Lenovo

ThinkSystem server
UEFI Parameter Reference Guide

For 2-socket server models with AMD EPYC (1st, 2nd Gen)

About this document

This document details the basic menu structure, parameters, and common tasks for servers that supports Unified Extensible Firmware Interface (UEFI) features.

Intended Audience

- Lenovo technical support engineers
- Partner technical support engineers
- Enterprise administrators
- Enterprise end users

Tenth Edition (October 2024)

Contents

Chapter 1. Get started

Lenovo ThinkSystem™ SR645/SR665 servers support Unified Extensible Firmware Interface (UEFI) features that enable you to perform a wide range of configuration activities, including:

- Viewing system information and event logs
- Enabling or disabling system features
- Configuring system devices, memory, and network
- Setting date and time
- Configuring BMC
- Configuring boot order
- Setting security policies

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. Save the setting.
4. Restart the server and press F1.
5. 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. Save the setting.
4. Restart the server and press F1.
5. Wait for about 90 seconds, the setup utilities window is displayed in graphic mode.

Chapter 2. System configuration and boot management

Use this section to understand UEFI setting menu structure, available options of each options, and default settings.

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).

Item	Operation	Description
System Configuration and Boot Management		
Select Language	• **English** • 中文（简体） • 中文（繁體） • Français • Deutsch • Italiano • 日本語 • 한국어 • Português(Brasil) • Español • Русский	Selectable option. Press [Enter] to change the language for the current system. The default language is English.
Launch Graphical System Setup		Selectable option. Press [Enter] to enter the graphical user interface for system setup utilities.
System Information		Sub menu. Display the basic details of the system.
System Settings		Sub menu. Display or modify system settings. Changes may not take effect immediately. Save any changed settings and reboot the system.
Date and Time		Sub menu. Set the local Date and Time of the system.
Start Options		Sub menu. Boot a desired selection from the primary boot sequence as specified under **Boot Manager**.
Boot Manager		Sub menu. Change boot order, boot parameters, and boot from a file.

Item	Operation	Description
BMC Settings		Sub menu. Configure the management controller.
System Event Logs		Sub menu. Clear or view the System Event Log.
User Security		Sub menu. Set or change Power-On and Administrator passwords.
Save Settings		Executive item. Press [Enter] to save the changes and commit them to BMC.
Discard Settings		Executive item. Press [Enter] to discard any changes during this login.
Load Default Settings		Executive item. Press [Enter] to load the default values for system settings.
Exit Setup Utility		Executive item. Press [Enter] to exit Setup.

System information

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

Table 1. System information details

Item	Operation	Description
System Summary		Sub menu. Displays the basic details of the system.
Product Data		Sub menu. Displays system firmware information.
Open Source License		Sub menu. Displays the open source license information.

System Summary

Item	Operation	Description
System Identification Data		
Machine Type/Model		Dynamic information. Displays the system machine type and model.
Serial Number		Dynamic information. Displays the tag for the serial number.
UUID Number		Dynamic information. Displays the tag for the UUID.
Asset Tag Number		Dynamic information. Displays a customer assigned system asset tag number.
Processor		
Installed CPU packages		Dynamic information. Displays the number of installed CPU packages.
Processor Speed		Dynamic information. Displays the processor speed.
Memory		
Memory Mode		Dynamic information. Displays the memory mode.
Memory Speed		Dynamic information. Displays the installed memory speed.
Total Memory Detected		Dynamic information. Displays the total amount of the memory from the sum of all DIMM installed.
Total Usable Memory Capacity		Dynamic information. Displays the amount of usable memory after deducting the overhead caused by mirroring mode, reserved or bad blocks, etc.

Product Data

Use this section to view product data.

Item	Operation	Description
Host Firmware		
Build ID		Dynamic information. Displays the build ID of the host firmware.
Version		Dynamic information. Displays the version of the host firmware.
Build Date		Dynamic information. Displays the build date of the host firmware.
BMC Firmware		
Build ID		Dynamic information. Displays the build ID of the BMC firmware.
Version		Dynamic information. Displays the version of the BMC firmware.
Build Date		Dynamic information. Displays the build date of the BMC firmware.

Open Source License

Use this section to view open source licenses.

Item	Operation	Description
Open Source License		
		Dynamic information. Displays the available open source licenses.

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

System Settings

This chapter details System Settings options.

Select **System Settings** and press Enter. Then, the following system setting options are displayed.

Notes:

- SAS/SATA drives or NVMe drives connected to a storage controller will be displayed in the storage controller submenu: **System settings → Storage → Storage controller xxxx**.
- NVMe drives connected to the system without raid controller (sometimes using a retimer) will be displayed in one of the following pages:
  - **System settings → Foreign Devices**
  - **System settings → Storage**

Table 2. System setting details

Item	Operation	Description
<FI> Start Control	• **Auto** • Tool Suite • Text Setup	Selectable option. Controls the tools that are started using the F1 key or equivalent IPMI command. • [Tool Suite] starts a graphical suite of tools which support System Information, UEFI setup, Platform Update, Raid Setup, OS installation and Diagnostics functions. • [Text Setup] starts a text mode UEFI setup utility. • [Auto] starts text mode UEFI setup if Serial Over Lan (SOL) or "Console Redirection" are enabled or SOL is configured to [Auto] and an active session is detected. Otherwise, [Auto] starts the graphical [Tool Suite].
“Device and I/O ports” on page 13		Sub menu. Press [Enter] to view onboard devices and I/O port options.
“Driver Health” on page 32		Sub menu. Press [Enter] to view the health of the controllers in the system as reported by their corresponding drivers.
“Foreign Devices” on page 34		Sub menu. Press [Enter] to view the list of foreign devices.
“Legacy BIOS” on page 35		Sub menu. Press [Enter] to configure system UEFI firmware execution environment preferences for supporting legacy OS and legacy Option ROM.
“Memory” on page 36		Sub menu. Press [Enter] to view or modify options to change the memory settings.
“Network” on page 41		Sub menu. Press [Enter] to configure network devices and network related settings.

Table 2. System setting details (continued)

“Operating Modes” on page 48		Sub menu. Press [Enter] to select the operating mode based on your preference. **Note:** Power savings and performance are also highly dependent on hardware configuration and the software running on the system.
“Power” on page 51		Sub menu. Press [Enter] to configure power scheme options.
“Processors” on page 52		Sub menu. Press [Enter] to view or modify options to change the processor settings.
“Recovery and RAS” on page 58		Sub menu. Press [Enter] to configure recovery policies and advanced reliability, availability, and serviceability settings.
“Security” on page 62		Sub menu. Press [Enter] to configure system security settings.
“Storage” on page 73		Sub menu. Press [Enter] to configure storage adapter options. Some systems may use planar devices and can be configured under **Devices and I/O Ports**.

Device and I/O ports

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

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

Item	Operation	Description
Active Video	• **Onboard Device** • Add-in Device	Selectable option. This setting only applies if the server has an add-in video adapter. When the option ROM is set to Legacy for both onboard and add-in video adapters, the Active Video setting controls which single adapter will display the System Setup utility. **Note:** This setting does not affect how the OS chooses to display its graphical desktop. The system boot early video is displayed at the onboard video only, and the management controller remote console shows the onboard video only.
PCI 64-Bit Resource Allocation	• Enable • Disable • **Auto**	Selectable option. Press [Enter] to enable or disable the allocation of 64-bit resources for PCI. **Auto** is the default setting, would allocate some resources below 4GB for legacy compatibility.
IOMMU	• Enable • Disable • **Auto**	Selectable option. Press [Enter] to enable or disable Input/Output Memory Management Unit (IOMMU). **Auto** is the default setting, would allow the system to flexibly enable or disable IOMMU by decision.
SRIOVs	• **Enable** • Disable	Selectable option. Press [Enter] to enable or disable the support of resource allocation for Single Root I/O Virtualization (SR-IOV) virtual functions during boot. **Enable** is the default setting.
PCIe Ten Bit Tag Support	• **Disabled** • Enabled	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.
“Enable/Disable Onboard Device (s)” on page 15		Sub menu. Press [Enter] to enable or disable onboard devices or slots.

“Enable/Disable Adapter Option ROM Support” on page 21		Sub menu. Press [Enter] to control Legacy and UEFI-compliant adapter support. Disabling UEFI/Legacy support may adversely affect pre-boot/boot functions.
“Set Option ROM Execution Order” on page 22		Sub menu. Press [Enter] to control legacy ROM load order.
“PCIe Gen Speed Selection” on page 24		Sub menu. Press [Enter] to choose the generation speed for available PCIe slots.
“Override Slot Bifurcation” on page 27		Sub menu. Press [Enter] to override the slot bifurcation setting of the physical x16 slot to support the adapter with multiple devices.
“Console Redirection Settings” on page 28		Sub menu. Press [Enter] to configure console redirection and COM port settings.
“USB Configuration” on page 31		Sub menu. Press [Enter] to enable or disable USB storage devices or individual ports.

Enable/Disable Onboard Device(s)

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

- SR665
- SR645

SR665

Item	Operation	Description
Onboard Video	• **Enable** • Disable	Selectable option. Disabling an entry will prevent the associated device from being enumerated during subsequent boots. **Enable** is the default setting. **Auto** is removing the port if there is no device or errors on that device. **Note:** **Auto** is the setting for PCIe devices by CPU only.
Onboard SATA	• **Enable** • Disable	Selectable option. Disabling an entry will prevent the associated device from being enumerated during subsequent boots. **Enable** is the default setting. **Auto** is removing the port if there is no device or errors on that device. **Note:** **Auto** is the setting for PCIe devices by CPU only.
Slot n (Displaying slot 1/2/3/4/5/6/7/8 depending on which riser card is installed)	• **Enable** • Disable or • **Enable** • Disable • Auto	Selectable option. Disabling an entry will prevent the associated device from being enumerated during subsequent boots. **Enable** is the default setting. **Auto** is removing the port if there is no device or errors on that device. **Note:** **Auto** is the setting for PCIe devices by CPU only.
Slot 9 (For OCP 3.0 adapter)	• **Enable** • Disable or • **Enable** • Disable • Auto	Selectable option. Disabling an entry will prevent the associated device from being enumerated during subsequent boots. **Enable** is the default setting. **Auto** is removing the port if there is no device or errors on that device. **Note:** **Auto** is the setting for PCIe devices by CPU only.

Item	Operation	Description
Slot 10 (For CFF RAID/HBA adapter)	• **Enable** • Disable or • **Enable** • Disable • Auto	Selectable option. Disabling an entry will prevent the associated device from being enumerated during subsequent boots. **Enable** is the default setting. **Auto** is removing the port if there is no device or errors on that device. **Note: Auto** is the setting for PCIe devices by CPU only.
Slot 11 (For CPU1 7mm SSD)	• **Enable** • Disable or • **Enable** • Disable • Auto	Selectable option. Disabling an entry will prevent the associated device from being enumerated during subsequent boots. **Enable** is the default setting. **Auto** is removing the port if there is no device or errors on that device. **Note: Auto** is the setting for PCIe devices by CPU only.
Slot 12 (For CPU2 7mm SSD)	• **Enable** • Disable or • **Enable** • Disable • Auto	Selectable option. Disabling an entry will prevent the associated device from being enumerated during subsequent boots. **Enable** is the default setting. **Auto** is removing the port if there is no device or errors on that device. **Note: Auto** is the setting for PCIe devices by CPU only.
Slot 13 (For CPU1 M.2 SSD)	• **Enable** • Disable or • **Enable** • Disable • Auto	Selectable option. Disabling an entry will prevent the associated device from being enumerated during subsequent boots. **Enable** is the default setting. **Auto** is removing the port if there is no device or errors on that device. **Note: Auto** is the setting for PCIe devices by CPU only.
Slot 14 (For CPU1 M.2 SSD)	• **Enable** • Disable	Selectable option. Disabling an entry will prevent the associated device from being enumerated during subsequent boots. **Enable** is the default setting. **Auto** is removing the port if there is no device or errors on that device. **Note: Auto** is the setting for PCIe devices by CPU only.

Item	Operation	Description
Slot 15 (For CPU2 M.2 SSD)	• **Enable** • Disable or • **Enable** • Disable • Auto	Selectable option. Disabling an entry will prevent the associated device from being enumerated during subsequent boots. **Enable** is the default setting. **Auto** is removing the port if there is no device or errors on that device. **Note: Auto** is the setting for PCIe devices by CPU only.
Slot 16 (For CPU2 M.2 SSD)	• **Enable** • Disable or • **Enable** • Disable • Auto	Selectable option. Disabling an entry will prevent the associated device from being enumerated during subsequent boots. **Enable** is the default setting. **Auto** is removing the port if there is no device or errors on that device. **Note: Auto** is the setting for PCIe devices by CPU only.

SR645

Item	Operation	Description
Onboard Video	• **Enable** • Disable	Selectable option. Disabling an entry will prevent the associated device from being enumerated during subsequent boots. **Enable** is the default setting. **Auto** is removing the port if there is no device or errors on that device. **Note: Auto** is the setting for PCIe devices by CPU only.
Onboard SATA	• **Enable** • Disable	Selectable option. Disabling an entry will prevent the associated device from being enumerated during subsequent boots. **Enable** is the default setting. **Auto** is removing the port if there is no device or errors on that device. **Note: Auto** is the setting for PCIe devices by CPU only.
Slot n (Displaying slot 1/2/3 depending on which riser card is installed)	• **Enable** • Disable or • **Enable** • Disable • Auto	Selectable option. Disabling an entry will prevent the associated device from being enumerated during subsequent boots. **Enable** is the default setting. **Auto** is removing the port if there is no device or errors on that device. **Note: Auto** is the setting for PCIe devices by CPU only.
Slot 4 (For OCP 3.0 adapter)	• **Enable** • Disable or • **Enable** • Disable • Auto	Selectable option. Disabling an entry will prevent the associated device from being enumerated during subsequent boots. **Enable** is the default setting. **Auto** is removing the port if there is no device or errors on that device. **Note: Auto** is the setting for PCIe devices by CPU only.
Slot 5 (For CFF RAID/HBA adapter)	• **Enable** • Disable	Selectable option. Disabling an entry will prevent the associated device from being enumerated during subsequent boots. **Enable** is the default setting. **Auto** is removing the port if there is no device or errors on that device. **Note: Auto** is the setting for PCIe devices by CPU only.

Item	Operation	Description
Slot 6 (For CPU1 7mm SSD)	• **Enable** • Disable or • **Enable** • Disable • Auto	Selectable option. Disabling an entry will prevent the associated device from being enumerated during subsequent boots. **Enable** is the default setting. **Auto** is removing the port if there is no device or errors on that device. **Note: Auto** is the setting for PCIe devices by CPU only.
Slot 7 (For CPU2 7mm SSD)	• **Enable** • Disable or • **Enable** • Disable • Auto	Selectable option. Disabling an entry will prevent the associated device from being enumerated during subsequent boots. **Enable** is the default setting. **Auto** is removing the port if there is no device or errors on that device. **Note: Auto** is the setting for PCIe devices by CPU only.
Slot 8 (For CPU1 M.2 SSD)	• **Enable** • Disable or • **Enable** • Disable • Auto	Selectable option. Disabling an entry will prevent the associated device from being enumerated during subsequent boots. **Enable** is the default setting. **Auto** is removing the port if there is no device or errors on that device. **Note: Auto** is the setting for PCIe devices by CPU only.
Slot 9 (For CPU1 M.2 SSD)	• **Enable** • Disable or • **Enable** • Disable • Auto	Selectable option. Disabling an entry will prevent the associated device from being enumerated during subsequent boots. **Enable** is the default setting. **Auto** is removing the port if there is no device or errors on that device. **Note: Auto** is the setting for PCIe devices by CPU only.

Item	Operation	Description
Slot 10 (For CPU2 M.2 SSD)	• **Enable** • Disable or • **Enable** • Disable • Auto	Selectable option. Disabling an entry will prevent the associated device from being enumerated during subsequent boots. **Enable** is the default setting. **Auto** is removing the port if there is no device or errors on that device. **Note: Auto** is the setting for PCIe devices by CPU only.
Slot 11 (For CPU2 M.2 SSD)	• **Enable** • Disable or • **Enable** • Disable • Auto	Selectable option. Disabling an entry will prevent the associated device from being enumerated during subsequent boots. **Enable** is the default setting. **Auto** is removing the port if there is no device or errors on that device. **Note: Auto** is the setting for PCIe devices by CPU only.

Enable/Disable Adapter Option ROM Support

Note: The items' actual order may be different from the table below for some of them are dynamically scanned.

If any onboard/slot device option is changed to <Legacy>, onboard video option will be automatically changed to <legacy>. And user cannot change onboard video option, but user can change it if the onboard/slot device option is not <legacy>.

Item	Operation	Description
Network	• Do not launch • **UEFI** • Legacy	Selectable option. Select whether UEFI or legacy option ROM of this device will be executed. [Do not launch] means both UEFI and legacy option ROM will not be executed. **UEFI** is the default setting.
Storage	• Do not launch • **UEFI** • Legacy	Selectable option. Select whether UEFI or legacy option ROM of this device will be executed. [Do not launch] means both UEFI and legacy option ROM will not be executed. **UEFI** is the default setting.
Video	• Do not launch • **UEFI** • Legacy	Selectable option. Select whether UEFI or legacy option ROM of this device will be executed. [Do not launch] means both UEFI and legacy option ROM will not be executed. **UEFI** is the default setting.
Other PCI devices	• Do not launch • **UEFI** • Legacy	Selectable option. Select whether UEFI or legacy option ROM of this device will be executed. [Do not launch] means both UEFI and legacy option ROM will not be executed. **UEFI** is the default setting.

Set Option ROM Execution Order

Note: The items' actual order may be different from the table below for some of them are dynamically scanned.

- SR665
- SR645

SR665

Item	Operation	Description
Set Option ROM Execution Order	• Onboard Video • Onboard SATA • Slot 1 • Slot 2 • Slot 3 • Slot 4 • Slot 5 • Slot 6 • Slot 7 • Slot 8 • Slot 9 • Slot 10 • Slot 11 • Slot 12 • Slot 13 • Slot 14 • Slot 15 • Slot 16	Selectable option. Select the load order for legacy PCI option ROM(s). Use the + key to execute the selected devices ROM sooner or – key to execute later. **Note:** This order may be overridden for devices controlled by UEFI drivers.

SR645

Item	Operation	Description
Set Option ROM Execution Order	• Onboard Video • Onboard SATA • Slot 1 • Slot 2 • Slot 3 • Slot 4 • Slot 5 • Slot 6 • Slot 7 • Slot 8 • Slot 9 • Slot 10 • Slot 11	Select the load order for legacy PCI option ROM(s). Use the + key to execute the selected devices ROM sooner or – key to execute later. **Note:** This order may be overridden for devices controlled by UEFI drivers.

PCIe Gen Speed Selection

- SR665
- SR645

SR665

Note: Some adapters may not operate correctly in Generation 2, Generation 3 or Generation 4. Make sure to power off and power on the system for these settings to take effect.

Item	Operation	Description
Slot n (Displaying slot 1/2/3/4/5/6/7/8 depending on which riser card is installed)	• **Auto** • Gen1 • Gen2 • Gen3 • Gen4 (Need riser supported)	Set the PCIe slot as Auto, Generation 1, Generation 2, Generation 3, or Generation 4.
Slot 9 (For OCP 3.0 adapter)	• **Auto** • Gen1 • Gen2 • Gen3 • Gen4	Set the PCIe slot as Auto, Generation 1, Generation 2, Generation 3, or Generation 4.
Slot 10 (For CFF RAID/HBA adapter)	• **Auto** • Gen1 • Gen2 • Gen3 • Gen4	Set the PCIe slot as Auto, Generation 1, Generation 2, Generation 3, or Generation 4.
Slot 11 (For CPU1 7mm SSD)	• **Auto** • Gen1 • Gen2 • Gen3 • Gen4	Set the PCIe slot as Auto, Generation 1, Generation 2, Generation 3, or Generation 4.
Slot 12 (For CPU2 7mm SSD)	• **Auto** • Gen1 • Gen2 • Gen3 • Gen4	Set the PCIe slot as Auto, Generation 1, Generation 2, Generation 3, or Generation 4.
Slot 13 (For CPU1 M.2 SSD)	• **Auto** • Gen1 • Gen2 • Gen3 • Gen4	Set the PCIe slot as Auto, Generation 1, Generation 2, Generation 3, or Generation 4.

Item	Operation	Description
Slot 14 (For CPU1 M.2 SSD)	• **Auto** • Gen1 • Gen2 • Gen3 • Gen4	Set the PCIe slot as Auto, Generation 1, Generation 2, Generation 3, or Generation 4.
Slot 15 (For CPU2 M.2 SSD)	• **Auto** • Gen1 • Gen2 • Gen3 • Gen4	Set the PCIe slot as Auto, Generation 1, Generation 2, Generation 3, or Generation 4.
Slot 16 (For CPU2 M.2 SSD)	• **Auto** • Gen1 • Gen2 • Gen3 • Gen4	Set the PCIe slot as Auto, Generation 1, Generation 2, Generation 3, or Generation 4.

SR645

Note: Some adapters may not operate correctly in Generation 2, Generation 3 or Generation 4. Make sure to power off and power on the system for these settings to take effect.

Item	Operation	Description
Slot n (Displaying slot 1/2/3 depending on which riser card is installed)	• **Auto** • Gen1 • Gen2 • Gen3 • Gen4 (Need riser supported)	Set the PCIe slot as Auto, Generation 1, Generation 2, Generation 3, or Generation 4.
Slot 4 (For OCP 3.0 adapter)	• **Auto** • Gen1 • Gen2 • Gen3 • Gen4	Set the PCIe slot as Auto, Generation 1, Generation 2, Generation 3, or Generation 4.
Slot 5 (For CFF RAID/HBA adapter)	• **Auto** • Gen1 • Gen2 • Gen3 • Gen4	Set the PCIe slot as Auto, Generation 1, Generation 2, Generation 3, or Generation 4.
Slot 6 (For CPU1 7mm SSD)	• **Auto** • Gen1 • Gen2 • Gen3 • Gen4	Set the PCIe slot as Auto, Generation 1, Generation 2, Generation 3, or Generation 4.
Slot 7 (For CPU2 7mm SSD)	• **Auto** • Gen1 • Gen2 • Gen3 • Gen4	Set the PCIe slot as Auto, Generation 1, Generation 2, Generation 3, or Generation 4.
Slot 8 (For CPU1 M.2 SSD)	• **Auto** • Gen1 • Gen2 • Gen3 • Gen4	Set the PCIe slot as Auto, Generation 1, Generation 2, Generation 3, or Generation 4.
Slot 9 (For CPU1 M.2 SSD)	• **Auto** • Gen1 • Gen2 • Gen3 • Gen4	Set the PCIe slot as Auto, Generation 1, Generation 2, Generation 3, or Generation 4.

Item	Operation	Description
Slot 10 (For CPU2 M.2 SSD)	• **Auto** • Gen1 • Gen2 • Gen3 • Gen4	Set the PCIe slot as Auto, Generation 1, Generation 2, Generation 3, or Generation 4.
Slot 11 (For CPU2 M.2 SSD)	• **Auto** • Gen1 • Gen2 • Gen3 • Gen4	Set the PCIe slot as Auto, Generation 1, Generation 2, Generation 3, or Generation 4.

Override Slot Bifurcation

Menu item	Operation	Function description
Override Slot Bifurcation		
		Dynamic information.

Console Redirection Settings

Item	Operation	Description
COM Port 1	• **Enable** • Disable	Enable or disable COM 1 device. If [Disable] is selected, the associated COM1 terminal settings will be hidden. **Enable** is the default setting.
COM Port 2	• **Enable** • Disable	Enable or disable COM 2 device. If [Disable] is selected, the associated COM 2 terminal settings will be hidden. **Enable** is the default setting.
Console Redirection	• Enable • Disable • **Auto**	Set remote console redirection preference to enable or disable console redirection. While [Auto] is selected, console redirection will be enabled automatically if IPMI Serial over LAN status is active. **Auto** is the default setting.
Serial Port Sharing	• Enable • **Disable**	Enable the system Baseboard Management Controller to allow access to the system serial port. If this option is set to [Enable], the BMC will be allowed to control the serial communication port as requested by remote control commands. If sharing is [Disable], the serial port will be assigned to the BMC unless the “Serial Port Access Mode” is set to [Disable]. **Disable** is the default setting.
Serial Port Access Mode	• Shared • Dedicated • **Disable**	This option allows you to control the access the system Baseboard Management Controller has over the system serial port. 1. Shared mode: By selecting [Shared], the serial port will be available for POST and operating system use; however the BMC will/can monitor the serial data for a takeover control sequence. 2. Dedicated mode: By selecting [Dedicated], the BMC will have complete control of the serial port and POST and/or the operating system will not be able to use the serial port. 3. Disable mode: By selecting [Disable], the BMC will not have any access to the serial port. **Disable** is the default setting.
SP Redirection	• Enable • **Disable**	This option is available only when **Console Redirection**, **COM Port 1**, and **COM Port 2** are set to [Enable]. It allows you to choose which COM port to have the redirection. **Disable** is the default setting.
Legacy OS/Option ROM Display	• COM Port 2 • **COM Port 1**	Select a COM port to display redirection of Legacy OS and Legacy option ROM messages. **COM Port 1** is the default setting.
COM1 Settings	N/A	Settings required for serial connections used for asynchronous start-stop communication.

Item	Operation	Description
COM1 Baud Rate	• **115200** • 57600 • 38400 • 19200 • 9600	Control the connection speed between the host and remote system. **115200** is the default setting.
COM1 Data Bits	• **8** • 7	Set the number of Data bits in each character.
COM1 Parity	• **None** • Odd • Even	Select parity bit in each character to be [None], [Odd], or [Even]. [None] means that no parity bit is sent at all. **None** is the default setting.
COM1 Stop Bits	• 2 • **1**	Set Stop Bits. Stop Bits sent at the end of every character allow the signal receiver to detect the end of a character and to resynchronize with the character stream.
COM1 Terminal Emulation	• VT100 • VT-UTF8 • **ANSI**	Select [VT100] only if the remote emulator does not support ANSI text graphics. Consult the emulator documentation for more information. **ANSI** is the default setting. **Note:** If needed, change the character encoding setting in the remote emulator to ensure the characters show correctly.
COM1 Active After Boot	• **Enable** • Disable	When [Disable] is selected, the Legacy Console Redirection is disabled before booting to legacy OS. When [Enable] is selected, the Legacy Console Redirection is enabled for legacy OS. **Enable** is the default setting.
COM1 Flow Control	• **Disable** • Hardware	Select [Hardware] only if the remote emulator support and is using hardware flow control. Consult the emulator documentation for more information. **Disable** is the default setting.
COM2 Settings		Settings required for serial connections used for asynchronous start-stop communication.
COM2 Baud Rate	• **115200** • 57600 • 38400 • 19200 • 9600	Control the connection speed between the host and remote system. **115200** is the default setting.
COM2 Data Bits	• **8** • 7	Set the number of Data bits in each character.
COM2 Parity	• **None** • Odd • Even	Select parity bit in each character to be [None], [Odd], or [Even]. [None] means that no parity bit is sent at all. **None** is the default setting.

Item	Operation	Description
COM2 Stop Bits	• 2 • **1**	Set Stop Bits. Stop Bits sent at the end of every character allow the signal receiver to detect the end of a character and to resynchronize with the character stream.
COM2 Terminal Emulation	• VT100 • VT-UTF8 • **ANSI**	Select [VT100] only if the remote emulator does not support ANSI text graphics. Consult the emulator documentation for more information. **ANSI** is the default setting.
COM2 Active After Boot	• **Enable** • Disable	When [Disable] is selected, the Legacy Console Redirection is disabled before booting to legacy OS. When [Enable] is selected, the Legacy Console Redirection is enabled for legacy OS. **Enable** is the default setting.
COM2 Flow Control	• **Disable** • Hardware	Select [Hardware] only if the remote emulator support and is using hardware flow control. Please consult the emulator documentation for more information. **Disable** is the default setting.

USB Configuration

Item	Operation	Description
USB Mass Storage Driver Support	• **Enable** • Disable	Enable/Disable USB Mass Storage Driver Support. This setting only takes effect in post time. **Enable** is the default setting. **Notes:** If the USB Mass Storage Driver Support is disabled, • The GUI tool for UEFI Setup utilities is disabled, in this case, the UEFI Setup utilities can only be launched in text mode. • Some other features relying on the USB Mass Storage Driver Support might be disabled as well.
USB 3 Front/Rear Port 1	• **Enable** • Disable	Enable or Disable USB individual ports. **Enable** is the default setting.
USB 2 Front Port	• **Enable** • Disable	Enable or Disabe USB individual ports. **Enable** is the default setting.

Driver health

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

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

Item	Operation	Description
POST Attempts Driver	• **Healthy** • Repair Required • Configuration Required • Operation Failed • Reconnect Required • Reboot Required • Shutdown Required • No Operation Required	Select this option to view the health of post attempts driver.
Partition Driver (MBR/GPT/El Torito)	• **Healthy** • Repair Required • Configuration Required • Operation Failed • Reconnect Required • Reboot Required • Shutdown Required • No Operation Required	Select this option to view the health of partition driver.

Foreign Devices

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

Notes:

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

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

Legacy BIOS

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

Item	Operation	Description
Legacy BIOS	• **Enable** • Disable	Enable or disable the system UEFI firmware execution environment for supporting legacy OS and legacy Option ROM. **Enable** is the default setting.
Rehook INT 19h	• Enable • **Disable**	[Enable] prevents devices from taking control of the boot process. **Disable** is the default setting.
Legacy BIOS is disabled due to secure boot is enabled.		**Note:** Available only when secure boot is enabled.

Memory

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

Note: Options that are marked as “N/A” are read-only information and cannot be changed.

Item	Operation	Description
“System Memory Details” on page 38		Provides status of System Memory.
Total Usable Memory Capacity	yyyy GB	Displays the total usable memory capacity.
Memory Speed	• Maximum • xxxxMHz • Minimum	Dynamic information. The memory speed is changed dynamically according to the combination of the installed CPU SKU, DIMM type, number of DIMMs per channel, and system motherboard support. The system operates at the rated speed of the slowest DIMM in the system when populated with different speed DIMMs. If DIMMs are installed with a rated speed below 2400, this will result in the memory speed getting set to the Minimum value.
Memory Power Down Enable	• **Enable** • Disable	Enable or disable low-power features for DIMMs. **Enable** is the default setting.
NUMA Nodes per Socket	• NPS0 • **NPS1** • NPS2 • NPS4	Specifies the number of desired NUMA nodes per CPU socket(e.g. NPS1 means 1 NUMA per socket). NPS0 will attempt to interleave the 2 CPU sockets together (non-NUMA mode).
DRAM Scrub Time	• Disable • 1 hour • 4 hour • 8 hour • 16 hour • **24 hour** • 48 hour	Sets the period of time between successive DRAM scrub events.
DRAM Post Package Repair	• **Enable** • Disable	Enable or disable DRAM Post Package Repair. **Enable** is the default setting.
SMEE	• Enable • **Disable**	Control secure memory encryption enable. **Disable** is the default setting.
SEV ASID Count	• 253 ASIDs • 509 ASIDs • **AUTO**	This field specifies the maximum valid ASID, which affects the maximum system physical address space. 16TB of physical address space is available for systems that support 253 ASIDs, while 8TB of physical address space is available for systems that support 509 ASIDs.
SEV-ES ASID Space Limit Control	• **AUTO** • Manual	Customize SEV-ES ASID space limit.

Item	Operation	Description
SEV-ES ASID Space Limit	1	SEV VMs using ASIDs below the SEV-ES ASID Space Limit must enable the SEV-ES feature. ASIDs from SEV-ES ASID Space Limit to (SEV ASID Count + 1) can only be used with SEV VMs. If this field is set to (SEV ASID Count + 1), all ASIDs are forced to be SEV-ES ASIDs. Hence, the valid values for this field is 1 - (SEV ASID Count + 1) Valid value: 1 - 510 **Note:** This option is available if "SEV-ES ASID Space Limit Control" is set to **Manual**.
SubUrgRefLowerBound	[4]	Specifies the stored refresh limit to required enter sub-urgent refresh mode. Constraint: SubUrgRefLowerBound is less than or equal to UrgRefLimit. Valid value: 6 ~ 1.
UrgRefLimit	[6]	Specifies the stored refresh limit to required enter urgent refresh mode. Constraint: SubUrgRefLowerBound is less than or equal to UrgRefLimit. Valid value: 6 ~ 1.
DRAM Refresh Rate	• **1x** • 2x	For better performance, a refresh rate of 1x is recommended. To mitigate rowhammer issue, choose refresh rate 2x, note that this may have a performance side effect. **1x** is the default setting.
TSME	• Disable • Enable • **AUTO**	TSME refers to Transparent Secure Memory Encryption. If choose Enable, the following parameters will be displayed: • AddrTweakEn = 1 • ForceEncrEn = 0 • DataEncrEn = 1 **AUTO** is the default setting.
"RAM Disk Configuration" on page 39		Sub menu. Press [Enter] to add or remove RAM disks.

System Memory Details

Item	Operation	Description
DIMM Details For Processor X		Display DIMM status.
DIMM Details		Display DIMM population list. **Note:** When a DIMM has double-bit errors (DBE), the [Enable] and [Disable] options will be available. For current generation, **Enable** is the default setting.

RAM Disk Configuration

Use this menu to add or remove RAM disks.

Item	Operation	Description
RAM Disk Configuration		
Disk Memory Type	• **Boot Service Data** • Reserved	Selectable option. Specifies type of memory to use from available memory pool in system to create a disk. **Boot Service Data** is the default setting.
Create raw		Selectable sub menu. Create a raw RAM disk.
Create from file		Executable item. Click [Enter] to create a RAM disk from a given file.
Created RAM disk list		Executable item. Select the created RAM disk list if you desire to remove it.
Remove selected RAM disk(s)		Executable item. Remove selected RAM disk(s).

Create raw

Use this menu to add a raw RAM disks.

Item	Operation	Description
Add A Raw RAM Disk		
Size (Hex)	1000	Text input. The valid RAM disk size should be multiples of the RAM disk block size. **Boot Service Data** is the default setting.
Create & Exit		Executable item. Click [Enter] to create a new RAM disk with the given starting and ending address.
Discard & Exit		Executable item. Click [Enter] to discard the changes.

Network

This menu displays network devices and network related setting.

Item	Operation	Description
Global Network Settings		
“Network Stack Settings” on page 42		Specify Network Stack Settings.
“Network Boot Settings” on page 43		Configure the network boot parameters.
“HTTP Boot Configuration” on page 44		Configure HTTP boot parameters.
“Tls Auth Configuration” on page 45		Select Tls authentication configuration.

Network Stack Settings

Item	Operation	Description
Network Stack	• **Enable** • Disable	Enable or disable UEFI Network Stack. **Enable** is the default setting.
IPv4 PXE Support	• **Enable** • Disable	Enable or disable IPv4 PXE Boot Support. If disabled, IPv4 PXE boot option will not be created. **Enable** is the default setting.
IPv4 HTTP Support	• Enable • **Disable**	Enable or disable IPv4 HTTP Boot Support. If disabled, IPv4 HTTP boot option will not be created. **Enable** is the default setting.
IPv6 PXE Support	• **Enable** • Disable	Enable IPv6 PXE Boot Support. If disabled, IPv6 PXE boot option will not be created. **Enable** is the default setting.
IPv6 HTTP Support	• Enable • **Disable**	Enable IPv6 HTTP Boot Support. If disabled IPv6 HTTP boot option will not be created. **Disable** is the default setting.
IPSEC Certificate	• **Enable** • Disable	Enable or disable IPSEC certificate for IKEV. **Enable** is the default setting.
PXE boot wait time	0	Wait time in seconds to press ESC key to abort the PXE boot. Use either +/- or numeric keys to set the value. **Notes:** When inputting an invalid value, the following popup message box will show up: • ERROR • Invalid Input Range • Ok
Media detect count	1	Number of times presence of media will be checked. Use either +/- or numeric keys to set the value. **Notes:** When inputting an invalid value, the following popup message box will show up: • ERROR • Invalid Input Range • Ok

Network Boot Settings

Item	Operation	Description
VLAN Configuration list List of NICs in the system Example: MAC:XX:XX:XX:XX:XX:XX Onboard PFA XX:XX:XX	N/A	Display the boot configuration parameters on below items based on the installed network adapter. Example: MAC XX:XX:XX:XX:XX:XX PCI Function Address: Bus XX:Dev XX:Func: XX

HTTP Boot Configuration

Note: This menu is displayed only when IPv4 or IPv6 HTTP is enabled. The device information will be displayed when the network adapter is installed in the system, otherwise, no information will be displayed under the **HTTP Boot Configuration** menu.

Item	Operation	Description
List of NICs in the system e.g. MAC:XX:XX:XX:XX:XX:XX		Set the boot configuration parameters. **Note:** To save the parameter settings, go back to the main menu and click **Save Settings**. Then, you will see the HTTP boot option in the **Start Options** list.

TIs Auth Configuration

Item	Operation	Description
Server CA Configuration		Press <Enter> to enroll or delete server CA certificate.
Client Cert Configuration		Configuring client certification is not allowed.

Server CA Configuration

Item	Operation	Description
Enroll Cert		Press <Enter> to enroll certificate.
Delete Cert		Press <Enter> to delete certificate.

Enroll Cert

Item	Operation	Description
Enroll Cert Using File		Press <Enter>. Select the storage device in the popped-up window. Then, select the file to enroll certificate.
Cert GUID		Press <Enter>. Input GUID of a certificate. Example: 11111111-2222-3333-4444-1234567890ab
Commit Changes and Exit		Press <Enter> to commit changes and exit the page.
Discard Changes and Exit		Press <Enter> to discard changes and exit the page.

Delete Cert

Item	Operation	Description
List of certificate GUID Example: *xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx*		**Note:** If there's no certificates, the list is empty.

Operating modes

Select the operating mode bases on your preference.

Item	Operation	Description
Choose Operating Mode	• **Maximum Efficiency** • Custom Mode • Maximum Performance	Selectable option. Select the operating mode based on your preference. Power savings and performance are also highly dependent on hardware and software running on the system. **Maximum Efficiency** is the default setting.
Determinisim Slider	• Power • **Performance**	Selectable option. When set to Performance, performance is more predictable (deterministic) and operates at the lowest common denominator among the cores. But aggregate peak performance may be reduced. When set to Power, cores can scale frequency independently. Aggregate performance may be higher, but predictability is lower. **Performance** is the default setting.
Core Performance Boost	• Disable • **Enable**	Selectable option. When set to [Enable], cores can go to turbo frequencies. **Enable** is the default setting.
cTDP	• Maximum • Manual • **Auto**	Selectable option. Sets the maximum power consumption for the CPU. Auto sets cTDP=TDP for the installed CPU SKU. Maximum sets the maximum allowed cTDP value for the installed CPU SKU. Usually, maximum is greater than TDP. If a manual value is entered that is larger than the max value allowed, the value will be internally limited to the maximum allowable value. cTDP is only configurable before OS boot. **Auto** is the default setting.

Item	Operation	Description
cTDP Manual	[0]	Numeric input Sets the maximum power consumption for the CPU. Auto sets cTDP=TDP for the installed CPU SKU. Maximum sets the maximum allowed cTDP value for the installed CPU SKU. Usually, maximum is greater than TDP. If a manual value is entered that is larger than the max value allowed, the value will be internally limited to the maximum allowable value. cTDP is only configurable before OS boot.
Package Power Limit	• Maximum • Manual • **Auto**	Selectable option. Sets the CPU package power limit. Compared to cTDP, PPL can also be changed at runtime and PPL supports a much lower effective limit than cTDP. If **Auto** is selected, it will be set to the maximum value allowed by the installed CPU. The maximum value allowed for PPL is the cTDP limit. **Auto** is the default setting.
Package Power Limit Manual	[0]	Numeric input If a manual value is entered that is larger than the maximum value allowed, the value will be internally limited to the maximum allowable value. The maximum value allowed for PPL is the cTDP limit.
Memory Speed	• xxxx MHz • ... • Minimum	Selectable option. The option number of memory speed is changed dynamically according to the combination of installed CPU SKU, DIMM type, number of DIMMs per channel, and system motherboard support. The system operate at the rated speed of the slowest DIMM in the system when populated with different speed DIMMs. Install DIMM which the rated speed below 2400 will result in the memory speed getting set to the minimum value.
Efficiency Mode	• **Enable** • Disable	Selectable option. Enables/disables efficiency mode. When enabled, uses power efficiency optimized CCLK DPM settings. **Enable** is the default setting.
4-link xGMI max Speed	• **Minimum** • 13Gbps • 16Gbps • 18Gbps	Selectable option. Sets the xGMI speed. 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. **Minimum** is the default setting.

Item	Operation	Description
Global C-state Control	• Disable • **Enable**	Selectable option. Global enables/disable for IO based C-state generation and DF C-states. **Enable** is the default setting.
SOC P-states	• **Auto** • P0 • P1 • P2 • P3	Selectable option. [Maximum Performance] allows the most aggressive use of turbo and power management functions are disabled, thereby increasing power consumption. [Minimal Power] disables turbo and maximizes the use of power management features. When a preset mode is selected, the low-level settings are not changeable and will be grayed out. If user would like to change the settings, please choose [Custom Mode] in “Operating Mode” located under “System Setting” submenu. **Auto** is the default setting.
DF C-States	• Disable • **Enable**	Selectable option. Enables/disable data fabric (DF) C-states. Data fabric C-states may be entered when all cores are in CC6. **Enable** is the default setting.
P-state 1	• **Enable** • Disable	Selectable option. Enables/disables CPU P1 P-state. **Enable** is the default setting.
P-State 2	• **Enable** • Disable	Selectable option. Enables/disables CPU P2 P-state. **Enable** is the default setting.
Memory Power Down Enable	• **Enable** • Disable	Selectable option. Enables/disables low-power features for DIMMs.
NUMA Nodes per Socket	• NPS0 • **NPS1** • NPS2 • NPS3	Selectable option. Specifies the number of desired NUMA nodes per CPU socket(e.g. NPS1 means 1 NUMA per socket). NPS0 will attempt to interleave the 2 CPU sockets together (non-NUMA mode).

Power

Use this menu to configure power scheme options.

Item	Operation	Description
ACPI Fixed Power Button	• **Enable** • Disable	Enable/Disable ACPI Fixed Power Button. When setting as disabled, physically pressing the power button on front of the system won't execute the Operating System's Power Button Policy such as shutdown, turn off monitor, etc. Also, when disabled the 'Shut down OS and ..." options under the iMM Server Power Actions feature will be disabled. **Enable** is the default setting.
Efficiency Mode	• **Enable** • Disable	Option Enables/disables efficiency mode. When enabled, uses power efficiency optimized CCLK DPM settings. **Enable** is the default setting.

Processors

This menu displays and provides options to change the processor settings.

Item	Operation	Description
Determinism Slider	• Power • **Performance**	Selectable option. When set to Performance, performance is more predictable (deterministic) and operates at the lowest common denominator among the cores. But aggregate peak performance may be reduced. When set to Power, cores can scale frequency independently. Aggregate performance may be higher, but predictability is lower. **Performance** is the default setting.
Core Performance Boost	• Disable • **Enable**	Selectable option. When set to Enable, cores can go to turbo frequencies. **Enable** is the default setting.
cTDP	• Maximum • Manual • **Auto**	Selectable option. Sets the maximum power consumption for the CPU. Auto sets cTDP=TDP for the installed CPU SKU. Maximum sets the maximum allowed cTDP value for the installed CPU SKU. Usually, maximum is greater than TDP. If a manual value is entered that is larger than the max value allowed, the value will be internally limited to the maximum allowable value. cTDP is only configurable before OS boot. **Auto** is the default setting.
cTDP Manual	**[0]**	Numeric input. Sets the maximum power consumption for the CPU. Auto sets cTDP=TDP for the installed CPU SKU. Maximum sets the maximum allowed cTDP value for the installed CPU SKU. Usually, maximum is greater than TDP. If a manual value is entered that is larger than the max value allowed, the value will be internally limited to the maximum allowable value. cTDP is only configurable before OS boot.
Package Power Limit	• Maximum • Manual • **Auto**	Selectable option. Sets the CPU package power limit. Compared to cTDP, PPL can also be changed at runtime and PPL supports a much lower effective limit than cTDP. If **Auto** is selected, it will be set to the maximum value allowed by the installed CPU. The maximum value allowed for PPL is the cTDP limit. **Auto** is the default setting.

Item	Operation	Description
Package Power Limit Manual	**[0]**	Numeric input If a manual value is entered that is larger than the maximum value allowed, the value will be internally limited to the maximum allowable value. The maximum value allowed for PPL is the cTDP limit.
4-Link xGMI Max Speed	• **Minumum** • 13Gbps • 16Gbps • 18Gbps	Selectable option. Sets the xGMI speed. 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. **Minimum** is the default setting.
Global C-state Control	• Disable • **Enable**	Selectable option. Global enables/disable for IO based C-state generation and DF C-states. **Enable** is the default setting.
SOC P-states	• **Auto** • P0 • P1 • P2 • P3	Selectable option. [Maximum Performance] allows the most aggressive use of turbo and power management functions are disabled, thereby increasing power consumption. [Minimal Power] disables turbo and maximizes the use of power management features. When a preset mode is selected, the low-level settings are not changeable and will be grayed out. If user would like to change the settings, please choose [Custom Mode] in “Operating Mode” located under “System Setting” submenu. **Auto** is the default setting.
DF C-States	• Disable • **Enable**	Selectable option. Enables/disable data fabric (DF) C-states. Data fabric C-states may be entered when all cores are in CC6. **Enable** is the default setting.
P-state 1	• **Enable** • Disable	Selectable option. Enables/disables CPU P1 P-state. **Enable** is the default setting.
P-State 2	• **Enable** • Disable	Selectable option. Enables/disables CPU P2 P-state. **Enable** is the default setting.

Item	Operation	Description
Preferred I/O Bus	• **Preferred** • Disable	Selectable option. When "No Priority" is selected, there is no preferred IO bus. When a specific bus is selected for higher IO priority, the format of the field is XX, where XX is the bus number in hex.
Preferred I/O Bus Number	[0]	Numeric input Preferred IO Bus Number 0x0-0xFF: Bus Number.
ACPI SRAT L3 Cache as NUMA Domain	• Enable • **Disable**	When enabled, each CCX in the system will be declared as a separate NUMA domain. When disabled, memory addressing/NUMA nodes per socket will be declared.
L1 Stream HW Prefetcher	• **Enable** • Disable	Selectable option. Enables/disable L1 stream HW prefetcher. Fetches the next cache line into the L1 cache when cached lines are reused within a certain time period or accessed sequentially.
L2 Stream HW Prefetcher	• **Enable** • Disable	Selectable option. Enables/disable L2 stream HW prefetcher. Fetches the next cache line into the L2 cache when cached lines are reused within a certain time period or accessed sequentially.
SMT Mode	• **Enable** • Disable	Selectable option. Can be used to disable symmetric multithreading. To re-enable SMT, a power cycle is needed after selecting Enable.
CPPC	• **Enable** • Disable	Selectable option. CPPC(cooperative processor performance control) is a way for the OS to influence the performance of a CPU on a contiguous and abstract scale without knowledge of power budgets or discrete processor frequencies.
BoostFmax	• **Auto** • Manual	Selectable option. Maximum boost frequency. Auto set the boost frequency to the fused value for the installed CPU. 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.

Item	Operation	Description
BoostFmax Manual	[0]	Numeric input Maximum boost frequency. Auto set the boost frequency to the fused value for the installed CPU. 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. **Note:** This item is only available when " BoostFmax" is set to Manual.
SVM Mode	• Disable • **Enable**	Enable/disable CPU Virtualization.
xGMI Maximum Link Width	• 0 • 1 • **Auto**	Sets the xGMI width. Auto sets maximum width based on the system capabilities.
APIC Mode	• xAPIC • X2APIC • **Auto**	APIC Mode. xAPIC scales to only 255 hardware threads. x2APIC scales beyond 255 hardware threads but is not supported by some legacy OS versions. Auto uses x2APIC only if 256 hardware threads are in the system. Otherwise xAPIC is used.
DLWM Support	• Disable • **Enable**	DLWM saves power during periods of low socket-to-socket data traffic by reducing the number active xGMI lanes per link from 16,8,2. Disabling this parameter can achieve a fixed xGMI link width.
Number of Enabled CPU Cores Per Socket	**All** List of all available core counts based on CCDs and Cores Per CCD.	Select the total number of enabled CPU cores per socket to be activated. Options available are dependent on CPU SKU topology. **Note:** Reducing the number of enabled CPU cores per socket can adversely impact performance. **Note:** *n is the maximum number of cores that installed processor support. For example, if the installed processor support 6 cores, it will show All,1,2,3,4,5.*
Processor Details		Selectable submenu. Displays summary of the installed processors.

Processor Details

Item	Operation	Description
Processor Details		
Processor Socket		Dynamic information. Displays processor Socket Table.
Processor ID		Dynamic information. Displays processor IDs.
Processor Frequency		Dynamic information. Displays processor frequency values.
Processor Revision		Dynamic information. Displays microcode revision values.
L1 Cache RAM		Dynamic information. Displays amount of L1 cache RAM.
L2 Cache RAM		Dynamic information. Displays amount of L2 cache RAM.
L3 Cache RAM		Dynamic information. Displays amount of L3 cache RAM.
PSB Fusing Status		Platform Secure Boot fusing status in the 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)		Dynamic information. Displays number of supported and enabled processor cores per processor socket.
Threads Per Socket (Supported/Enabled)		Dynamic information. Displays number of supported and enabled processor threads per processor socket.
Dies Per CPU (Supported/ Enabled)		N/A

Item	Operation	Description
Processor 1 Version		Dynamic information. Displays version of Processor 1. **Note:** The string might be read as generic string format. If any concern, you might check with Intel dear customer letter (DCL) for more detail. Such as the “Brand String” field in the document.
Processor n Version		Dynamic information. Displays version of Processor n. **Note:** The string might be read as generic string format. If any concern, you might check with Intel dear customer letter (DCL) for more detail. Such as the “Brand String” field in the document.

Recovery and RAS

Use this menu to configure recovery policies and advanced reliability, availability, and serviceability settings.

Item	Operation	Description
POST Attempts		Sub menu.
Advanced RAS		Sub menu.
System Recovery		Sub menu.

POST Attempts

Use this menu to configure POST attempt limits.

Item	Operation	Description
POST Attempts		
Post Attempt Limit	• Disable • 9 • 6 • **3**	Selectable options When the number of consecutive failed POST attempts reaches the limit, the system will reboot with the factory default settings. **3** is the default setting.

Note: You may encounter some message boxes when post attempts. Follow the message for setup.

Advanced RAS

Use this menu to configure advanced reliability, availability, and serviceability settings.

Item	Operation	Description
Advanced RAS		
PCI Error Recovery	• Enable • **Disable**	Selectable option. Allow the system to recover from an uncorrectable PCIe fault when enabled. The faulting PCIe device will be disabled for error containment and the OS will be notified to rescan the PCIe buses. An uncorrectable PCIe fault will result in an NMI when disabled. **Disable** is the default setting.
Reset after sync flood	• **Enable** • Disable	Selectable option. Enable AB to forward downstream sync-flood message to system controller. **Enable** is the default setting.

System Recovery

Use this menu to configure recovery policies.

Item	Operation	Description
POST Watchdog Timer	• Enable • **Disable**	Selectable options Enable/Disable POST Watchdog Timer. **Disable** is the default setting.
POST Watchdog Timer Value	[5]	Numeric input. Enter POST loader Watchdog timer value in minutes from the specified range (5-20).
Reboot System On NMI	• **Enable** • Disable	Selectable options Enable/Disable reboot of the system during non-maskable interrupt. **Enable** is the default setting. **Notes:** • If NMI is triggered by NMI button as diagnostic interrupt, XCC would only drive NMI without reboot action. • If NMI is triggered by XCC WebUI/IPMIcmd as software NMI, XCC would perform action based on setting. The default reboot timeout is 60 seconds.

Security

Use this menu to configure system security settings.

Item	Operation	Description
Security		
Physical Presence Policy Configuration		Sub menu. Change Physical Presence Policy options. **Notes:** • Check your UEFI firmware version to decide whether asserting physical presence is required before any changes to security settings. – UEFI firmware before v2.02 Asserting physical presence is required. – UEFI firmware v2.02 and later Asserting physical presence is no longer required, all local accounts and some authorized remote accounts can directly change the settings.
Secure Boot Configuration		Sub menu. Configure Secure Boot options.
Trusted Platform Module		Sub menu. Configure the TPM Setup options.

Physical Presence Policy Configuration

Use this menu to configure physical presence policy settings.

Item	Operation	Description
Physical Presence Policy Configuration		
Physical Presence Policy	• **Enabled** • Disabled	Selectable option. Enable/Disable "Remote Physical Presence Policy". The option is modifiable when "Physical Presence State" is asserted. Enabled allows Remote Physical Presence to be asserted without the need for Hardware Physical Presence. Once enabled, a time-out value is used to assert the policy for a specified number of minutes. NOTE: If moved to the Disabled state it will require Hardware Physical Presence to re-enable this policy. **Enable** is the default setting. **Note:** If moved to the Disabled state, it will require Hardware Physical Presence to re-enable this policy.
Minutes To Assert	30	Dynamic information. Number of minutes (range 1-100) to have Remote Physical Presence asserted. Physical Presence Policy must be Enabled and a value set to have remote physical Presence asserted.
Physical Presence State	• Hardware Physical Presence Asserted • Remote Physical Presence Asserted • Hardware and Remote Physical Presence are Asserted • **De-asserted**	If Hardware Physical Presence Jumper is Asserted, the only way to de-assert Physical Presence is to change the jumper on the planar. Asserting allows Physical Presence to be set for a duration listed in minutes even if Hardware Physical Presence Jumper is not asserted. Asserting does not require a reboot. Both the Hardware Physical Presence Jumper on the planar and the Remote Physical Presence are Asserted. De-asserting turns off Physical Presence (unless the HW Physical Presence Jumper is asserted). De-asserting does not require a reboot. **De-asserted** is the default setting
Toggle Remote Physical Presence Assert	• Asserted • De-asserted	Selectable option. Switch the Remote Physical Presence between Asserted and De-asserted when "Physical Presence Policy" is enabled. **Note:** The option is NOT modifiable when "Physical Presence Policy" is disabled.

Secure Boot Configuration

Use this menu to configure secure boot settings.

Notes:

- Check your UEFI firmware version to decide whether asserting physical presence is required before any changes to security settings.
  - UEFI firmware before v2.02

    Asserting physical presence is required.
  - UEFI firmware v2.02 and later

    Asserting physical presence is no longer required, all local accounts and some authorized remote accounts can directly change the settings.

Item	Operation	Description
Secure Boot		
Physical Presence	• Asserted • **De-asserted**	Dynamic information. Display the current Physical Presence status. Physical Presence is a form of authorization to perform certain security functions. [Asserted] means being authorized. “Secure Boot Setting” and “Secure Boot Policy” is modifiable when “Physical Presence” is asserted. **De-asserted** is the default setting **Note:** When the setting is De-asserted, the whole page is grayed.
Secure Boot Status	• **Disabled** • Enabled	Dynamic information. Display the current secure boot status. **Disabled** is the default setting.
Secure Boot Mode	• Setup Mode • **User Mode**	Selectable option. System will do secure boot authentication when “Secure Boot Mode” is [User Mode] and secure boot is enabled. **User Mode** is the default setting.

Item	Operation	Description
Secure Boot Setting	• Enable • **Disable**	Selectable option. Enable/Disable secure boot. This setting is modifiable when “Physical Presence” is asserted and cannot be loaded to default in Setup Utility. **User Mode** is the default setting. **Notes:** • When you attempt to enable secure boot while CSM is enabled, there is a prompt to tell you. • Legacy BIOS will be disabled when secure boot is enabled. • When you fail to change secure boot settings, verify physical presence and retry.
Secure Boot Policy	• **Factory Policy** • Custom Policy • Delete All Keys • Delete PK • Reset All Keys to Default	Selectable option. This setting is modifiable when "Physical Presence" is asserted and cannot be loaded to default in Setup Utility. [Factory Policy]: Factory default keys will be used after reboot. **Factory Policy** is the default setting. [Custom Policy]: Customized keys will be used after reboot. [Delete All Keys]: PK, KEK, DB and DBX will be deleted after reboot. [Delete PK]: PK will be deleted after reboot. "Secure Boot Mode" is [Setup Mode] and "Secure Boot Policy" is [Custom Policy] after PK is deleted. [Reset All Keys to Default]: All the keys will be set to factory defaults and "Secure Boot Policy" is [Factory Policy] after reboot.
View Secure Boot Keys		Sub menu. View the details of PK(Platform Key) , KEK (Key Exchange Key) , DB (Authorized Signature Database) and DBX (Forbidden Signature Database).
Secure Boot Custom Policy		Sub menu. Customize PK (Platform Key), KEK (Key Exchange Key), DB (Authorized Signature Database) and DBX (Forbidden Signature Database). This item is available when **Secure Boot Policy** is set as [Custom Policy].

View Secure Boot Keys

Use this menu to view secure boot keys.

Item	Operation	Description
View Secure Boot Keys		
Secure Boot variable		Dynamic information. Displays the platform keys, key exchange keys, authorized signature database, and forbidden signature database.
Size		Dynamic information. Displays the number of key bytes.
Keys		Dynamic information. Displays all certificates.
Key Source		Dynamic information. Displays the certificate sources. The sources can be **Factory Default**, **No Keys**, **Mixed**, or **Customized**.

Secure Boot Custom Policy

Use this menu to configure secure boot custom policy.

Item	Operation	Description
Secure Boot Custom Policy		
Enroll UEFI Image		Executive item. Enrolls the SHA256 hash of the selected UEFI image binary into the authorized signature database.
Secure Boot variable		Dynamic information. Displays the platform keys, key exchange keys, authorized signature database, and forbidden signature database.
Size		Dynamic information. Displays the number of bytes.
Keys		Dynamic information. Displays the number of certificates.
Key Source		Dynamic information. Displays the certificate sources. The sources can be **Factory Default**, **No Keys**, **Mixed**, or **Customized**.
PK		Executive item. Enrolls a PK or delete the existing key.
KEK		Executive item. Enrolls a KEK or delete the existing key.
DB		Executive item. Enrolls a DB or delete the existing key.
DBX		Executive item. Enrolls a DBX or delete the existing key.

Trusted Platform Module

Use this menu to configure TPM.

Trusted Platform Module (TPM 2.0)

Item	Operation	Description
Trusted Platform Module		
TPM 2.0		Sub menu. Configure the TPM 2.0 setup options.
TPM Version		Dynamic information. Displays the TPM version.
Update to TPM 1.2 compliant **Note:** If current TPM version doesn't support version toggling, this item will be hid.		Selectable option. Press [Enter] to update the TPM to TPM 1.2. **Notes:** • Change is effective after system reboot and physical presence confirmed. You can only switch TPM firmware 128 times. • Click this button, a pop-up warning message will show up to confirm the action. Update is a significant change. Once completed, all keys and encrypted data will be lost.
Update to TPM 2.0 firmware version 7.2.2.0 **Note:** If current TPM version doesn't support version toggling, this item will be hid.		Selectable option. Press [Enter] to update the TPM 2.0 firmware from 7.2.1.0 to 7.2.2.0. **Note:** This action is irreversible, you won't be able to change to TPM 1.2 or an earlier firmware version of TPM 2.0. The updated firmware will be effective after system reboot.

Trusted Platform Module (TPM 1.2)

Item	Operation	Description
Trusted Platform Module		
TPM 1.2		Sub menu. Configure the TPM 1.2 setup options.
TPM Version		Dynamic information. Displays the TPM version.

Item	Operation	Description
Update to TPM 2.0 compliant **Note:** If current TPM version doesn't support version toggling, this item will be hid.		Selectable option. Press [Enter] to update the TPM to TPM 2.0. **Notes:** • Change is effective after system reboot and physical presence confirmed. You can only switch TPM firmware 128 times. • Click this button, a pop-up warning message will show up to confirm the action. Update is a significant change. Once completed, all keys and encrypted data will be lost.
Update to TPM 1.2 firmware version 7.4.0.1 **Note:** If current TPM version doesn't support version toggling, this item will be hid.		Selectable option. Press [Enter] to update the TPM 1.2 firmware from 7.4.0.0 to 7.4.0.1. **Note:** This action is irreversible, you won't be able to change to TPM 2.0 or an earlier firmware version of TPM 1.2. The updated firmware will be effective after system reboot.

Trusted Platform Module (TPM 2.0)

Use this menu to configure TPM 2.0 setup options.

Item	Operation	Description
Trusted Platform Module (TPM 2.0)		
[TPM Status]		
TPM Vendor		Dynamic information. Displays the TPM vendor.
TPM Firmware Version		Dynamic information. Displays the current TPM firmware version.
TPM Physical Presence	• Asserted • Not Assearted	Dynamic information. Displays the current state of the TPM physical presence. **Note:** For models with 7002 series processors and UEFI firmware before v2.02, this must be asserted for TPM commands to succeed, otherwise this item will be hid, and it is not necessary to assert Physical Presence.
[TPM Settings]		
TPM2 Operation	• **No Action** • Clear	Selectable option. Select [Clear] to clear TPM data. WARNING: This will erase the contents of the TPM. This command requires the TPM Physical Presence to be asserted. System reboot required. **No Action** is the default setting.
SHA-1 PCR Bank	• **Enabled** • Disabled	Selectable option. Select [Enabled] or [Disabled] to enable or disable SHA-1 PCR Bank. **Enabled** is the default setting.

Trusted Platform Module (TPM 1.2)

Use this menu to configure TPM 1.2 setup options.

Item	Operation	Description
Trusted Platform Module (TPM 1.2)		
[TPM Status]		
TPM Vendor		Dynamic information. Displays the TPM vendor.
TPM Firmware Version		Dynamic information. Displays the current TPM firmware version.
TPM Physical Presence	• Asserted • Not Assearted	Dynamic information. Displays the current state of the TPM physical presence. **Note:** For models with 7002 series processors and UEFI firmware before v2.02, this must be asserted for TPM commands to succeed, otherwise this item will be hid, and it is not necessary to assert Physical Presence.
TPM Device State		Dynamic information. Displays the current state of the TPM device.
TPM Ownership		Dynamic information. Displays the current status of ownership.
[TPM Settings]		
TPM Device	• **Enabled** • Disabled	Selectable option. Enable/Disable the TPM device. **Enable** is the default setting. **Note:** For models with 7002 series processors and UEFI firmware before v2.02, this option requires the TPM Physical Presence to be asserted.

Item	Operation	Description
TPM State	• **Activate** • Deactivate	Selectable option. Activate/Deactivate the TPM device. This command requires the TPM physical presence to be asserted. System reboot is required. **Activate** is the default setting.
TPM Operation	• **No Action** • Clear	Selectable option. Select [Clear] to clear TPM data. **No Action** is the default setting. **Notes:** • This will erase the contents of the TPM. • For models with 7002 series processors and UEFI firmware before v2.02, this command requires the TPM Physical Presence to be asserted. • System reboot is required.

Storage

Use this menu to manage storage adapter options. Some systems may use planar devices and can be configured under **Devices and I/O ports**.

Item	Description
Storage	
NVMe	NVMe Devices list.
	Dynamic information. Display the device information based on your system installation and system settings.

Notes:

- The device list is based on your system configuration and system setting. The contents in this page are dynamically generated by installed storage vendor's HII utilities.
- All onboard NVMe drives connected to the system will be only displayed in the page: **System settings → Storage → NVMe**.
- Onboard NVMe devices will not list when VMD is enabled.

Date and time

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

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

Start options

Use this menu to select start option for next boot.

Item	Operation	Function
Start Options		
CD/DVD		Executable item Select the hexadecimal device address and the server will be boot from this device next time.
Hard Disk		Executable item Select the hexadecimal device address and the server will be boot from this device next time.
Network		Executable item Select the hexadecimal device address and the server will be boot from this device next time.
USB Storage		Executable item Select the hexadecimal device address and the server will be boot from this device next time.

Boot manager

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

Item	Operation	Description
Boot Manager		
Boot Sequence		
Add Generic Boot Option		Executable item. Add one generic boot device as boot option.
Add UEFI Full Path Boot Option		Sub menu. Add one UEFI application or one removable file system as boot option.
Delete Boot Option		Sub menu. Add one generic boot device as boot option.
Change Boot Order		Sub menu. Remove boot option(s) from “Boot Order”.
Set Boot Priority		Sub menu. Set boot priority of the devices in a device group.
Other Boot Functions		
Boot From File		Executable item. Boot system from a file or a device.
Select Next One-Time Boot Option		Sub menu. Select the one-time boot option for next boot.
System		
Boot Modes		Sub menu. Change between UEFI boot mode and legacy boot mode.
Reboot System		Executable item. Prompt to reboot the system.

Add UEFI Full Path Boot Option

Use this menu to add UEFI full path boot option.

Item	Operation	Description
Add UEFI Full Path Boot Option		
Boot option File Path		Dynamic information. Displays file path for newly created boot option.
Input the Description		Text input. Specify name for the new boot option
Select Device Path Option	• Xxxx {xxxx-xxx-xxx…} • Xxxx {xxxx-xxx-xxx…} • Xxxx {xxxx-xxx-xxx…}	Selectable option. Select device path option.
Commit Changes and Exit		Executable item. Save changes and exit.

Delete Boot Option

Use this menu to remove boot option(s) from “Boot Order”.

.

Item	Operation	Description
Delete Boot Option		
CD/DVD Rom	[X]	Executable item. VenHw(B2AD3248-4F72-4950-A966-CFE5062DB83A,02000000)
Hard Disk	[X]	Executable item. VenHw(B2AD3248-4F72-4950-A966-CFE5062DB83A,01000000)
Network	[X]	Executable item. VenHw(B2AD3248-4F72-4950-A966-CFE5062DB83A,05000000)
Commit Changes and Exit		Executable item. Save changes and exit.

Change Boot Order

Use this menu to modify the boot order.

Item	Operation	Description
Change the Order	• CD/DVD Rom • Hard Disk • Network • USB Storage	Selectable option. Change the boot order. Once set, the boot option will be displayed on the “Start Options” page.
Commit Changes and Exit	N/A	Save changes and exit.

Set Boot Priority

Use this menu to set boot priority of the devices in a device group.

Item	Operation	Description
CD/DVD Priority		Sub menu. Set boot priority in the CD/DVD group if multiple devices exist in the system.
Hard Disk Priority		Sub menu. Set boot priority in the Hard Disk group if multiple devices exist in the system.
Network Priority		Sub menu. Set boot priority in the Network group if multiple devices exist in the system.
USB Priority		Sub menu. Set boot priority in the USB group if multiple devices exist in the system.

CD/DVD Priority

Use this menu to set boot priority in the CD/DVD device group.

Item	Operation	Description
CD/DVD Priority		
Boot Priority		Selectable sub menu. Set boot priority in the CD/DVD group if multiple devices exist in the system.
Commit Changes and Exit		Executable item. Save changes and exit.

Hard Disk Priority

Use this menu to set boot priority in the hard disk device group.

Item	Operation	Description
Hard Disk Priority		
Boot Priority		Selectable sub menu. Change the boot priority for devices in the hard disk device group.
Commit Changes and Exit		Executable item. Save changes and exit.

Network Priority

Use this menu to set boot priority in the network device group.

Item	Operation	Description
Network Priority		
Boot Priority		Selectable sub menu. Change the boot priority for devices in the network priority.
Commit Changes and Exit		Executable item. Save changes and exit.

USB Priority

Use this menu to set boot priority in the USB device group.

Item	Operation	Description
USB Priority		
Boot Priority		Selectable sub menu. Set boot priority in the USB group if multiple devices exist in the system.
Commit Changes and Exit		Executable item. Save changes and exit.

Select Next One-Time Boot Option

Use this menu to select one-time boot option.

.

Item	Operation	Description
Select Next One-Time Boot Option		
Boot Option	• CD/DVD Rom • Hard Disk • Network • USB Storage • System Setup • **NONE**	Selectable option. Select the one-time boot option for next boot.

Boot Modes

Use this menu to set system boot mode.

Item	Operation	Description
Boot Modes		
System Boot Mode	• **UEFI Mode** • Legacy Mode	Selectable option. Drivers, option ROMs and OS loaders the “Boot Manager” attempt to boot. [UEFI Mode]: Run UEFI drivers and boot a UEFI OS loader [Legacy Mode]: Run option ROMs and boot a legacy OS. **UEFI Mode** is the default setting. **Note:** This setting will be forced to [UEFI Mode] when Legacy BIOS is disabled in **System Settings** ->**Legacy BIOS** ->**Legacy BIOS.**.
Infinite Boot Retry	• Enable • **Disable**	Selectable option. Drivers, option ROMs and OS loaders the “Boot Manager” attempt to boot. Continuously retry the Boot Order. Please ensure a bootable device is specified in “Boot Order”. **Disable** is the default setting.
Prevent OS Changes To Boot Order	• Enable • **Disable**	Selectable option. When set to [Enable], UEFI will remove the boot option which is created by OS or OS Installer from Boot Order List. **Disable** is the default setting.

BMC settings

Use this menu to configure the management controller.

Item	Operation	Description
BMC settings		
Power Restore Policy	• Always Off • Restore • Always On	Selectable option. Determine the mode of operation after loss of power. • **[Always Off]** : System remains off upon power restore. • **[Restore]**: System restores to the state it was before power failed. • **[Always On]**: System turns on upon power restore. Allow a few minutes for the changes to take effect. **Note:** This option is configuration dependent, and this item could not use Setup load default to back to default value.
Power Restore Random Delay	• Enable • Disable	Selectable option. Provides a random delay between 1 and 15 seconds for Power On. If set to [Enable], when the system was on before a power failure, the system will delay power on once power is restored. **Note:** This item is not available when **Power Restore Policy** is set as [Always Off].
Ethernet over USB interface	• Enable • Disable	Selectable option. [Enable] for using the xClarity Essentials in-band update utility. [Disable] will prevent xClarity Essentials and other applications that are running on the server from requesting the BMC to perform tasks. When user modifies the "Ethernet Over USB Interface" related settings, the setting values may keep stale for a while and do not immediately reflect the new settings.
Network Settings		Sub menu. Configure the network of the management controller.
Reset Factory Defaults Setting		Executive item. Restore all management controller settings to factory defaults, including network configuration and credentials, the management controller will be restarted automatically.
Restart BMC		Executive item. Restart the BMC.

Network settings

Use this menu to configure the BMC network.

Item	Operation	Description
Network settings		
Network Interface Port	• **Dedicated** • Shared	Selectable option. Select the System Management Network Interface Port. **Dedicated** is the default setting. **Note:** This option is configuration dependent.
Shared NIC on	OCP Card	Selectable option. Select the shared NIC port. **Note:** This item is only on when network interface port is on Shared, and this option is configuration dependent.
Fail-Over Rule	• **None** • Failover to shared (Optional Card ML2) • Failover to shared (Optional Card PHY) • Failover to shared (Onboard Port)	Selectable option. Setting to control Fail-Over types allowed. **None** is the default setting. **Note:** This item is only on when network interface port is on Shared, and this option is configuration dependent.
Burned-in MAC Address		
Hostname		Numeric input. Change the host name. The new name should be within 1 to 63 characters.
DHCP Control	• Static IP • DHCP Enabled • **DHCP with Fallback**	Selectable option. Configure DHCP Control or manually configure a static IP address. Fallback will use static IP address if DHCP fails. Select Static to enter IPV4 address manually. **DHCP with Fallback** is the default setting.
IP Address		Numeric input. Enter IP address in dotted-decimal notation. Example: x.x.x.x
Subnet Mask		Numeric input. Enter Subnet Mask in dotted-decimal notation. Example: x.x.x.x

Item	Operation	Description
Default Gateway		Numeric input. Enter Default Gateway in dotted-decimal notation. Example: x.x.x.x
IP6	• **Enable** • Disable	Selectable option. Enable/Disable IPv6 support on management port. **Enable** is the default setting.
Local Link Address		
VLAN Support	• Enable • **Disable**	Selectable option. Enable VLAN Support to specify the 802.1q VLAN ID on the management port network device. **Disable** is the default setting.
VLAN ID		Dynamic information. Displays the enabled VLAN ID.
Advanced Setting for BMC Ethernet		Selectable sub menu. Displays **Advanced Setting for BMC Ethernet** sub menu.
Save Network Settings		Executable item. Save the BMC network settings.

Advanced Settings for BMC Ethernet

Use this menu to configure advanced BMC Ethernet settings.

Item	Operation	Description
Advanced Settings for BMC Ethernet		
Autonegotiation	• No • **Yes**	Selectable option. Choose whether the Data rate and Duplex network settings are configurable or not. **Yes** is the default setting.
Data rate	Autonegotiation is 'Yes': **Auto** Autonegotiation is 'No': 100 Mb (Ethernet) 10 Mb (Ethernet)	Selectable option. Set amount of data to be transferred per second over LAN connection. **Yes** is the default setting.
Duplex	Autonegotiation is 'Yes': **Auto** Autonegotiation is 'No': Half Full	Selectable option. Type of communication channel used in your network. [Full]: Allow data to be transferred in both directions at once. [Half]: Allow data to be transferred in either one direction or the other, but not both at the same time. **Yes** is the default setting.
Maximum Transmission Unit	**1500**	Numeric input. Specify the maximum size of a packet (in bytes) for the network interface. The valid range is 68 – 1500. **1500** is the default setting.

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.

Item	Operation	Description
System Event Logs		
POST Event Viewer		Sub menu. Displays POST events.
System Event Log		Sub menu. Displays system event logs.
Clear System Event Log		Executive item. Clears system event logs.

System event logs

Use this menu to view system event logs.

Item	Operation	Description
System Event Log		
Total SEL entries		Dynamic information. Displays total number of system event logs retrieved from the BMC. This does not include any associated extended logs.
Previous Page		Executive item. Press [Enter] to view system event logs in the previous page.
[n]		Dynamic information. Displays related information.
Next Page		Executive item. Press [Enter] to view system event logs in the next page.

POST Event Viewer

Use this menu to view POST events.

Item	Operation	Description
POST Event Viewer		
Entry [n]		Dynamic information. Displays POST events.

User security

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

Item	Operation	Description
User security		
Password Rule and Policy		Sub menu. Sets password rules and policies.
Set Power-On Password		Text or numeric input. Set the power-On password.
Clear Power-On Password		Text or numeric input. Clear the Power-On password.
Set Administrator Password		Text or numeric input. Set the Administrator password.
Clear Administrator Password		Executive item. Clear the Administrator password.

Password Rule and Policy

Use this menu to set password rules and policies.

Item	Operation	Description
Password Rule and Policy		
Minimum password length	8~20	Numeric input. Input a value from 8 to 20. The minimum number of characters that can be used to specify a valid password.
Password expiration period	0~365	Numeric input. Input a value from 0 to 365. The number of days a password may be used before it must be changed. If set to 0 the passwords never expire.
Password expiration warning period	0~365	Numeric input. Input a value from 0 to 365. The number of days before receiving a warning about the expiration of the password. If set to 0 the passwords never warned.
Minimum password change interval	0~240	Numeric input. Input a value from 0 to 240. The number of hours that must elapse before changing a password. The value specified for this setting cannot exceed the value specified for the “Password expiration period”. If set to 0 the passwords may be changed immediately.
Minimum password reuse cycle	0~10	Numeric input. Input a value from 0 to 10. The minimum number of times a unique password must be set before reusing a previous password. If set to 0 the passwords may be reused immediately.
Maximum number of login failures	0~100	Numeric input. Input a value from 0 to 100. The number of login attempts that can be made with an incorrect password before the user account is locked out. The account is locked out for the time specified in “Lockout period after maximum login failures”. If set to 0 accounts are never locked. The failed login counter is reset to zero after a successful login.
Lockout period after maximum login failures	0~2880	Numeric input. Input a value from 0 to 2880. The number of minutes that must pass before a locked out user can attempt to login. Entering a valid password does not unlock the account during the lockout period. If set to 0 the accounts will not be locked out even if the “Maximum number of login failures” is exceeded.

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.