 6 bytes, default value are derived from MAC address. Only last 3 bytes are configurable. Example: Update 0ABBCCDDEEFF to 0ABBCCF07901 by input F07901.
Enable DHCP	• **[Empty]** (Default) • [X]	Enable DHCP
Initiator IP Address **Note:** This item appears when **Enable DHCP** is not enabled.	0.0.0.0	Enter IP address. **Note: ISCSI Message → Invalid IP address! → Ok**
Initiator Subnet Mask **Note:** This item appears when **Enable DHCP** is not enabled.	0.0.0.0	Enter IP address. **Note: ISCSI Message → Invalid Subnet Mask! → Ok**
Gateway **Note:** This item appears when **Enable DHCP** is not enabled.	0.0.0.0	Enter IP address. **Note: ISCSI Message → Invalid Gateway! → Ok**
Get target info via DHCP **Note:** This item appears when **Enable DHCP** is not enabled.	• **[Empty]** (Default) • [X]	Get target info via DHCP.
Target Name **Note:** This item will not appear when **Get target info via DHCP** is enabled	N/A	The worldwide unique name of the target. Only iqn. format is accepted. Range is from 4 to 223. **Note: ISCSI Message → Invalid iSCSI Name!! → Ok**
Target Address **Note:** This item will not appear when **Get target info via DHCP** is enabled.	N/A	Enter Target address in IPv4,IPv6 or URL format. You need to configure DNS server address in advance if input a URL string.
Target Port **Note:** This item will not appear when **Get target info via DHCP** is enabled.	[3260]	Target Port
Boot LUN **Note:** This item will not appear when **Get target info via DHCP** is enabled.	[0]	Hexadecimal representation of the LUN number. Examples are: 4751-3A4F-6b7e-2F99, 6734-9-156f-127, 4186-9. **Note: ISCSI Message → Invalid LUN string! → Ok**

Table 22. Attempt Settings (continued)

Authentication Type	• CHAP • **None** (Default)	Authentication method: [CHAP] or [None].
CHAP Type **Note:** This item appears when Authentication Type is CHAP.	• One way • **None** (Default)	[One way] or [Mutual].
CHAP Name **Note:** This item appears when **Authentication Type** is CHAP.	N/A	CHAP Name
CHAP Secret **Note:** This item appears when **Authentication Type** is CHAP.	N/A	The minimum length is 12 bytes and the maximum length is 16 bytes. **Notes:** • **Create New Password → Confirm New Password** – **ERROR → Invalid Password → Ok** – **ERROR → Invalid Input Range → Ok**
CHAP Status **Note:** This item appears when **Authentication Type** is CHAP.	• **Not Installed** (Default) • Installed	[Not Installed] if “CHAP Name” and “CHAP Secret” are not set. [Installed] if “CHAP Name” and “CHAP Secret” are set.
Reverse CHAP Name **Note:** This item appears when **CHAP Type** is Mutual.		Reverse CHAP Name.
Reverse CHAP Secret **Note:** This item appears when **CHAP Type** is Mutual.		The minimum length is 12 bytes and the maximum length is 16 bytes. **Notes:** • **Create New Password → Confirm New Password** – **ERROR → Invalid Password → Ok** – **ERROR → Invalid Input Range → Ok**
Reverse CHAP Status **Note:** This item appears when **CHAP Type** is Mutual.	• **Not Installed** (Default) • Installed	[Not Installed] if “Reverse CHAP Name” and “Reverse CHAP Secret” are not set. [Installed] if “Reverse CHAP Name” and “Reverse CHAP Secret” are set.
Save Changes	N/A	Must reboot System manually for changes to take place.
Back to Previous Page	N/A	Back to previous page.

Delete Attempts

Table 23. Delete Attempts

Item	Options	Description
Example, Attempt 1 **Note:** List of Attempts	- **[Empty]** (Default) - [X]	MAC: XX:XX:XX:XX:XX:XX, PFA: Bus XX | Dev XX | Func XX, “iSCSI Mode”: [%s1], “Internet Protocol”: [%s2] **Notes:** Exact value will be different depends on the attempt settings. - %s1 will be option name for iSCSI Mode. - %s2 will be the setting name for Internet Protocol.
Commit Changes and Exit	N/A	Commit Changes and Exit.
Discard Changes and Exit	N/A	Discard Changes and Exit.

Change Attempt Order

Table 24. Change Attempt Order

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

Network Stack Settings

Table 25. Network Stack Settings

Item	Options	Description
Network Stack	- **Enabled** (Default) - Disabled	Enable/Disable UEFI Network Stack.
IPv4 PXE Support	- **Enabled** (Default) - Disabled	Enable Ipv4 PXE Boot Support. If disabled Ipv4 PXE boot option will not be created.
IPv4 HTTP Support	- Enabled - **Disabled** (Default)	Enable Ipv4 HTTP Boot Support. If disabled Ipv4 HTTP boot option will not be created.
IPv6 PXE Support	- **Enabled** (Default) - Disabled	Enable Ipv6 PXE Boot Support. If disabled Ipv6 PXE boot option will not be created.
IPv6 HTTP Support	- Enabled - **Disabled** (Default)	Enable Ipv6 HTTP Boot Support. If disabled Ipv6 HTTP boot option will not be created.

Table 25. Network Stack Settings (continued)

Item	Options	Description
PXE boot wait time	0	Wait time in seconds to press **Esc** key to abort the PXE boot. Use either **+/-** or numeric keys to set the value. **Note: ERROR → Invalid Input Rang → Ok**
Media detect count	1	Number of times presence of media will be checked. Use either +/- or numeric keys to set the value. **Note: ERROR → Invalid Input Rang → Ok**

Network Boot Settings

Table 26. Network Boot Settings

Item	Description
The table lists MAC, VLAN Configuration List, Ipvx, etc. in the system: Example: • MAC: XX:XX:XX:XX:XX:XX • Onboard PFA XX:XX:XX	Set the boot configuration parameters on MAC XX:XX:XX:XX:XX:XX PCI Function Address: Bus XX:Dev XX:Func: XX

HTTP Boot Configuration

Notes:

- When you enable **Network → Network Stack Setting → IPv4 HTTP Support** or **Ipv6 HTTP support, HTTP Boot Configuration** will be displayed in Network page.
- When the network adapter is installed in the system, you will see the submenu, or nothing will be displayed in **HTTP Boot Configuration form**.

Table 27. HTTP Boot Configuration

Item	Description
Example: MAC:XX:XX:XX:XX:XX:XX HTTP Boot Configuration **Note:** List of NICs in the system.	Configure HTTP Boot parameters. (MAC: XXXXXXXXXXXX).

Tls Auth Configuration

Note: These forms are from AMI/Intel CRB. When you enable **Network**->**Network Stack Setting**->**Ipv4 HTTP Support** or **Ipv6 HTTP** support, Tls Auth Configuration will be displayed in Network page.

Table 28. Tls Auth Configuration

Item	Description
"Server CA Configuration" **on page 24**	Press **Enter** to configure Server CA.
Client Cert Configuration	Client cert configuration is unsupported currently.

Server CA Configuration

Table 29. Server CA Configuration

Item	Description
"Enroll Cert" on page 24	Press **Enter** to enroll cert.
"Delete Cert" on page 24	Press **Enter** to delete cert.

Enroll Cert

Table 30. Enroll Cert

Item	Description
Enroll Cert Using File	Enroll Cert Using File. **Note:** Pop up message box to select the storage device and then select the file.
Cert GUID	Input digit character in 11111111-2222-3333-4444-1234567890ab format. **Note:** Pop up message box to input Cert GUID.
Commit Changes and Exit	Commit 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	• **[Empty]** • [X]	GUID for Cert. **Note:** If there is no cert file, the default is empty.

Operating Modes

Select the operating mode based on your preference.

Table 32. Operating Modes

Item	Options	Description
Choose Operating Mode	• **Maximum Efficiency** (Default) • Custom Mode • Maximum Performance	Select the operating mode based on your preference. Power savings and performance are also highly dependent on hardware and software running on the system.
Determinisim Slider	• Power • **Performance** (Default)	When set to [Performance], performance is more predictable (deterministic) and operates at the lowest common denominator among the cores. But aggregate peak performance may be reduced. When set to [Power], cores can scale frequency independently. Aggregate performance may be higher, but predictability is lower.

Table 32. Operating Modes (continued)

Item	Options	Description
Core Performance Boost	• Disabled • **Enabled** (Default)	When set to [Enabled], cores can go to turbo frequencies.
cTDP	• Maximum • Manual • **Auto** (Default)	Set the maximum power consumption for the processor. **[Auto]** sets cTDP=TDP for the installed processor SKU. **[Maximum]** sets the maximum allowed cTDP value for the installed processor SKU. Usually, maximum is greater than TDP. If a manual value is entered that is larger than the max value allowed, the value will be internally limited to the maximum allowable value. cTDP is only configurable before OS boot.
cTDP Manual	[0]	Set the maximum power consumption for the processor. **[Auto]** sets cTDP=TDP for the installed processor SKU. **[Maximum]** sets the maximum allowed cTDP value for the installed processor SKU. Usually, maximum is greater than TDP. If a manual value is entered that is larger than the max value allowed, the value will be internally limited to the maximum allowable value. cTDP is only configurable before OS boot.
Package Power Limit	• Maximum • Manual • **Auto** (Default)	Sets the processor package power limit. If [Auto] is selected, it will be set to the maximum value allowed by the installed processor. If a manual value is entered that is larger than the maximum value allowed, the value will be internally limited to the maximum allowable value. The maximum value allowed for PPL is the cTDP limit. Compared to cTDP, PPL can also be changed at runtime and PPL supports a much lower effective limit than cTDP.
Package Power Limit Manual	[0]	Package Power Limit (PPT) [W].
Memory Speed	• Maximum • xxxx MHz • Minimum	The option number of the memory speed is changed dynamically according to the combination of the installed processor SKU, DIMM type, number of DIMMs per channel, and system board support. The system operates at the rated speed of the slowest DIMM in the system when populated with different speed DIMMs. If DIMMs are installed with a rated speed below 3600, this will result in the memory speed getting set to the Minimum value.
Efficiency Mode	• **Enabled** (Default) • Disabled	Enables/disables efficiency mode. When enabled, uses power efficiency optimized CCLK DPM settings.
Global C-state Control	• Disabled • **Enabled** (Default)	Global enables/disable for IO based C-state generation and DF C-states.

Table 32. Operating Modes (continued)

Item	Options	Description
DF P-states	• **Auto** (Default) • P0 • P1 • P2 • P3 • P4	When [Auto] is selected, the processor DF P-states (uncore P-states) will be dynamically adjusted. That is, their frequency will dynamically change based on the workload. Selecting P0, P1, P2, P3 or P4 forces the DF to a specific P-state frequency.
DF C-States	• Disabled • **Enabled** (Default)	Enables/disable data fabric (DF) C-states. Data fabric C-states may be entered when all cores are in CC6.
MONITOR/MWAIT	• **Enabled** (Default) • Disabled	MONITOR/MWAIT instructions are used to engage C-states. Some operating systems will re-enable C-states even when they are disabled in CMOS. To prevent this: 1. Disable MONITOR/MWAIT. 2. Choose **Custom Mode** in **Operating Mode** and **Disabled** in **Global C-state Control** located under **System Setting** submenu.
P-state 1	• **Enabled** (Default) • Disabled	Enable/disable processor P1 P-state.
P-State 2	• **Enabled** (Default) • Disabled	Enable/disable processor P2 P-state.
Memory Power Down Enable	• **Enabled** (Default) • Disabled	Enable/disable low-power features for DIMMs.
NUMA Nodes per Socket	• NPS0 • **NPS1** (Default) • NPS2 • NPS4	Specify the number of desired NUMA nodes per processor socket (e.g. NPS1 means 1 NUMA per socket). NPS0 will attempt to interleave the 2 processor sockets together (non-NUMA mode).
L1 Stream HW Prefetcher	• **Enabled** (Default) • Disabled	Enable/disable L1 stream HW prefetcher. Fetches the next cache line into the L1 cache when cached lines are reused within a certain time period or accessed sequentially.
L2 Stream HW Prefetcher	• **Enabled** (Default) • Disabled	Enable/disable L2 stream HW prefetcher. Fetches the next cache line into the L2 cache when cached lines are reused within a certain time period or accessed sequentially.
SMT Mode	• **Enabled** (Default) • Disabled	Can be used to disable symmetric multithreading. To re-enable SMT, a power cycle is needed after selecting Enable.

Table 32. Operating Modes (continued)

Memory Interleave	• **Enabled** (Default) • Disabled	Enable or disable memory interleaving. Note that the NUMA nodes per socket value will be honored regardless of this setting.
Chipselect Interleaving	• **Disabled** (Default) • Auto	This setting specifies if the system should use a DRAM rank also known as chipselect interleaving. This feature will spread memory accesses across the banks of memory within a channel and will increase memory block access performance. This setting requires that the populated DIMMs have the same bank size, type, and that the number of banks is a power of two. It is strongly recommended that DIMMs with the same part number be populated.
ACPI SRAT L3 Cache as NUMA Domain	• **Enabled** (Default) • Disabled	When enabled, each CCX in the system will be declared as a separate NUMA domain. When disabled, memory addressing/NUMA nodes per socket will be declared.
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.

Power

Use this menu to configure power plan options.

Table 33. Power

Item	Options	Description
ACPI Fixed Power Button	• **Enabled** (Default) • Disabled	Enable/Disable ACPI Fixed Power Button. When setting as disabled, physically pressing the power button on front of the system won't execute the Operating System's Power Button Policy such as shutdown, turn off monitor, etc. Also, when disabled the **"Shut down OS and ..."** options under the iMM Server Power Actions feature will be disabled.
Efficiency Mode	• **Enabled** (Default) • Disabled	Enable/disable efficiency mode. When [Enabled] is selected, use power efficiency optimized CCLK DPM settings.
PCIe Power Brake	• Reactive • **Proactive** (Default) • Disabled	PCIe Power Brake quickly reduces the power consumption and performance of high-powered PCIe devices. Performance of PCIe devices that are low power are not impacted by this setting. A high powered PCIe device is one that is rated at 75W TDP or greater.

Processors

This menu offers options to change the processor settings.

Table 34. Processors

Item	Options	Description
Determinism Slider	• Power • **Performance** (Default)	When set to [Performance], performance is more predictable (deterministic) and operates at the lowest common denominator among the cores. But aggregate peak performance may be reduced. When set to [Power], cores can scale frequency independently. Aggregate performance may be higher, but predictability is lower.
Core Performance Boost	• Disabled • **Enabled** (Default)	When set to [Enable], cores can go to turbo frequencies.
cTDP	• Maximum • Manual • **Auto** (Default)	Set the maximum power consumption for the processor. [Auto] sets cTDP=TDP for the installed processor SKU. [Maximum] sets the maximum allowed cTDP value for the installed processor SKU. Usually, maximum is greater than TDP. If a manual value is entered that is larger than the max value allowed, the value will be internally limited to the maximum allowable value. cTDP is only configurable before OS boot.

Table 34. Processors (continued)

Item	Options	Description
cTDP Manual	[0]	Set the maximum power consumption for the processor. [Auto] sets cTDP=TDP for the installed processor SKU. [Maximum] sets the maximum allowed cTDP value for the installed processor SKU. Usually, maximum is greater than TDP. If a manual value is entered that is larger than the max value allowed, the value will be internally limited to the maximum allowable value. cTDP is only configurable before OS boot.
Package Power Limit	• Maximum • Manual • **Auto** (Default)	Set the processor package power limit. If [Auto] is selected, it will be set to the maximum value allowed by the installed processor. If a manual value is entered that is larger than the maximum value allowed, the value will be internally limited to the maximum allowable value. The maximum value allowed for PPL is the cTDP limit. Compared to cTDP, PPL can also be changed at runtime and PPL supports a much lower effective limit than cTDP.
Package Power Limit Manual	[0]	Package Power Limit (PPT) [W].
Global C-state Control	• Disabled • **Enabled** (Default)	Global enables/disable for IO based C-state generation and DF C-states.
DF P-states	• **Auto** (Default) • P0 • P1 • P2 • P3 • P4	When [Auto] is selected, the processor DF P-states (uncore P-states) will be dynamically adjusted. That is, their frequency will dynamically change based on the workload. Selecting P0, P1, P2, P3 or P4 forces the DF to a specific P-state frequency.
DF C-States	• Disabled • **Enabled** (Default)	Enable/disable data fabric (DF) C-states. Data fabric C-states may be entered when all cores are in CC6.
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 CMOS. To prevent this: 1. Disable MONNITOR/MWAIT. 2. Choose **Custom Mode** in **Operating Mode** and **Disabled** in **Global C-state Control** located under **System Setting** submenu.
P-state 1	• **Enabled** (Default) • Disabled	Enable/disable processor P1 P-state.
P-State 2	• **Enabled** (Default) • Disabled	Enable/disable processor P2 P-state.

Table 34. Processors (continued)

Item	Options	Description
ACPI SRAT L3 Cache as NUMA Domain	• Enabled • **Disabled** (Default)	When [Enabled], each CCX in the system will be declared as a separate NUMA domain. When [Disabled], memory addressing/NUMA nodes per socket will be declared.
L1 Stream HW Prefetcher	• **Enabled** (Default) • Disabled	Enable/disable L1 stream HW prefetcher. Fetch the next cache line into the L1 cache when cached lines are reused within a certain time period or accessed sequentially.
L2 Stream HW Prefetcher	• **Enabled** (Default) • Disabled	Enable/disable L2 Stream HW Prefetcher. Fetch the next cache line into the L2 cache when cached lines are reused within a certain time period or accessed sequentially.
L1 Stride Prefetcher	• Disabled • **Enabled** (Default)	Enable/disable L1 Stride Prefetcher. Use memory access history to fetch additional data lines into L1 cache when each access is a constant distance from the previous. Some workloads may benefit from having it [Disabled].
L1 Region Prefetcher	• Disabled • **Enabled** (Default)	Enable/disable L1 Region Prefetcher. Fetch additional data lines into L1 cache when the data access for a given instruction tends to be followed by a consistent pattern of subsequent accesses. Some workloads may benefit from having it [Disabled].
L2 Up/Down Prefetcher	• Disabled • **Enabled** (Default)	Enable or disable L2 Up/Down Prefetcher. Uses memory access history to determine whether to fetch the next or previous line for all memory accesses. Some workloads may benefit from having it [Disabled].
SMT Mode	• **Enabled** (Default) • Disabled	Can be used to disable symmetric multithreading. To re-enable SMT, a power cycle is needed after selecting [Enabled].
CPPC	• **Enabled** (Default) • Disabled	CPPC (cooperative processor performance control) is a way for the OS to influence the performance of a CPU on a contiguous and abstract scale without knowledge of power budgets or discrete processor frequencies.
BoostFmax	• **Auto** (Default) • Manual	Maximum boost frequency. [Auto] set the boost frequency to the fused value for the installed processor. When a manual value is entered, the value entered is a 4 digit number representing the maximum boost frequency in MHZ. The value entered applies to all cores.

Table 34. Processors (continued)

Item	Options	Description
BoostFmax Manual	[0]	Maximum boost frequency. [Auto] set the boost frequency to the fused value for the installed processor. When a manual value is entered, the value entered is a 4 digit number representing the maximum boost frequency in MHZ. The value entered applies to all cores.
SVM Mode	• Disabled • **Enabled** (Default)	Enable/disable processor Virtualization.
APIC Mode	• xAPIC • x2APIC • **Auto** (Default)	APIC Mode. [xAPIC] scales to only 255 hardware threads. [x2APIC] scales beyond 255 hardware threads but is not supported by some legacy OS versions. [Auto] uses [x2APIC] only if 256 hardware threads are in the system. Otherwise xAPIC is used.
SEV-SNP Support	• Enabled • **Disabled** (Default)	Enable the support for Secure Encrypted Virtualization and Secure Nested Paging.
HSMP Support	• Disabled • Enabled • **Auto**(Default)	Select HSMP support enable or disable.
Enhanced REP MOVSB/STOSB	• Disabled • **Enabled**(Default)	(ERSM) Can be disabled for analysis purposes as long as OS supports it.
Number of Enabled Processor Cores Per Socket	**All** (Default) List of all available core counts based on CCDs and Cores Per CCD.	Select the total number of enabled CPU cores per socket to be activated. Options available are dependent on CPU SKU topology. **Note:** Reducing the number of processor cores activated can adversely impact performance.
"Secured-Core" on page 31	N/A	Secured-Core configuration setup page.
"Processor Details" on page 32	N/A	Display summary of the installed processors.

Secured-Core

Item	Operation	Description
Secured-Core		
Secured-Core	• **Custom** (Default) • Enabled	Enable Secured-Core support. When Secured-core is "Enabled", the 4 related settings are 'Enabled' and locked. When Secured-core is "Custom" ,the related settings can be changed independently as needed. If all 4 related settings are 'Enabled', it is effectively equivalent to Secured-core being 'Enabled'.
IOMMU	• Disabled • **Enabled** (Default)	Enable/Disable IOMMU.

Item	Operation	Description
DMAr Support	• **Disabled** (Default) • Enabled	Enable DMAr system protection during POST.
DMA Protection	• **Disabled** (Default) • Enabled	Enable DMA remap support in IVRS IVinfo Field.
DRTM Virtual Device Support	• **Disabled** (Default) • Enabled	Enable DRTM ACPI virtual device.
TSME	• **Disabled** (Default) • Enabled	Transparent SME: • AddrTweakEn = 1 • ForceEncrEn = 0 • DataEncrEn = 1
DRTM Memory Reservation	• **Disabled** (Default) • Enabled	Reserve 128MB memory below Bottom IO for DRTM. It is required to be enabled for Secured-Core Server function.

Processor Details

Table 35. Processor Details

Item	Format	Description
Processor Socket	• Socket 1 • Socket n	Processor Socket Table.
Processor ID	ASCII string	Tag for the Processor ID.
Processor Frequency	ASCII string	Value for the Processor Frequency.
Processor Revision	ASCII string	Value for the Microcode Revision.
L1 Cache RAM	ASCII string	Amount of L1 Cache RAM.
L2 Cache RAM	ASCII string	Amount of L2 Cache RAM.
L3 Cache RAM	ASCII string	Amount of L3 Cache RAM.
PSB Fusing Status	ASCII string	Platform Secure Boot fusing status in processor: • [Fused] processor is fused for PSB enabling • [Unfused] processor is not fused for PSB and it is in neutral state
Cores Per Socket (Supported/ Enabled)	ASCII strings	Number of supported and enabled processor cores per processor socket.
Threads Per Socket (Supported/Enabled)	ASCII strings	Number of supported and enabled processor threads per processor socket.
Dies Per CPU (Supported/ Enabled)	ASCII strings	The number of dies per installed processor can be used to calculate the total activated cores based. See the "**Number of Enabled CPU Cores Per Socket**" menu selection.
Processor 1 Version	ASCII string	Version of Processor 1.
Processor n Version	ASCII string	Version of Processor n.

Recovery and RAS

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

Table 36. Recovery and RAS

Item	Description
"POST Attempts" **on page 33**	Configure the number of attempts to POST before the recovery mechanisms is invoked.
"Advanced RAS" on page 35	Choose whether to enable various advanced RAS options.
"Disk GPT Recovery" **on page 35**	Disk GPT (GUID Partition Table) Recovery Options.
"System Recovery" on page 36	Configure system recovery settings.

POST Attempts

Table 37. POST Attempts

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

1. Press power button to do power off and then power on at "UEFI:DXE INIT" for the times set in "POST Attempts Limit", then allow server finish the POST, the message box below would be popped up.

1st line	The number of consecutive failed POST attempts reached the limit.
2nd line	System booted with factory default settings.
3th line	Press any key to enter Setup Utility to modify previously saved settings.
4th line	If no key is pressed,
5th line	system will automatically perform a warm reboot with previously saved settings.

2. Do not press any key, and repeat the actions in step 1 again, the message box below would be popped up.

1st line	The number of consecutive failed POST attempts reached the limit.
2nd line	System booted with factory default settings.
3th line	Press any key to enter Setup Utility to modify previously saved settings.
4th line	If no key is pressed,
5th line	system will automatically perform a warm reboot with previously saved settings.

3. Do not press any key, and repeat the actions in step 1 for the 3rd time, the message box below would be popped up.

1st line	The number of consecutive failed POST attempts reached the limit.
2nd line	System booted with factory default settings.
3th line	Press any key to enter Setup Utility to modify previously saved settings.
4th line	If no key is pressed,
5th line	system will shutdown.

4. Repeat action in step 1 and press any key when message box is popped up. After any key is pressed, below message box is popped up.

1st line	The number of consecutive failed POST attempts reached the limit.
2nd line	System booted with factory default settings.
3th line	Press any key to enter Setup Utility to modify previously saved settings.
4th line	If no key is pressed,
5th line	system will automatically do warm reboot with previously saved settings
6th line	A key press has been detected, system will enter Setup Utility soon.

5. Use OneCLI to change any settings. Repeat action in step 1.

1st line	The number of consecutive failed POST attempts reached the limit.
2nd line	System booted with factory default settings.
3th line	Previously saved settings have been changed externally through the BMC.
4th line	Press any key to enter Setup Utility to view or modify the new settings.
5th line	If no key is pressed,
6th line	system will automatically do cold reboot with the new settings.

6. Use OneCLI to change any settings. Repeat action in step 1 and press any key.

1st line	The number of consecutive failed POST attempts reached the limit.
2nd line	System booted with factory default settings.
3th line	Previously saved settings have been changed externally through the BMC.
4th line	Press any key to enter Setup Utility to view or modify the new settings.
5th line	If no key is pressed,

6th line	system will automatically do cold reboot with the new settings.
7th line	Key is pressed, will enter Setup Utility soon.

Advanced RAS

Table 38. Advanced RAS

Item	Options	Description
PCI Error Recovery	• **Enabled** (Default) • Disabled	Allow the system to recover from an uncorrectable PCIe fault when [Enabled]. The faulting PCIe device will be disabled for error containment and the OS will be notified to rescan the PCIe buses. An uncorrectable PCIe fault will result in an NMI when [Disabled].
Platform First Error Handling	• **Enabled** (Default) • Disabled	Enable/disable PFEH, cloak individual banks, and mask deferred error interrupts from each bank.

Disk GPT Recovery

Table 39. Disk GPT Recovery

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

Table 40. Disk GPT Recovery Message Box

Message Box	Comment
DiskGUID: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx Primary/Backup GPT corruption detected. Press **R** to repair or **N** to skip	This message box is popped up only when “**Disk GPT Recovery**” is set to [Manual] and Primary or Backup GPT is corrupted.
Repairing GPT, please wait...	This Message Box only display if user press “**R**” or “**r**” while “Press **R** to repair or **N** to skip” message Box display.

System Recovery

Table 41. System Recovery

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

Security

Use this menu to configure system security settings.

Table 42. Security

Item	Description
"Secure Boot Configuration" on page 36	Configure Secure Boot options.
"Trusted Platform Module" **on page 41**	Configure the TPM Setup options.

Secure Boot Configuration

Table 43. Secure Boot Configuration

Item	Operation	Description
Secure Boot Status	• Disabled • Enabled	Display the current secure boot status.
Secure Boot Mode	• Setup Mode • User Mode • Audit Mode • Deploy Mode	System will do secure boot authentication when "Secure Boot Mode" is [User Mode] and secure boot is enabled.
Secure Boot Setting	• Enabled • **Disabled** (Default)	Secure Boot feature is Active if Secure Boot is Enabled, Platform Key(PK) is enrolled and the System is in User mode. The mode change requires platform reset Legacy BIOS will be disabled when secure boot is enabled.

Table 43. Secure Boot Configuration (continued)

Item	Operation	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, KEK, DB, and DBX will be deleted after reboot. **[Delete PK]**: PK will be deleted after reboot. **Secure Boot Mode** is [Setup Mode] and **Secure Boot Policy** is [Custom Policy] after PK is deleted. [Reset All Keys to Default]: All keys will be set to factory defaults and **Secure Boot Policy** is [Factory Policy] after reboot. **Notes:** • Confirm change “Secure Boot Policy”? – Yes – No • Press 'Yes' to install factory default keys. – Yes – No • Secure Boot Policy **Secure Boot Policy** is changed successfully.
View Secure Boot Keys	N/A	View the details of: • PK (Platform Key) • KEK (Key Exchange Key) • DB (Authorized Signature Database) • DBX (Forbidden Signature Database)
Secure Boot Custom Policy	N/A	Customize • PK (Platform Key) • KEK (Key Exchange Key) • DB (Authorized Signature Database) • DBX (Forbidden Signature Database) User could enter this page when **Secure Boot Policy** is [Custom Policy].

View Secure Boot Keys

Table 44. View Secure Boot Keys

Item	Options	Description
Secure Boot variable	Column shows PK, KEK, DB, and DBX	
Size	Column shows the number of keys bytes	
Keys	Column shows the Number of certificates (integer)	
Key Source	• **Factory** (Default) • No Keys • Mixed • Customized	
PK		View Certificate in PK (Platform Key). **Note:** The system can only have one PK.
KEK		View all Certificates in KEK (Key Exchange Key).
DB		View all Certificates in DB (Authorized Signature Database).
DBX		View all Certificates in DBX (Forbidden Signature Database).

Message box information for Key Detail

Message Box	Comment
%s1 List | Sig.Type | Count | Size | Owner GUID | Certificate Legend Key information of each section above	This message box is popped up when press **Enter** on each Key items.

Secure Boot Custom Policy

Table 45. Secure Boot Custom Policy

Item	Options	Description
Enroll Efi Image		Enroll the SHA256 hash of the selected EFI image binary into the Authorized Signature Database (DB). **Notes: Select a File system → Select File → Enroll Efi Image → Confirm update of '%s1' with content from the file '%s2** • Yes • No %s1 can be PK %s2 is the file name selected **Success → Ok**

Table 45. Secure Boot Custom Policy (continued)

Item	Options	Description
Secure Boot variable	Column shows PK, KEK, DB, and DBX	
Size	Column shows the number of key bytes	
Keys	Column shows the number of certificates (integer)	
Key Source	• **Factory** (Default) • No Keys • Mixed • Customized	
PK		Enroll a PK (from a Public Key Certificate file format) or delete the existing PK. **Notes:** • The system can only have one PK. • – PK – Add – Details – Delete • **Select a File system → File systems are listed → Select File → Input File Format → Public Key Certificate → Public Key Certificate → Add → Confirm update of '%s1' with content from the file '%s2'** – Yes – No %s1 can be PK %s2 is the file name selected **Add → Success → Ok** **Add → Failed → Ok** • **Delete Security Key/Database → WARNING: Removing PK will change "Secure Boot Mode" to [Setup Mode] → Ok** • **Delete Security Key/Database → Confirm deletion of 'PK' variable from NVRAM** – Yes **Note: Delete Security Key/Database → Success → Ok** – No

Table 45. Secure Boot Custom Policy (continued)

Item	Options	Description
KEK		Enroll a KEK entry (from a Public Key Certificate file format), or delete an existing entry from the KEK. **Notes:** • **KEK → Details → Add → Delete one Key/Certificate → Delete this variable** • **Select a File system → File systems are listed → Select File → Input File Format → Public Key Certificate → Authenticated Variable → Confirm update of '%s1' with content from the file '%s2'** – Yes – No %s1 can be PK %s2 is the file name selected **Add → Success → Ok** **Add → Failed → Ok** • **Delete Security Key/Database → Success → Ok** • Delete Security Key/Database. Press 'Yes' to delete the 'KEK' variable. This will delete all Certificates in 'KEK'! • **Delete Security Key/Database → Confirm deletion of 'KEK' variable form NVRAM** – Yes **Note: Delete Security Key/ Database → Success → Ok** – No
DB		Enroll a DB entry (from a Public Key Certificate file format or an EFI image file), or delete an existing entry from the DB. **Notes:** • **DB → Details → Add → Delete one Key/Certificate → Delete this variable** • **Select a File system → File systems are listed → Select File → Input File Format → Public Key Certificate → Authenticated Variable → EFI PE/ COFF image → Confirm update of '% s1' with content from the file '%s2'** – Yes – No %s1 can be PK

Table 45. Secure Boot Custom Policy (continued)

Item	Options	Description
		%s2 is the file name selected **Add → Success → Ok** **Add → Failed → Ok** - **Delete Security Key/Database → Confirm certificate removal from "DB" database** – Yes **Note: Delete Security Key/ Database → Success → Ok** – No
DBX		

Message box information for security boot

Message Box	Comment
Secure Boot Violation An unauthorized EFI image is detected. To use this image, enroll this EFI image or disable secure boot at "**Secure Boot Configuration**" in Setup Utility. Ok	This message box is popped up when booting form an unsigned shell.efi or OS with secure boot is enabled.

Trusted Platform Module

The menu below is for TPM Firmware Update from TPM2.0 to TPM1.2.:

Table 46. Trusted Platform Module

Item	Description
TPM 2.0	Configure the TPM 2.0 Setup options.
TPM Versoin	
Update to TPM1.2 compliant	**CAUTION:** **Change is effective after system reboot. You can only switch TPM firmware 128 times.** Update to TPM1.2 compliant is a significant change to the system since TPM 1.2 and 2.0 are not compatible. All TPM data will be cleared! Do you want to proceed? - <Y>: Reboot system – Successfully cleared TPM, please reboot system to begin TPM version update progress. Press <Enter> to continue. - <ESC>: Abort and discard the change

The menu below is for TPM 2.0

Table 47. Trusted Platform Module (TPM2.0)

Item	Options	Function description
TPM Status		
TPM Vendor	N/A	Display TPM vendor
TPM Firmware Version	N/A	Display the current firmware version of the TPM device.
[TPM Settings]		
TPM2 Operation	• **No Action** (Default) • Clear • TPM Device has been cleared.	Select [Clear] to clear TPM data. • This will erase the contents of the TPM. System reboot required. • Operation success, system reboot is required to take effect. Press <Enter> to continue. TPM Device has been cleared. Error clearing TPM. Press <Enter>to continue.
SHA-1 PCR Bank	• Enabled • **Disabled** (Default)	Enable or disable SHA-1 PCR Bank.

The menu below is for TPM Firmware Update from 1.2 to 2.0

Table 48. Trusted Platform Module

Item	Description
TPM 1.2	Configure TPM 1.2 Setup options.
TPM Version	
Update to TPM2.0 compliant	**CAUTION:** **when update TPM version to TPM2.0 compliant, do not boot a legacy OS due to security consideration. Change is effective after system reboot. You can only switch TPM firmware 128 times.** Update to TPM2.0 compliant is a significant change to the system since TPM 2.0 and 1.2 are not compatible. All TPM data will be cleared! Do you want to proceed? • <Y>: Reboot system – Successfully cleared TPM, please reboot system to begin TPM version update progress. Press <Enter> to continue. • <ESC>: Abort and discard the change

This menu is used to update the TPM 2.0 Firmware

Table 49. Trusted Platform Module (TPM 2.0)

Item	Options	Description
TPM Status		
TPM Vendor		Display TPM Vendor
TPM Firmware Version		Display the current firmware version of the TPM device.
TPM Device Sate	Dynamic String depend on current TPM status	Display the current state of the TPM Device.
TPM Ownership	Dynamic String depend on current TPM status	Display the current status of ownership
[TPM Settings]		
TPM Device	• **Enabled** (Default) • Disabled	Enable or disable the TPM Device. Operation success, system reboot is required to take effect. Press <Enter > to continue.
TPM State	• **Activate** (Default) • Deactivate	Activate/deactivate the TPM device. Operation success, system reboot is required to take effect. Press <Enter > to continue.
TPM Operation	• **No Action** (Default) • Clear • TPM1.2 Device has been cleared	Select [Clear] to clear TPM data. • This will erase the contents of the TPM. System reboot required. • Operation success, system reboot is required to take effect. Press <Enter> to continue. TPM1.2 Device has been cleared. • Error clearing TPM. TPM deactivated, reboot required. Press <Enter>to continue. • Error clearing TPM. TPM deactivated, reboot required. Press <Enter>to continue. • Error clearing TPM. TPM deactivated, reboot required. Retry after reboot.

This menu is for TPM 1.2

Table 50. Trusted Platform Module (TPM 1.2)

Item	Options	Description
TPM Status		
TPM Vendor	N/A	Display TPM Vendor
TPM Firmware Version	N/A	Display the current firmware version of the TPM device.
TPM Device Sate	Dynamic String depend on current TPM status	Display the current state of the TPM Device.

Table 50. Trusted Platform Module (TPM 1.2) (continued)

Item	Options	Description
TPM Ownership	Dynamic String depend on current TPM status	Display the current status of ownership.
[TPM Settings]		
TPM Device	• **Enabled** (Default) • Disabled	Enable/disable the TPM Device. Operation success, system reboot is required to take effect. Press <Enter> to continue.
TPM State	• **Activate** (Default) • Deactivate	Activate/deactivate the TPM State. Operation success, system reboot is required to take effect. Press <Enter> to continue.
TPM Operation	• **No Action** (Default) • Clear • TPM1.2 Device has been cleared	Select [Clear] to clear TPM data. • This will erase the contents of the TPM. System reboot required. • Operation success, system reboot is required to take effect. Press <Enter> to continue. TPM1.2 Device has been cleared. • Error clearing TPM. TPM deactivated, reboot required. Press <Enter>to continue. • Error clearing TPM. TPM deactivated, reboot required. Press <Enter>to continue. • Error clearing TPM. TPM deactivated, reboot required. Retry after reboot.

Storage

This menu allows you to manage storage adapter options.

Table 51. Storage

Item	Description
"NVMe" **on page 45**	NVMe Devices list.
Notes: • The device list is based on your system installation and system setting. The contents in this page are dynamically generated by installed storage vendor's HII utilities. This will not enlist in setup spec. • The device entries will contain slot number after 18B. These entries would not be sorted by any order. • Onboard NVMe devices will not list when VMD is enabled.	
"RAM Disk Configuration" **on page 46**	Press <Enter> to add/remove RAM disks.
"SATA Drives" **on page 46**	Display SATA information.

NVMe

Table 52. NVMe

Item	Description
Bay X: NVMe Bus-Dev-Fun	Bay X: NVMe Bus-Dev-Fun

Notes:

- All onboard NVMe will remove from the Storage and Foreign Device pages then only display on this page.
- Format:
  - Bay X: This string define by platform, each platform may display a different string, X is bay number.
  - Bus-Dev-Fun is PCI address value.

NVMe Detail Information

Table 53. NVMe Detail Information

Item	Format	Description
Model Name	ASCII string	Model Name
Serial Number	ASCII string	Serial Number
Firmware Revision	ASCII string	Firmware Revision
Vendor ID	0xXXXX (XXXX is hex number)	Vendor ID
Device ID	0xXXXX (XXXX is hex number)	Device ID
Subsystem Vendor ID	0xXXXX (XXXX is hex number)	Subsystem Vendor ID
Subsystem ID	0xXXXX (XXXX is hex number)	Subsystem ID
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
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 (TB will change to GB or MB when the size too small)	Total Size

Table 53. NVMe Detail Information (continued)

Item	Format	Description
Device driver data link:		
Device HII Title	N/A	Device Hii description **Note:** Title and description are taken from device. If the device does not provide Hii data for setup display, will display N/A.

RAM Disk Configuration

Table 54. RAM Disk Configuration

Item	Options	Description
Disk Memory Type:	• **Boot Service Data** (Default) • Reserved	Specifies type of memory to use from available memory pool in system to create a disk.
"Create raw" **on page 46**		Create a raw RAM disk.
Create from file		Create a RAM disk from a given file.
Created RAM disk list:		
Remove selected RAM disk(s)	Executing item	Remove selected RAM disk(s).

Create raw

Table 55. Add A Raw RAM Disk

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

SATA Drives

Table 56. SATA Drives

Item	Description
Bay X Model Name	Bay X: details: • (*) **Model Number:** XXXX • (*) **Serial Number:** YYYY

Notes:

- All onboard SATA will remove from the Storage and Foreign Device pages then only display on this page.
- Format:

- Bay X: This string is defined by platform, each platform may display a different string, X is bay number.
- If there is no SATA drive installed, this page is blank.

SATA Drive Information

Table 57. 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 TB will change to GB or MB when the size too small	Size

Date and Time

Use this menu to set the local Date and Time of the system.

Table 58. Date and Time

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

Start Options

Use this menu to select start option for next boot.

Table 59. Start Options

Item	Function
CD/DVD ROM	VenHw(B2AD3248-4F72-4950-A966-CFE5062DB83A,02000000)
Hard Disk	VenHw(B2AD3248-4F72-4950-A966-CFE5062DB83A,01000000)
Network	VenHw(B2AD3248-4F72-4950-A966-CFE5062DB83A,05000000)
USB Storage	VenHw(B2AD3248-4F72-4950-A966-CFE5062DB83A,04000000)

Note: The device entries will contain slot number after 18B. These entries would not be sorted by any order.

Boot Manager

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

Table 60. Boot Manager

Item	Operation	Description
Boot Sequence		
"Add Generic Boot Option" **on page 48**	N/A	Add one generic boot device as boot option.
Add UEFI Full Path Boot Option	N/A	Add one EFI application or one removable file system as boot option.
Delete Boot Option	N/A	Remove boot option(s) from "boot order".
Change Boot Order	N/A	Modify the ordering of selections within "Boot Order".
Set Boot Priority	N/A	Set boot priority of the devices in a device group.
Other Boot Functions		
"Boot From File" **on page 51**	Xxxx {xxxx-xxx-xxx…}	Boot the system from a specific file or a device.
Select Next One-Time Boot Option	N/A	Select the one-time boot option for next boot.
System		
Boot Modes	N/A	Change between UEFI boot mode and the legacy boot mode.
"Reboot System" **on page 52**	N/A	Prompt to reboot 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 61. Add UEFI Full Path Boot Option

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

Add UEFI Full Path Boot Option Message Box

Message Box	Comment
ERROR: Invalid Input Range → Ok	This message box is popped up when click "**Input the Description**" but inputting is invalid.
Select a File System	This message box is popped up when click "**Select Device Path Option**".
Select a File to Boot	This Message Box only display if user select device path in "**Select a File System**".
No Valid File System → No Valid File System Available → Ok	This message box is popped up when click "**Select Device Path Option**" but no valid file system is present.
WARNING: Please set Boot Option Name and File Path → Ok	This Message Box only display if user select "**Commit Changes and Exit**".
No Valid File → No Valid File Available in the Selected File System → Ok	This message box is popped up when click "**Select a File System**" but no valid file in a file system.
SUCCESS → Boot Option Created SuccessfullyFile System → Ok	This Message Box only display if user select "**Commit Changes and Exit**" but set valid parameters.

Delete Boot Option

Table 62. Delete Boot Option

Item	Options	Function description
CD/DVD Rom	[X]	VenHw(B2AD3248-4F72-4950-A966-CFE5062DB83A,02000000)
Hard Disk	[X]	VenHw(B2AD3248-4F72-4950-A966-CFE5062DB83A,01000000)
Network	[X]	VenHw(B2AD3248-4F72-4950-A966-CFE5062DB83A,05000000)
USB Storage	[X]	VenHw(B2AD3248-4F72-4950-A966-CFE5062DB83A,04000000)
Commit Changes and Exit	N/A	Save changes and exit.

Message box for "Delete Boot Option":

Message Box	Comment
Delete Boot Option → Boot Order requires at least one boot option → Press <Enter> to continue → Ok	This message box is popped up when deleting all boot options.

Change Boot Order

Table 63. Change Boot Order

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

Set Boot Priority

Set Boot Priority

Item	Description
"CD/DVD Priority" on page 50	Set boot priority in the CD/DVD group if multiple devices exist in the system.
"Hard Disk Priority" on page 50	Set boot priority in the Hard Disk group if multiple devices exist in the system.
"Network Priority" on page 51	Set boot priority in the Network group if multiple devices exist in the system.
"USB Priority" on page 51	Set boot priority in the USB group if multiple devices exist in the system.

CD/DVD Priority

Table 64. CD/DVD Priority

Item	Options	Description
Boot Priority	None	Change the boot priority for devices in the CD/DVD group.
Commit Changes and Exit	N/A	Save changes and exit.

Hard Disk Priority

Table 65. Hard Disk Priority

Item	Options	Description
Boot Priority	None	Change the boot priority for devices in the Hard Disk group.
Commit Changes and Exit	N/A	Save changes and exit.

Network Priority

Table 66. Network Priority

Item	Options	Description
Boot Priority	None	Change the boot priority for devices in the Network group.
Commit Changes and Exit	N/A	Save changes and exit.

USB Priority

Table 67. USB Priority

Item	Options	Description
Boot Priority	None	Change the boot priority for devices in the USB group.
Commit Changes and Exit	N/A	Save changes and exit.

Boot From File

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

Boot From File Message Box

Message Box	Comment
Select a File System	This message box is popped up when click “**Boot From File**”.
Select a File to Boot	This Message Box only display if user select device path in “**Select a File System**”.
No Valid File System → No Valid File System Available → OK	This message box is popped up when click “**Boot From File**” but no valid file system is present.
No Valid File → No Valid File Available in the Selected → File System → OK	This message box is popped up when click “**Boot From File**” but no valid file in a file system.

Select Next One-Time Boot Option

Table 68. Select Next One-Time Boot Option

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

Boot Mode

Table 69. Boot Mode

Item	Options	Description
System Boot Mode	• **UEFI Mode** (Default) • Legacy Mode	Drivers, option ROMs and OS loaders the “Boot Manager” attempt to boot. [UEFI Mode]: Run UEFI drivers and boot a UEFI OS loader. [Legacy Mode]]: Run UEFI drivers and boot a UEFI OS loader. **Note:** This setting will be forced to [UEFI Mode] when Legacy BIOS is disabled in **System Settings → Legacy BIOS → Legacy BIOS**.
Infinite Boot Retry	• Enabled • **Disabled** (Default)	Continuously retry the Boot Order. Ensure a bootable device is specified in “Boot Order”.
Prevent OS Changes To Boot Order	• Enabled • **Disabled** (Default)	When set to "Enable", UEFI will remove the boot option which is created by OS or OS Installer from Boot Order List.

Reboot System

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

Reboot System Message Box

Message Box	Comment
Reboot System Do you want to reboot system immediately? • **<Y>** Reboot system immediately. • **<ESC>** Return to System Setup.	This message box is popped up when click **Reboot System**.

BMC Settings

This menu allows you to configure the management controller.

Table 70. BMC Settings

Item	Options	Description
Power Restore Policy	• Always Off • Restore • Always On	Determine the mode of operation after loss of power. [Always Off]: System remains off upon power restore. [Restore]: System restores to the state it was before power failed. [Always On]: System turns on upon power restore. Allow a few minutes for the changes to take effect.
Power Restore Random Delay	• Enabled • Disabled	Provides a random delay between 1 and 15 seconds for Power On. If system state was on before power failed, the system will delay Power On once power is restored.

Table 70. BMC Settings (continued)

Item	Options	Description
Ethernet over USB interface	• Enabled • Disabled	[Enabled] for using the xClarity Essentials in-band update utility. [Disabled] will prevent xClarity Essentials and other applications that are running on the server from requesting the BMC to perform tasks. When user modifies the "Ethernet Over USB Interface" related settings, the setting values may keep stale for a while and do not immediately reflect the new settings.
"Network Settings" **on page 53**	N/A	Configure the network of the management controller.
Reset Factory Defaults Setting	N/A	Restore all management controller settings to factory defaults, including network configuration and credentials, the management controller will be restarted automatically. **Note: Attention → <Enter> Continue, <ESC> Return to Setup Utility → Ok → Error in retrieving BMC configuration. → Exit this page and try again later. → Error in retrieving BMC network configuration. → Exit this page and try again later.**
Restart BMC	N/A	Restart the BMC. **Note: BMC Restart command has been sent successfully. → BMC will now be inaccessible for several minutes. During this time, please do not attempt to make any further changes to any BMC settings.**

Network Settings

Attention: Must click the "Save Network Settings" at the bottom of this page to save any change on this page and its subpage.

Table 71. Network Settings

Item	Options	Description
Network Interface Port	• Dedicated • Shared	Select the System Management Network Interface Port.
Shared NIC on	**OCP Card**	Select the shared NIC port.
Fail-Over Rule	• None • Failover to shared (Optional Card ML2) • Failover to shared (Optional Card PHY) • Failover to shared (Onboard Port)	Setting to control Fail-Over types allowed.

Table 71. Network Settings (continued)

Item	Options	Description
Network Setting	• Synchronization • Independence	The item will be selectable when Fail-Over Rule enabled to onboard port or optional card. Setup the share mode network settings after changing "Synchronization" to "Independence" in nic failover mode.
Burned-in MAC Address	Unknown	
Hostname	Unknown	Change the host name. The new name should be within 1 to 63 characters.
DHCP Control	• Static IP • DHCP Enabled • DHCP with Fallback	Configure DHCP Control or manually configure a static IP address. Fallback will use static IP address if DHCP fails. Fallback will use static IP address if DHCP fails.
IP Address	**x.x.x.x**	Enter IP Address in dotted-decimal notation. **Note: Press <ESC> to return to Setup Utility → Invalid IP address! → ERROR → Invalid Input Range → Ok**
Subnet Mask	**x.x.x.x**	Enter Subnet Mask in dotted-decimal notation. **Note: Press <ESC> to return to Setup Utility → Invalid Subnet Mask! → ERROR → Invalid Input Range → OkPress <ESC> to return to Setup Utility**
Default Gateway	**x.x.x.x**	Enter Default Gateway in dotted-decimal notation. **Note: Invalid Gateway! → ERROR → Invalid Input Range → Ok**
IPv6	• Enabled • Disabled	Enable/disable IPv6 support on management port.
Local Link Address	Unknown	
VLAN Support	• Enabled • Disabled	Enable VLAN Support to specify the 802.1q VLAN ID on the management port network device.
VLAN ID	1	VLAN ID Range is 1 to 4094. **Note: ERROR → Invalid Input Range → Ok**

Table 71. Network Settings (continued)

Item	Options	Description
"Advanced Settings for BMC Ethernet" on page 55	N/A	Advanced Setting for BMC Ethernet.
Save Network Settings	N/A	Commit the changes to BMC. Please allow a few minutes for the changes to take effect. **Note: Network Settings have been saved successfully → Please allow a few minutes for the changes to take effect → Press <Enter> to Continue → Press <ESC> to return to Setup Utility → BMC Error – Cannot Save Network Settings!**

Advanced Settings for BMC Ethernet

Table 72. Advanced Settings for BMC Ethernet

Item	Options	Description
Autonegotiation	• No • Yes	• If auto-negotiation is 'No', you can manually choose the data rate and duplex mode. • If auto-negotiation is 'Yes', there is no manual configuration needed.
Data rate	• 100 Mb (Ethernet) • 10 Mb (Ethernet)	Amount of data to be transferred per second over LAN connection.
Duplex	• Half • Full	Type of communication channel used in your network. [Full]: Allow data to be transferred in both directions at once. [Half]: Allow data to be transferred in either one direction or the other, but not both at the same time.
Maximum Transmission Unit	**1500**	Specify the maximum size of a packet (in bytes) for the network interface. For IPv4-only networks, the valid MTU range is 68 – 1500. For networks that implement IPv6, the valid MTU range is 1280 – 1500. **Note:** **ERROR → Invalid Input Range → Ok**
Note: Changes will be valid after saving network settings in previous page.		

System Event Logs

Use this menu to clear or view system event logs.

Table 73. System Event Logs

Item	Description
“POST Event Viewer” **on page 56**	View the POST Event Viewer.
“System Event Log” **on page 56**	View the System Event Log.
Clear System Event Log	Clear the System Event Log.

POST Event Viewer

Table 74. POST Event Viewer

Item	Description
Entry [N]:	Information.

System Event Log

Table 75. System Event Log

Item	Description
Total SEL entries	Total number of System Event Logs retrieved from the BMC. This does not include any associated extended logs.
Previous Page	View the System Event Log.
Entry [N]:	Information.
Next Page	View the System Event Log.

User Security

Use this menu to set or change Power-On and Administrator passwords.

Table 76. User Security

Item	Description
“Password Rule and Policy” **on page 59**	Set password rule and policy.

Table 76. User Security (continued)

Item	Description
Set Power-On Password	Set the power-On password. The password can only contain the following characters (no white-space characters allowed): 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 combinations: • 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 8 characters if doesn't select other value in "Minimum password length" option. **Notes:** • Please type in your password. • Please type in your new password. • Please confirm your new password. • Power-On Password has been set successfully. • The password failed to meet the "Minimum password reuse cycle" requirements. • Please enter enough characters. Press <Enter> to continue. • The password can't be changed because the "Minimum password change interval" time is not exceeded. • The password does not meet the minimum password complexity requirements. Please check the help for "Set Power-On Password" or "Set Administrator Password" settings. • Passwords are not the same Press <Enter> to continue. • Incorrect Password. Press <Enter> to continue. • Passwords operation have unknown problem. Press <Enter> to continue. **Note:** When IPMI command has no response then pop out this message.
Clear Power-On Password	Clear Power-On password. **Notes:** • Power-On Password is not set. Press <Enter> to continue. • An existing Power-On Password will be deleted <Enter> continue. <ESC> Return to Setup Utility. • Power-On Password has been cleared successfully. Press <Enter> to continue.

Table 76. User Security (continued)

Item	Description
Set Administrator Password	Set the Administrator password. The password can only contain the following characters (no white-space characters allowed): 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 combinations: • 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 8 characters if doesn't select other value in "Minimum password length" option. **Notes:** • Please type in your password. • Please type in your new password. • Please confirm your new password. • Administrative Password has been set successfully. • The password failed to meet the "Minimum password reuse cycle" requirements. • The password can't be changed because the "Minimum password change interval" time is not exceeded. • The password does not meet the minimum password complexity requirements. Please check the help for "Set Power-On Password" or "Set Administrator Password" settings. • Please enter enough characters. Press <Enter> to continue. • Passwords are not the same. Press <Enter> to continue. • Incorrect Password. Press <Enter> to continue. • Passwords operation have unknown problem. Press <Enter> to continue. **Note:** When IPMI command has no response then pop out this message.
Clear Administrator Password	Clears Administrator password. **Notes:** • An existing Administrative Password will be deleted <ENTER> Continue. <ESC> Return to Setup Utility. • Administrative Password has been cleared successfully. Press <ENTER> to continue. • Administrative Password is not set. Press <ENTER> to continue.

Password Rule and Policy

Table 77. Password Rule and Policy

Item	Options	Function
Minimum password length	8-20	Input a value from 8 to 20. The minimum number of characters that can be used to specify a valid password. The length value will take affect right after the value get changed. “Save Setting” from Main Menu if would like to keep setting after system reboot.
Password expiration period	0-365	Input a value from 0 to 365. The number of days a password may be used before it must be changed. If set to 0 the passwords never expire.
Password expiration warning period	0-365	Input a value from 0 to 365. The number of days before receiving a warning about the expiration of the password. If set to 0 the passwords never warned.
Minimum password change interval	0-240	Input a value from 0 to 240. The number of hours that must elapse before changing a password. The value specified for this setting cannot exceed the value specified for the “Password expiration period”. If set to 0 the passwords may be changed immediately.
Minimum password reuse cycle	0-10	Input a value from 0 to 10. The minimum number of times a unique password must be set before reusing a previous password. If set to 0 the passwords may be reused immediately. The reuse cycle value will take affect right after the value get changed. “Save Setting” from Main Menu if would like to keep setting after system reboot.

Table 77. Password Rule and Policy (continued)

Item	Options	Function
Maximum number of login failures	0-100	Input a value from 0 to 100. The number of login attempts that can be made with an incorrect password before the user account is locked out. The account is locked out for the time specified in "Lockout period after maximum login failures". If set to 0 accounts are never locked. The failed login counter is reset to zero after a successful login.
Lockout period after maximum login failures	0-2880	Input a value from 0 to 2880. The number of minutes that must pass before a locked out user can attempt to login. Entering a valid password does not unlock the account during the lockout period. If set to 0 the accounts will not be locked out even if the "Maximum number of login failures" is exceeded.

- When password is expired, system should pop out menu to inform user the password is expired and ask user to set new password or not. If user select YES, direct user to set password menu. If user selects NO, the expired password will be cleared. The warning message is **"The password is expired. Press <Y> to set new password Press <N> to clear password"**.
- If the password reach Password expiration warning period, after user input correct password for POP or PAP, system should pop out **"The password is going to be expired in "x" days."** message where "x" stands for numbers of days password to be expired.
- If users try to change password when the time doesn't exceed Minimum password change interval, system should pop out **"The password can't be changed because the "Minimum password change interval" time is not exceeded."** warning message.
- When users try to set minimum password change interval to be a number exceed the value specified for the password expiration period or reverse, system should pop out **"Minimum password change interval" can't exceed the value specified for the "Password expiration period".**warning message.
- System should pop out warning message when the wrong password is entered **"Incorrect password entered."** If maximum login failures is set add the following **"The system will be locked in Y attempts."**
- System should pop out **"The system is locked due to the "maximum number of login failures" being exceeded. System will be unlocked in Y minutes."** warning message to notify users the system will be locked when users reach maximum number of login failures.
- System should pop out **"The password does not meet the minimum password complexity requirements. Please check the help for "Set Power-On Password" or "Set Administrator Password" settings."** warning message to notify users when the inputted passwords don't meet the password rules.
- When system is in lock state, system should show **"The system is locked due to the "maximum number of login failures" being exceeded. System will be unlocked in Y minutes."** Warning message on screen to notify users system is in lock state and also the time for system kept in lock state. "Y" value is depended on Lockout period after maximum login failures setting.
- If users try to set a password that is the same as the old password in reuse cycle. System should pop out **"The password failed to meet the "Minimum password reuse cycle" requirements."** where x is the Minimum password reuse cycle.

System reset or DC, and AC cycle should not release system from a lockout state. Only when the end of lockout time is reached, system can release from lockout state.

UEFI will store a timestamp variable when system need to be lockup and will compare the variable with current timestamp when boot if the variable existed.

Password rule and policy setting will not support change through ASU in GA.

F12 One Time Boot Device

Use this menu to manage boot devices in the system.

Table 78. Boot Devices Manager

Item	Options	Description
Legacy Mode	• [ ] • [X]	Override the "System Boot Mode" specified in the "Boot Mode" menu. "Set Option ROM Execution Order" setting under the "Devices and I/O Ports" menu may still affect boot ordering. Some network cards' legacy PXE boot option need have "PCI 64-Bit Resource Allocation" as "Disable" in the "Device and I/O Ports" menu. • CD/DVD Rom • Hard Disk • Network • USB Storage
List of UEFI Boot Options	N/A	Enter in specified Boot Device.

Appendix1:

A system reboots the first time during showing Setup Menu if the uEFI F/W has just been updated. This process works as design.

Appendix2:

The password field doesn't have a default value, which requires a range of numbers.

Appendix3:

If the item string of Text Mode does not match with LXPM Mode, please refer to the LXPM Specification.

Table A:

	Maximum Efficiency	**Maximum Performance**
Determinism slider	Performance	Power
Core performance boost	Enabled	Enabled
cTDP	Auto	Maximum
Package Power Limit	Auto	Maximum
Memory Speed	Maximum	Maximum

Efficiency Mode	Enabled	Disabled
Global C-state Control	Enabled	Enabled
DF P-states	Auto	Auto
DF C-states	Enabled	Enabled
MONITOR/MWAIT	Enabled	Enabled
P-State 1	Enabled	Enabled
P-State 2	Enabled	Enabled
Memory Power Down Enable	Enabled	Enabled
NUMA Nodes per Socket	NPS1	NPS1
L1 Stream HW Prefetcher	Enabled	Enabled
L2 Stream HW Prefetcher	Enabled	Enabled
SMT Mode	Enabled	Enabled
Memory Interleave	Enabled	Enabled
Chipselect Interleaving	Auto	Auto
ACPI SRAT L3 Cache as NUMA Domain	Disabled	Disabled
Acoustic modes	Disabled	Disabled

Appendix A. Notices

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

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

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

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

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

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

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

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

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

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

Trademarks

LENOVO and LENOVO logo are trademarks of Lenovo.

Lenovo