

Lenovo

ThinkSystem Server with AMD EPYC™ processor (4th Gen) UEFI Manual



**Server Models: SR635 V3, SR645 V3, SR655 V3, SR665 V3, SR675
V3, SD665 V3, SD665-N V3 and SD535 V3**

Sixth Edition (April 2024)

© Copyright Lenovo 2022, 2024.

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

Contents

| | | | |
|--|----------|--|-----------|
| Contents | i | Date and Time | 37 |
| Chapter 1. UEFI Overview | 1 | Start Options | 38 |
| Chapter 2. Get started. | 3 | Boot Manager | 38 |
| Chapter 3. System configuration and boot management | 5 | Add Generic Boot Option | 39 |
| System Information | 5 | Add UEFI Full Path Boot Option. | 39 |
| System Summary | 5 | Delete Boot Option. | 39 |
| Product Data | 6 | Change Boot Order | 40 |
| Open Source License. | 7 | Set Boot Priority. | 40 |
| System Settings | 7 | Boot From File | 41 |
| Devices and I/O Ports | 8 | Select Next One-Time Boot Option | 41 |
| Driver Health | 13 | Boot Mode | 41 |
| Foreign Devices | 14 | Reboot System | 41 |
| Legacy BIOS | 15 | BMC Settings | 42 |
| Memory | 15 | Network Settings | 43 |
| Network | 18 | System Event Logs | 45 |
| Operating Modes | 21 | POST Event Viewer | 45 |
| Power | 23 | System Event Log | 45 |
| Processors | 24 | User Security | 45 |
| Recovery and RAS | 31 | Password Rule and Policy | 47 |
| Security | 32 | F12 One Time Boot Device | 48 |
| Storage | 36 | Appendix A. Notices. | 49 |
| | | Trademarks | 50 |

Chapter 1. UEFI Overview

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

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

- SR635 V3
- SR645 V3
- SR655 V3
- SR665 V3
- SR675 V3
- SD665 V3
- SD665-N V3
- SD535 V3

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 the display language. |
| Launch Graphical System Setup | N/A | Start the graphical user interface for system setup, provisioning manager, and RAID configuration. If there is no screen output to console in Graphical System Setup, use VGA monitor for Graphical System Setup. |
| “System Information” on page 5 | N/A | Display basic details of the system. |
| “System Settings” on page 7 | N/A | Display or modify system settings. Changes might not take effect immediately. Save changes and reboot the system. |

Table 1. Main menu (continued)

| Item | Options | Description |
|--|----------------|---|
| “Date and Time” on page 37 | N/A | Set date and time of the system. |
| “Start Options” on page 38 | N/A | Boot a desired selection from the primary boot sequence in the Boot Manager menu. |
| “Boot Manager” on page 38 | N/A | Change boot order, boot parameters, and boot from a file. |
| “BMC Settings” on page 42 | N/A | Configure Baseboard Management Controller (BMC) . |
| “System Event Logs” on page 45 | N/A | Clear or view the system event log. |
| “User Security” on page 45 | 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 | Displays the open-source license. |

System Summary

Table 3. System Summary

| Item | Format | Description |
|-------------------------------------|---|---|
| System Identification Data | | |
| Machine Type/Model | ASCII string of 10 or 8 characters | Display the system machine type and model. |
| Serial Number | ASCII string of 10 or 8 characters | Display the tag for Serial Number. |
| UUID Number | 16-byte Hexadecimal string of 32 characters | Display the tag for UUID. |
| Asset Tag Number | ASCII string of 32 characters | Display the assigned Asset Tag Number. |
| Processor | | |
| Installed CPU packages | ASCII string of 1 character | Display the number of installed CPU packages. |
| Processor Speed | y.yyy GHz | Display the processor speed. |
| Memory | | |
| Memory Mode | ASCII string | Display the memory mode. |
| Memory Speed | yyyy MHz | Display the speed of the installed memory. |
| Total Memory Detected | yyyy GB | Display total capacity of all installed DIMMs. |
| Total Usable Memory Capacity | yyyy GB | Display the 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 | Description |
|----------------------|--|---|
| Host Firmware | | |
| Build ID | ASCII string of 7 characters | Display the build ID of the host firmware. |
| Version | 4-character string format: 1.xx | Display the version of the host firmware. |
| Build Date | Character string format: MM/DD/YYYY | Display the build date of the host firmware. |
| BMC Firmware | | |
| Build ID | ASCII string | Display the build ID of the Baseboard Management Controller (BMC) firmware. |
| Version | ASCII string | Display the version of the BMC firmware. |
| Build Date | Character string format: MM/DD/YYYY | Display the build date of the BMC firmware. |

Open Source License

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

System Settings

This menu displays the system settings.

Table 5. System Settings

| Item | Options | Description |
|--|---|---|
| <F1> Start Control | <ul style="list-style-type: none">• Auto (Default)• Tool Suite• Text Setup | <p>You can use the F1 key or send the IPMI command to control the tools.</p> <ul style="list-style-type: none">• [Tool Suite] starts a graphical suite of tools which support System Information, UEFI setup, Platform Update, Raid Setup, OS installation and Diagnostics functions.• [Text Setup] starts a text mode UEFI setup utility.• [Auto] starts text mode UEFI setup if Serial Over Lan (SOL) or "Console Redirection" are enabled or SOL is set 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 | Display health status of the drivers. |
| "Foreign Devices" on page 14 | N/A | Display a list of foreign devices. |
| "Legacy BIOS" on page 15 | N/A | Set the 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 21 | N/A | Select the operating mode based on the preference. Note: Power savings and performance are also highly dependent on hardware configuration and the software running on the system. |
| "Power" on page 23 | N/A | Configures power plan options. |
| "Processors" on page 24 | N/A | Display and provide options to change the processor settings. |
| "Recovery and RAS" on page 31 | N/A | Configure recovery policies and advanced reliability, availability, and serviceability settings. |
| "Security" on page 32 | N/A | Configure system security settings. |
| "Storage" on page 36 | N/A | Manage storage adapter options. Some systems may use planar devices and can be configured in the Devices and I/O Ports menu. |

Devices and I/O Ports

Table 6. Devices and I/O ports

| Item | Options | Description |
|--|--|---|
| Active Video | <ul style="list-style-type: none"> • Onboard Device (Default) • Add-in Device | <p>This feature is available only when the server has an add-in video adapter. When option ROM is set to [Legacy] for both onboard and add-in video adapters, the setting controls which single adapter displays the System Setup utility.</p> <p>Regardless of this setting, the system boot early video is displayed at the onboard video only, and the management controller remote console shows the onboard video only. This setting does not affect how the operating system (OS) displays its graphical desktop.</p> |
| PCI 64-Bit Resource Allocation | <ul style="list-style-type: none"> • Enabled • Disabled • Auto (Default) | <p>[Enabled] or [Disabled]: Enable or disable the allocation of 64-bit resources for PCI devices.</p> <p>[Auto]: Allocate some resources below 4GB for legacy compatibility.</p> |
| IOMMU | <ul style="list-style-type: none"> • Disabled • Enabled(Default) | <p>Enable or disable Input/Output Memory Management Unit (IOMMU).</p> <p>Note: [Disabled] option will be grayed out if APIC Mode is set as [x2APIC]</p> |
| SRIOV | <ul style="list-style-type: none"> • Enabled (Default) • Disabled | <p>Enable or disable the support of resource allocation for Single Root I/O Virtualization (SR-IOV) virtual functions during system boot.</p> |
| PCIe ARI Forwarding | <ul style="list-style-type: none"> • Disabled(Default) • Enabled | <p>Enable ARI Forwarding for each downstream port.</p> |
| PCIe Ten Bit Tag Support | <ul style="list-style-type: none"> • Disabled(Default) • Enabled | <p>Provides information on enabling the PCIe Ten Bit tag for improved performance. Enable the PCIe Ten Bit Tag to increase the number of non posted requests from 256 to 768 for better performance. As latency increases, the increase in unique tags is required to maintain the peak performance at 16 GT/s.</p> |
| “Enable/Disable Onboard Device(s)” on page 9 | N/A | <p>Enable or disable onboard devices or slots.</p> |
| “Enable/Disable Adapter Option ROM Support” on page 9 | N/A | <p>Control Legacy and UEFI-compliant adapter support.</p> <p>Disabling UEFI/Legacy support may adversely affect pre-boot/boot functions.</p> |
| “Set Option ROM Execution Order” on page 10 | N/A | <p>Set load order for Legacy ROMs.</p> |
| “PCIe Gen Speed Selection” on page 10 | N/A | <p>Choose the generation speed for available PCIe slots.</p> |
| “Override Slot Bifurcation” on page 10 | N/A | <p>Override the slot bifurcation of the physical slot to support the adapter with multiple devices.</p> |
| “Console Redirection Settings” on page 11 | N/A | <p>Configure console redirection and COM port settings.</p> |
| “USB Configuration” on page 12 | N/A | <p>Enable or disable USB storage devices or individual ports.</p> |

Enable/Disable Onboard Device(s)

Table 7. Enable/Disable Onboard Device(s)

| Item | Operation | Description |
|--|--|--|
| Onboard Video | <ul style="list-style-type: none"> • Enabled (Default) • Disabled | Disabling an entry prevents the associated device from being enumerated during the subsequent boot. |
| Onboard SATA Controllers (for ODD) | <ul style="list-style-type: none"> • Enabled (Default) • Disabled | Disabling an entry will prevent the associated device from being enumerated during subsequent boots. |
| Onboard LAN | <ul style="list-style-type: none"> • Enabled (Default) • Disabled | Disabling an entry will prevent the associated device from being enumerated during subsequent boots. |
| Slot (n...) (depending on which riser card is installed) | <ul style="list-style-type: none"> • Enabled (Default) • Disabled | Disabling an entry will prevent the associated device from being enumerated during subsequent boots. |
| NVMe Bay (n...) (depending on which riser card is installed) | <ul style="list-style-type: none"> • Enabled (Default) • Disabled | Disabling an entry will prevent the associated device from being enumerated during subsequent boots. |

Enable/Disable Adapter Option ROM Support

Table 8. Enable/Disable Adapter Option ROM Support

| Item | Options | Description |
|--------------------------|--|---|
| Network | <ul style="list-style-type: none"> • Do not launch • UEFI (Default) • Legacy | Control the execution of UEFI and Legacy Network OpROM (Option ROM). |
| Storage | <ul style="list-style-type: none"> • Do not launch • UEFI (Default) • Legacy | Control the execution of UEFI and Legacy Storage OpROM. |
| Video | <ul style="list-style-type: none"> • Do not launch • UEFI (Default) • Legacy | Control the execution of UEFI and Legacy Video OpROM. |
| Other PCI devices | <ul style="list-style-type: none"> • Do not launch • UEFI (Default) • Legacy | Determine the OpROM execution policy for devices except Network, Storage, or Video. |

Set Option ROM Execution Order

Table 9. Set Option ROM Execution Order

| Item | Options | Description |
|---------------------------------------|--|--|
| Set Option ROM Execution Order | <ul style="list-style-type: none"> Onboard Video Onboard SATA Slot 1 Slot 2 Slot n... Onboard LAN Port 1 Onboard LAN Port n... NVMe Bay 0 NVMe Bay n... | <p>Select the load order for legacy PCI option ROM(s). Press + to execute the selected devices ROM sooner or press - to execute it later.</p> <p>Notes:</p> <ul style="list-style-type: none"> [Onboard LAN Port n...] depends on whether PHY card is installed or not. Slot 1 to Slot n varies depending on which riser card is installed. This order may be overridden for devices controlled by UEFI thunk drivers. |

PCIe Gen Speed Selection

Table 10. PCIe Gen Speed Selection

| Item | Operation | Description |
|--|---|--|
| Slot 1 (depending on which riser card is installed) | <ul style="list-style-type: none"> Auto (Default) Gen1 Gen2 Gen3 Gen4 Gen5 | Set the maximum speed supported by individual PCIe slot. |
| Slot 2 (depending on which riser card is installed) | <ul style="list-style-type: none"> Auto (Default) Gen1 Gen2 Gen3 Gen4 Gen5 | Set the maximum speed supported by individual PCIe slot. |
| Slot (n...) (depending on which riser card is installed) | <ul style="list-style-type: none"> Auto (Default) Gen1 Gen2 Gen3 Gen4 Gen5 | Set the maximum speed supported by individual PCIe slot. |

Override Slot Bifurcation

This page allows you to override the slot bifurcation settings.

Console Redirection Settings

Table 11. Console Redirection Settings

| Item | Options | Description |
|-------------------------------------|--|---|
| COM Port 1 | <ul style="list-style-type: none"> • Enabled (Default) • Disabled | <p>Enable or disable COM 1 device.</p> <p>When [Disabled] is selected, the associated COM 1 terminal settings are hidden.</p> |
| Virtual COM Port 2 | <ul style="list-style-type: none"> • Enabled (Default) • Disabled | <p>Enable or disable virtual COM 2 device.</p> <p>When [Disabled] is selected, the SSH connection will be disabled.</p> |
| Console Redirection | <ul style="list-style-type: none"> • Enabled • Disabled • Auto (Default) | <p>Set remote console redirection preference to enable or disable console redirection.</p> <p>When [Auto] is selected, Console Redirection is enabled automatically if IPMI Serial over LAN status is active.</p> |
| Serial Port Sharing | <ul style="list-style-type: none"> • Enabled • Disabled (Default) | <p>Enable system BMC to allow access to the system serial port.</p> <p>When [Enabled] is selected, BMC is allowed to control the serial communication port as requested by remote control commands.</p> <p>When [Disabled] is selected, the serial port is assigned to BMC unless "Serial Port Access Mode" is set to [Disabled].</p> |
| Serial Port Access Mode | <ul style="list-style-type: none"> • Shared • Dedicated • Disabled (Default) | <p>Control the access to the system BMC over the system serial port.</p> <ul style="list-style-type: none"> • [Shared]: Serial port is available for both of POST and operating system. However, BMC can monitor the serial data for a takeover control sequence. • [Dedicated]: BMC has complete control of the serial port for POST and/or OS use. • [Disabled]: BMC does not have any access to the serial port. |
| SP Redirection | <ul style="list-style-type: none"> • Enabled • Disabled (Default) | <p>Serial Over LAN (SOL) or SSH redirection enables a system administrator to use the BMC as a serial terminal server. It allows to choose which mode to have the redirection. If this option is set to [Disabled], it will be configured with Serial over Lan (SOL). If this option is set to [Enabled], a server serial port can be accessed from SSH connection (Virtual COM 2).</p> <p>Note: This feature appears only when Console Redirection is set to [Enabled].</p> |
| Legacy OS/Option ROM Display | <ul style="list-style-type: none"> • Virtual COM Port 2 • COM Port 1 (Default) | <p>Select a COM port to display the redirection of Legacy OS and Legacy OPROM (Option ROM) Messages.</p> |

Table 11. Console Redirection Settings (continued)

| Item | Options | Description |
|-----------------------------------|--|---|
| COM Port Active After Boot | <ul style="list-style-type: none"> Enabled Disabled (Default) | <p>When [Disabled] is selected, Legacy Console Redirection is disabled before booting to legacy OS.</p> <p>When [Enabled] is selected, Legacy Console Redirection is enabled for legacy OS.</p> |
| COM1 Settings | | |
| COM1 Baud Rate | <ul style="list-style-type: none"> 115200 (Default) 57600 38400 19200 9600 | Control the connection speed between the host and the remote system. |
| COM1 Data Bits | <ul style="list-style-type: none"> 8 (Default) 7 | Set the number of Data Bits in each character. |
| COM1 Parity | <ul style="list-style-type: none"> None (Default) Odd Even | <p>Set the parity bit in each character to be [None], [Odd], or [Even].</p> <p>[None] means that no parity bit is transmitted.</p> |
| COM1 Stop Bits | <ul style="list-style-type: none"> 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 resynthesized with the character stream. |
| COM1 Terminal Emulation | <ul style="list-style-type: none"> VT100 VT100Plus VT-UTF8 ANSI (Default) | <p>Select [VT100] only if the remote emulator does not support ANSI text graphics.</p> <p>Note: If needed, change the character encoding setting in the remote emulator to ensure the characters show correctly.</p> |
| COM1 Flow Control | <ul style="list-style-type: none"> Disabled (Default) Hardware | Select [Hardware] only if the remote emulator supports and is using hardware flow control. |

USB Configuration

Table 12. USB Configuration

| Item | Options | Description |
|--|--|--|
| USB Mass Storage Driver Support | <ul style="list-style-type: none"> Enabled (Default) Disabled | Enable or disable USB Mass Storage Driver Support. This feature only takes effect during the POST process. |
| USB Up Front Port | <ul style="list-style-type: none"> Enabled (Default) Disabled | Enable or disable USB individual ports. |
| USB Down Front Port | <ul style="list-style-type: none"> Enabled (Default) Disabled | Enable or disable USB individual ports. |
| USB Up Rear Port | <ul style="list-style-type: none"> Enabled (Default) Disabled | Enable or disable USB individual ports. |

Table 12. USB Configuration (continued)

| Item | Options | Description |
|--------------------|--|---|
| USB Down Rear Port | <ul style="list-style-type: none"> • Enabled (Default) • Disabled | Enable or disable USB individual ports. |
| USB Left Rear Port | <ul style="list-style-type: none"> • Enabled (Default) • Disabled | Enable or disable USB individual ports. |

Driver Health

Table 13. Driver Health

| Item | Options | Description |
|----------------------------------|---|--|
| The platform is: | The platform is: <ul style="list-style-type: none"> • Healthy (Default) • Repair Required • Configuration Required • Operation Failed • Reconnect Required • Reboot Required • Shutdown Required • No Operation Required | Display health statuses of the drivers. |
| Driver/Controller Status: | | |
| Controller Name - Status | <ul style="list-style-type: none"> • Healthy (Default) • Repair Required • Configuration Required • Operation Failed • Reconnect Required • Reboot Required • Shutdown Required • No Operation Required | Display health status of the controller. |

Table 13. Driver Health (continued)

| Item | Options | Description |
|--|--|--|
| POST Attempts Driver | <ul style="list-style-type: none"> • Healthy (Default) • Repair Required • Configuration Required • Operation Failed • Reconnect Required • Reboot Required • Shutdown Required • No Operation Required | Display health status of the POST Attempts Driver. |
| Partition Driver (MBR/GPT/EFI Torito) | <ul style="list-style-type: none"> • Healthy (Default) • Repair Required • Configuration Required • Operation Failed • Reconnect Required • Reboot Required • Shutdown Required • No Operation Required | Display health status of the Partition Driver. |

Foreign Devices

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

Table 14. Foreign Devices

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

Notes:

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

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 | <ul style="list-style-type: none"> • Enabled (Default) • Disabled | Enable or disable the system UEFI firmware execution environment for supporting legacy OS and legacy Option ROM. |
| Rehook INT 19h | <ul style="list-style-type: none"> • Enabled • Disabled (Default) | [Enable] prevents devices from taking control of the boot process. |
| Non-Onboard PXE | <ul style="list-style-type: none"> • Enabled (Default) • Disabled | Enable/Disable legacy PXE boot for installed network adapters. |
| <p>Legacy BIOS is disabled due to secure boot is enabled.</p> <p>Note: This feature appears only when Secure Boot is enabled.</p> | | |

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 | Display status of the system memory. |
| Total Usable Memory Capacity | yyyy GB | Display Total Usable Memory Capacity. |
| Memory Speed | <ul style="list-style-type: none"> • Maximum • xxxxMHz • Minimum | <p>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.</p> <p>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 cause the memory speed set to the minimum value.</p> <p>Note: This option is dynamically generated based on the memory configuration.</p> |
| Memory Power Down Enable | <ul style="list-style-type: none"> • Enabled (Default) • Disabled | Enable or disable low-power features for DIMMs. |
| NUMA Nodes per Socket | <ul style="list-style-type: none"> • NPS0 • NPS1 (Default) • NPS2 • NPS4 | <p>Specify the number of desired NUMA nodes per processor socket (e.g. NPS1 means 1 NUMA per socket).</p> <p>NPS0 will attempt to interleave the 2 processor sockets together (non-NUMA mode).</p> |

Table 16. Memory (continued)

| Item | Options | Description |
|---------------------------------|--|---|
| DRAM Scrub Time | <ul style="list-style-type: none"> • Disable • 1 hour • 4 hour • 6 hour • 8 hour • 12 hour • 16 hour • 24 hour (Default) • 48 hour | Set the period of time between successive DRAM scrub events. |
| DRAM Post Package Repair | <ul style="list-style-type: none"> • Enabled (Default) • Disabled | Enable or disable DRAM Post Package Repair. |
| DDR Healing BIST | <ul style="list-style-type: none"> • Disabled (Default) • PMU Mem BIST • Self-Healing Mem BIST • PMU and Self-Healing Mem BIST | <p>[Disabled]: Disable memory self-healing feature.</p> <p>[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.</p> <p>[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.</p> <p>[PMU and Self-Healing Mem BIST]: Run PMU Mem BIST and then Self-Healing Mem BIST tests sequentially.</p> |
| SMEE | <ul style="list-style-type: none"> • Enabled • Disabled (Default) | Control secure memory encryption enable. Note: This option will be grayed out if “ SME-MK ” is set to [Enabled]. |
| Memory Interleave | <ul style="list-style-type: none"> • Enabled (Default) • Disabled | Enable or disable memory interleaving. Value of NUMA nodes per socket will be honored regardless of this setting. |
| SubUrgRefLowerBound | <ul style="list-style-type: none"> • 1 (Default) • 2 • 3 • 4 • 5 • 6 | Specify the stored refresh limit to required enter sub-urgent refresh mode. Constraint: SubUrgRefLowerBound is less than or equal to UrgRefLimit. Valid value: 6 ~ 1. Note: This option will be different according to UrgRefLimit . |

Table 16. Memory (continued)

| Item | Options | Description |
|--|---|--|
| UrgRefLimit | <ul style="list-style-type: none"> • 6 • 5 • 4 (Default) • 3 • 2 • 1 | <p>Specify the stored refresh limit to required enter urgent refresh mode.</p> <p>Constraint: SubUrgRefLowerBound is less than or equal to UrgRefLimit.</p> <p>Valid value: 6 ~ 1.</p> <p>Note: This option will be different according to SubUrgRefLowerBound .</p> |
| DRAM Refresh Rate | <ul style="list-style-type: none"> • 1x (Default) • 2x | <p>For better performance, a refresh rate of 1x is recommended.</p> <p>To mitigate the rowhammer issue, choosing refresh rate 2x may affect the performance.</p> |
| TSME | <ul style="list-style-type: none"> • Enabled • Disabled (Default) | <p>TSME stands for Transparent Secure Memory Encryption.</p> <p>[Enabled] is selected, the following parameters will be displayed:</p> <ul style="list-style-type: none"> • AddrTweakEn = 1 • ForceEncrEn = 0 • DataEncrEn = 1 |
| SME-MK | <ul style="list-style-type: none"> • Enabled • Disabled (Default) | <p>SME-MK encryption mode.</p> <p>Note: This option will be grayed out if “SMEE” is set to [Enabled].</p> |
| SEV-ES ASID Space Limit | <p>[1]</p> <p>Range: 1-510</p> | <p>SEV VMs using ASIDs below the SEV-ES ASID Space Limit must enable the SEV-ES feature.</p> <p>ASIDs from SEV-ES ASID Space Limit to (SEV ASID Count + 1) can only be used with SEV VMs.</p> <p>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)</p> |
| SEV Control | <ul style="list-style-type: none"> • Enabled(Default) • Disabled | <p>Can be used to disable SEV. To re-enable SEV, a POWER CYCLE is needed after selecting the 'Enabled' option.</p> |
| 1TB remap | <ul style="list-style-type: none"> • Do not remap • Attempt to remap (Default) | <p>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.</p> |
| RAM Disk Configuration | N/A | Press Enter to add or remove RAM disks. |

System Memory Details

Table 17. System Memory Details

| Item | Description |
|-------------------------------------|----------------------|
| DIMM Details For Processor X | Display DIMM status. |

DIMM Details

This menu displays DIMM population list.

RAM Disk Configuration

Table 18. RAM Disk Configuration

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

Create Raw

Table 19. Create Raw

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

Network

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

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

Table 20. Network

| Item | Description |
|--|--|
| Global Network Settings | |
| "iSCSI Settings" on page 18 | Configure the iSCSI parameters. |
| "Network Stack Settings" on page 19 | Specify the Network Stack Settings. |
| "Network Boot Settings" on page 20 | Configure the network boot parameters. |
| "HTTP Boot Configuration" on page 20 | Configure the HTTP Boot parameters. |
| "TIs Auth Configuration" on page 20 | Press Enter to select TIs Auth Configuration. |

iSCSI Settings

Table 21. iSCSI Settings

| Item | Description |
|---|---------------------------------------|
| "Host iSCSI Configuration" on page 19 | Display the Host iSCSI Configuration. |

Host iSCSI Configuration

Table 22. Host iSCSI configuration

| Item | Description |
|-----------------------------|--|
| iSCSI Initiator Name | Displays the worldwide unique name of iSCSI Initiator. Only IQN format is accepted. Range is from 4 to 233 |
| Add an Attempt | Adds an attempt. |
| List of Attempts | <p>MAC: XX:XX:XX:XX:XX:XX, PFA: Bus XX Dev XX Func XX, "iSCSI Mode": [%s1], "Internet Protocol": [%s2]</p> <p>Notes:</p> <ul style="list-style-type: none"> • The values vary with the attempt settings. • %s1 is the option name for iSCSI Mode. • %s2 is the setting name for Internet Protocol. |
| Delete Attempts | Delete one or more attempts. |
| Change Attempt Order | Change attempt order by using +/- keys, and use arrow keys to select an attempt and press +/- to move the attempt up/down in the attempt order list. |

Network Stack Settings

Table 23. Network Stack Settings

| Item | Options | Description |
|---------------------------|--|--|
| Network Stack | <ul style="list-style-type: none"> • Enabled (Default) • Disabled | Enable or disable UEFI Network Stack. |
| IPv4 PXE Support | <ul style="list-style-type: none"> • Enabled (Default) • Disabled | <p>Enable or disable IPv4 PXE Boot Support.</p> <p>If this feature is disabled, IPv4 PXE boot option will not be created.</p> |
| IPv4 HTTP Support | <ul style="list-style-type: none"> • Enabled • Disabled (Default) | <p>Enable or disable IPv4 HTTP Boot Support.</p> <p>If this feature is disabled, IPv4 HTTP boot option will not be created.</p> |
| IPv6 PXE Support | <ul style="list-style-type: none"> • Enabled (Default) • Disabled | <p>Enable or disable IPv6 PXE Boot Support.</p> <p>If this feature is disabled, IPv6 PXE boot option will not be created.</p> |
| IPv6 HTTP Support | <ul style="list-style-type: none"> • Enabled • Disabled (Default) | <p>Enable or disable IPv6 HTTP Boot Support.</p> <p>If this feature is disabled, IPv6 HTTP boot option will not be created.</p> |
| PXE boot wait time | 0 | Use either +/- or numeric keys to set a specific wait time (in seconds) before which you can press Esc to abort the PXE boot. |
| Media detect count | 1 | Use either +/- or numeric keys to set the number of times to detect media. |

Network Boot Settings

Table 24. Network Boot Settings

| Item | Description |
|--|---|
| MAC, VLAN Configuration list 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 under **HTTP Boot Configuration**.

Table 25. HTTP Boot Configuration

| Item | Description |
|--|--|
| List of NICs in the system Example: MAC:XX:XX:XX:XX:XX:XX HTTP Boot Configuration | Configure the HTTP Boot parameters. (MAC: XXXXXXXXXXXXX). Note: After you input the information to create the new http boot option, you need to save it from the front-page -System Configuration and Boot Management -> Save Settings , then you will see the boot option in Start Options. |

Tls Auth Configuration

Table 26. Tls Auth Configuration

| Item | Description |
|---|---|
| “Server CA Configuration” on page 20 | Press Enter to configure Server CA. |
| Client Cert Configuration | Client cert configuration is unsupported currently. |

Server CA Configuration

Table 27. Server CA Configuration

| Item | Description |
|---------------------------------|------------------------------------|
| “Enroll Cert” on page 20 | Press Enter to enroll cert. |
| “Delete Cert” on page 21 | Press Enter to delete cert. |

Enroll Cert

Table 28. Enroll Cert

| Item | Description |
|-------------------------------|--|
| Enroll Cert Using File | Enroll Cert Using File. |
| Cert GUID | Enter Cert GUID in the following format: 11111111-2222-3333-4444-1234567890ab. |

Table 28. Enroll Cert (continued)

| Item | Description |
|---------------------------------|---------------------------|
| Commit Changes and Exit | Commit changes and exit. |
| Discard Changes and Exit | Discard changes and exit. |

Delete Cert

Table 29. Delete Cert

| Item | Options | Description |
|--------------------------------------|---|---|
| XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX | <ul style="list-style-type: none"> • Empty • X | <p>GUID for Cert.</p> <p>Note: If there is no cert file, the default value is [Empty].</p> |

Operating Modes

Select the operating mode based on your preference.

Table 30. Operating Modes

| Item | Options | Description |
|-------------------------------|---|---|
| Choose Operating Mode | <ul style="list-style-type: none"> • Maximum Efficiency (Default) • Custom Mode • Maximum Performance | <p>Select the operating mode based on your preference.</p> <p>Power savings and performance are heavily dependent on the hardware and the software running on the system.</p> |
| Determinism Slider | <ul style="list-style-type: none"> • Power • Performance (Default) | <p>When this feature is 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.</p> <p>When this feature is set to [Power], cores can scale frequency independently. Aggregate performance may be higher, but predictability is lower.</p> |
| Core Performance Boost | <ul style="list-style-type: none"> • Disabled • Enabled (Default) | <p>When this feature is set to [Enabled] is selected, the cores can run at turbo frequencies.</p> |
| cTDP | <ul style="list-style-type: none"> • Maximum • Manual • Auto (Default) | <p>Set the maximum power consumption for the processor.</p> <p>[Auto] sets cTDP=TDP for the installed processor SKU.</p> <p>[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 greater than the maximum value allowed, the value will be internally limited to the maximum allowable value. cTDP is only configurable before booting the operating system.</p> |
| cTDP Manual | [0] | <p>Set the power consumption for the processor manually.</p> <p>Note: This feature appears only when cTDP is set to [Manual].</p> |

Table 30. Operating Modes (continued)

| Item | Options | Description |
|--|---|---|
| Package Power Limit | <ul style="list-style-type: none"> • Maximum • Manual • Auto (Default) | <p>Sets the CPU package power limit.</p> <p>If [Auto] is selected, it will be set to the maximum value allowed by the installed processor.</p> <p>If a manual value is entered that is greater than the maximum value allowed, the value will be internally limited to the maximum allowable value.</p> <p>The maximum value allowed for PPL is the cTDP limit. Compared to cTDP, Package Power Limit (PPL) can be changed at runtime and PPL supports a much lower effective limit than cTDP.</p> |
| Package Power Limit Manual | [0] | Package Power Limit (PPT) [W]. |
| Memory Speed | <ul style="list-style-type: none"> • Maximum • xxxx MHz • Minimum | <p>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.</p> <p>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 cause the memory speed set to the minimum value.</p> <p>Note: This option is dynamically generated based on the memory configuration.</p> |
| Efficiency Mode | <ul style="list-style-type: none"> • Enabled (Default) • Disabled | <p>Enable or disable efficiency mode.</p> <p>When this feature is enabled, use power efficiency optimized CCLK DPM settings.</p> |
| 4-Link xGMI Max Speed Note: Only available on SD665 V3 servers. | <ul style="list-style-type: none"> • Minimum(Default) • 18Gbps • 25Gbps • 32Gbps | <p>Sets the xGMI speed.</p> <p>N is the maximum speed and is auto-calculated from the system board capabilities. For system boards that do not support 4 discrete xGMI speed choices, some menu choices besides "Minimum" will result in the xGMI speed getting set to the minimum value.</p> |
| 3-Link xGMI Max Speed Note: Only available on SR675 V3 servers. | <ul style="list-style-type: none"> • Minimum(Default) • 18Gbps • 25Gbps • 32Gbps | <p>Sets the xGMI speed.</p> <p>N is the maximum speed and is auto-calculated from the system board capabilities. NUMA-unaware workloads may need maximum xGMI bandwidth because of extensive cross socket communications. NUMA-aware workloads may want to minimize xGMI power because they do not have a lot of cross socket traffic and prefer to use the increased CPU boost.</p> |
| Global C-state Control | <ul style="list-style-type: none"> • Disabled • Enabled (Default) | <p>Enable or disable IO based C-state generation and DF C-states.</p> |

Table 30. Operating Modes (continued)

| Item | Options | Description |
|---------------------------------|---|---|
| DF P-states | <ul style="list-style-type: none"> • Auto (Default) • P0 • P1 • P2 | <p>When [Auto] is selected, the processor DF P-states (uncore P-states) are dynamically adjusted. The frequency dynamically changes based on the workload.</p> <p>Selecting P0, P1, or P2 forces the DF to a specific P-state frequency.</p> |
| DF C-States | <ul style="list-style-type: none"> • Disabled • Enabled (Default) | <p>Enable or disable data fabric (DF) C-states.</p> <p>Data fabric C-states may be entered when all cores are in CC6.</p> |
| MONITOR/MWAIT | <ul style="list-style-type: none"> • Enabled (Default) • Disabled | <p>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, do the following:</p> <ol style="list-style-type: none"> 1. Disable MONNITOR/MWAIT. 2. Choose System Settings > Operating Modes > Choose Operating Mode > Custom Mode. and choose System Settings > DF C-States > Disabled |
| P-state 1 | <ul style="list-style-type: none"> • Enabled (Default) • Disabled | <p>Enable or disable processor P1 P-state.</p> |
| P-State 2 | <ul style="list-style-type: none"> • Enabled (Default) • Disabled | <p>Enable or disable processor P2 P-state.</p> <p>Note: If P-state 1 is set to [Disabled], this option will be hidden and can not be changed (custom mode).</p> |
| Memory Power Down Enable | <ul style="list-style-type: none"> • Enabled (Default) • Disabled | <p>Enable or disable low-power features for DIMMs.</p> |

Power

Use this menu to configure power plan options.

Table 31. Power

| Item | Options | Description |
|--------------------------------|--|---|
| ACPI Fixed Power Button | <ul style="list-style-type: none"> • Enabled (Default) • Disabled | <p>Enable or disable ACPI Fixed Power Button.</p> <p>When [Disabled] is selected, physically pressing the power button in front of the system will not execute the Operating System's Power Button Policy such as shutdown, turn off monitor, etc. Also, when disabled, the following options under the BMC Server (Web) Power Actions feature will be disabled:</p> <ul style="list-style-type: none"> • Power Off Server Normally • Restart Server Normally |
| Efficiency Mode | <ul style="list-style-type: none"> • Enabled (Default) • Disabled | <p>Enable or disable Efficiency Mode.</p> <p>When [Enabled] is selected, use power efficiency optimized CCLK DPM settings.</p> |
| PCIe Power Brake | <ul style="list-style-type: none"> • Reactive • Proactive (Default) • Disabled | <p>PCIe Power Brake quickly reduces the power consumption and performance of high-powered PCIe devices. Performance of low-powered PCIe devices are not impacted by this setting. A high-powered PCIe device is the one that is rated at 75W TDP or higher.</p> <p>Note: This is platform dependent. Refer to platform document for details.</p> |

Processors

This menu offers options to change the processor settings.

Table 32. Processors

| Item | Options | Description |
|-------------------------------|--|---|
| Determinism Slider | <ul style="list-style-type: none"> • Power • Performance (Default) | <p>When [Performance] is selected, performance is more predictable (deterministic) and operates at the lowest common denominator among the cores. But aggregate peak performance may be reduced.</p> <p>When [Power] is selected, cores can scale frequency independently. Aggregate performance may be higher, but predictability is lower.</p> |
| Core Performance Boost | <ul style="list-style-type: none"> • Disabled • Enabled (Default) | <p>When [Enabled] is selected, cores can run at turbo frequencies.</p> |
| cTDP | <ul style="list-style-type: none"> • Maximum • Manual • Auto (Default) | <p>Set the maximum power consumption for the processor.</p> <p>[Auto] sets cTDP=TDP for the installed processor SKU.</p> <p>[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 greater than the maximum value allowed, the value will be internally limited to the maximum allowable value. cTDP is only configurable before booting the operating system.</p> |

Table 32. Processors (continued)

| Item | Options | Description |
|--|---|---|
| cTDP Manual | [0] | Set the power consumption for the processor. Note: This feature appears only when cTDP is set to [Manual]. |
| Package Power Limit | <ul style="list-style-type: none"> • Maximum • Manual • Auto (Default) | <p>Set the CPU package power limit.</p> <p>If [Auto] is selected, it will be set to the maximum value allowed by the installed processor.</p> <p>If a manual value is entered that is greater than the maximum value allowed, the value will be internally limited to the maximum allowable value.</p> <p>The maximum value allowed for PPL is the cTDP limit. Compared to cTDP, Package Power Limit (PPL) can be changed at runtime and PPL supports a much lower effective limit than cTDP.</p> |
| Package Power Limit Manual | [0] | Package Power Limit (PPT) [W]. |
| 4-Link xGMI Max Speed Note: Only available on SD665 V3 servers. | <ul style="list-style-type: none"> • Minimum(Default) • 18Gbps • 25Gbps • 32Gbps | <p>Sets the xGMI speed.</p> <p>N is the maximum speed and is auto-calculated from the system board capabilities. For system boards that do not support 4 discrete xGMI speed choices, some menu choices besides “Minimum” will result in the xGMI speed getting set to the minimum value.</p> |
| 3-Link xGMI Max Speed Note: Only available on SR675 V3 servers. | <ul style="list-style-type: none"> • Minimum(Default) • 18Gbps • 25Gbps • 32Gbps | <p>Sets the xGMI speed.</p> <p>N is the maximum speed and is auto-calculated from the system board capabilities. NUMA-unaware workloads may need maximum xGMI bandwidth because of extensive cross socket communications. NUMA-aware workloads may want to minimize xGMI power because they do not have a lot of cross socket traffic and prefer to use the increased CPU boost.</p> |
| Global C-state Control | <ul style="list-style-type: none"> • Disabled • Enabled (Default) | Enable or disable IO based C-state generation and DF C-states. |
| DF P-states | <ul style="list-style-type: none"> • Auto (Default) • P0 • P1 • P2 • P3 • P4 | <p>When [Auto] is selected, the processor DF P-states (uncore P-states) are dynamically adjusted. The frequency dynamically changes based on the workload.</p> <p>Selecting P0, P1, P2, P3 or P4 forces the DF to a specific P-state frequency.</p> |
| DF C-States | <ul style="list-style-type: none"> • Disabled • Enabled (Default) | <p>Enable or disable data fabric (DF) C-states.</p> <p>Data fabric C-states may be entered when all cores are in CC6.</p> |

Table 32. Processors (continued)

| Item | Options | Description |
|--|--|---|
| MONITOR/MWAIT | <ul style="list-style-type: none"> • Enabled (Default) • Disabled | <p>MONITOR/MWAIT instructions are used to engage C-states. Some operating systems re-enable C-states even when they are disabled in setup. To prevent this, do the following:</p> <ol style="list-style-type: none"> 1. Disable MONNITOR/MWAIT. 2. Choose System Settings > Operating Modes > Choose Operating Mode > Custom Mode. and choose System Settings > DF C-States > Disabled |
| P-state 1 | <ul style="list-style-type: none"> • Enabled (Default) • Disabled | Enable or disable processor P1 P-state. |
| P-State 2 | <ul style="list-style-type: none"> • Enabled (Default) • Disabled | <p>Enable or disable processor P2 P-state.</p> <p>Note: If P1 P-state is set to [Disabled], this feature will be hidden and can not be changed.</p> |
| ACPI SRAT L3 Cache as NUMA Domain | <ul style="list-style-type: none"> • Enabled • Disabled (Default) | <p>If [Enabled] is selected, each CCX in the system will be declared as a separate NUMA domain.</p> <p>If [Disabled] is selected, memory addressing/NUMA nodes per socket will be declared.</p> |
| L1 Stream HW Prefetcher | <ul style="list-style-type: none"> • Enabled (Default) • Disabled | <p>Enable or disable L1 stream HW prefetcher.</p> <p>Fetch the next cache line into the L1 cache when cached lines are reused within a certain time period or accessed sequentially.</p> |
| L2 Stream HW Prefetcher | <ul style="list-style-type: none"> • Enabled (Default) • Disabled | <p>Enable or disable L2 Stream HW Prefetcher.</p> <p>Fetch the next cache line into the L2 cache when cached lines are reused within a certain time period or accessed sequentially.</p> |
| L1 Stride Prefetcher | <ul style="list-style-type: none"> • Disabled • Enabled (Default) | <p>Enable or disable L1 Stride Prefetcher.</p> <p>Use memory access history to fetch additional data lines into L1 cache when each access is at a constant distance from the previous one. Some workloads may benefit when this feature is set to [Disabled].</p> |
| L1 Region Prefetcher | <ul style="list-style-type: none"> • Disabled • Enabled (Default) | <p>Enable or disable L1 Region Prefetcher.</p> <p>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 when this feature is set to [Disabled].</p> |
| L2 Up/Down Prefetcher | <ul style="list-style-type: none"> • Disabled • Enabled (Default) | <p>Enable or disable L2 Up/Down Prefetcher.</p> <p>Use memory access history to determine to fetch the next or previous line for all memory accesses. Some workloads may benefit when this feature is set to [Disabled].</p> |
| SMT Mode | <ul style="list-style-type: none"> • Enabled (Default) • Disabled | This feature can be used to disable symmetric multithreading. To re-enable SMT, a power cycle is needed after selecting [Enabled]. |

Table 32. Processors (continued)

| Item | Options | Description |
|--|--|--|
| CPPC | <ul style="list-style-type: none"> • Enabled (Default) • Disabled | CPPC (cooperative processor performance control) is a way for the operating system to affect the performance of a processor on a contiguous and abstract scale without knowledge of power budgets or discrete processor frequencies. |
| BoostFmax | <ul style="list-style-type: none"> • Auto (Default) • Manual | <p>Maximum boost frequency.</p> <p>[Auto] sets the boost frequency to the fused value for the installed processor.</p> <p>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.</p> |
| BoostFmax Manual | [0] | <p>Maximum boost frequency.</p> <p>Note: This feature is available only when BoostFmax is set to [Manual].</p> |
| SVM Mode | <ul style="list-style-type: none"> • Disabled • Enabled (Default) | Enable or disable processor Virtualization. |
| xGMI Maximum Link Width Note: Available on 2-socket platforms only. | <ul style="list-style-type: none"> • x4 • x8 • x16 • Auto (Default) | <p>Sets the xGMI maximum allowable link width. The actual xGMI link width can vary between the minimum and maximum width selected.</p> <p>[Auto]: Set the maximum xGMI link width based on the system capabilities.</p> |
| APIC Mode | <ul style="list-style-type: none"> • xAPIC • x2APIC • Auto (Default) | <p>[xAPIC] scales to only 255 hardware threads.</p> <p>[x2APIC] scales beyond 255 hardware threads but not supported by some legacy OS versions.</p> <p>[Auto] uses [x2APIC] only if 256 hardware threads are in the system. Otherwise, use [xAPIC].</p> <p>Note: [x2APIC] option will be grayed out if IOMMU is set as [Disabled].</p> |
| SEV-SNP Support | <ul style="list-style-type: none"> • Enabled • Disabled (Default) | Enable the support for Secure Encrypted Virtualization and Secure Nested Paging. |
| HSMP Support | <ul style="list-style-type: none"> • Disabled • Enabled • Auto(Default) | <p>HSMP (Host System Management Port) is an interface to provide OS-level software with access to system management functions via a set of mailbox registers</p> <ul style="list-style-type: none"> • [Auto]: Use hardware default value. • [Enabled]: Enable HSMP interface support. • [Disabled]: Disable HSMP interface support. |
| Enhanced REP MOVSB/STOSB | <ul style="list-style-type: none"> • Disabled • Enabled(Default) | (ERSM) Can be disabled for analysis purposes as long as OS supports it. |

Table 32. Processors (continued)

| Item | Options | Description |
|---|---|--|
| Fast Short REP MOVSB | <ul style="list-style-type: none"> Disabled Enabled(Default) | (FSRM) Can be disabled for analysis purposes as long as OS supports it. |
| SNP Memory (RMP Table) Coverage | <ul style="list-style-type: none"> Disabled(Default) Enabled Custom | [Enabled] means that the ENTIRE system memory is covered. |
| Amount of Memory to Cover | 2000 | Specify MB of System Memory to be covered in Hex. Note: This item is only available when SNP Memory (RMP Table) Coverage is set to [Custom]. |
| Split RMP Table | <ul style="list-style-type: none"> Disabled(Default) Enabled | Control RMP Table Allocation. <ul style="list-style-type: none"> [Enabled]: Split RMP Table across sockets. [Disabled]: Allocate RMP Table at the end of memory. Note: This item is only available when SNP Memory (RMP Table) Coverage is set to [Custom]. |
| 3D V-Cache | <ul style="list-style-type: none"> Auto(Default) Disabled | 3D V-Cache only takes effect in systems powered by AMD EPYC Processors equipped with AMD 3D V-Cache technology. Lenovo recommends setting this option to [Auto] to leverage the extra cache. If your application is not cache or memory bandwidth sensitive, then Lenovo recommends setting this option to [Disabled]. |
| ACPI CST C2 Latency | 800 | Enter in microseconds (decimal value). Larger C2 latency values will reduce the number of C2 transitions and reduce C2 residency. Fewer transitions can help when performance is sensitive to the latency of C2 entry and exit. Higher residency can improve performance by allowing higher frequency boost and reduce idle power. The best value will be dependent on kernel version, use case, and workload. |
| Split RMP Table | <p>All (Default)</p> <p>List of all available core counts based on CCDs and Cores Per CCD.</p> | Select total number of enabled CPU cores per socket to be activated. Available options are dependent on processor SKU topology. Notes: <ul style="list-style-type: none"> Reducing the number of processor cores activated can adversely affect the performance. n is the maximum number of cores that installed processor supports. For example, it will show [All], [1], [2], [3], [4], [5] if the installed processor supports 6 cores. |
| “Secured-Core” on page 29 | N/A | Secured-Core configuration setup page. |
| “Processor Details” on page 29 | N/A | Display summary of the installed processors. |

Secured-Core

| Item | Operation | Description |
|------------------------------------|---|---|
| Secured-Core | | |
| Secured-Core | <ul style="list-style-type: none"> • Custom(Default) • Enabled | <p>Enable Secured-Core support.</p> <p>When “Enabled” is selected, the 6 related settings are 'Enabled' and locked.</p> <p>When “Custom” is selected, the related settings can be changed independently as needed. If all 6 related settings are 'Enabled', it is effectively equivalent to Secured-core being 'Enabled'.</p> |
| IOMMU | <ul style="list-style-type: none"> • Disabled • Enabled(Default) | Enable or disable IOMMU. |
| DMAr Support | <ul style="list-style-type: none"> • Disabled(Default) • Enabled | Enable DMAr system protection during POST. |
| DMA Protection | <ul style="list-style-type: none"> • Disabled(Default) • Enabled | Enable DMA remap support in IVRS IVinfo Field. |
| DRTM Virtual Device Support | <ul style="list-style-type: none"> • Disabled(Default) • Enabled | Enable DRTM ACPI virtual device. |
| TSME | <ul style="list-style-type: none"> • Disabled(Default) • Enabled | <p>Transparent SME:</p> <ul style="list-style-type: none"> • AddrTweakEn = 1 • ForceEncrEn = 0 • DataEncrEn = 1 <p>Auto is the default setting.</p> |
| DRTM Memory Reservation | <ul style="list-style-type: none"> • 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 33. Processor Details

| Item | Format | Description |
|----------------------------|--|--|
| Processor Socket | <ul style="list-style-type: none"> • Socket 1 • Socket n | Display processor socket table. |
| Processor ID | ASCII string | Display tag for the processor ID. |
| Processor Frequency | ASCII string | Display value for the processor frequency. |
| Processor Revision | ASCII string | Display value for the microcode revision. |
| L1 Cache RAM | ASCII string | Display amount of L1 Cache RAM. |
| L2 Cache RAM | ASCII string | Display amount of L2 Cache RAM. |
| L3 Cache RAM | ASCII string | Display amount of L3 Cache RAM. |

Table 33. Processor Details (continued)

| Item | Format | Description |
|---|---------------|---|
| 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 | Display number of supported and enabled processor cores per processor socket. |
| Threads Per Socket (Supported/Enabled) | ASCII strings | Display number of supported and enabled processor threads per processor socket. |
| Dies Per CPU (Supported/ Enabled) | ASCII strings | Display number of dies per installed processor, which can be used to calculate the total activated cores based. See the "Number of CPU Cores Activated" menu selection. Note: Dies Per CPU = NumberOfCcds + NumberOfComplexes |
| Processor 1 Version | ASCII string | Display version of processor 1. |
| Processor n Version | ASCII string | Display version of processor n. |

Recovery and RAS

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

Table 34. Recovery and RAS

| Item | Description |
|--|---|
| “POST Attempts” on page 31 | Configure the number of attempts to POST before the recovery mechanisms is invoked. |
| “Advanced RAS” on page 31 | Choose whether to enable various advanced RAS options. |
| “Disk GPT Recovery” on page 31 | Disk GPT (GUID Partition Table) Recovery Options. |
| “System Recovery” on page 32 | Configure system recovery settings. |

POST Attempts

Table 35. POST Attempts

| Item | Options | Description |
|---------------------------|--|--|
| Post Attempt Limit | <ul style="list-style-type: none"> • 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. |

Advanced RAS

Table 36. Advanced RAS

| Item | Options | Description |
|--------------------------------------|--|--|
| PCI Error Recovery | <ul style="list-style-type: none"> • Enabled (Default) • Disabled | <p>When [Enabled] is selected, it allows the system to recover from an uncorrectable PCIe fault. The faulting PCIe device will be disabled for error containment and the OS will be notified to re-scan the PCIe buses.</p> <p>When [Disabled] is selected, an uncorrectable PCIe fault will result in an NMI.</p> |
| Platform First Error Handling | <ul style="list-style-type: none"> • Enabled (Default) • Disabled | Enable or disable PFEH, cloak individual banks, and mask deferred error interrupts from each bank. |

Disk GPT Recovery

Table 37. Disk GPT Recovery

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

System Recovery

Table 38. System Recovery

| Item | Options | Description |
|----------------------------------|--|--|
| POST Watchdog Timer | <ul style="list-style-type: none"> Enabled Disabled (Default) | Enable or 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 | <ul style="list-style-type: none"> Enabled (Default) Disabled | Enable or disable reboot of the system during non-maskable interrupt. |

Security

Use this menu to configure system security settings.

Table 39. Security

| Item | Description |
|---|----------------------------------|
| “Secure Boot Configuration” on page 32 | Configure Secure Boot options. |
| “Trusted Platform Module (TPM1.2) or (TPM2.0)” on page 34 | Configure the TPM Setup options. |

Secure Boot Configuration

Table 40. Secure Boot Configuration

| Item | Operation | Description |
|----------------------------|--|---|
| Secure Boot Status | <ul style="list-style-type: none"> Disabled Enabled | Display the current secure boot status. |
| Secure Boot Mode | <ul style="list-style-type: none"> Setup Mode User Mode | System performs secure boot authentication when this feature is set to [User Mode] and secure boot is enabled. |
| Secure Boot Setting | <ul style="list-style-type: none"> Enabled Disabled (Default) | <p>When [Enabled] is selected, the Secure Boot feature is Active, Platform Key (PK) is enrolled, and the system is in user mode.</p> <p>To change the mode, resetting the platform is required.</p> |

Table 40. Secure Boot Configuration (continued)

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

View Secure Boot Keys

Table 41. View Secure Boot Keys

| Item | Description |
|-----------------------------|--|
| Secure Boot variable | Display platform keys (PK), key exchange keys (KEK), authorized signature database (DB), and forbidden signature database (DBX). |
| Size | Display the number of key bytes. |
| Keys | Display the Number of certificates (integer). |
| Key Source | Display certificate sources. The sources can be Factory Default , No Keys , Mixed , or Customized . |
| PK | <p>Display the Certificate in PK (Platform Key).</p> <p>Note: There is only one PK in the system.</p> |
| KEK | Display all Certificates in KEK (Key Exchange Key). |

Table 41. View Secure Boot Keys (continued)

| Item | Description |
|------|---|
| DB | Display all Certificates in DB (Authorized Signature Database). |
| DBX | Display all Certificates in DBX (Forbidden Signature Database). |

Secure Boot Custom Policy

Table 42. Secure Boot Custom Policy

| Item | Description |
|----------------------|--|
| Enroll Efi Image | Enroll the SHA256 hash of the selected EFI image binary into the Authorized Signature Database (DB). |
| Secure Boot variable | Display platform keys (PK), key exchange keys (KEK), authorized signature database (DB), and forbidden signature database (DBX). |
| Size | Display the number of key bytes. |
| Keys | Display the number of certificates (integer). |
| Key Source | Display certificate sources. The sources can be Factory Default, No Keys, Mixed, or Customized . |
| PK | Enroll a PK (from a Public Key Certificate file format) or delete the existing PK. Note: There is only one PK in the system. |
| KEK | Enroll a KEK entry (from a Public Key Certificate file format), or delete an existing entry from the KEK. |
| 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. |
| DBX | Enroll a DBX entry (from a Public Key Certificate file format or an EFI image file), or delete the existing entry from the DBX. |

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

For updating the TPM firmware from 2.0 to 1.2:

Table 43. Trusted Platform Module

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

For TPM 2.0 firmware:

Table 44. Trusted Platform Module (TPM2.0)

| Item | Options | Description |
|-----------------------------|---|--|
| TPM Status | | |
| TPM Vendor | | |
| TPM Firmware Version | | |
| [TPM Settings] | | |
| TPM2 Operation | <ul style="list-style-type: none"> • No Action (Default) • Clear • TPM Device has been cleared. | Select [Clear] to clear TPM data. Attention: This will erase the contents of the TPM. System reboot is required. |
| SHA-1 PCR Bank | <ul style="list-style-type: none"> • Enabled • Disabled (Default) | Enable or disable SHA-1 PCR Bank. |

For upgrading the TPM firmware from 1.2 to 2.0:

Table 45. Trusted Platform Module

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

For updating the TPM 2.0 firmware:

Table 46. Trusted Platform Module (TPM 2.0)

| Item | Options | Description |
|-----------------------------|--|-----------------------------------|
| TPM Status | | |
| TPM Vendor | | |
| TPM Firmware Version | | |
| TPM Device State | | |
| TPM Ownership | | |
| [TPM Settings] | | |
| TPM Device | <ul style="list-style-type: none"> • Enabled (Default) • Disabled | Enable or disable the TPM Device. |

Table 46. Trusted Platform Module (TPM 2.0) (continued)

| Item | Options | Description |
|----------------------|---|--|
| TPM State | <ul style="list-style-type: none"> • Activate (Default) • Deactivate | Activate or deactivate the TPM State. |
| TPM Operation | <ul style="list-style-type: none"> • No Action (Default) • Clear • TPM1.2 Device has been cleared | Select [Clear] to clear TPM data. Attention: This will erase the contents of the TPM. System reboot is required. |

For TPM 1.2 firmware:

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

Table 47. Trusted Platform Module (TPM 1.2)

| Item | Options | Description |
|-----------------------------|---|--|
| TPM Status | | |
| TPM Vendor | | |
| TPM Firmware Version | | |
| TPM Device Sate | | |
| TPM Ownership | | |
| [TPM Settings] | | |
| TPM Device | <ul style="list-style-type: none"> • Enabled (Default) • Disabled | Enable or disable the TPM Device. |
| TPM State | <ul style="list-style-type: none"> • Activate (Default) • Deactivate | Activate or deactivate the TPM State. |
| TPM Operation | <ul style="list-style-type: none"> • No Action (Default) • Clear • TPM1.2 Device has been cleared | Select [Clear] to clear TPM data. Attention: This will erase the contents of the TPM. System reboot is required. |

Storage

This menu allows you to manage storage adapter options.

Table 48. Storage

| Item | Description |
|-----------------------------------|---|
| “NVMe” on page 37 | Display a list of NVMe devices. Note: Onboard NVMe devices do not appear when VMD is enabled. |

NVMe

Table 49. NVMe

| Item | Description |
|-------------------------|-----------------------------------|
| Bay X: NVMe Bus-Dev-Fun | Bus-Dev-Fun is PCI address value. |

Table 50. NVMe Detail Information

| Item | Format | Description |
|---------------------------------|--|------------------------------------|
| Model Name | ASCII string | Display model name. |
| Serial Number | ASCII string | Display serial number. |
| Firmware Revision | ASCII string | Display firmware revision. |
| Vendor ID | 0XXXXX (XXXX is hex number) | Display vendor ID. |
| Device ID | 0XXXXX (XXXX is hex number) | Display device ID. |
| Subsystem Vendor ID | 0XXXXX (XXXX is hex number) | Display subsystem vendor ID. |
| Subsystem ID | 0XXXXX (XXXX is hex number) | Display subsystem ID. |
| Maximum Link Speed | Gen N (N is number) | Display maximum link speed. |
| Maximum Link Width | xN (N is number) | Display maximum link width. |
| Negotiated Link Speed | Gen N (N is number) | Display negotiated link speed. |
| Negotiated Link Width | xN (N is number) | Display negotiated link width. |
| Number of Namespaces | N (N is number) | Display number of namespaces. |
| Total Size | X.XX TB (Unit can be GB or MB, depending on the size) | Display total size. |
| Device driver data link: | | |
| Device HII Title | N/A | Display description of device HII. |

Date and Time

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

Table 51. Date and Time

| Item | Format | Description |
|--------------------|------------|---|
| System Date | MM/DD/YYYY | Use the +/- or the numeric keys to set the date of the server. |
| System Time | HH:MM:SS | Use the +/- or the numeric keys to set the time of the server. Use a 24 hour format for entering hours. |

Start Options

Use this menu to select start option for next boot.

Table 52. Start Options

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

Boot Manager

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

Table 53. Boot Manager

| Item | Operation | Description |
|--|------------------------|--|
| Boot Sequence | | |
| “Add Generic Boot Option” on page 39 | N/A | Add one generic boot device as the boot option. |
| Add UEFI Full Path Boot Option | N/A | Add one EFI application or one removable file system as the boot option. |
| Delete Boot Option | N/A | Remove boot option(s) from the boot order. |
| Change Boot Order | N/A | Modify the ordering of selections within the 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 41 | Xxxx {xxxx-xxx-xxx...} | Boot the system from a specific file or a device. |
| Select Next One-Time Boot Option | N/A | Select one-time boot option for the next boot. |
| System | | |

Table 53. Boot Manager (continued)

| Item | Operation | Description |
|-----------------------------------|-----------|---|
| Boot Modes | N/A | Change between the UEFI boot mode and the legacy boot mode. |
| “Reboot System” on page 41 | N/A | 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 54. Add UEFI Full Path Boot Option

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

Delete Boot Option

Table 55. Delete Boot Option

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

Change Boot Order

Table 56. Change Boot Order

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

Set Boot Priority

Table 57. Set Boot Priority

| Item | Description |
|---|--|
| “CD/DVD Priority” on page 40 | Set boot priority for CD/DVD if multiple devices exist in the system. |
| “Hard Disk Priority” on page 40 | Set boot priority for Hard Disk if multiple devices exist in the system. |
| “Network Priority” on page 40 | Set boot priority for Network if multiple devices exist in the system. |
| “USB Priority” on page 41 | Set boot priority for USB if multiple devices exist in the system. |

CD/DVD Priority

Table 58. CD/DVD Priority

| Item | Description |
|-------------------------|--|
| Boot Priority | Change the boot priority for the CD/DVD devices. |
| Commit Changes and Exit | Save changes and exit. |

Hard Disk Priority

Table 59. Hard Disk Priority

| Item | Description |
|-------------------------|---|
| Boot Priority | Change the boot priority for the hard disk devices. |
| Commit Changes and Exit | Save changes and exit. |

Network Priority

Table 60. Network Priority

| Item | Description |
|-------------------------|---|
| Boot Priority | Change boot priority for the network devices. |
| Commit Changes and Exit | Save changes and exit. |

USB Priority

Table 61. USB Priority

| Item | Description |
|-------------------------|---|
| Boot Priority | Change the boot priority for the USB devices. |
| Commit Changes and Exit | Save changes and exit. |

Boot From File

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

Select Next One-Time Boot Option

Table 62. Select Next One-Time Boot Option

| Item | Options | Description |
|-------------|---|---|
| Boot Option | <ul style="list-style-type: none">• CD/DVD Rom• Hard Disk• Network• USB Storage• System Setup• NONE (Default) | Selects one-time boot option for the next boot. |

Boot Mode

Table 63. Boot Mode

| Item | Options | Description |
|----------------------------------|--|--|
| System Boot Mode | <ul style="list-style-type: none">• UEFI Mode (Default)• Legacy Mode | Drivers, option ROMs and OS loaders the Boot Manager attempts to boot. [UEFI Mode] runs UEFI drivers and boot the OS in UEFI Mode. [Legacy Mode] runs option ROMs and boot the OS in Legacy Mode. Note: This feature is set to [UEFI Mode] when Legacy BIOS is disabled. |
| Infinite Boot Retry | <ul style="list-style-type: none">• Enabled• Disabled (Default) | The system continuously attempts the Boot Order. Make sure that a bootable device is specified in Boot Order. |
| Prevent OS Changes To Boot Order | <ul style="list-style-type: none">• Enabled• Disabled (Default) | When [Enabled] is selected, UEFI removes the boot option which is created by OS or OS Installer from the boot order list. |

Reboot System

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

BMC Settings

This menu allows you to configure the management controller.

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

Table 64. BMC Settings

| Item | Options | Description |
|---|---|---|
| Power Restore Policy | <ul style="list-style-type: none"> Always Off Restore (Default) Always On | <p>Determines operation mode after a power loss.</p> <p>[Always Off]: The system remains off even when power is restored.</p> <p>[Restore]: The system returns to the state before power was lost.</p> <p>[Always On]: The system turns on when power is restored.</p> <p>Note: This feature is unable to reset to default value by using the load default in Setup.</p> |
| Power Restore Random Delay | <ul style="list-style-type: none"> Enabled Disabled (Default) | <p>Provides a random delay of 1 to 15 seconds for Power On. If the server status is on before a power failure occurs, the power-on will be delayed once power is restored.</p> <p>Notes:</p> <ul style="list-style-type: none"> <p>Notes:</p> <ul style="list-style-type: none"> This option is platform dependent. This feature is unable to reset to default value by using the load default in Setup. This feature does not appear when Power Restore Policy is set to [Always Off]. |
| Ethernet over USB interface | <ul style="list-style-type: none"> Enabled (Default) Disabled | <p>[Enabled] makes the xClarity Essentials in-band update utility available.</p> <p>[Disabled] prevents xClarity Essentials and other applications running on the server from requesting the BMC to perform tasks.</p> <p>If you modify the "Ethernet Over USB Interface" related settings, the setting values may keep stale for a while and do not immediately reflect the new settings.</p> |
| "Network Settings" on page 43 | N/A | Configure the network of the management controller. |
| Reset Factory Defaults Setting | N/A | Restore all management controller settings to factory defaults, including network configuration and credentials. The management controller will be restarted automatically. |
| Restart BMC | N/A | Restart the BMC. |

Network Settings

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

Table 65. Network Settings

| Item | Options | Description |
|-------------------------------|--|--|
| Network Interface Port | <ul style="list-style-type: none"> • Dedicated (Default) • Shared | Select System Management Network Interface Port. |
| Shared NIC on | OCP Card | Select shared NIC port. Note: This feature appears only when Network Interface Port is set to [Shared]. |
| Fail-Over Rule | <ul style="list-style-type: none"> • None (Default) • Failover to shared (Optional Card ML2) • Failover to shared (Optional Card PHY) • Failover to shared (Onboard Port) | Control the fail-over types allowed. Note: This feature appears only when Network Interface Port is set to [Dedicated]. |
| Network Setting | <ul style="list-style-type: none"> • Synchronization (Default) • Independence | The feature is selectable only when Fail-Over Rule is enabled to onboard port or optional card. |
| Burned-in MAC Address | N/A | Display MAC addresses from the network interface controller. |
| Hostname | N/A | Change host name. The length must be within 1 to 63 characters. |
| DHCP Control | <ul style="list-style-type: none"> • Static IP • DHCP Enabled • DHCP with Fallback (Default) | Configure DHCP Control or configure a static IP address manually. Fallback uses static IP address if DHCP fails. Selects [Static IP] to enter IPV4 address manually. |
| IP Address | x.x.x.x | Enter IP Address in dotted-decimal notation. |
| Subnet Mask | x.x.x.x | Enter Subnet Mask in dotted-decimal notation. |
| Default Gateway | x.x.x.x | Enter Default Gateway in dotted-decimal notation. |
| IPv6 | <ul style="list-style-type: none"> • Enabled (Default) • Disabled | Enable or disable IPv6 support on management port. Note: This feature is unable to reset to default value by using the load default in Setup. |
| Local Link Address | N/A | Display local link address. |

Table 65. Network Settings (continued)

| Item | Options | Description |
|---|--|---|
| VLAN Support | <ul style="list-style-type: none"> Enabled Disabled (Default) | <p>Enable or disable VLAN Support to specify the 802.1q VLAN ID on the management port network device.</p> <p>Note: This feature is unable to reset to default value by using the load default in Setup.</p> |
| VLAN ID | 1 | <p>VLAN ID Range is 1 to 4094.</p> <p>Note: This feature appears only when VLAN Support is enabled.</p> |
| “Advanced Settings for BMC Ethernet” on page 44 | N/A | Provide advanced settings for BMC Ethernet. |
| Save Network Settings | N/A | Save changes in BMC. |

Advanced Settings for BMC Ethernet

Table 66. Advanced Settings for BMC Ethernet

| Item | Options | Description |
|------------------------|---|---|
| Autonegotiation | <ul style="list-style-type: none"> No Yes | <ul style="list-style-type: none"> [No]: You can manually choose the data rate and duplex mode. [Yes]: There is no manual configuration needed. <p>Notes:</p> <ul style="list-style-type: none"> This option is platform dependent (for instance, Protolino does not support it). This feature is unable to reset to default value by using the load default in Setup. |
| Data rate | <ul style="list-style-type: none"> 100 Mb (Ethernet) 10 Mb (Ethernet) | <p>Configure amount of the data to be transferred per second over LAN connection.</p> <p>Notes:</p> <ul style="list-style-type: none"> This feature appears only when Autonegotiation is set to [No]. This feature is unable to reset to default value by using the load default in Setup. |
| Duplex | <ul style="list-style-type: none"> Half Full | <p>Set type of communication channel used in the network.</p> <p>[Full] allows the data to be transferred in both directions simultaneously.</p> <p>[Half] allows the data to be transferred in one direction at a time.</p> <ul style="list-style-type: none"> This feature appears only when Autonegotiation is set to [No]. This feature is unable to reset to default value by using the load default in Setup. |

Table 66. Advanced Settings for BMC Ethernet (continued)

| Item | Options | Description |
|--|-------------|---|
| Maximum Transmission Unit | 1500 | Specify the maximum size of a packet (in bytes) for the network interface. For IPv4 networks, the MTU range is from 68-1500 bytes For IPv6 networks, the MTU range is from 1280-1500 bytes. |
| Note: Changes will be valid after saving network settings in previous page. | | |

System Event Logs

Use this menu to clear or view system event logs.

Table 67. System Event Logs

| Item | Description |
|--|----------------------------|
| "POST Event Viewer" on page 45 | Display POST Event Viewer. |
| "System Event Log" on page 45 | Display System Event Log. |
| Clear System Event Log | Clear System Event Log. |

POST Event Viewer

Table 68. POST Event Viewer

| Item | Description |
|-------------------|--------------|
| Entry [N]: | Information. |

System Event Log

Table 69. System Event Log

| Item | Description |
|--------------------------|--|
| Total SEL entries | |
| Previous Page | Displays system event logs in the previous page. |
| Entry [N]: | Information. |
| Next Page | Displays system event logs in the next page. |

User Security

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

Table 70. User Security

| Item | Description |
|---|---|
| "Password Rule and Policy" on page 47 | Set password rule and policy. |
| Set Power-On Password | <p>Set power-on password.</p> <p>The password can only contain the following characters (excluding white-space characters): A-Z, a-z, 0-9, ~!@#\$\$%^&*()-+={} ;":'<>,?/_</p> <p>Must contain at least one letter.</p> <p>Must contain at least one number.</p> <p>Must contain at least 2 of the following:</p> <ul style="list-style-type: none"> • At least one upper-case letter • At least one lower-case letter • At least one special character <p>No more than 2 consecutive occurrences of the same character</p> <p>Must be at least x characters set in Minimum password length, or 8 characters if Minimum password length is not set.</p> |
| Clear Power-On Password | Clear Power-On password. |
| Set Administrator Password | <p>Set Administrator Password.</p> <p>The password can only contain the following characters (excluding white-space characters): A-Z, a-z, 0-9, ~!@#\$\$%^&*()-+={} ;":'<>,?/_</p> <p>Must contain at least one letter.</p> <p>Must contain at least one number.</p> <p>Must contain at least 2 of the following:</p> <ul style="list-style-type: none"> • At least one upper-case letter • At least one lower-case letter • At least one special character <p>No more than 2 consecutive occurrences of the same character</p> <p>Must be at least x characters set in Minimum password length, or 8 characters if Minimum password length is not set.</p> |
| Clear Administrator Password | Clears Administrator password. |

Password Rule and Policy

Table 71. Password Rule and Policy

| Item | Options | Function |
|---|---------|---|
| Minimum password length | 8-20 | <p>Set a value between 8 and 20.</p> <p>This value indicates the minimum number of characters, which is part of the rules to specify a valid password.</p> <p>Changes take effect right after the value is set. Click “Save Setting” on Main Menu if you would like to keep the setting after the system reboot.</p> |
| Password expiration period | 0-365 | <p>Set passwords to expire after a number of days between 1 and 365, or you can specify that passwords never expire by setting the value to 0.</p> |
| Password expiration warning period | 0-365 | <p>Set a number of days between 0 and 365 before a password expiration to receive a password expiration warning.</p> <p>If you set the value to 0, there is no password expiration warning.</p> |
| Minimum password change interval | 0-240 | <p>Set a value between 0 and 240.</p> <p>This feature allows you to set the minimum interval (in hours) at which users can change the passwords. The value specified for this feature can not exceed the value specified for Password expiration period.</p> <p>If you set the value to 0, users can change the password immediately.</p> |
| Minimum password reuse cycle | 0-10 | <p>Set a value between 0 and 10.</p> <p>This feature allows you to determine the number of unique new passwords that must be set before an old password can be reused.</p> <p>If you set the value to 0, an old password can be reused immediately.</p> <p>Changes take effect right after the value is set. Click “Save Setting” on Main Menu if you would like to keep the setting after the system reboot.</p> |

Table 71. Password Rule and Policy (continued)

| Item | Options | Function |
|--|---------|---|
| Maximum number of login failures | 0-100 | <p>Set a value between 0 and 100.</p> <p>This feature allows you to set a maximum number of times users attempt to login with an incorrect password before user account is locked out. The lockout duration depends on the value of the Lockout period after maximum login failures.</p> <p>If you set the value to 0, the account will never be locked out.</p> |
| Lockout period after maximum login failures | 0-2880 | <p>Set a value between 0 and 2880.</p> <p>This feature allows you to set the number of minutes to lock out an account when the maximum number of failed login attempts is reached. The account is locked even the correct password is entered during the lockout period.</p> <p>If you set the value to 0, the account will never be locked out even the number of Lockout period after maximum login failures is exceeded.</p> |

F12 One Time Boot Device

Use this menu to manage boot devices in the system.

Table 72. Boot Devices Manager

| Item | Options | Description |
|----------------------------------|---|---|
| Legacy Mode | <ul style="list-style-type: none"> • <input type="checkbox"/> • <input checked="" type="checkbox"/> | <p>Override System Boot Mode in the Boot Mode menu.</p> <p>Setting Option ROM Execution Order in the Devices and I/O Ports menu may still affect the boot ordering.</p> <p>It is needed to have PCI 64-Bit Resource Allocation in the Device and I/O Ports menu set to [Disabled] for some network cards' legacy PXE boot option.</p> <p>Notes: When selecting this feature, the page is refreshed to show legacy group:</p> <ul style="list-style-type: none"> • CD/DVD Rom • Hard Disk • Network • USB Storage |
| List of UEFI Boot Options | N/A | Enter in specified boot device. |

Appendix A. Notices

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

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

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

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

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

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

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

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

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

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

Trademarks

LENOVO and LENOVO logo are trademarks of Lenovo.

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

Lenovo

