Lenovo

ThinkSystem server UEFI Parameter Reference Guide

For 1-socket server models with AMD EPYC (1st, 2nd, 3rd Gen)

Ninth Edition (March 2024)

Contents

Chapter 1. Introduction

This documentation explains how to set the System Setup Utility for ThinkSystem servers SR635 or SR655.

The System Setup Utility is Unified Extensible Firmware Interface (UEFI) 2.5 compliant. You can use the System Setup Utility to view and change the settings of your server, regardless of which operating system you are using. However, the operating system settings might override any similar settings in the System Setup Utility.

Get started

The UEFI setup utilities can be launched in text mode only.

1. Connect the local keyboard, video, and mouse (KVM) to the server using a cable, or open the **Remote Console** page on the ThinkSystem Manager web user interface (BMC 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.

Chapter 2. System configuration and boot management

Depending on the BIOS version of your server, some menu or item information might differ slightly from the information in this topic.

Notes:

- The default settings already are optimized for you. Use the default value for any item you are not familiar with. Do not change the value of unfamiliar items to avoid unexpected problems. If you consider changing the server configuration, proceed with extreme caution. Setting the configuration incorrectly might cause unexpected results.
- If you have changed any hardware in the server, you might need to upgrade the BIOS and the TSM firmware.

The following menus are listed on the **System Setup Utility** screen:

Main menu

After entering the System Setup Utility, you can see the **Main** menu.

Menu item	Options	Description
BIOS Version	N/A	Display the BIOS version.
BIOS Copyright	N/A	Display the BIOS copyright.
Build Date and Time	MM/DD/YYYY HH:MM:SS	Display the build date and time.
PSP BootLoader Version	N/A	Display the PSP BootLoader version.
SMU FW Version	N/A	Display the SMU FW version.
BMC Version	N/A	Display the BMC version.
System Language	**English** | 中文 (简体)	Choose the system language. The default option is English.
System Date	[Week MM/DD/YYYY]	Set the Date. Use Tab to switch between Date elements. Default Ranges: Year: 2018-2099 Months: 1-12 Days: dependent on month

Menu item	Options	Description
System Time	[HR:MIN:SEC]	Set the Time. Use Tab to switch between Time elements.
LLC as NUMA Node	Disable | Enable | **Auto**	Enable or disable the performance for highly NUMA optimized workloads.
Memory Speed	Auto| **2933 MHz** | 2666 MHz | 2400 MHz	View and select the desired memory speed or Auto. The default option is **2933 MHz**.
Operating Modes	See the submenu	View and select the operating mode based on your preference.
Access Level	Administrator	Display the access level.

Operating Modes

The ThinkSystem SR635 and SR655 servers offer two preset operating modes, Maximum Efficiency and Maximum Performance. These modes are a collection of predefined low-level UEFI settings that simplify the task of tuning the server for either maximum performance or energy efficiency.

Use the following submenu to set the operating mode.

For more information, refer to *Tuning UEFI Settings for Performance and Energy Efficiency on Lenovo ThinkSystem SR635 and SR655 Servers* at https://lenovopress.com/lp1267-tuning-uefi-for-performance-energy-efficiency-sr635-sr655.

Submenu item	Options	Description
Set Operating Mode	Maximum Efficiency | Maximum Performance	Select the operating mode based on your preference.
Operating Mode	N/A	Display the operating mode that you set.
Determinism Slider	Auto | **Power** | Performance	Auto = Use default performance determinism settings The default option is **Power**.
Core Performance Boost	Disable | **Auto**	Disable **Core Performance Boost**. The default option is **Auto**.
cTDP Control	Manual | **Auto**	Manual = User can set customized cTDP Auto = Use the fused cTDP The default option is **Auto**
cTDP	0	cTDP [W] 0 = Invalid value.
Memory Speed	Auto| **2933 MHz** | 2666 MHz | 2400 MHz	Select the desired memory speed or **Auto**. The default option is **2933 MHz**
L1 Stream HW Prefetcher	Disable | Enable | **Auto**	Enable or disable the L1 Stream HW Prefetcher. The default option is **Auto**.

Submenu item	Options	Description
L2 Stream HW Prefetcher	Disable | Enable | **Auto**	Enable or disable the L2 Stream HW Prefetcher. The default option is **Auto**.
Global C-state Control	Disable | **Enable** | Auto	Enables or disables for IO based C-state generation and DF C-states control. The default option is **Enable**.
SMT Mode	Disable | **Auto**	Disable symmetric multithreading. To re-enable SMT, a POWER CYCLE is needed after selecting the **Auto** option. The default option is **Auto**.
Memory Interleaving	Disable | **Auto**	Disable the memory interleaving. The default option is **Auto**.
NUMA nodes per socket	NPS0 | **NPS1** | NPS2 | NPS4 | Auto	Specify the number of desired NUMA nodes per socket. **NPS0** means to interleave the two sockets together. The default option is **NPS1**.
EfficiencyModeEn	Auto | **Enable**	Enable the Efficiency Mode. The default option is **Enable**.
Package Power Limit Control	Manual | **Auto**	**Manual** = Set the customized PPT. **Auto** = Use the fused Package Power Limit (PPT). The default option is **Auto**.
Package Power Limit	0	PPT [W]
Chipselect Interleaving	Disable | **Auto**	Interleave memory blocks across the DRAM chip selects for node 0. The default option is **Auto**.
LLC as NUMA Node	Disable | Enable | **Auto**	Enable or disable the performance for highly NUMA optimized workloads. The default option is **Auto**.

Advanced menu

You can view or change various server component settings on the **Advanced** menu in the System Setup Utility.

The **Advanced** menu contains the following items. Some items are displayed on the menu only if the server supports the corresponding features. For more information, enter the corresponding items and refer to the instructions on the screen.

Menu item	Description
CPU Configuration	View and set microprocessor configuration parameters.
Memory Configuration	View and set memory configuration parameters.

Menu item	Description
ACPI Configuration	View and set the Advanced Configuration and Power Interface (ACPI) parameters.
Power	Set power setting.
PCIe Configuration	View and set PCIe configuration parameters
SATA Configuration	View SATA devices information.
NVMe Configuration	View onboard NVMe device options settings.
Serial Port Console Redirection	View and set the serial port console redirection configuration parameters.
Network Stack Configuration	View the network stack settings for UEFI only.
USB Configuration	View and set USB configuration parameters.
CSM Configuration	View and set the Compatibility Support Module (CSM) parameters.
iSCSI Configuration	View and configure the iSCSI parameters.
Drive Health	View UEFI Drivers/Controllers status.

CPU Configuration

Use this submenu to set the microprocessor configuration parameters.

Submenu item	Options	Description
CPU 1 Information	N/A	Press <Enter> to view the information related to CPU 1.
SMT Mode	Disable | **Auto**	Can be used to disable symmetric multithreading. To re-enable SMT, a POWER CYCLE is needed after selecting Enable. The default option is **Auto**.
Core Performance Boost	Disable | **Auto**	Disable CPB. The default option is **Auto**.
CPPC	Disable | **Enable**	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.
BoostFmaxEn	Manual | **Auto**	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.
BoostFmax	0	Specify the boost Fmax frequency, the value entered is a 4 digit number representing the maximum boost frequency in MHz. The value entered applies to all cores.

Submenu item	Options	Description
CPU Cores Activated	**Auto** | 1 Cores Per Die | 2 Cores Per Die | 3 Cores Per Die | 4 Cores Per Die | 5 Cores Per Die | 6 Cores Per Die | 7 Cores Per Die	Total activated cores = # Cores Per Die * Dies Per CPU * Number of Installed CPUs. Dies Per CPU is in the CPU1 Information page. The total number of activated cores is limited by the maximum number of cores of the installed CPU SKU. The default option is **Auto**.
L1 Stream HW Prefetcher	Disable | Enable | **Auto**	Enable or disable the L1 Stream HW Prefetcher. The default option is **Auto**.
L1 Stride Prefetcher	Disable | Enable | **Auto**	Enable or disable L1 stride prefetcher. The default option is **Auto**. Use memory access history to fetch additional data lines into L1 cache when each access is a constant distance from the previous. Some workloads may benefit from having it disabled.
L1 Region Prefetcher	Disable | Enable | **Auto**	Enable or disable L1 region prefetcher. The default option is **Auto**. Fetch additional data lines into L1 cache when the data access for a given instruction tends to be followed by a consistent pattern of subsequent accesses. Some workloads may benefit from having it disabled.
L2 Stream HW Prefetcher	Disable | Enable | **Auto**	Enable or disable the L2 Stream HW Prefetcher. The default option is **Auto**.
L2 Up/Down Prefetcher	Disable | Enable | **Auto**	Enable or disable L2 Up/Down prefetcher. The default option is **Auto**. Use memory access history to determine whether to fetch the next or previous line for all memory accesses. Some workloads may benefit from having it disabled.
Preferred IO Bus	Preferred | **No Priority**	The default option is **No Priority**. 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 (For Redfish, the bus number is in decimal).
Preferred I/O Bus Number	0	When the item **Preferred IO Bus** set to the preferred I/O device bus number, you will see this item.
Enhanced Preferred IO Mode (For 3rd Gen CPU only)	**Disable** | Enable	Enabling the Enhanced Preferred I/O mode assures an LCLK valuate for best performance. (Note: Setting 'LCLK Freq Control' on the same Root Complex which the Preferred IO Bus belongs to, to anything other than 'Auto' will override the Enhanced Preferred IO Mode.)

Submenu item	Options	Description
LCLK Frequency Control (For 3rd Gen CPU only)	N/A	Click to see the submenu.
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.
Fast Short REP MOVSB	Disable | Enable | **Auto**	(FSRM) Can be disabled for analysis purposes as long as OS supports it.
Enhanced REP MOVSB/ STOSB	Disable | Enable | **Auto**	(ERMSB) Can be disabled for analysis purposes as long as OS supports it.
Secured-Core	**Custom** | Enable	Enable Secured-Core support. When Secured-core is 'Enable', the 4 related settings are 'Enable' and locked. When Secured-core is 'Custom', the related settings can be changed independently as needed. If all 4 related settings are 'Enable', it is effectively equivalent to Secured-core being 'Enable'. The default option is **Custom**.
DMAr Support	**Disable** | Enable	Enable DMAr system protection during POST. The default option is **Disable**.
DRTM Virtual Device Support	**Disable** | Enable	Enable DRTM ACPI virtual device. The default option is **Disable**.
TSME	Disable | Enable | **Auto**	Enable or Disable Transparent Secure Memory Encryption. TSME provides hardware memory encryption for all data stored in system memory. Disabling TSME will result in a small decrease to memory latency.
CPU C State		
Global C-State Control	Disable | **Enable** | Auto	Enables or disables the IO based C-state generation and DF C-states control. The default option is **Enable**.
CPU Virtualization		
SVM Mode	Disable | **Enable**	Enable or disable CPU Virtualization. The default option is **Enable**.
IOMMU	Disable | Enable | **Auto**	Enable or disable IOMMU. The default option is **Auto**.
CPU Performance		
Determinism Slider	Auto | **Power** | Performance	**Auto**: Use default performance determinism settings. The default option is **Power**.

Submenu item	Options	Description
cTDP Control	Manual | **Auto**	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. The default option is **Auto**.
AMD SEV-ES	**Disable** | Enable	Enable AMD SEV-ES support
SEV ASID Count	253 ASIDs | 509 ASIDs | **Auto**	This fields 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	N/A
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)
SEV-SNP Support	Disable | **Enable**	Enable or Disable SEV-SNP Support
HSMP Support	Disable | Enable| **Auto**	Enable or Disable HSMP support

Memory Configuration

Use this submenu to set the memory configuration parameters.

Submenu item	Options	Description
Memory Information	N/A	Press <Enter> to view the memory information.
Memory interleaving	Disable | **Auto**	Disable the memory interleaving. The default option is **Auto**.
Memory interleaving size	256 Bytes | 512 Bytes | 1KB | 2KB | **Auto**	Control the memory interleaving size. The default option is **Auto**.
Chipselect Interleaving	Disable | **Auto**	Interleave memory blocks across the DRAM chip selects for node 0. The default option is **Auto**.

Submenu item	Options	Description
DRAM Scrub Time	Disable | 1 hour| 4 hours | 8 hours | 16 hours | **24 hours**| 48 hours	Sets the period of time between successive DRAM scrub events. The default option is **24 hours**.
TSME	Disable | Enable | **Auto**	Enable or Disable Transparent Secure Memory Encryption. TSME provides hardware memory encryption for all data stored in system memory. Disabling TSME will result in a small decrease to memory latency. The default option is **Auto**.
DRAM Refresh Rate	**1x** | 2x	A refresh rate of 1x is recommended for better performance. Choose refresh rate 2x to mitigate rowhammer issue, this may have a performance side effect. The default option is **1x**.
Sub-urgent Refresh Lower Bound	[4]	Specifies the stored refresh limit to required enter sub-urgent refresh mode. Constraint: Sub-urgent Refresh Lower Bound <= Urgent Refresh Limit. Valid value: 6 ~ 1.
Urgent Refresh Limit	[6]	Specifies the stored refresh limit to required enter urgent refresh mode. Constraint: Sub-urgent Refresh Lower Bound <= Urgent Refresh Limit. Valid value: 6 ~ 1.
DRAM Post Package Repair	Disable | **Enable**	Enable or Disable DRAM Post Package Repair. The default option is **Enable**.
SMEE	**Disable** | Enable	Control secure memory encryption. The default option is **Disable**.

ACPI Configuration

Use this submenu to set ACPI configuration parameters.

Submenu item	Options	Description
Power Button	Lock | **Unlock**	Lock or unlock the Power button. The default option is **Unlock**. **Note:** This item doesn't support load BIOS default function.
Restore AC Power Loss	Power Off |Power On | **Last State**	The default option is **Last State**. **Note:** This item doesn't support load BIOS default function.
Restore AC Power Loss Current State	Last State	Show the current state of the restore AC power loss.

Power

Use this submenu to set the power.

Submenu item	Options	Description
Zero Output	**Disable** | Advance Mode	When zero output is enabled and multiple power supplies are installed in the server, some of the PSUs will be automatically placed into a low power state under light load conditions. This helps to save power. The default option is **Disable**.

PCIe Configuration

Use this submenu to set the PCIe configuration parameters.

Submenu item	Options	Description
OnBrd/Ext VGA Select	Auto | **Onboard** | External	Select between onboad or external VGA support. The default option is **Onboard**.
Above 4G Decoding	Disable | **Enable**	Globally enable or disable 64 bit capable devices to be decoded in above 4G address space (only if system supports 64 bit PCI Decoding). The default option is **Enable**.
SR-IOV Support	**Disable** | Enable	If system has SR-IOV capable PCIe Devices, this option enables or disables the Single Root IO Virtualization Support. The default option is **Disable**.
PCIe ARI Support	Disable | Enable | **Auto**	Enable Alternative Routing-ID Interpretation The default option is **Auto**.
NVMe Hot-plug	Disable | **Enable**	NVMe Hot-Plug Option. The default option is **Enable**.
PCIe Slot 1	Disable | **Enable**	This submenu is available depending on your system. Enable or disable PCIe Slot 1. The default option is **Enable**.
PCIe Slot 2	Disable | **Enable**	This submenu is available depending on your system. Enable or disable PCIe Slot 2. The default option is **Enable**.

Submenu item	Options	Description
PCIe Slot 3	Disable | **Enable**	This submenu is available depending on your system. Enable or disable PCIe Slot 3. The default option is **Enable**.
PCIe Slot 4	Disable | **Enable**	This submenu is available depending on your system. Enable or disable PCIe Slot 4. The default option is **Enable**.
PCIe Slot 5	Disable | **Enable**	This submenu is available depending on your system. Enable or disable PCIe Slot 5. The default option is **Enable**.
PCIe Slot 6	Disable | **Enable**	This submenu is available depending on your system. Enable or disable PCIe Slot 6. The default option is **Enable**.
PCIe Slot 7	Disable | **Enable**	This submenu is available depending on your system. Enable or disable PCIe Slot 7. The default option is **Enable**.
PCIe Slot 8	Disable | **Enable**	This submenu is available depending on your system. Enable or disable PCIe Slot 8. The default option is **Enable**.
PCIe Slot 9	Disable | **Enable**	This submenu is available depending on your system. Enable or disable PCIe Slot 9. The default option is **Enable**.
OCP3	Disable | **Enable**	Enable or disable OCP3. The default option is **Enable**.

SATA Configuration

Use this submenu to view the SATA HDD detect status.

Note: Port number is not the drive number on BMC web UI. Port number define is aimed at SATA controller.

Following is an example of **SATA Configuration** submenu:

SATA Configuration	
SATA Controller (S:00 B:43 D:00 F:00)	
Port 0	Not Present
Port 1	Not Present
Port 2	Not Present
Port 3	Not Present
Port 4	Not Present
Port 5	Not Present
Port 6	Not Present
Port 7	Not Present

Note: The x value in the **S:***xx* **B:***xx* **D:***xx* **F:***xx* depends on your system.

NVMe Configuration

Use this submenu to view the NVMe configuration.

Following is an example of NVMe **Drive 0** information.

Drive No	Drive 0
Seg:Bus:Dev:Func	00:01:00:00
Model Number	MZQLB1T9HAJR-00V3
Serial Number	S471NF0M400234
Total Size	192.3 GB
Vendor ID	144D
Device ID	A808
SubVendor ID	1d49
SubDevice ID	403b
Link Capability	x4, 8.0 GT/s
Link Status	x4, 8.0 GT/s

Serial Port Console Redirection

Use this submenu to view or set the Serial Port Console Redirection.

Submenu item	Options	Description
COM1(Pci Bus0,Dev0,Func0,Port1)		
Console Redirection	Disable | **Enable**	Enable or disable the console redirection for COM1. The default option is **Enable**.

Submenu item	Options	Description
Console Redirection Settings	N/A	COM1: The settings specify how the host computer and the remote computer (which the user is using) will exchange data. Both computers should have the same or compatible settings. Press <Enter> to view console redirection settings. See the submenu.
Legacy Console Redirection		
Legacy Console Redirection Settings	N/A	Press <Enter> to view Legacy Console Redirection Settings. See the submenu.
Serial Port for Out-of-Band Management		
Windows Emergency Management Services (EMS)		
Console Redirection	Disable | **Enable**	Enable or disable the Console Redirection for Windows Emergency Management Services (EMS). The default option is **Enable**.
Console Redirection Settings	N/A	EMS: The settings specify how the host computer and the remote computer (which the user is using) will exchange data. Both computers should have the same or compatible settings. Press <Enter> to view the console redirection settings. See the submenu.

Console Redirection Settings for COM1 (Pci Bus0,Dev0,Func0,Port1)

Submenu item	Options	Description
Terminal Type	VT100 | **VT100+** | VT-UTF8 | ANSI	**ANSI**: Extended ASCII char set. **VT100**: ASCII char set. **VT100+**: Extends VT100 to support color, function keys, etc. **VT-UTF8**: Uses UTF8 encoding to map Unicode chars onto 1 or more bytes. The default option is **VT100+**.
Bits per second	9600 | 19200 | 38400 | 57600 | **115200**	Select serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds. The default option is **115200**.

Submenu item	Options	Description
Data Bits	7 | **8**	Data Bits. The default option is **8**.
Parity	**None** | Even | Odd | Mark | Space	Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/ stop signals. The default option is **None**.
Stop Bits	**1** | 2	Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit. The default option is **1**.
Flow Control	**None** | Hardward RTS/CTS	Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/ stop signals. The default option is **None**.
VT-UTF8 Combo Key Support	Disable | **Enable**	Enable or disable VT-UTF8 Combination Key Support for ANSI/ VT100 terminals. The default option is **Enable**.
Recorder Mode	**Disable** | Enable	With this mode enabled only text will be sent. This is to capture Terminal data. The default option is **Disable**.
Resolution 100x31	**Disable** | Enable	Enable or disable extended terminal resolution. The default option is **Disable**.
Putty KeyPad	**VT100** | LINUX | XTERMR6 | SCO | ESCN | VT400	Select FunctionKey and KeyPad on Putty. The default option is **VT100**.

Legacy Console Redirection Settings

Submenu item	Options	Description
Resolution	**80x24** | 80x25	On Legacy OS, the Number of Rows and Columns supported redirection. The default option is **80x24**.
Redirect After POST	**Always Enable** | BootLoader	When **BootLoader** is selected, then **Legacy Console Redirection** is disabled before booting to legacy OS. When **Always Enable** is selected, then **Legacy Console Redirection** is enabled for legacy OS. The default option is **Always Enable**.

Console Redirection Settings for Serial Port for Out-of-Band Management

Submenu item	Options	Description
Terminal Type	VT100 | VT100+ | **VT-UTF8** | ANSI	**VT-UTF8** is the preferred terminal type for out-of-band management. The next best choice is **VT100+** and then **VT100**. See above, in **Console Redirection Settings** page, for more Help with **Terminal Type**/**Emulation**
Bits per second	9600 | 19200 | 57600 | **115200**	Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds. The default option is **115200**.
Flow Control	**None** | Hardward RTS/CTS | Software Xon/Xoff	Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/ stop signals.
Data Bits	8	Show the Data Bits.
Parity	None	Show the Parity.
Stop Bits	1	Show the Stop Bits.

Network Stack Configuration

Use this submenu to set network stack configuration parameters.

Submenu item	Options	Description
Network Stack		
Ipv4 PXE Support	Disable | **Enable**	Enable or disable IPv4 PXE boot support. The default option is **Enable**.
IPv4 HTTP Support	**Disable** | Enable	Enable or disable IPv4 HTTP boot support. When it is enabled, booting *.efi executables is supported, but booting disk image files is not. The default option is **Disable**.
IPv6 PXE Support	Disable | **Enable**	Enable or disable IPv6 PXE boot support. The default option is **Enable**.
IPv6 HTTP Support	**Disable** | Enable	Enable or disable IPv6 HTTP boot support. When it is enabled, booting *.efi executables is supported, but booting disk image files is not. The default option is **Disable**.
PXE Boot wait time	N/A	Wait time in seconds to press ESC key to abort the PXE boot. Use either +/- or numeric keys to set the value.
Media detect count	N/A	Number of times the presence of media will be checked. Use either +/- or number keys to set the value.
Global Network Settings	N/A	Global Network Settings

USB Configuration

Use this submenu to set the USB configuration parameters.

Submenu item	Options	Description
USB Configuration		
USB Devices:		
3 Drives, 1 Keyboards, 1 Mouse , 1 Hubs		
Legacy USB Support	**Enable** | Disable | Auto	Enable or disable Legacy USB Support. **AUTO** option disables legacy support if no USB devices are connected. **DISABLE** option will keep USB devices available only for EFI applications. The default option is **Enable**.
Rear USB Port	Disable | **Enable**	Enable or disable rear USB Port at the same time. The default option is **Enable**.
Front USB Port0	Disable | **Enable**	Enable or disable front USB Port 0. The default option is **Enable**.

Submenu item	Options	Description
Front USB Port 1	Disable | **Enable**	Enable or disable front USB Port 1. The default option is **Enable**.
USB Mass Storage Driver Support	Disable | **Enable**	Enable or disable USB Mass Storage Driver Support. The default option is **Enable**.
Mass Storage Devices:		
AMI Virtual CDROM 1.00	**Auto** | Floppy | Forced FDD | Hard Disk | CD-ROM	Mass storage device emulation type. **AUTO** enumerates devices according to their media format. Optical drivers are emulated as **CD-ROM**, drives with no media will be emulated according to a drive type. The default option is **Auto**.
AMI Virtual HDisk0 1.00	**Auto** | Floppy | Forced FDD | Hard Disk | CD-ROM	Mass storage device emulation type. **AUTO** enumerates devices according to their media format. Optical drivers are emulated as **CD-ROM**, drives with no media will be emulated according to a drive type. The default option is **Auto**.

CSM Configuration

Use this submenu to set the CSM configuration parameters.

Submenu item	Options	Description
Compatibility Support Module Configuration		
CSM Support	Disable | **Enable**	Enable or disable CSM support. The default option is **Enable**.
CSM16 Module Version	07.84	
Option ROM Execution		
Network	Do not launch | **UEFI** | Legacy	Controls the execution of UEFI and Legacy Network OpROM. The default option is **UEFI**.
Storage	Do not launch | **UEFI** | Legacy	Controls the execution of UEFI and Legacy Storage OpROM. The default option is **UEFI**.
Video	Do not launch | **UEFI** | Legacy	Controls the execution of UEFI and Legacy Video OpROM. The default option is **UEFI**.
Other PCI Devices	Do not launch | **UEFI** | Legacy	Determines OpROM execution policy for devices other than Network, Storage, or Video. The default option is **UEFI**.

Server Mgmt menu

You can view or change BMC settings on the **Server Mgmt** menu in the System Setup Utility. Some items are displayed on the menu only if the server supports the corresponding features.

The **Server Mgmt** menu contains the following items. For more information, enter the corresponding items and refer to the instructions on the screen.

Menu item	Description
System Event Log	View and set system event log parameters.
Product Information	View product information.
BMC Network Configuration	View and set BMC configuration parameters.
View System Event Log	View system event log parameters.
BMC User Settings	Add, delete and set privilege level for users.
BMC DNS Configuration	View and set BMC DNS configuration parameters.
SOL Configuration	View and set SOL configuration parameters.
BMC Warm Reset	Press <Enter> to do Warm Reset BMC.
Reset Factory Defaults Setting	Restore all management controller settings to factory defaults, including network configuration and credentials, the management controller will be restarted automatically.

System Event Log

Use this submenu to set the system event log parameters.

Note: All values changed here do not take effect until computer is restarted.

Submenu item	Options	Description
Enabling/Disabling Options		
Erasing Settings		
Erase SEL	**No** | Yes, On next reset | Yes, On every reset	Choose options for erasing SEL. The default option is **No**.
When SEL is Full	**Do Nothing** | Erase Immediately | Delete Oldest Record	Choose options for reactions to a full SEL. The default option is **Do Nothing**.

Product Information

Use this submenu to view the product information.

Note: All values changed here do not take effect until computer is restarted.

Submenu item	Description
Product Information	
System Manufacturer	Show the system manufacture.
System Product Name	Show the system product name.
System Version	Show the system version.
System Serial Number	Show the system serial number.
Board Manufacturer	Show the board manufacturer.
Board Product Name	Show the board product name.
Board Version	Show the board version.
Board Serial Number	Show the serial number.
Chassis Manufacturer	Show the chassis manufacturer.
Chassis Serial Number	Show the chassis serial number.
System UUID	Show the system UUID.
System Asset Tag	Show the system asset tag.

BMC Network Configuration

Use this submenu to set the BMC network configuration parameters.

Submenu item	Options	Description
BMC network configuration		
Configure IPv4 support		
Lan channel 1 (Shared NIC)		
Configuration Address source	**Unspecified** | Static | DynamicBmcDhcp | DHCP with Fallback	Select to configure LAN channel parameters statically, dynamically or DHCP with fallback (will get IP after 120s). **Unspecified** option will not modify any BMC network parameters during BIOS phase The default option is **Unspecified**.
Current Configuration Address source	N/A	Show the current configuration address source.
Station IP address	N/A	Enter station IP address.
Subnet mask	N/A	Enter subnet mask.
Station MAC address	N/A	Show the station MAC address.
Router IP address	N/A	Enter router IP address.
Router MAC address	N/A	Enter router MAC address.
Lan channel 2 (Dedicated NIC)		

Submenu item	Options	Description
Configuration Address source	**Unspecified** | Static | DynamicBmcDhcp | DHCP with Fallback	Select to configure LAN channel parameters statically, dynamically or DHCP with fallback (will get IP after 120s). **Unspecified** option will not modify any BMC network parameters during BIOS phase The default option is **Unspecified**.
Current Configuration Address source	N/A	Show the current configuration address source.
Station IP address	N/A	Enter station IP address.
Subnet mask	N/A	Enter subnet mask.
Station MAC address	N/A	Show the station MAC address.
Router IP address	N/A	Enter router IP address.
Router MAC address	N/A	Enter router MAC address.
Configure IPv6 support		
Lan channel 1 (Shared NIC)		
IPv6 Support	Disable | **Enable**	Enable or disable LAN1 IPv6 support. The default option is **Enable**.
Configuration Address source	**Unspecified** | Static | DynamicBmcDhcp	Select to configure LAN channel parameters statically or dynamically(by BIOS or BMC). **Unspecified** option will not modify any BMC network parameters during BIOS phase. The default option is **Unspecified**.
Current Configuration Address source	N/A	Show the current configuration address source.
Station IPv6 address	N/A	Enter station IPv6 address.
Prefix Length	N/A	Change the prefix length.
IPv6 Router1 IP Address	N/A	Change the IPv6 Router1 IP Address.
IPv6 addrss status	Active	Show the IPv6 addrss status.
IPv6 DHCP Algorithm	DHCPv6	Show the IPv6 DHCP Algorithm.
Lan channel 2 (Dedicated NIC)		
IPv6 Support	Disable | **Enable**	Enable or disable LAN2 IPv6 support. The default option is **Enable**.
Configuration Address source	**Unspecified** | Static | DynamicBmcDhcp	Select to configure LAN channel parameters statically or dynamically(by BIOS or BMC). **Unspecified** option will not modify any BMC network parameters during BIOS phase The default option is **Unspecified**.
Current Configuration Address source	N/A	Show the current configuration address source.
Station IPv6 address	N/A	Enter station IPv6 address.

Submenu item	Options	Description
Prefix Length	N/A	Change the prefix length.
IPv6 Router1 IP Address	N/A	Change the IPv6 Router1 IP Address.
IPv6 addrss status	Active	Show the IPv6 addrss status.
IPv6 DHCP Algorithm	DHCPv6	Show the IPv6 DHCP Algorithm.

View System Event Log

Use this submenu to view the system event log parameters.

Following is an example of **View System Event Log** submenu:

No. of log entries in SEL : 1			
DATE	**TIME**	**SENSOR**	**TYPE**
05/26/19	20:06:34	Event	Logging Disabled

BMC User Setting

Use this submenu to set the BMC User Setting parameters.

Submenu item	Description
BMC User Settings	
Add User	Press <Enter> to add a User. See the submenu.
Delete User	Press <Enter> to delete a User. See the submenu.
Change User Settings	Press <Enter> to change user setting. See the submenu.

Add user

Use this submenu to add BMC user.

Submenu item	Options	Description
BMC Add User Details		
User Name	N/A	Enter BMC User Name.
User Password	N/A	Enter BMC User Password.
User Access	Enable | **Disable**	Enable or disable the BMC User's Access. The default option is **Disable**.
Channel No	N/A	Value Range: 0 - 15 When create new User, you need input **Channel No**.
User Privilege Limit	**No Access** | Callback | User | Operator | Administrator	Enter BMC user privilege limit for selected channel. The default option is **No Access**.

Delete user

Use this submenu to delete BMC user.

Submenu item	Description
BMC Delete User Details	
User Name	Enter BMC User Name.
User Password	Enter BMC User Password.

Change User Settings

Use this submenu to change the user settings.

Submenu item		Description
BMC Change User Settings		
User Name	N/A	Enter BMC User Name.
User Password	N/A	Enter BMC User Password.
Change User Password	N/A	Enter New Password to change.
User Access	Enable | **Disable**	Enable or disable the BMC User's Access. The default option is **Disable**.
Channel No	N/A	Value Range: 0 - 15 When change user settings, you need check **Channel No** corresponding.
User Privilege Limit	**No Access** | Callback | User | Operator | Administrator	Enter BMC user privilege limit for selected channel. The default option is **No Access**.

BMC DNS Configuration

Use this submenu to set the BMC DNS Configuration parameters.

Submenu item	Options	Description
BMC DNS Configuration		
To Change	**No** | Yes	To Change BMC DNS Configuration. The default option is **No**.
Domain Name Serivce Configuration		
DNS Service	**Enable** | Disable	Enable or disable DNS Service. The default option is **Enable**.
Host Configuration		
Host Settings	Manual | **Automatic**	The default option is **Automatic**.
Host Name	N/A	Display the host name.
Register BMC		

Submenu item	Options	Description
eth0	**Enable** | Disable	The default option is **Enable**.
Register Method	**Nsupdate** | DHCP Client FQDN | Hostname	The default option is **Nsupdate**.
eth1	**Enable** | Disable	The default option is **Enable**.
Register Method	**Nsupdate** | DHCP Client FQDN | Hostname	The default option is **Nsupdate**.
Domain Name Configuration		
Domain Settings	Manual | eth0_v4 | eth0_v6 | **eth1_v4** | eth1_v6	The default option is **eth1_v4**.
Domain Name	N/A	Display the domain name.
Domain Name Server Configuration		
DNS Server Settings	Manual | eth0 | **eth1**	The default option is **eth1**.
IP Priority	**IPv4** | IPv6	The default option is **IPv4**.
DNS Server1	N/A	Display the DNS Server1.
DNS Server2	N/A	Display the DNS Server2.
DNS Server3	N/A	Display the DNS Server3.

SOL Configuration Parameters

Use this submenu to set the SOL configuration parameters.

Submenu item	Options	Description
SOL Configuration Parameters		
SOL Bit Rate (non-volatile)	9600 | 19200 | 38400 | 57600 | **115200**	Bits per second.
SOL Bit Rate (volatile)	9600 | 19200 | 38400 | 57600 | **115200**	Bits per second.
SOL Retry Count	N/A	Value Range: 0 ~ 7 0 = no retries after packet is transmitted. Packet will be dropped if no ACK/NACK received by time retries expire.
SOL Retry Interval	N/A	Value Range: 0 ~ 255 0 = Retries sent back-to-back. Retry Interval in 10 ms increments.

Security menu

You can set passwords on the **Security** menu in the System Setup Utility.

The **Security** menu contains the following main items:

Menu item	Description
Administrator Password	Set an administrator password to protect against unauthorized access to your server.
User Password	Set a user password to protect against unauthorized access to your server.
Password Rule and Policy	View and set password rule and policy.
Trusted Computing	View and set trusted computing settings.
TPM Toggling	TPM 1.2/2.0 Toggling and only support onboard Nuvoton TPM. (Need Physical Presence assert first)
Secure Boot	View and set Secure Boot configuration parameters. (Need Physical Presence assert first).

For more information about the difference between an administrator password and a user password, see "Using passwords" on page 25.

Using passwords

By using the System Setup Utility, you can set a password to prevent unauthorized access to your server.

You do not have to set a password to use your server. However, using a password improves computing security. If you decide to set a password, read the following topics.

System Setup Utility password types

The following types of passwords are available in the System Setup Utility:

Administrator password

Setting an administrator password deters unauthorized users from changing configuration settings. If you are responsible for maintaining the configuration settings of several servers, you might want to set an administrator password.

When an administrator password is set, you are prompted to type a valid password each time you try to access the System Setup Utility. The System Setup Utility cannot be accessed until a valid password is entered.

If both the user password and administrator password are set, you can enter either password. However, you must use your administrator password to change any configuration settings.

User password

When user password is set, you are prompted to enter a valid password each time the server is turned on. The server cannot be used until the valid password is entered. You can use a user password to add another layer of security to your server.

Password Rule and Policy

The Password Rules and Policy to specify the rules for things like password length, password expiration period and other related settings. These should be set to values defined in your organization's password policy.

Use the this submenu to set the password rule and policy parameters.

Submenu item	Description
Password Rule and Policy	
Minimum password length	Input a value from 8 to 20. The minimum number of characters that can be used to specify a valid password.
Password expiration period	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	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	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	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	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	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.

Password considerations

For security reasons, it is recommended that you use a strong password that cannot be easily compromised.

Notes:

- The System Setup Utility passwords are case sensitive.
- The server supports System Setup Utility passwords that consist of up to twenty characters.

To set a strong password, use the following guidelines:

- The password can only contain the following characters (no white-space characters allowed): A-Z, a-z, 0-9, ~`!@#$%^&*()-+={}[]|:;"'<>,?/._
- Contain at least one alphabetic character and one numeric character
- Contain at least two of the following combinations:
  - At least one upper-case letter
  - At least one lower-case letter
  - At least one special character
- No more than two consecutive occurrences of the same character
- Must be at least eight characters if it does not select other value in “Minimum password length” option.

Setting, changing, or deleting a password

This topic provides instructions on how to set, change, or delete a password in the System Setup Utility.

To set, change, or delete a password in the System Setup Utility, do the following:

1. Start the System Setup Utility. See "Get started" on page 1.
2. On the **Security** menu, select **Administrator Password** to set an administrator password or select **User Password** to set a user password.
3. See "Password considerations" on page 26. Then, follow the instructions on the screen to set or change a password.
4. If you want to delete a password, type your current password. Press Enter when you are prompted to type a new password. Then, press Enter to confirm the new password. The previous password will be cleared.

   Note: For security reasons, it is recommended that you always set a password for your server.
5. Press F4 to save settings and exit the System Setup Utility.

If you have forgotten the password, you can use the Clear Password jumper on the system board to erase the password.

Configuring Trusted Computing

The Trusted Platform Module (TPM) is a component of most modern computer systems. It is classified as a secure crypto processor. It is used to help assure the integrity of the platform. It is used as part of the secure boot process to store and report on certain security metrics during the boot process. On some systems it is also used to securely store a full-disk encryption key.

The Trusted Computing Group continues to revise the TPM specifications. There are currently two versions of the specification deployed; 1.2 and 2.0. When possible, update to TPM 2.0 compliance. TPM 2.0 supports newer cryptographic algorithms. It also is more flexible when cryptographic algorithms need to change.

Only systems that support UEFI can update to TPM 2.0 or TPM 1.2 compliance so only change to TPM 2.0 or TPM 1.2 if your system supports UEFI.

To enable the TPM function in the System Setup Utility, do the following:

1. Start the System Setup Utility. See "Get started" on page 1.
2. On the **Security** menu, select **Trusted Computing → Security device support**. Ensure that **Security device support** is set to **Enable**.
3. When **Security device support** is set to **Enable**, the **TPM State** item is displayed. Set **TPM State** to **Enable**. (Only support on TPM 1.2.)
4. Press F4 to save settings and exit the System Setup Utility. The server will restart in order to enable the TPM function.

   Note: Before you configure Trusted Computing or Secure Boot function, set the hardware Physical Presence jumper on the system board to assert Physical Presence first. On the **Security** menu, select **Trusted Computing → Physical Presence**. Ensure that **Physical Presence** is **Asserted** or **Not Asserted**.

Trusted Computing submenu for TPM20 Device Found

Submenu item	Options	Description
Configuration		
TPM20 Device Found		
Firmware Version:	7.2	Show the firmware version.
Vendor:	NTC	Show the vendor.
Physical Presence	Not Asserted.	Show the physical presence information.
Security Device Support	**Enable** | Disable	Enables or disables BIOS support for security device. O.S. will not show Security Device. TCG EFI protocol and INT1A interface will not be available. The default option is **Enable**.
Active PCR banks	N/A	Show the active PCR bank.
Available PCR banks	N/A	Show the available PCR banks.
SHA-1 PCR Bank	**Enable** | Disable	Enable or Disable SHA-1 PCR Bank. The default option is **Enable**.
SHA256 PCR Bank	**Enable** | Disable	Enable or Disable SHA256 PCR Bank. The default option is **Enable**.
SHA384 PCR Bank	Enable | **Disable**	Enable or Disable SHA384 PCR Bank. The default option is **Disable**.
Pending operation	**None** | TPM Clear	Schedule an Operation for the Security Device. **Note:** NOTE: Your Computer will reboot during restart in order to change State of Security Device. The default option is **None**.
Platform Hierarchy	**Enable** | Disable	Enable or disable platform hierarchy. The default option is **Enable**.
Storage Hierarchy	**Enable** | Disable	Enable or disable storage hierarchy. The default option is **Enable**.
Endorsement Hierarchy	**Enable** | Disable	Enable or disable endorsement hierarchy. The default option is **Enable**.
TPM2.0 UEFI Spec Version	TCG_1_2 | **TCG_2**	Select the TCG2 Spec Version Support. **TCG_1_2**:compatible mode for Win8/Win10. **TCG_2**: Support new TCG2 protocol and event format for Win10 or later. The default option is **TCG_2**.

Submenu item	Options	Description
Physical Presence Spec Version	1.2 | **1.3**	Select to Tell O.S. to support PPI Spec Version 1.2 or 1.3. **Note:** some HCK tests might not support 1.3. The default option is **1.3**.
TPM 20 InterfaceType	TIS	Show the TPM 20 interface type.

Trusted Computing submenu for TPM12 Device Found

Submenu item	Options	Description
Configuration		
Physical Presence	Not Asserted.	Show the physical presence information.
Security Device Support	**Enable** | Disable	Enables or disables BIOS support for security device. O.S. will not show Security Device. TCG EFI protocol and INT1A interface will not be available. The default option is **Enable**.
Active PCR banks	SHA-1, SHA256	Show the currently active PCR banks.
Available PCR banks	SHA-1, SHA256, SHA384	Show the currently available PCR banks.
SHA-1 PCR Bank	**Enable** | Disable	Enable or Disable SHA-1 PCR Bank. The default option is **Enable**.
SHA256 PCR Bank	**Enable** | Disable	Enable or Disable SHA256 PCR Bank. The default option is **Enable**.
SHA384 PCR Bank	Enable | **Disable**	Enable or Disable SHA384 PCR Bank. The default option is **Disable**.
TPM State	**Enable** | Disable	Enable or disable Security Device. **Note:** Your Computer will reboot during restart in order to change State of the Device. The default option is **Enable**.
Pending operation	**None** | TPM Clear	Schedule an Operation for the Security Device. **Note:** Your Computer will reboot during restart in order to change State of Security Device. The default option is **None**.
Current Status Information		
TPM Enabled Status:	N/A	Show the current TPM enabled status.
TPM Active Status:	N/A	Show the current TPM active status.
TPM Owner Status:	N/A	Show the current TPM owner status.

TPM Toggling

Use this submenu to view the TPM information.

Table 1. Trusted Platform Module (TPM 2.0)

Submenu item	Description
TPM Firmware Version:	Show the TPM firmware version. **CAUTION:** **Change is effective after system reboot and physical presence confirmed. You can only switch TPM firmware 128 times.**
Update to TPM 2.0 firmware version 7.2.1.0 **Note:** If the current TPM version doesn't support version toggling, this item will be hidden.	Selectable option. Press [Enter] to update to the TPM 2.0 firmware v7.2.1.0. **Notes:** • Toggling between TPM 2.0 firmware v7.2.1.0 and TPM 1.2 firmware v7.4.0.0 is supported. In other words, you can update from v7.4.0.0 to v7.2.1.0, or downgrade from v7.2.1.0 to v7.4.0.0. • The updated firmware will be effective after system reboot.
Update to TPM 2.0 firmware version 7.2.2.0 **Note:** If the current TPM version doesn't support version toggling, this item will be hidden.	Selectable option. Press [Enter] to update the TPM 2.0 firmware from 7.2.1.0 to 7.2.2.0. **Notes:** • This action is irreversible. TPM 2.0 Firmware v7.2.1.0 can be updated to v7.2.2.0 , but TPM 2.0 Firmware v7.2.2.0 cannot be downgraded to v7.2.1.0 or earlier versions. • TPM 2.0 cannot be downgraded to TPM 1.2. • The updated firmware will be effective after system reboot.

Table 2. Trusted Platform Module (TPM 1.2)

Submenu item	Description
TPM Firmware Version:	Show the TPM firmware version. **CAUTION:** **Change is effective after system reboot and physical presence confirmed. You can only switch TPM firmware 128 times.**

Table 2. Trusted Platform Module (TPM 1.2) (continued)

Update to TPM 1.2 firmware version 7.4.0.0 **Note:** If the current TPM version doesn't support version toggling, this item will be hidden.	Selectable option. Press [Enter] to update to the TPM 1.2 firmware v7.4.0.0. • Toggling between TPM 2.0 firmware v7.2.1.0 and TPM 1.2 firmware v7.4.0.0 is supported. In other words, you can update from v7.4.0.0 to v7.2.1.0, or downgrade from v7.2.1.0 to v7.4.0.0. • The updated firmware will be effective after system reboot.
Update to TPM 1.2 firmware version 7.4.0.1 **Note:** If the current TPM version doesn't support version toggling, this item will be hidden.	Selectable option. Press [Enter] to update the TPM 1.2 firmware from 7.4.0.0 to 7.4.0.1. **Notes:** • This action is irreversible. TPM 1.2 Firmware v7.4.0.0 can be updated to v7.4.0.1, but TPM 1.2 Firmware v7.4.0.1 cannot be downgraded to v7.4.0.0 or earlier versions. • The updated firmware will be effective after system reboot.

Secure Boot

Secure boot is functionality built into UEFI's specification. Physical Presence must be asserted if you are going to enable UEFI Secure Boot. When Secure Boot is enabled and properly configured, it protects computers against attacks and infections from malware that installs rootkits and boot kits.

Secure Boot detects when software like the boot loader and key operating system files and other things like option ROMs have been tampered with. It does this by validating each component's digital signature. Any component whose digital signature verification fails is not loaded during the boot process. Depending upon the OS and drivers you are using on the server it may not always be possible to enable secure boot.

To enable the Secure Boot in the System Setup Utility, do the following:

1. Start the System Setup Utility. See "Get started" on page 1.
2. On the **Security** menu, select **Secure Boot → Secure Boot**. Ensure that **Secure Boot** is set to **Enable**.

Use this submenu to set the Secure Boot parameter.

Submenu item	Option	Description
System Mode	Setup	Show the system mode.
Vendor Keys	Modified	Show the vendor keys.
Physical Presence	Not Asserted	N/A
Secure Boot	**Disable** | Enable	Secure Boot feature is Active if **Secure Boot** is **Enable**, Platform Key(PK) is enrolled and the System is in User mode. The mode change requires platform reset. The default option is **Disable**.

Submenu item	Option	Description
Secure Boot Customization	**Custom** | Standard	Secure Boot options: **Standard** or **Custom**. In **Custom** mode, Secure Boot Policy variables can be configured by a physically present user without full authentication. The default option is **Custom**.
Restore Factory Keys	**Yes** | No	Force System to User Mode. Install factory default Secure Boot key databases. The default option is **Yes**.
Restore To Setup Mode	**Yes** | No	Delete all Secure Boot key databases from NVRAM. The default option is **Yes**.
Key Management	N/A	Enables expert users to modify Secure Boot Policy variables without full authentication. See the submenu.

Secure Boot Customization

Under most circumstances, it is not necessary to change the Secure Boot Customization from its default settings. The most common case when this might be necessary is when the OS is Linux and there are drivers that are not part of the distribution being installed. This is sometimes called an out-of-box driver, vs in-the-box drivers that are part of standard Linux distributions. In these cases, it may be necessary to customize the secure boot policy.

To set the Secure Boot Customization in the System Setup Utility, do the following:

1. Start the System Setup Utility. See “Get started” on page 1.
2. On the **Security** menu, select **Secure Boot → Secure Boot → Secure Boot Customization**. Ensure that **Secure Boot Customization** is set to **Custom** or **Standard**.

To add or delete Secure Boot Keys for Secure Boot, do the following:

1. Start the System Setup Utility. See “Get started” on page 1.
2. On the **Security** menu, select **Secure Boot → Secure Boot → Secure Boot Customization**. Ensure that **Secure Boot Customization** is set to **Custom**.
3. If you are using an “out-of-box driver” you likely will need to add your own keys to the Secure Boot database using a Secure Boot Custom. The keys that you need are usually required include the Platform Key (PK), the Key Exchange Key (KEK), the Authorized Signature Database and the Forbidden Signature Database (DBX). These keys are used by the UEFI firmware to validate the components of the system being loaded during the boot process.
4. Delete Unnecessary Secure Boot Keys.

   When the secure boot policy is set to **Custom**, you can delete secure boot keys that are stored in the database if you do not require the existing key. You can also reset all keys back to the factory defaults if required.

Key Management

Use this submenu to set the secure boot policy variables.

Submenu item	Option	Description
Factory Key Provision	**Disable** | Enable	Install factory default Secure Boot keys after the platform reset and while the System is in Setup mode. The default option is **Disable**.
Enroll Efi Image	OK	Allow the image to run in Secure Boot mode. Enroll SHA256 Hash certificate of a PE image into Authorized Signature Database (db)
Device Guard Ready		
Remove 'UEFI CA' from DB	N/A	Device Guard ready system must not list 'Microsoft UEFI CA' Certificate in Authorized Signature database (db)
Resotre DB defaults	N/A	Restore DB variable to factory defaults
Secure Boot variable		
Platform Key(PK)	N/A	Enroll Factory Defaults or load certificates from a file: 1. Public Key Certificate: a. EFI_SIGNATURE_LIST b. EFI_CERT_X509 (DER) c. EFI_CERT_RSA2048 (bin) d. EFI_CERT_SHAXXX 2. Authenticated UEFI Variable 3. EFI PE/COFF Image(SHA256) Key Source: Factory, External, Mixed
Key Exchange Keys	N/A	
Authorized Signatures	N/A	
Forbidden Signatures	N/A	

Boot menu

The **Boot** menu in the System Setup Utility lists all the bootable devices installed in your server and the listed items vary depending on your server configuration. You can view or change the server startup options, including the startup sequence and boot priority for various devices.

The **Boot** menu contains the following items. For more information, enter the corresponding items and refer to the instructions on the screen.

Menu item	Option	Description
Setup Prompt Timeout	N/A	Value Range: 1 -- 0xFFFF Set the time-out seconds to wait for setup activation key.
Bootup NumLock State	**On** | Off	Select the keyboard Numlock state.
Launch LXPM Lite	N/A	Launch the EFI application of LXPM Lite.
Boot Mode	UEFI and Legacy | Legacy Only |**UEFI Only**	Set boot mode settings. The default option is **UEFI Only**.
Infinite Boot Retry	Enable | **Disable**	Continuously retry the Boot Order. Please ensure a bootable device is specified in "Boot Order".

Menu item	Option	Description
Boot Option Priorities	N/A	Sets the system boot order.
Boot Option #1	N/A	Select a device as the first startup device.
Boot Option #2	N/A	Select a device as the second startup device.
Boot Option #3	N/A	Select a device as the third startup device.
Boot option #4	N/A	Select a device as the fourth startup device.
CD/DVD ROM Drive BBS Priorities	N/A	Set the order of the legacy devices in this group.
Hard Drive BBS Priorities	N/A	Set the order of the legacy devices in this group.
Network Device BBS Priorities	N/A	Set the order of the legacy devices in this group.
Floppy Drive BBS Priorities	N/A	Set the order of the legacy devices in this group.

Selecting a startup device

If your server does not start up from a desired device such as the disc or HDD as expected, do one of the following to select the startup device you want:

Note: Not all discs, HDDs, or other removable devices are bootable.

- To select a temporary startup device, do the following:

  Note: Selecting a startup device using the following method does not permanently change the startup sequence.

  1. Turn on or restart your server.
  2. When you see the logo screen, press F12 to display the boot menu. The boot device selection window opens.
  3. In the boot device selection window, use the up and down arrow keys on the keyboard to switch between the selections. Press Enter to select the device of your choice. Then, the server will start up from the selected device.
- To view or permanently change the configured startup device sequence, do the following:
  1. Start the System Setup Utility. See “Get started” on page 1.
  2. On the **Boot** menu, follow the instructions on the screen to set the startup device depending on your needs. You also can set the boot priority for various devices. See “Boot menu” on page 33.
  3. Press F4 to save settings and exit the System Setup Utility. The server will follow the startup device sequence you have set each time you turn on the server.

Save & Exit menu

You can use the **Save & Exit** menu to save changes, discard changes, or load default values, and then exit the program. Press Enter to select the item on the **Save & Exit** menu, and then select **Yes** when prompted to confirm the action.

The **Save & Exit** menu contains the following items:

Menu item	Description
Save Changes and Exit	Save changes and exit the System Setup Utility.
Save Changes and Reset	Reset the system after saving the changes.
Discard Changes	Discard changes done so far to any of the setup options.
Restore Defaults	Restore/Load Default values for all the setup options.

Exiting the System Setup Utility

After you finish viewing or changing settings, press Esc to return to the System Setup Utility main interface. If you are on a nested submenu, press Esc repeatedly until you reach the main interface. To exit the System Setup Utility, you also can do the following:

- Press F4 to save the new settings and exit the System Setup Utility.
- Press F3 to return to the Optimized Default settings.

For more information about the **Save & Exit** menu in the System Setup Utility, see “Save & Exit menu” on page 34.

Chapter 3. BIOS setup

This section provides instructions on how to update the BIOS and how to recover from a POST and BIOS update failure.

System program is the basic layer of software built into your server. System program includes the POST, the UEFI BIOS, and the System Setup Utility. The POST is a set of tests and procedures that are performed each time you turn on your server. The UEFI BIOS is a layer of software that translates instructions from other layers of software into electrical signals that the server hardware can execute. You can use the System Setup Utility to view or change the configuration settings of your server, see Chapter 2 “System configuration and boot management” on page 3.

Lenovo might make changes and enhancements to the BIOS and TSM firmware. When updates are released, they are available for download on the Lenovo Web site at https://datacentersupport.lenovo.com. You can update the server firmware by downloading an update package and following the instructions on the Web page.

You also can use the Firmware Updater program to help you keep the server firmware up-to-date.

Updating the BIOS

This topic provides instructions on how to update (flash) the BIOS.

Notes:

- Update the BIOS on your server only if the newer BIOS version specifically solves a problem you have. We do not recommend BIOS updates for servers that do not need them. You can view the updated information for the new BIOS version in the installation instructions for the BIOS update utility program.
- Downgrading the BIOS to an earlier version is not recommended and might not be supported. An earlier BIOS version might not contain the support for the latest system configurations.
- If the power to your server is interrupted while the POST and BIOS are being updated, your server might not restart properly. Ensure that you perform the BIOS update procedure in an environment with a steady power supply. Besides, ensure that your server can restart successfully without encountering hardware problems.
- After you have updated the BIOS firmware, all the BIOS settings will be preserved. If you want to do any specific setting changes, please configure the BIOS settings.

To update (flash) the BIOS, do the following:

1. Go to https://datacentersupport.lenovo.com and follow the instructions on the Web page to locate the BIOS update package.
2. Download the BIOS update package and the TXT file that contains installation instructions.
3. Print the TXT file and follow the instructions to update (flash) the BIOS.

Recovering from a BIOS update failure

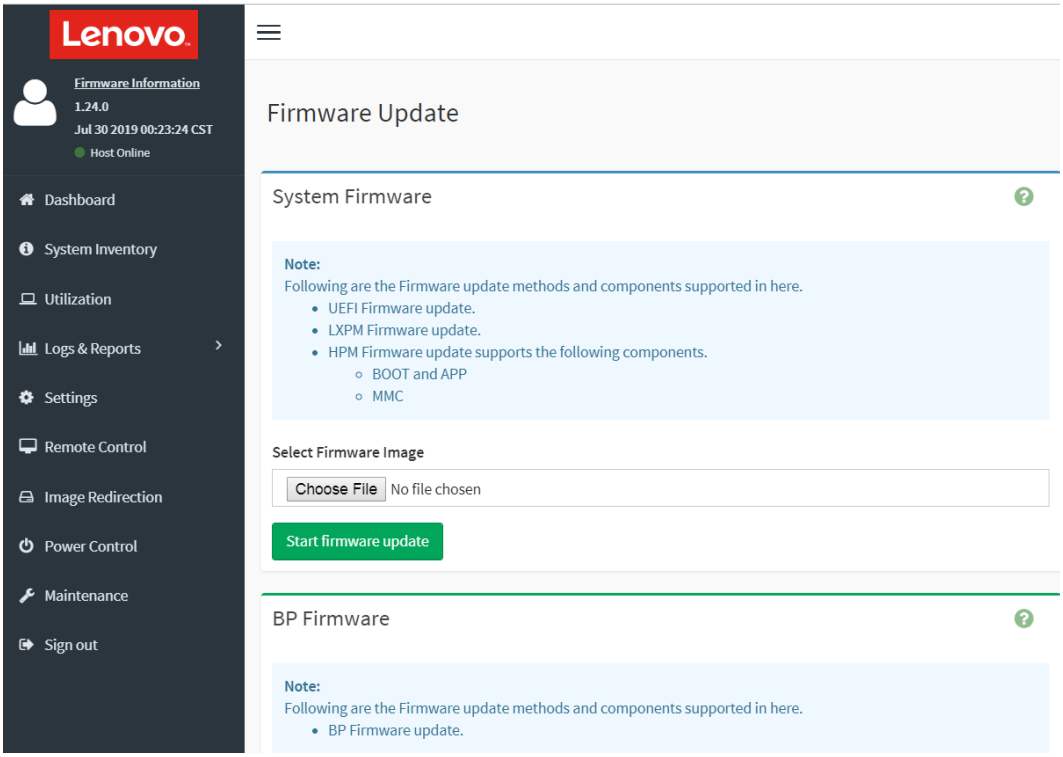
If the server BIOS has become corrupted, such as from a power failure during an update, you can recover the server BIOS in following way:

- Automate recovery from TSM: when the system hangs over ten minutes during POST, TSM will automate recovery UEFI BIOS to let the server to power on again.

- Out-of-band method: use the TSM Web interface to update the firmware, using the latest UEFI BIOS package.

To recover from a BIOS update failure, do the following:

1. Go to https://datacentersupport.lenovo.com and follow the instructions on the Web page to download the UEFI BIOS package.
2. Put the ROM file to your client system.
3. Reconnect the server to an ac power source and make sure the TSM heartbeat LED is blinking.
4. Login in TSM and follow the steps to update UEFI firmware.
   a. Go to **Home → Maintenance → Firmware Update → Select Firmware Image → Input the filename**.



   b. Click **Start Firmware Update**.
   c. Click **Processed to Flash**.
   d. Click **OK**.
   e. When you see the message as below, please click **OK** and then press the power button to turn on the server.
      `Firmware update is completed. The system will wait 10 seconds then will reboot into regular operating mode.`
   f. Check and configure the BIOS settings for your specific needs. See Chapter 2 “System configuration and boot management” on page 3.

Note: If you cannot recover the BIOS after using the instructions in this topic. You must replace the system board. Contact the Lenovo Customer Support Center.

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.

Appendix B. Trademarks

LENOVO and LENOVO logo are trademarks of Lenovo.

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


Lenovo