ThinkSystem HS350X V3 UEFI User Guide

Machine Type: 7DE3

First Edition (March 2024)

Contents

Chapter 1. UEFI Overview

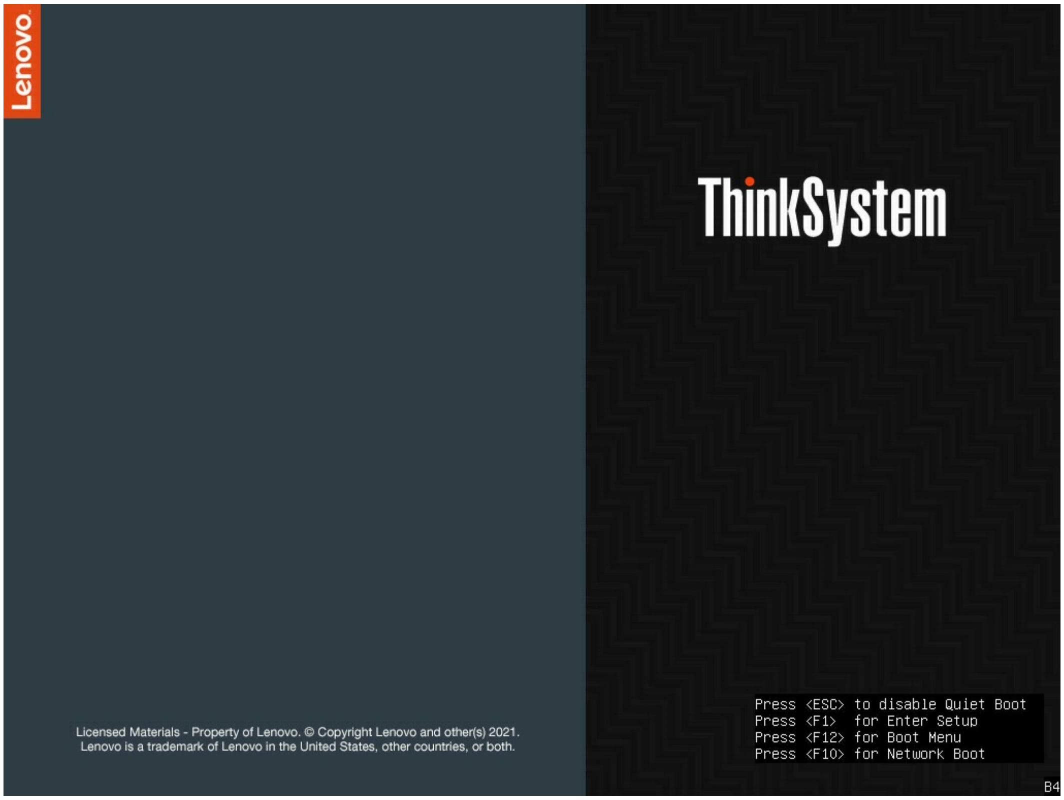
This topic provides a general introduction to the Unified Extensible Firmware Interface (UEFI).

UEFI is an interface packed with various features, including system information and settings, boot and runtime services, BMC settings, system event logs, and user security.

Enter Setup

Follow below steps to launch UEFI Setup Utility.

1. Connect a local keyboard, video and mouse (KVM) to boot or reboot the system.



Licensed Materials - Property of Lenovo. © Copyright Lenovo and other(s) 2021.
Lenovo is a trademark of Lenovo in the United States, other countries, or both.

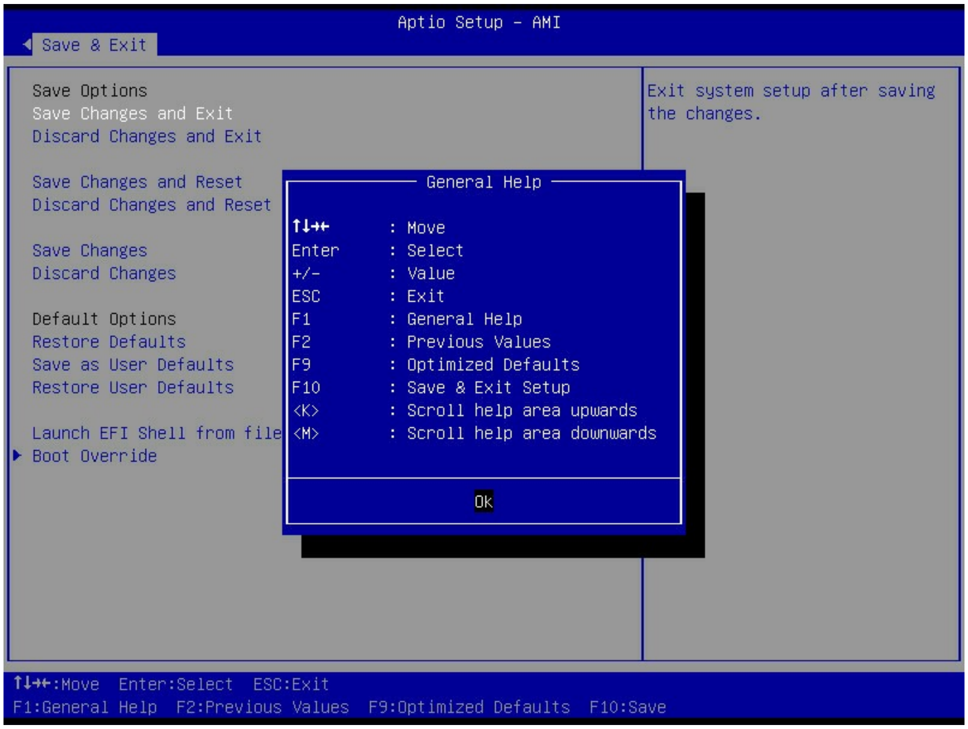
```
Press <ESC> to disable Quiet Boot
Press <F1>  for Enter Setup
Press <F12> for Boot Menu
Press <F10> for Network Boot
```

Figure 1. Enter Setup

2. Press F1 for entering setup. Press F10 for Network Boot. Press F12 to get Boot menu. Press ESC to disable Quiet Boot.

Function keys

Here are function keys for general help.



```
                         Aptio Setup - AMI
 Save & Exit

 Save Options                                         Exit system setup after saving
 Save Changes and Exit                                the changes.
 Discard Changes and Exit

 Save Changes and Reset   ──────── General Help ────────
 Discard Changes and Reset
                          ↑↓→←       : Move
 Save Changes             Enter      : Select
 Discard Changes          +/-        : Value
                          ESC        : Exit
 Default Options          F1         : General Help
 Restore Defaults         F2         : Previous Values
 Save as User Defaults    F9         : Optimized Defaults
 Restore User Defaults    F10        : Save & Exit Setup
                          <K>        : Scroll help area upwards
 Launch EFI Shell from file <M>      : Scroll help area downwards
▶ Boot Override

                                         Ok

 ↑↓→←:Move  Enter:Select  ESC:Exit
 F1:General Help  F2:Previous Values  F9:Optimized Defaults  F10:Save
```

Figure 2. Function keys

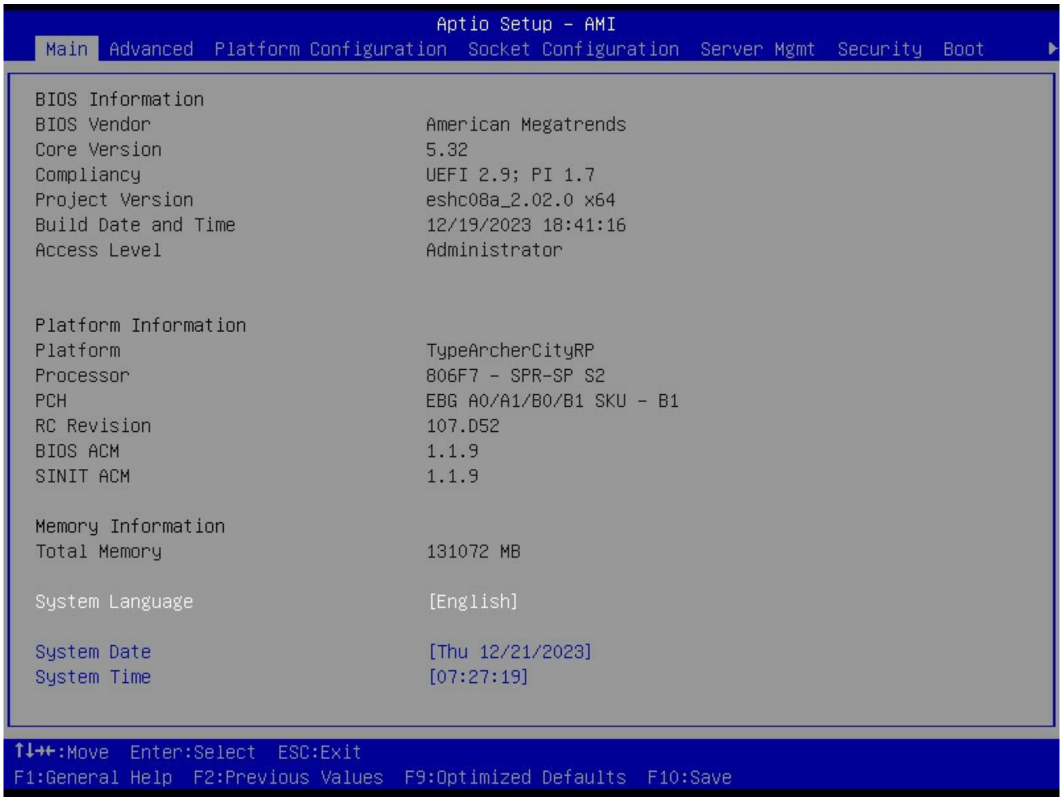
Main menu

The following list details the main menu.

- Chapter 2 “Main” on page 3
- Chapter 3 “Advanced” on page 5
- Chapter 4 “Platform Configuration” on page 17
- Chapter 5 “Socket Configuration” on page 29
- Chapter 6 “Server Mgmt” on page 43
- Chapter 7 “Security” on page 49
- Chapter 8 “Boot” on page 57
- Chapter 9 “Save & Exit” on page 61

Chapter 2. Main

Main is for looking up basic BIOS information, and setting up the BIOS system. The page details BIOS information, platform information, memory information and system setup.


Aptio Setup – AMI
Main
Advanced
Platform Configuration
Socket Configuration
Server Mgmt
Security
Boot
↑↓→←:Move Enter:Select ESC:Exit
F1:General Help F2:Previous Values F9:Optimized Defaults F10:Save

```
BIOS Information
BIOS Vendor                           American Megatrends
Core Version                          5.32
Compliancy                            UEFI 2.9; PI 1.7
Project Version                       eshc08a_2.02.0 x64
Build Date and Time                   12/19/2023 18:41:16
Access Level                          Administrator


Platform Information
Platform                              TypeArcherCityRP
Processor                             806F7 - SPR-SP S2
PCH                                   EBG A0/A1/B0/B1 SKU - B1
RC Revision                           107.D52
BIOS ACM                              1.1.9
SINIT ACM                             1.1.9

Memory Information
Total Memory                          131072 MB

System Language                       [English]

System Date                           [Thu 12/21/2023]
System Time                           [07:27:19]
```

Figure 3. Main

Table 1. Item and description

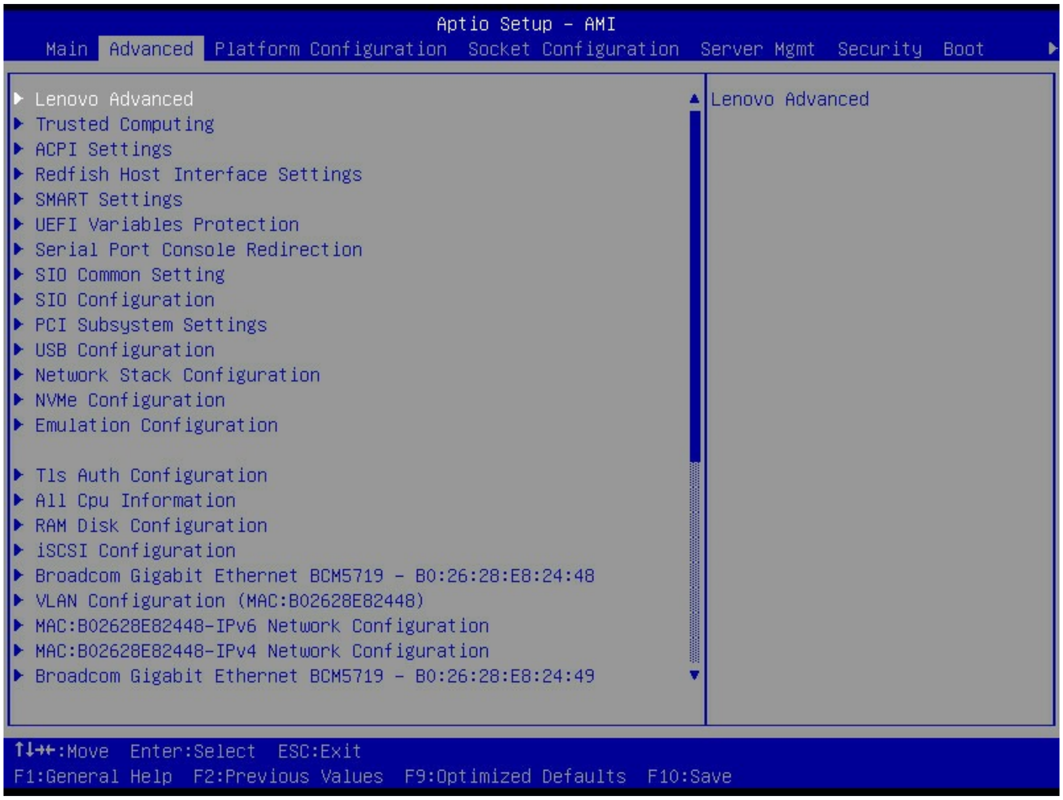
Item	Description
BIOS Vendor	Displays BIOS vendor.
Core Version	Displays core version.
Compliancy	Displays compliant versions of UEFI and PI.
Project Version	Displays current BIOS version.
Build Date and Time	Displays current build date and time.
Access Level	Displays current access level, administrator or user.
Platform	TypeArcherCityRP
Processor	Displays the processor type that the system is running on.
PCH	Displays the Platform Controller Hub (PCH) type that the system is running on.
RC Version	Displays the dynamic value base on which code base BIOS included.

Table 1. Item and description (continued)

Item	Description
BIOS ACM	Displays the dynamic value base on which code base BIOS included.
SINIT ACM	Displays the dynamic value base on which code base BIOS included.
Total Memory	Displays the total memory capacity of the system.
System Language	Displays BIOS setup language.
System Date	Displays the current date by default.
System Time	Displays the current time by default.

Chapter 3. Advanced

Advanced displays a series of advanced settings for BIOS.



```
                              Aptio Setup - AMI
   Main  Advanced  Platform Configuration  Socket Configuration  Server Mgmt  Security  Boot

 ▶ Lenovo Advanced                                             Lenovo Advanced
 ▶ Trusted Computing
 ▶ ACPI Settings
 ▶ Redfish Host Interface Settings
 ▶ SMART Settings
 ▶ UEFI Variables Protection
 ▶ Serial Port Console Redirection
 ▶ SIO Common Setting
 ▶ SIO Configuration
 ▶ PCI Subsystem Settings
 ▶ USB Configuration
 ▶ Network Stack Configuration
 ▶ NVMe Configuration
 ▶ Emulation Configuration

 ▶ Tls Auth Configuration
 ▶ All Cpu Information
 ▶ RAM Disk Configuration
 ▶ iSCSI Configuration
 ▶ Broadcom Gigabit Ethernet BCM5719 - B0:26:28:E8:24:48
 ▶ VLAN Configuration (MAC:B02628E82448)
 ▶ MAC:B02628E82448-IPv6 Network Configuration
 ▶ MAC:B02628E82448-IPv4 Network Configuration
 ▶ Broadcom Gigabit Ethernet BCM5719 - B0:26:28:E8:24:49

 ↑↓→←:Move  Enter:Select  ESC:Exit
 F1:General Help  F2:Previous Values  F9:Optimized Defaults  F10:Save
```

Figure 4. Advanced

Table 2. Item and description

Item	Description
"Lenovo Advanced" on page 6	Lenovo Advanced allows users to view and do settings for processor, memory, storage, USB, ACPI and VMD.
"Trusted Computing" on page 7	Trusted Computing lists firmware, security device, platform and storage hierarchy, and allows users to select TPM versions.
"ACPI Setting" on page 8	ACPI Setting shows system ACPI parameters and allows users to enable or disable BIOS ACPI auto configuration.
"Redfish Host Interface Settings" on page 8	Redfish Host Interface Settings lists Redfish versions and requires users to enter IP related items.
"SMART Settings" on page 9	SMART Settings allows users to run SMART Self Test on all HDDs during POST.
"UEFI Variables Protection" on page 9	UEFI Variables Protection shows NVRAM Runtime Variable Protection Settings.

Table 2. Item and description (continued)

Item	Description
"Serial Port Console Redirection" on page 9	Serial Port Console Redirection details how the host computer and the remote computer (which the user is using) will exchange data.
"SIO Common Setting" on page 12	SIO Common Setting enables or disables Lock of Legacy Resources.
"SIO Configuration" on page 12	SIO Configuration details System Super IO chip parameters.
"PCI Subsystem Settings" on page 12	PCI Subsystem Settings shows PCI, PCI-X and PCI Express Settings.
"USB Configuration" on page 13	USB Configuration lists USB related information and allows users to do settings between OSes and USB.
"UEFI Network Stack Configuration" on page 14	UEFI Network Stack Configuration details IPv4 PXE boot, IPv4 HTTP boot and IPv6 PXE boot settings.
"NVMe Configuration" on page 14	NVMe Configuration lists NVME Device Options Settings.
"Emulation Configuration" on page 15	Emulation Configuration details uBIOS Generation, Hybrid SLE Mode, and MSR Trace for PM.

Lenovo Advanced

Lenovo Advanced allows users to view and do settings for processor, memory, storage, USB, ACPI and VMD.

Table 3. Lenovo Advanced

Item			Description or format	Options or value
Add UEFI Shell To Boot Option			Enables or disables Built-In EFI Shell in Boot Option.	• **Disable** • Enable
Processor Settings	KTI Link Speed		Slow or 1S Configuration	N/A
Memory Settings	Total System Memory		2048.0 GB	N/A
	Current Memory Speed		4800 MT/s	N/A
	Memory RAS Configuration	Set MCA memory CMCI	Forces set MCA memory related Banks as CMCI for correctable error.	• Disable • **Enable**
		Mirror Failover Handle by Bios	Forces set Memory Mirror Failover error trigger SMI.	• Disable • **Enable**
Storage Settings	NVME Information		SOP2A (M.2#0): Not Installed	N/A
			SOP2B (M.2#1): Not Installed	

Table 3. Lenovo Advanced (continued)

Item		Description or format	Options or value
		SOP4C (NVME2): Not Installed,HotPlug Capable	
		SOP4D (NVME3): Not Installed,HotPlug Capable	
USB Settings	USB Port Support	USB Port 1 (Front Port 1)	• Disable • **Enable**
		USB Port 2 (Rear Port 1)	• Disable • **Enable**
		USB Port 3 (Rear Port 2)	• Disable • **Enable**
ACPI and Performance Settings	Fan Profile	N/A	• Performance • Automatic • Acoustic • **Unspecified**
	Current Fan Profile Status	N/A	Acoustic
	Power Technology	Enables the power management features.	• Energy Efficient • **Custom** • Max Performance • Nominal Frequency
VMD Settings		N/A	• **None** • VMD Group 1 (M.2) • VMD Group 2 (NVM) • VMD Group 2 (M.2 and NVM)

Trusted Computing

Trusted Computing lists firmware, security device, platform and storage hierarchy, and allows users to select TPM versions.

Table 4. Trusted Computing

Item	Description or format	Options
TPM2.0 Device Found		
Firmware Version:	7.2	N/A
Vendor:	NTC	N/A
Security Device Support	N/A	• Disable • **Enable**
Active PCR banks	SHA256	N/A
Available PCR banks	SHA256, SHA384	N/A

Table 4. Trusted Computing (continued)

Item	Description or format	Options
SHA256 PCR Bank	N/A	• Disabled • **Enabled**
SHA384 PCR Bank	N/A	• **Disabled** • Enabled
Pending operation	N/A	• **None** • TPM Clear
Platform Hierarchy	N/A	• Disabled • **Enabled**
Storage Hierarchy	N/A	• Disabled • **Enabled**
Endorsement Hierarchy	N/A	• Disabled • **Enabled**
Physical Presence Spec Version	N/A	• 1.2 • **1.3**
TPM 2.0 Interface Type	TIS	N/A
Device Select	N/A	• TPM 1.2 • TPM 2.0 • **Auto**

ACPI Setting

ACPI Setting shows system ACPI parameters and allows users to enable or disable BIOS ACPI auto configuration.

Table 5. ACPI Setting

Item	Description	Options
Enable ACPI Auto Configuration	Enables or disables BIOS ACPI auto configuration.	• **Disabled** • Enabled

Redfish Host Interface Settings

Redfish Host Interface Settings lists Redfish versions and requires users to enter IP related items.

Table 6. Redfish Host Interface Settings

Item	Description, format or instruction	Options
Redfish	Enables or disables AMI Redfish.	• Disabled • **Enabled**
BMC Redfish Version	1.15.1	N/A
BIOS Redfish Version	1.11.0	N/A
BIOS RTP Version	RB_1.0.16	N/A
Authentication mode	Selects authentication mode.	• **Basic Authentication** • Session Authentication
Redfish BMC Settings		

Table 6. Redfish Host Interface Settings (continued)

Item	Description, format or instruction	Options
IP address	Enter IP address.	N/A
IP Mask address	Enter IP Mask address.	N/A
IP Port	Enter IP Port.	N/A

SMART Settings

SMART Settings allows users to run SMART Self Test on all HDDs during POST.

Table 7. SMART Settings

Item	Description	Options
AST2600 Super IO Configuration		
SMART Self Test	Runs SMART Self Test on all HDDs during POST.	• **Disabled** • Enabled

UEFI Variables Protection

UEFI Variables Protection shows NVRAM Runtime Variable Protection Settings.

Table 8. UEFI Variables Protection

Item	Description	Options
Password protection of Runtime Variable	N/A	• Disabled • **Enabled**

Serial Port Console Redirection

Serial Port Console Redirection details how the host computer and the remote computer (which the user is using) will exchange data.

Table 9. Serial Port Console Redirection

Item	Description or format	Options
COM1		
Console Redirection	Console redirection enable or disable	• Disable • **Enable**
Console Redirection Settings	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.	
COM1		
Console Redirection Settings		

Table 9. Serial Port Console Redirection (continued)

Item		Description or format	Options
	Terminal Type	Emulation: 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.	• VT100 • VT100Plus • VT-UTF8 • **ANSI**
	Bits per second	Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.	• 9600 • 19200 • 38400 • 57600 • **115200**
	Data Bits	N/A	• 7 • **8**
	Parity	A parity bit can be sent with the data bits to detect some transmission errors. Even: parity bit is 0 if the num of 1's in the data bits is even. Odd: parity bit is 0 if num of 1's in the data bits is odd. Mark: parity bit is always 1. Space: Parity bit is always 0. Mark and Space Parity do not allow for error detection. They can be used as an additional data bit.	• **None** • Even • Odd • Mark • Space
	Stop Bits	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.	• **1** • 2
	Flow Control	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.	• **None** • Hardware RTS • CTS

Table 9. Serial Port Console Redirection (continued)

Item		Description or format	Options
	VT-UTF8 Combo Key Support	Enables VT-UTF8 Combination Key Support for ANSI/VT100 terminals.	• Disabled • **Enabled**
	Recorder Mode	With this mode enabled only text will be sent. This is to capture Terminal data.	• **Disabled** • Enabled
	Resolution 100x31	Enables or disables extended terminal resolution.	• Disabled • **Enabled**
	Putty KeyPad	Selects FunctionKey and KeyPad on Putty.	VT100

Table 10. Serial Port Console Redirection

Item		Description or format	Options
Serial Port for Out-of-Band Management/Windows Emergency Management Services (EMS)			
Console Redirection EMS		Console redirection enabling or disabling.	• Disabled • **Enabled**
	Out-of-Band Mgmt Port	COM1	N/A
	Terminal Type EMS	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.	• VT100 • VT100Plus • VT-UTF8 • **ANSI**
	Bits per second EMS	Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.	• 9600 • 19200 • 38400 • 57600 • **115200**
	Flow Control EMS	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 or stop signals.	• **None** • Hardware RTS/CTS • Software Xon/Xoff
	Data Bits EMS	8	N/A

Table 10. Serial Port Console Redirection (continued)

Item		Description or format	Options
	Parity EMS	None	N/A
	Stop Bits EMS	1	N/A

SIO Common Setting

SIO Common Setting enables or disables Lock of Legacy Resources.

Table 11. SIO Common Setting

Item	Description	Options
Lock Legacy Resources	Enables or disables Lock of Legacy Resources.	• **Disabled** • Enabled

SIO Configuration

SIO Configuration details System Super IO chip parameters.

Table 12. SIO Configuration

Item		Description or format	Options
AMI SIO Driver Version :			
Super IO Chip Logical Device(s) Configuration			
[*Active*] Serial Port		Set Parameters of COM0	
	Serial Port Configuration	COM1	N/A
	Use This Device	Enables or disables serial port (COM).	• Disabled • **Enabled**
	Logical Device Settings:		
	Current:	IO=2F8h; IRQ=3;	
	Possible	Allows the user to change the device resource settings. New settings will be reflected on this setup page after system restarts.	• **Use Automatic Settings** • IO=2F8h; IRQ=3; DMA • IO=3F8h; IRQ=3,4,5,7,9,10,11,12; DMA • IO=2E8h; IRQ=3,4,5,7,9,10,11,12; DMA • IO=3E8h; IRQ=3,4,5,7,9,10,11,12; DMA • IO=2E8h; IRQ=3,4,5,7,9,10,11,12; DMA
	Attention: Disabling SIO Logical Devices may have unwanted side effects. PROCEED WITH CAUTION.		

PCI Subsystem Settings

PCI Subsystem Settings shows PCI, PCI-X and PCI Express Settings.

Table 13. PCI Subsystem Settings

Item	Description	Options
PCI Bus Driver Version	A5.01.30	N/A
PCI Devices Common Settings:		
Above 4G Decoding	Enables or disables 64 bits capable devices to be decoded in Above 4G address space (Only if system supports 64bit PCI decoding).	• Disabled • **Enabled**
SR-IOV Support	If system has SR-IOV capable PCIe devices, this option enable or disable single root IO virtualization support.	• Disabled • **Enabled**
BME DMA Mitigation	Re-enables Bus Master Attribute disabled during PCI enumeration for PCI Bridges after SMM Locked.	• **Disabled** • Enabled

USB Configuration

USB Configuration lists USB related information and allows users to do settings between OSes and USB.

Table 14. USB Configuration

Item	Description or format	Options
USB Module Version：32		
USB Controllers: 1 XHCI		
USB Devices: 2 Keyboard, 1 Mouse, 1 Hub		
Legacy USB Support	Enables 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.	• Disabled • **Enabled** • Auto
XHCI Hand-off	This is a workaround for OSes without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver.	• Disabled • **Enabled**
USB Mass Storage Driver Support	Enables/disables USB Mass Storage Driver Support.	• Disabled • **Enabled**
Port 60/64 Emulation	Enables I/O port 60h/64h emulation support. This should be enabled for the complete USB keyboard legacy support for non-USB aware OSes.	• Disabled • **Enabled**

Table 15. USB Configuration

Item	Description or format	Options
USB hardware delays and time-outs:		
USB transfer time-out	The time-out value for Control, Bulk, and Interrupt transfers.	• 1 sec • 5 sec • 10 sec • **20 sec**
Device reset time-out	The time-out value for Control, Bulk, and Interrupt transfers.	• 10 sec • **20 sec** • 30 sec • 40 sec
Device power-up delay	Maximum time the device will take before it properly reports itself to the Host Controller. 'Auto' uses default value: for a Root port it is 100 ms, for a Hub port the delay is taken from Hub descriptor.	• Auto • **Manual**

UEFI Network Stack Configuration

UEFI Network Stack Configuration details IPv4 PXE boot, IPv4 HTTP boot and IPv6 PXE boot settings.

Table 16. UEFI Network Stack Configuration

Item	Description	Options or values
Network Stack	Enables or disables UEFI Network Stack.	• Disabled • **Enabled**
Ipv4 PXE Support	Enables or disables IPv4 PXE boot support. If disabled, IPv4 PXE boot support will not be available.	• Enabled • **Disabled**
Ipv4 HTTP Support	Enables or disables IPv4 HTTP boot support. If disabled, IPv4 HTTP boot support will not be available.	• Enabled • **Disabled**
Ipv6 HTTP Support	Enables or disables IPv6 PXE boot support. If disabled, IPv6 PXE boot support will not be available.	• Enabled • **Disabled**
PXE boot wait time	Wait time in seconds to press ESC key to abort the PXE boot. Use either +/- or numeric keys to set the value.	0
Media detect count	Number of times the presence of media will be checked. Use either +/- or numeric keys to set the value.	1

NVMe Configuration

NVMe Configuration lists NVME Device Options Settings.

Table 17. NVMe Configuration

Item	Description or value
NVMe controller and Drive information	
Bus:40 Dev:0 Func:0	SAMSUNG MZ1LB960HAJQ-00007
Nvme Size	960.1GB

Emulation Configuration

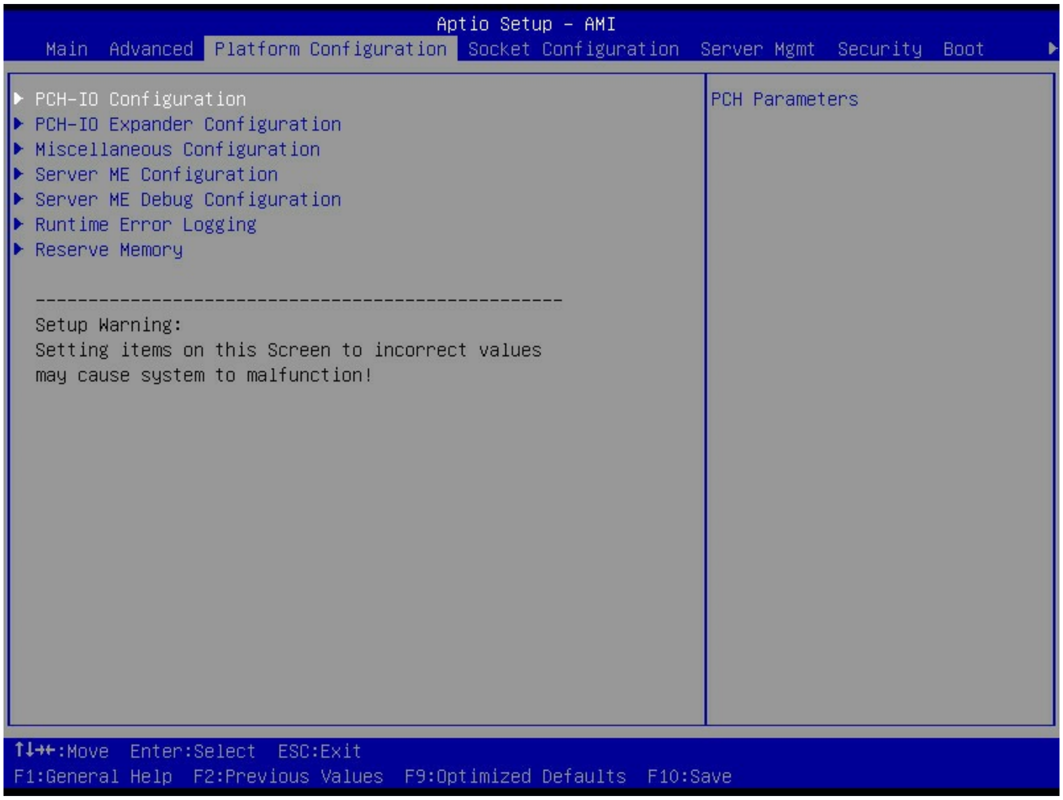
Emulation Configuration details uBIOS Generation, Hybrid SLE Mode, and MSR Trace for PM.

Table 18. Emulation Configuration

Item	Description	Options
Emulation Configuration "--"		
uBIOS Generation	Enables or disables uBIOS Generation.	• Disabled • Enabled • **Auto**
Hybrid SLE Mode	Enables or disables Hybrid System Level Emulation Mode.	• Disabled • Enabled • **Auto**
MSR Trace for PM	Enables or disables MSR Trace for Power management in uBIOS.	• Disabled • Enabled • **Auto**

Chapter 4. Platform Configuration

This configuration controls the features or behaviors of PCH.



```
                          Aptio Setup - AMI
   Main  Advanced  Platform Configuration  Socket Configuration  Server Mgmt  Security  Boot  ►

► PCH-IO Configuration                                           PCH Parameters
► PCH-IO Expander Configuration
► Miscellaneous Configuration
► Server ME Configuration
► Server ME Debug Configuration
► Runtime Error Logging
► Reserve Memory

  --------------------------------------------------
  Setup Warning:
  Setting items on this Screen to incorrect values
  may cause system to malfunction!

↑↓→←:Move  Enter:Select  ESC:Exit
F1:General Help  F2:Previous Values  F9:Optimized Defaults  F10:Save
```

Figure 5. Platform Configuration

Table 19. Item and description

Item	Description
"PCH-IO Configuration" on page 17	PCH-IO Configuration details debug settings.
"Miscellaneous Configuration" on page 18	Miscellaneous Configuration lists a series of settings that are pertinent to the system.
"Runtime Error Logging" on page 20	Runtime Error Logging lists eMCA, Whea, and Error Injection Settings. It also allows users to do Memory Error, IIO Error, PCIe Error settings. Press <Enter> view or change the runtime error log configuration.

PCH-IO Configuration

PCH-IO Configuration details debug settings.

Table 20. PCH-IO Configuration

Item		**Description**	**Options**
Debug Setting			
	DCI Enable	If 'Enabled' is selected, it is taken as user has 'opt-in' for debug. **Note:** This policy does not reflect the current platform debug status.	• **Auto** • Disabled • Enabled
	USB DbC Enable Mode	This BIOS option enables Debug Class (DbC) interface for platform debug only. Select 'No Change' will do nothing to DbC setting, or choose specifically USB2 or USB3. Select 'Disabled' to disable both USB2 and USB3 interface. **Note:** This BIOS option is auto-selected and intended for advanced configuration only.	• Disabled • USB2 • USB3 • Both • **No Change**
	USB Overcurrent Override for DbC	This option overrides USB Over Current enablement state that USB OC will be disabled after enabling this option. Enabled when DbC is used to avoid signaling conflicts.	• **Disabled** • Enabled

Miscellaneous Configuration

Miscellaneous Configuration lists a series of settings that are pertinent to the system.

Table 21. Miscellaneous Configuration

Item	**Description or format**	**Options**
Application Profile Configuration	Application Profile Configuration provides a quick method of BIOS knob tuning accordingly to application. It's based on benchmark tests and may be not suitable to all workloads. You can still override the options.	• **Auto** • General Computing • Memory BandWidth • Matrix Calculation • Entry Efficiency • Server Side Jave • OLTP • Virtualization
KCS Access Control Policy	Decides when IPMI commands shall be sent through KCS interface. Allow All - Always Restricted - until BIOS DONE is signalled Deny All - Never	• **Allow All** • Restricted • Deny All

Table 21. Miscellaneous Configuration (continued)

Item	**Description or format**	**Options**
Reset Platform on Memory Map Change	Causes a platform reset if the memory map has changed. Required for S4 resume to function at first boot.	• **Disabled** • Enabled
Wake On Lan Support	Enables or disables Wake On Lan Support.	• **Disable** • Enable
Breakpoint Type	Halts at specified points in BIOS.	• **None** • After MRC • After KTI RC • After Resource Allocation • After POST • After Full Speed Setup • Ready for IBIST

Serial Debug Message Level	Disable = no messages
	Minimum = critical messages
	Normal = critical & informational messages
	Maximum = all messages
	Auto = Minimum (default) or Normal (Advanced Debug mode)
		• Disable
		• Minimum
		• Normal
		• Maximum
		• **Auto**
		• Fixed PCD

Trace Messages	Enables display of every IO access.	• **Disable** • Enable • Enable for registry writes only
Training Messages	Enables to display the training results. Training results also get displayed if debug messages is set to Maximum.	• **Disable** • Enable
Active Video	Selects active Video type.	• Auto • **Onboard Device** • PCI Device
ARI Support	Enables or disables the ARI support.	• Disable • **Enable**
RTC Wake system from S4/S5	Enables or disables System wake on alarm event. When enabled, system will wake on the day : : hr : : min : : sec specified.	• **Disable** • Enable
Firmware Configuration	Firmware Configuration options.	• Ignore Policy Update • Production • Test • Internal • **Restricted** • Restricted SV

Table 21. Miscellaneous Configuration (continued)

Item	Description or format	Options
Warm-Reset Elimination	When enabled, BIOS will skip warm-reset on the cold-reset path.	• **Disable** • Enable • Auto
External SSC - CK440	Enables Spread Spectrum - only affects external clock generator.	• SSC Off • SSC = -0.3% • SSC = -0.5% • **Hardware**
Emulation BIOS Skip S3M Access	Emulation BIOS use it to skip S3M access. nEnable: S3M is skipped. nDisable: S3M is not skipped.	• Disable • Enable • **Auto**
Force Boot With FULL Socket Number	Forces Boot With FULL Socket Number, otherwise system will do PowerGood Reset.	• **Disable** • 1 Socket • 2 Sockets • 4 Sockets • 8 Sockets

Runtime Error Logging

Runtime Error Logging lists eMCA, Whea, and Error Injection Settings. It also allows users to do Memory Error, IIO Error, PCIe Error settings. Press <Enter> view or change the runtime error log configuration.

Table 22. Runtime Error Logging

Item	Description	Options
System Errors	System Error Enable/Disable setup options.	• Disable • **Enable**
S/W Error Injection Support	When Enabled, S/W Error Injection is supported by unlocking MSR 0x790.	• **Disable** • Enable
RAS Log Level	RAS Log setup options.	• **None** • MIN (BASIC_FLOW) • MID (BASIC_FLOW,FUNC_FLOW) • MAX (BASIC_FLOW,FUN_FLOW, REG)
System Memory Poison	Enables/disables System Memory Poison.	• Disable • **Enable**
Viral Status	N/A	• **Disable** • Enable
Cloak Devhide registers from being accessible from OS	Enables/disables OS to access Devhide registers.	• **Disable** • Enable
System Cloaking	When enabled, corrected and UCMA errors are masked from OS/SW visibility.	• **Disable** • Enable
UboxToPcuMca Enabling	N/A	**Enable**

Table 22. Runtime Error Logging (continued)

Item	Description	Options
FatalErrDebugHalt	DEBUG loop for McBank Fatal error case ONLY. **Attention:** Enabling this knob only in conjunction with ITP as thread will halt in Fatal error flow.	- **Disable** - Enable
Mca Bank Warm Boot Clear Errors	Enables/disables Mca Bank Warm Boot Clear Errors.	- Disable - **Enable**
Shutdown Suppression	Configures Shutdown Suppression and Log MCA IERR Support.	- Disable - **Shutdown Suppression and Log MCA IERR** - Shutwown Log MCA IERR

- "eMCA Settings" on page 21
- "Whea Settings" on page 22
- "Error Injection Settings" on page 22
- "Memory Error Enabling" on page 22
- "IIO Error Enabling" on page 23
- "PCIe Error Enabling" on page 25
- "Error Control Setting" on page 27
- "Crash Log Enabling" on page 27
- "DWR Configuration" on page 28

eMCA Settings

Press <Enter> to view or change the eMCA configuration.

Table 23. eMCA Settings

Item	Description	Options
EMCA Logging Support	Enables or disables EMCA Logging.	- Disable - **Enable**
LMCE Support	Enables or disables Local MCE firmware support.	- Disable - **Enable**
Ignore OS EMCA Opt-in	Enables or disables Ignore OS EMCA Opt-in and log.	- **Disable** - Enable
EMCA CMCI-SMI Morphing	Enables or disables EMCA CSMI.	- Disable - **EMCAgen 2 CSMI**
EMCA CMCI-SMI Threshold	Sets the threshold of correctable error for signaling CMCI-CSMI.	0
CSMI Dynamic Disable	[Enable] - BIOS disables CSMI when error threshold reached. [Disabled] - CSMI always on.	- **Disable** - Enable
EMCA MCE-SMI Enable	Enables or disables EMCA Uncorrected SMI for gen2.	- Disable - **EMCAgen 2 MSMI**

Table 23. eMCA Settings (continued)

Item	Description	Options
Corrected Error eLog	Enables or disables Corrected Error eLog.	• Disable • **Enable**
Memory Error eLog	Enables or disables Memory Error eLog.	• Disable • **Enable**
Processor Error eLog	Enables or disables Processor Error eLog.	• Disable • **Enable**
Opportunistic Spare Core	Enables or disables Opportunistic Spare Core Support.	• **Disable** • Enable
Ubox Error Mask	Masks SMI generation for Ubox Error.	• **Disable** • Enable

Whea Settings

Press <Enter> to view or change the WHEA configuration.

Table 24. Whea Settings

Item	Description	Options
Whea Support	Enables or disables WHEA support.	• Disable • **Enable**
Whea Log Memory Error	Enables or disables Whea Log Memory Error.	• Disable • **Enable**
Whea Log Processor Error	Enables or disables Whea Log Processor Error.	• Disable • **Enable**
Whea Log PCI Error	Enables or disables Whea Log PCI Error.	• Disable • **Enable**

Error Injection Settings

Press <Enter> to view or change the Error Injection configuration.

Table 25. Error Injection Settings

Item	Description	Options
Mca Bank Error Injection Support	Enables or disables Mca Bank Error Injection Support.	• **Disable** • Enable
Pmem Error Injection	Enables or disables Pmem Error Injection.	• **Disable** • Enable
WHEA Error Injection Support	Enables or disables WHEA Error Injection Support.	• **Disable** • Enable

Memory Error Enabling

Press <Enter> to view or change the Memory Error Enabling options.

Table 26. Memory Error Enabling

Item	Description	Options
Memory Corrected Error	Enables or disables Memory Corrected Error.	- Disable - **Enable**
Spare Interrupt	Spare Interrupt Selection	- Disable - **SMI** - Error Pin - CMCI
Pfd	Pfd is to identify hard error out from errors. Auto indicates PFD is enabled dynamically based on system configuration.	- Disable - Enable - **Auto**
PMem CTLR Errors	Enables or disables PMem CTLR Error Reporting & Logging.	- Disable - **Enable**
PMem CTLR Low Priority Error Singnaling	Selection of signaling for errors bucketed as Low Priority.	- Disable - **SMI** - Error Pin
PMem CTLR High Priority Error Singnaling	PMem CTLR High Priority Error Singnaling.	- Disable - **SMI** - Error Pin
Set PMem Address Range Scrub	Enables or disables PMem DIMM Physical Address Range scrub.	- **Disable** - Enable
Set PMem Host Alert Policy for Patrol Scrub	Enables or disables signaling DDRP interrupt upon receiving Uncorrectable Error for PMem Patrol Scrub.	- Disable - **Enable**
Enable Reporting SPA to OS	Enables Preporting SPA to OS (Only disable for MCE recovery validation).	- Disable - **Enable**
Set PMem Host Alert Policy for DPA Error	N/A	- **Poison** - Viral

IIO Error Enabling

Press <Enter> to view or change the IIO errors enabling options.

Table 27. IIO Error Enabling

Item	Description	Options
IIO/PCH Global Error Support	Enables or disables IIO/PCH Global Error Support.	- Disable - **Enable**
Os Native AER Support	Select FFM or OS native for AER error handling. If select OS native, BIOS also initializes FFM first until handshake, which depends on OS capacity.	- **Disable** - Enable
IIO MCA Support	Enables or disables IIO MCA Support.	- **Disable** - Enable
IIO Error Pin0 Enable	Enables or disables IIO Error Pin0.	- **Disable** - Enable

Table 27. IIO Error Enabling (continued)

Item	Description	Options
IIO Error Pin1 Enable	Enables or disables IIO Error Pin1.	- **Disable** - Enable
IIO Error Pin2 Enable	Enables or disables IIO Error Pin2.	- **Disable** - Enable
IIO OOB Mode	Enables or disables System Event Generation when Error Pin is enabled.	- Disable - **Enable**
IIO Error Registers Clear	Enables or disables Clear IIO Error Registers.	- Disable - **Enable**
IIO eDPC Support	Enables or disables IIO eDPC Support.	- **Disable** - On Fatal Error - On Fatal and Non-Fatal Error
IIO eDPC Interrupt	Enables or disables IIO eDPC Interrupt.	- Disable - **Enable**
IIO eDPC ERR_COR Message	Enables or disables IIO ERR_COR Message.	- Disable - **Enable**
IIO Coherent Interface Error	Enables or disables IIO Coherent Interface Error.	- Disable - **Enable**
IIO IRP0 protocol parity error	Enables or disables Coherent Interface protocol IIO parity error reporting.	- Disable - **Enable**
IIO IRP0 protocol qt overflow underflow error	Enables or disables Coherent Interface protocol queue table overflow or underflow error reporting.	- Disable - **Enable**
IIO IRP0 protocol rcvd unexprsp	Enables or disables Coherent Interface protocol layer received unexpected response or completion error reporting.	- Disable - **Enable**
IIO IRP0 csr acc 32b unaligned	Enables or disables Coherent Interface CSR Access Croessing 32-bit Boundary error reporting.	- Disable - **Enable**
IIO IRP0 wrcache uncecccs0 error	Enables or disables IIO Coherent Interface Write Cache Un-correctable ECC error reporting.	- Disable - **Enable**
IIO IRP0 wrcache uncecccs1 error	Enables or disables IIO Coherent Interface Write Cache Un-correctable ECC error reporting.	- Disable - **Enable**
IIO IRP0 protocol rcvd poison error	Enables or disables IIO Coherent Interface Protocol Layer Received Poisoned Packet error reporting.	- Disable - **Enable**
IIO IRP0 wrcache correcccs0 error	Enables or disables IIO Coherent Interface Write Cache Correctable ECC error reporting.	- Disable - **Enable**
IIO IRP0 wrcache correcccs1 error	Enables or disables IIO Coherent Interface Write Cache Correctable ECC error reporting.	- Disable - **Enable**

Table 27. IIO Error Enabling (continued)

Item	Description	Options
IIO Misc. Error	Enables or disables IIO Misc. Error.	• Disable • **Enable**
IIO Vtd Error	Enables or disables IIO Vtd Error.	• Disable • **Enable**
IIO Dma Error	Enables or disables IIO Dma Error.	• Disable • **Enable**
IIO Dmi Error	Enables or disables IIO Dmi Error.	• Disable • **Enable**
PCIE Error	Enables or disables PCIE Error.	• Disable • **Enable**
IIO PCIE Additional Corrected Error	Enables or disables IIO PCIE Additional Corrected Error.	• Disable • **Enable**
IIO PCIE Additional Uncorrected Error	Enables or disables IIO PCIE Additional Uncorrected Error.	• Disable • **Enable**
IIO PCIE Additional Received Completion With UR	Enables or disables IIO PCIE Additional Received Completion With UR.	• **Disable** • Enable
ITC/OTC CA/MA Errors	Enables or disables Completer Abort and Master Abort (Unsupported Request) on ITC and OTC.	• **Disable** • Enable
PSF UR Error	Enables or disables Unsupported Request Error on PSF.	• Disable • **Enable**
PMSB Router Parity Error	Enables or disables PMSB Router Parity Error.	• Disable • **Enable**

PCIe Error Enabling

Press <Enter> to view or change the PCIe errors enabling options.

Table 28. PCIe Error Enabling

Item	Description	Options
Corrected Error	Enables and escalates Correctable Errors to error pins.	• Disable • **Enable**
Uncorrected Error	Enables and escalates Uncorrectable/Recoverable to error pins.	• Disable • **Enable**
Fatal Error Enable	Enables and escalates Fatal Errors to error pins.	• Disable • **Enable**
PCIE Corrected Error Threshold Counter	Enables or disables PCIE Corrected Error Counter	• Disable • **Enable**
PCIE Corrected Error Threshold	Disable/2000/4000/8000	2000
PCIE Corrected Error Limit Check	Enables or disables the feature to disable reporting PCIe corrected errors for a device if they exceed a given limit.	• **Disable** • Enable

Table 28. PCIe Error Enabling (continued)

Item	Description	Options
PCIE Corrected Error Limit	N/A	80
PCIE ARE Corrected Errors	Enables or disables PCIE ARE corrected Errors.	• Disable • **Enable**
PCIE ARE NonFatal Error	Enables or disables PCIE ARE NonFatal Error.	• Disable • **Enable**
PCIE ARE Fatal Error	Enables or disables PCIE ARE Fatal Error.	• Disable • **Enable**
PCIE AER Advisory Nonfatal Error	Enables or disables PCIE AER Advisory Nonfatal Error.	• Disable • **Enable**
PCIE ECRC Error	Enables or disables PCIE ECRC Error.	• **Disable** • Enable
PCIE Surprise Link Down Error	Enables or disables PCIE Surprise Link Down Error.	• **Disable** • Enable
PCIE Unsupported Request Error	Enables or disables PCIE Unsupported Request Error.	• **Disable** • Enable
Assert NMI on SERR	On SERR, generates an NME and log and error. **Note:** [Enabled] must be selected for the Assert NMI on PEER setup option to be visible.	• Disable • **Enable**
Assert NMI on PERR	On PERR, generates an NME and log and error. **Note:** This option is only active if the Assert NMI on SERR option has [Enabled] selected.	• Disable • **Enable**

Table 29. PCIe Error Enabling

Item	Description	Options or values
Leaky Bucket Feature		
Expected BER	Sets the expected Bit Error Rate for all speeds.	34359738367
Time Window(Gen1/2)	Sets the error burst protection time window for Gen1 and Gen2 speeds. A burst of errors within the window is counted as one.	65535
Time Window(Gen3/4)	Sets the error burst protection time window for Gen3 and Gen4 speeds. A burst of errors within the window is counted as one.	2
Error Threshold (Gen1/2)	Sets the error threshold for Gen1 and Gen2 speeds. An event is triggered when the error count exceeds the threshold.	0

Table 29. PCIe Error Enabling (continued)

Item	Description	Options or values
Error Threshold (Gen3/4)	Sets the error threshold for Gen3 and Gen4 speeds. An event is triggered when the error count exceeds the threshold.	16
Gen3/4/5 Re-Equaliztion	Enables or disables Gen3 and Gen4 re-equalization. Applies only when operating at Gen2 or Gen4 speeds. When an event is triggered, equalization is re-run.	• Disable • **Enable**
Gen2 Link Degradation	Enables or disables Gen2 link degradation. Applies only when operating at Gen2 speeds. When an event is triggered, 5GT/s and higher modes are disabled.	• Disable • **Enable**
Gen3 Link Degradation	Enables or disables Gen3 link degradation. Applies only when operating at Gen3 speeds. When an event is triggered, 8GT/s and higher modes are disabled.	• Disable • **Enable**
Gen4 Link Degradation	Enables or disables Gen4 link degradation. Applies only when operating at Gen4 speeds. When an event is triggered, 16GT/s and higher modes are disabled.	• Disable • **Enable**
Gen5 Link Degradation	Enables or disables Gen5 link degradation. Applies only when operating at Gen5 speeds. When an event is triggered, 32GT/s and higher modes are disabled.	• Disable • **Enable**

Error Control Setting

Press <Enter> to view or change the Error Control Setting options.

Table 30. Error Control Setting

Item	Description	Options
2LM Correctable Error Logging in m2mem	Enables or disables 2LM correctable error logging in m2mem.	• Disable • **Enable**
Latch First Corrected Error in KTI	Enables or disables latch first corrected error in KIT.	• **Disable** • Enable
Patrol Scrub Error Reporting	N/A	UCNA
LLC EWB Error Control	N/A	• **UCNA** • SRAO

Crash Log Enabling

Press <Enter> to view or change the Crash Log enabling options.

Table 31. Crash Log Enabling

Item	Description	Options
CPU CrashLog Feature	The feature helps collecting crash data from OOBMSM SSRAM.	• Disable • Enable • **Auto**
Core CrashLog Disable	The feature helps to disable CPU Core crash log.	• **No** • Yes
OR CrashLog Disable	The feature helps to disable CPU TOR crash log.	• **No** • Yes
Uncore CrashLog Disable	The feature helps to disable CPU Uncore crash log.	• **No** • Yes
MCERR Trigger CrashLog Disable	The feature helps to disable MCERR to trigger crash log.	• **No** • Yes
CPU Clear CrashLog	Option to clear CPU CrashLog after collection.	• Disable • **Enable**
CPU Crashlog ReArm	Option to ReArm CPU CrashLog after collection.	• Disable • **Enable**

Table 32. Crash Log Enabling

Item	Description	Options
PCH CrashLog Feature	The feature helps collecting crash data from PMC SSRAM.	• Disable • **Enable**
PCH CrashLog Collect On All Reset	Option to invoke PCH CrashLog collection on all reset.	• **Disable** • Enable
PCH Clear CrashLog	Option to clear PCH CrashLog after collection.	• **Disable** • Enable
PCH ReArm CrashLog	Option to ReArm PCH CrashLog after collection.	• Disable • **Enable**

DWR Configuration

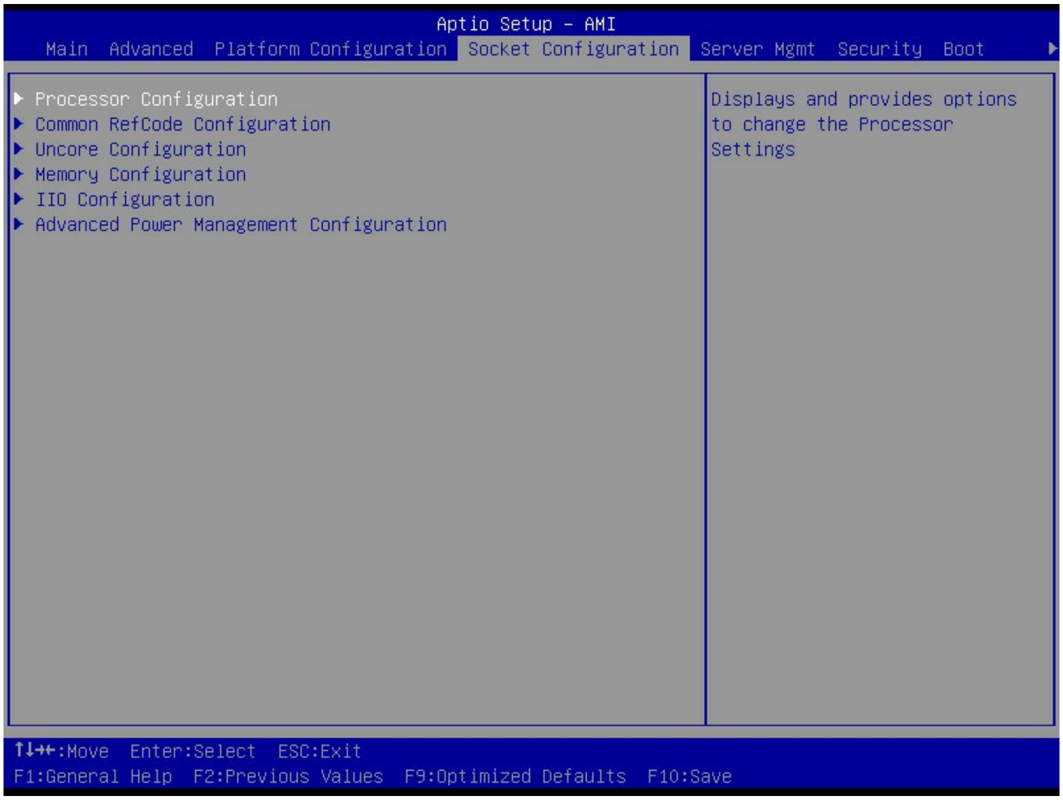
DWR Configuration is short for Dirty Warm Reset Configuration.

Table 33. DWR Configuration

Item	Description	Options
Dirty Warm Reset	Enables or disables Dirty Warm Reset. It promotes regular reset to DWR under internal error conditions.	• Disable • **Enable**
Ierr Global Reset	Enable = when Ierr error present in last boot, do Global reset	• Disable • **Enable**
DWR/IERR Error harvesting stall	When enabled, system will enter spin loop during dirty warm reset allowing manual error collection.	• **Disable** • Enable
BMC RootPort	RootPort that BMC is connected to.	• **6** • 12

Chapter 5. Socket Configuration

This configuration controls the features or behaviors of the processor.



Displays and provides options to change the Processor Settings

Figure 6. Socket Configuration

"Processor Configuration" on page 29	Processor Configuration displays and provides options to change the Processor Settings.
"Common RefCode Configuration" on page 32	Common RefCode Configuration displays and provides option to change the Common RefCode Settings.
"Uncore Configuration" on page 32	Uncore Configuration displays and provides option to change the UnCore Settings.
"Memory Configuration" on page 34	Memory Configuration displays and provides option to change the Memory Settings.
"IIO Configuration" on page 36	IIO Configuration displays and provides option to change the IIO Settings.
"Advanced Power Management Configuration" on page 38	Advanced Power Management Configuration displays and provides option to change the Power Management Settings.

Processor Configuration

Processor Configuration displays and provides options to change the Processor Settings.

Table 34. Processor Configuration

Per-Socket Configuration			
	CPU Socket 0 Configuration		
		CPU Socket 0 Configuration	
		Available Bitmap:	000000000ACACD9B
		Core Disable Bitmap (Hex)	0[Note]
Processor Revision	C06F2 - ENR-SP Ax	• **0** • FFFFFFFFFFF **Note:** 0: enables all cores. FFFFFFFFFFF: disables all cores. At least one core per CPU must be enabled. Disabling all cores is invalid configuration.	
Processor Socket	Socket 0		
Processor ID	000C06F2*		
Processor Frequency	2.000GHz		
Processor Max Ratio	14H		
Processor Min Ratio	08H		
Microcode Revision	21000190		
L1 Cache (Per Core)	80KB		
L2 Cache (Per Core)	2048KB		
L3 Cache (Per Package)	327680KB		
Processor 0 Version	Intel® Xeon (R) Platinum 8592V		

Table 35. Processor Configuration

Item	**Description**	**Options**
Enable LP [Global]	Enables Logical processor (Software Method to Enables or disables Logical Processor threads).	• **All LPs** • Single LP
Skip Flex Ratio Override	Skips Flex Ratio overrides to use power-on default Flex Ratio values. In multi-socket systems, this will allow mixed flex ratio limits.	• **Disable** • Enable
Check CPU BIST Result	Disable failed BIST core when enabled, otherwise, ignore BIST result.	• Disable • **Enable**
Machine Check	Enables or disables the Machine Check.	• Disable • **Enable**
Hardware Prefetcher	= MLC Streamer Prefetcher (MSR 1A4h Bit[0])	• **Enable** • Disable
Adjacent Cache Prefetch	= MLC Spatial Prefetcher (MSR 1A4h Bit[1])	• **Enable** • Disable
DCU Streamer Prefetcher	DCU streamer prefetcher is an L1 data cache prefetcher (MSR 1A4h [2]).	• **Enable** • Disable
DCU IP Prefetcher	DCU IP prefetcher is an L1 data cache prefetcher (MSR 1A4h [3]).	• **Enable** • Disable

Table 35. Processor Configuration (continued)

Item	**Description**	**Options**
LLC Prefetch	Enables or disables LLC Prefetch on all threads.	• Enable • **Disable**
Extended APIC	Enables or disables extended APIC support. **Note:** When enabled, VT-d & Interrupt Remapping will be automatically enabled.	• Disable • **Enable**
Enable Intel® TXT	Enables Intel(R) TXT.	• **Disable** • Enable
VMX	Enables the Vanderpool Technology, takes effect after reboot.	• Disable • **Enable**
Enable SMX	Enables Safer Mode Extensions.	• **Disable** • Enable
Lock Chipset	Locks or unlocks chipset.	• Disable • **Enable**
MSR Lock Control	Enables - MSR 3Ah and CSR 80h will be locked. Power Good reset is needed to remove lock bits.	• Disable • **Enable**
PPIN Control	Unlocks and enables or disables PPIN Control.	• Lock/Disable • **Unlock/Enable**

Table 36. Processor Configuration

Item	**Description**	**Options**
TME , MK-TME , TDX		
Memory Encryption(TME)	Enables or disables Memory Encryption(TME).	• **Disable** • Enable
Trust Domain Extension(TDX)	N/A	**Disable**
TDX Secure Arbitration Mode Loader (SEAM Loader)	N/A	**Disable**

Table 37. Processor Configuration

Item	**Description or format**	**Options**
Common PRM size for all features(SGX,S@F,…)		
PRM Size	0 MiB	
Software Guard Extension(SGX)		
SGX Factory Reset	Enables or disables Memory Encryption(TME).	**Disable**
SW Guard Extensions(SGX)	N/A	**Disable**
SGX Package Info In-Band Access	N/A	**Disable**
SGX PRM Size	N/A	**[Auto]**

Table 38. Processor Configuration

Item	Description	Option
In Field Scan (IFS)		
Scan at Field(SAF,S@F)	To enable IFS features please enable TME Enable SAF.	**Disabled**

Table 39. Processor Configuration

Item			Description	Options
PSMI Configuration				
Global PSMI Enable				
	Socket 0 Configuration		N/A	• Disable • **Enable**
		PSMI Enable	N/A	• Disable • **Enable**

Common RefCode Configuration

Common RefCode Configuration displays and provides option to change the Common RefCode Settings.

Table 40. Common RefCode Configuration

Item	Description	Options
Numa	Enables or disables Non uniform memory access (NUMA).	• Disable • **Enable**
Virtual Numa	Divides physical NUMA nodes into evenly sized virtual NUMA nodes in ACPI table. This may improve Windows performance on CPUs with more than 64 logical processors.	• **Disable** • Enable

Uncore Configuration

Uncore Configuration displays and provides option to change the UnCore Settings.

Table 41. Uncore Configuration

Item		Description or format	Options
Uncore General Configuration			
Uncore Status			
	Uncore Status		
	Number of CPU	1	N/A
	Current UPI Liink Speed	Slow or 1S Configuration	N/A
	Current UPI Liink Frequnency	Unknowm or 1S configuration	N/A
	Global MMIO Low Base / Limit	90000000 / FBFFFFFF	N/A
	Global MMIO High Base / Limit	0000200000000000 / 0000209FFFFFFFFF	N/A

Table 41. Uncore Configuration (continued)

Item		Description or format	Options
	Pci-e Configuration Base / Size	80000000 / 10000000	N/A
Degrade Precedence		Chooses Topology Precedence to degrade features if system options are in conflict or choose Feature Precedence to degrade topology if system options are in conflict.	• **Topology Precedence** • Feature Precedence
Degrade 4S Topology Preference		Chooses 4S Topology Preference when system can be degraded to either 4S1LFullyConnect or 4S2LRing topology.	• **4S Fully Connect(Single Link)** • 4S Ring (Dual Link)
Link Speed Mode		Fast - Train the UPI link to Fast speed (default) \nSlow - Keep slow speed.	• **Fast** • Slow
Link Frequnency Select		Allows for selecting the UPI Link Frequency, Auto - Auto decides based on Si Compatibility.	• 12.8GB/s • 14.4GB/s • 16.0GB/s • **Auto** • Use Per Link Setting
Link L0p Enable		Enable - Set the c_l0p_en, Disable - Reset it, Auto - Auto decides based on Si Compatibility.	• Disable • Enable • **Auto**
Link L1 Enable		Enable - Set the c_l1_en, Disable - Reset it, Auto - Auto decides based on Si Compatibility.	• Disable • Enable • **Auto**
UPI Dynamic Link Width Reduction Support		Recovers from hard failure on one or more UPI data lanes by dynamically resizing UPI link to 1/2 width, Auto - Auto decides based on Si Compatibility.	• Disable • Enable • **Auto**
Directory Mode Enable		Directory Mode Enable, Auto - Auto decides based on Si Compatibility.	• Disable • Enable • **Auto**
KTI Prefetch		KTI Prefetch, Auto - Auto decides based on Si Compatibility.	• Disable • Enable • **Auto**

Table 41. Uncore Configuration (continued)

Item	Description or format	Options
SNC(Sub NUMA)	Disable supports 1-cluster and 4-IMC way interleave. Enable SNC2 supports 2-clusters SNC and 2-way IMC interleave. Enable SNC4 supports 4-cluster and 1-IMC way interleave. Auto decides based on Si Compatibility.	• **Auto** • Disable • Enable SNC2 (2-clusters) • Enable SNC4 (4-clusters)
Limit CPU PA to 46 bits	Limit CPU physical address to 46 bits to support older Hyper-v. If enabled, automatically disables TME-MT.	• Disable • **Enable**

Memory Configuration

Memory Configuration displays and provides option to change the Memory Settings.

Table 42. Memory Configuration

Item	Description	Options or value
Integrated Memory Controller (iMC)		
PPR Type	Selects Post Package Repair. Type - Hard / Soft / Disabled. Auto - Sets it to the MRC default setting; current default is Soft PPR.	• **PPR Disabled** • Hard PPR • Soft PPR • Auto
Memory Frequency	Maximum Memory Frequency Selections in Mhz. If Enforce POR is disabled, user will be able to run at higher frequencies than the memory support (limited by processor support). Do not select Reserved.	• **Auto** • 3200 • 3600 • 4000 • 4400 • 4800 • 5200 • 5699
MemTest	Enable - Enables memory test during normal boot. Disable - Disables this feature.	• **Enable** • Disable
MemTest Loops	Number of memory test loops during normal boot, set to 0 to run memtest infinitely.	1
Training Result Offset	Enable - Enables training results to be offset. Disable - Disables this feature; current default is Enable.	• Enable • **Disable**

Table 42. Memory Configuration (continued)

Item	Description	Options or value
Memory Type	Selects the Memory type supported by this platform.	• RDIMMs only • UDIMMs only • **UDIMMs and RDIMMs**
Attempt Fast Boot	Enable - Portions of memory reference code will be skipped when possible to increase boot speed on warm boots. Disable - Disables this feature. Auto - Sets it to the MRC default setting; current default is Disable.	• **Enable** • Disable • Auto
Attempt Fast Cold Boot	Enable - Portions of memory reference code will be skipped when possible to increase boot speed on cold boots. Disable - Disables this feature. Auto - Sets it to the MRC default setting; current default is Disable.	• **Enable** • Disable • Auto
MemTest On Cold Fast Boot	Enable - Enables memory test during cold fast boot. Disable - Disables this feature. Auto - Sets it to the MRC default setting; current default is Disable.	• Enable • **Disable** • Auto

Table 43. Memory Configuration

Item	Description	Options or value
Memory RAS Configuration		
Mirror Mode	Full Mirror Mode will set entire 1LM memory in system to be mirrored, consequently reducing the memory capacity by half. Partial Mirror Mode will enable the required size of memory to be mirrored. If rank sparing is enabled partial mirroring will not take effect. Enabling any type of Mirror Mode will disable XPT Prefetch.	• **Disabled** • Full Mirror Mode • Partial Mirror Mode
Mirror TAD0	Enables Mirror on entire memory for TAD0.	• Enabled • **Disabled**
UEFI ARM Mirror	Imitates behavior of UEFI based Address Range Mirror with setup option.	• Enabled • **Disabled**

Table 43. Memory Configuration (continued)

Item	Description	Options or value
Memory Correctable Error Flood Policy	[Disabled] - Don't deal with Memory CE flood. [Once] - Only First Memory CE will trigger SMI, and BIOS will disable this rank silicon side to trigger SMI. [Frequency] - Disable SMI when Memory CE reache threshold within time limits.	• **Frequency** • Disable • Once
Correctable Error Threshold	Correctable Error Threshold (0x01 - 0x7fff) used for sparing, and leaky bucket.	7FFF
Trigger SW Error Threshold	Enables or disables Sparing trigger SW Error Match Threshold.	• Enabled • **Disabled**
Leaky bucket time window based interface	Enables or disables leaky bucket time window based interface.	• Enabled • **Disabled**
Leaky bucket time window based interface Hour	Leaky bucket time window based interface Hour (0 - 24).	24
Leaky bucket time window based interface Minute	Leaky bucket time window based interface Minute (0 - 60).	0
Leaky bucket low bit	Leaky bucket low bit (1 - 63).	14
Leaky bucket high bit	Leaky bucket high bit (1 - 63).	17
ADDDC Sparing	Enables or disables ADDDC Sparing.	• Enabled • **Disabled**
Patrol Scrub	Enables or disables Patrol Scrub.	• Disabled • **Enable at End of POST**
Patrol Scrub Interval	Selects the number of hours (1-24) required to complete full scrub. A value of zero means auto.	24

IIO Configuration

IIO Configuration displays and provides option to change the IIO Settings.

Table 44. IIO Configuration

Item			Description	Options or value
Intel® VMD technology			Press <Enter> to bring up the Intel® VMD for Volume Management Device Configuration menu.	N/A
	Intel VMD for Volume Management Device on Socket 0			
		VMD Config for IOU 1		
		Enable /Disable VMD	Enables or disables VMD in this Stack.	• Enable • **Disable**

Table 44. IIO Configuration (continued)

Item		Description	Options or value
	VMD port A	Enables or disables Intel® Volume Management Device Technology on specific root port.	• Enable • **Disable**
	VMD port B	Enables or disables Intel® Volume Management Device Technology on specific root port.	• Enable • **Disable**
	VMD port C	Enables or disables Intel® Volume Management Device Technology on specific root port.	• Enable • **Disable**
	VMD port D	Enables or disables Intel® Volume Management Device Technology on specific root port.	• Enable • **Disable**
	Hot Plug Capable	Enables or disables Hot Plug for PCIe Root Ports.	• Enable • **Disable**
	CfgBar size	Sets up VMD Config BAR size (in bits Min = 20, Max = 27). Example: 20 bits = 1 MB, 27 bits = 128 MB	25
	CfgBar attribute	Sets up VMD Config BAR attribute, like 64-bit or prefetchable.	• 32-bit non-prefetchable • 64-bit non-prefetchable • **64-bit prefetchable**
	MemBar1 size	Sets up VMD Memory BAR1 size (in bits Min = 20). Example: 20 bits = 1 MB, 22 bits = 4 MB, 26 bits = 64 MB	26
	MemBar1 attribute	Sets up VMD Memory BAR1 attribute, like 64-bit or prefetchable.	• **32-bit non-prefetchable** • 64-bit non-prefetchable • 64-bit prefetchable

Table 44. IIO Configuration (continued)

Item		Description	Options or value
	MemBar2 size	Sets up VMD Memory BAR1 size (in bits Min = 20). Example: 20 bits = 1 MB, 22 bits = 4 MB, 26 bits = 64 MB	21
	MemBar2 attribute	Sets up VMD Memory BAR1 attribute, like 64-bit or prefetchable	• 32-bit non-prefetchable • **64-bit non-prefetchable** • 64-bit prefetchable
	VMD for Direct Assign	Enables or disables VMD for Direct Assign.	• Enable • **Disable**

Table 45. IIO Configuration

Item	Description	Options
IIO-PCIE Express Global Options		
PCIe Train by BIOS	Assumes IIO is strapped for Wait-for-BIOS because straps are unreliable in A-0 Silicon.	• No • **Yes**
PCIe Hot Plug	Enables or disables PCIe Hot Plug globally.	• No • **Yes**

Advanced Power Management Configuration

Advanced Power Management Configuration displays and provides option to change the Power Management Settings.

Table 46. Advanced Power Management Configuration

Item	Description	Options
CPU P State Control		
EIST (Pstates)	Enables or disables EIST (P-States).	• **Enable** • Disable
EIST PSD Function	Chooses HW_ALL/SW_ALL in _PSD return.	• **HW_ALL** • SW_ALL
Boot performance mode	Selects the performance state that the BIOS will set before OS hand off.	• **Max Performance** • Max Efficient • Set by Intel Node Manager
Energy Efficient Turbo	Energy Efficient Turbo Disable, MSR 0x1FC [19].	• **Enable** • Disable
Turbo Mode	Enables or disables processor Turbo Mode (requires EMTTM enabled too).	• **Enable** • Disable

Table 46. Advanced Power Management Configuration (continued)

Item	**Description**	**Options**
CPU Flex Ratio Override	Enables or disables CPU Flex Ratio Programming.	• Enable • **Disable**
CPU Core Flex Ratio	Non-Turbo Mode Processor Core Ratio Multiplier.	23

Table 47. Advanced Power Management Configuration

Item	**Description**	**Options**
Hardware PM State Control		
Hardware P-States	Disable: Hardware chooses a P-state based on OS Request (Legacy P-States)\nNative. Mode: Hardware chooses a P-state based on OS guidance\nOut of Band. Mode: Hardware autonomously chooses a P-state (no OS guidance).	• **Native Mode** • Out of Band Mode • Native Mode with No Legacy • Disable
HardwarePM Interrupt	Enables or disables Hardware PM Interrupt.	• Enable • **Disable**
EPP Enable	When disabled, HW masks EPP in CPUID[6].10 and uses EPB for EPP	• **Enable** • Disable
APS rocketing	Enables or disables the rocketing mechanism in the HWP p-state selection pcode algorithm. Rocketing enables the core ratio to jump to max turbo instantaneously as opposed to a smooth ramp up.	• Enable • **Disable**
Scalability	Enables or disables Core Performance to Frequency Scalability Based Optimizations in the CPU.	• Enable • **Disable**
Native ASPM	Enabled - OS Controlled ASPM. Disabled - ASPM Off. AUTO - BIOS Controlled ASPM.	• **Auto** • Enable • Disable

Table 48. Advanced Power Management Configuration

Item	**Description**	**Options**
CPU C State Control		
Enable Monitor MWAIT	Allows Monitor and MWAIT instructions.	• **Auto** • Enable • Disable
CPU C1 auto demotion	Allows CPU to automatically demote to C1. Takes effect after reboot.	• **Auto** • Enable • Disable

Table 48. Advanced Power Management Configuration (continued)

Item	Description	Options
CPU C1 auto undemotion	Allows CPU to automatically undemote from C1. Takes effect after reboot.	• **Auto** • Enable • Disable
CPU C6 report	Enables or disables CPU C6(ACPI C3) report to OS.	• **Auto** • Enable • Disable
Enhanced Halt State(C1E)	Core C1E auto promotion Control. Takes effect after reboot.	• **Enable** • Disable
OS ACPI Cx	Reports CC3/CC6 to OS ACPI C2 or ACPI C3.	• **ACPI C2** • ACPI C3

Table 49. Advanced Power Management Configuration

Item	Description	Options
Package C State Control		
Package C State	Package C State limit.	• CO/C1 state • C2 state • C6 (non Retention) state • C6 (Retention) state • No Limit • **Auto**

Table 50. Advanced Power Management Configuration

Item	Description	Options
CPU Thermal Management		
PROCHOT Modes	N/A	• Disable • **Input-only**

Table 51. Advanced Power Management Configuration

Item		Description	Options
CPU - Advanced PM Tuning			
	Energy Perf BIAS		
	Power Performance Tuning	Options decides who Controls EPB. In OS mode: IA32_ ENERGY_PERF_BIAS is used. In BIOS mode: ENERGY_ PERF_BIAS_CONFIG is used. In PECI mode: PCS53 is used.	• OS Controls EPB • **BIOS Controls EPB** • PECI Controls EPB

Table 51. Advanced Power Management Configuration (continued)

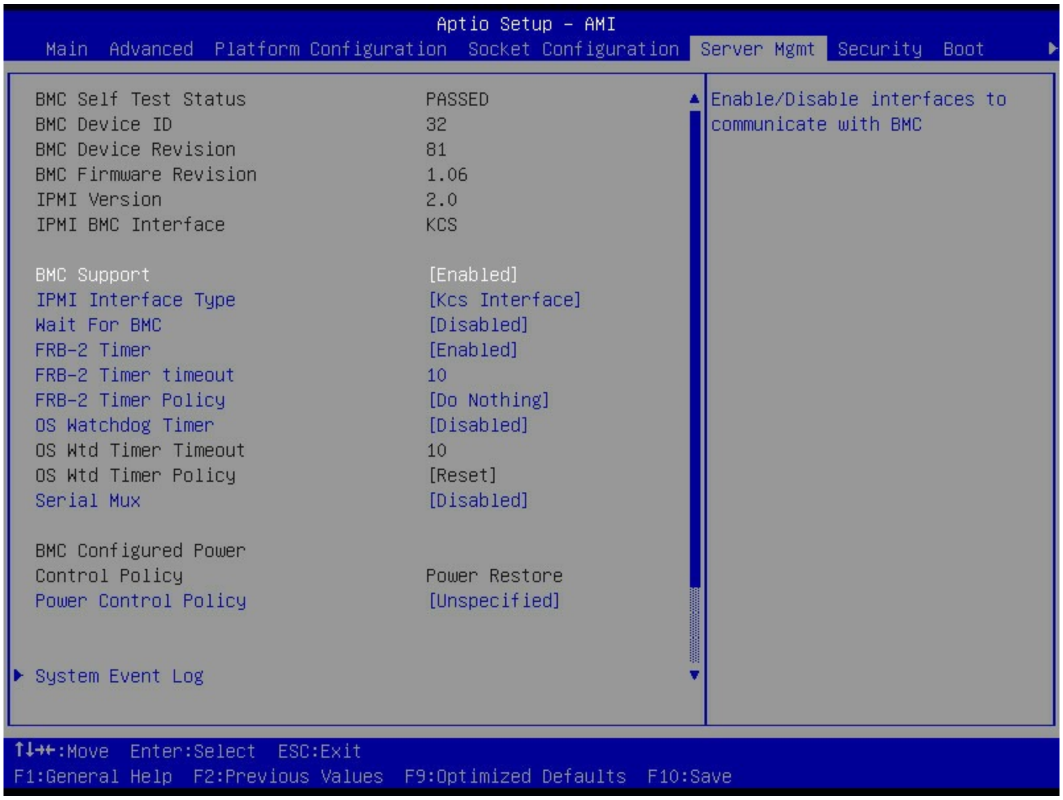
Item		**Description**	**Options**
	ENERGY_PERF_BIAS_ CFG mode	Use input from ENERGY_ PERF_BIAS_CONFIG mode selection.	• Performance • **Balanced Performance** • Balanced Power • Power

Table 52. Advanced Power Management Configuration

Item			**Description**	**Options**
Memory Power & Thermal Configuration				
	Memory Thermal		Sets memory thermal settings.	N/A
		Throttling Mode	Configures Thermal Throttling Mode.	• **CLTT** • CLTT with PECI • Disable
	MemHot INPUT		Configures Memhot input.	• **Disable** • Enable
	MemHot OUTPUT		Configures Memhot output.	• Disable • **Enable only temphi** • Enable only temphi & mid • Enable only temphi, mid and low
	Memory Power Savings Advanced Options		Advanced Settings for CKE and related Memory Power Savings Features.	N/A
		CKE Throttling	Configures CKE Throttling.	• **Auto** • Manual
		SREF Feature	Selects manual or auto programming Self Refresh feature.	• **Auto** • Manual

Chapter 6. Server Mgmt

Server Mgmt allows users to view and set up parameters of managing the server.


Aptio Setup – AMI
Main Advanced Platform Configuration Socket Configuration Server Mgmt Security Boot
↑↓→←:Move Enter:Select ESC:Exit
F1:General Help F2:Previous Values F9:Optimized Defaults F10:Save

```
BMC Self Test Status                 PASSED          Enable/Disable interfaces to
BMC Device ID                        32              communicate with BMC
BMC Device Revision                  81
BMC Firmware Revision                1.06
IPMI Version                         2.0
IPMI BMC Interface                   KCS

BMC Support                          [Enabled]
IPMI Interface Type                  [Kcs Interface]
Wait For BMC                         [Disabled]
FRB-2 Timer                          [Enabled]
FRB-2 Timer timeout                  10
FRB-2 Timer Policy                   [Do Nothing]
OS Watchdog Timer                    [Disabled]
OS Wtd Timer Timeout                 10
OS Wtd Timer Policy                  [Reset]
Serial Mux                           [Disabled]

BMC Configured Power
Control Policy                       Power Restore
Power Control Policy                 [Unspecified]


▶ System Event Log
```

Figure 7. Server Mgmt

Table 53. Server Mgmt

Item	Value
BMC Self Test Status	PASSED
BMC Device ID	32
BMC Device Revision	81
BMC Firmware Revision	[Major.Minor]
IPMI Version	2.0
IPMI BMC Interface	KCS

Table 54. Server Mgmt

Item	Description	Options or value
BMC Support	Enables or disables interfaces to communicate with BMC.	• **Enabled** • Disabled
IPMI Interface Type	Type of Interface to communicate BMC from HOST.	Kcs Interface

Table 54. Server Mgmt (continued)

Item	Description	Options or value
Wait For BMC	Waits For BMC response for specified time out. In PILOTII, BMC starts at the same time when BIOS starts during AC power ON. It takes around 30 seconds to initialize Host to BMC interfaces.	• Enabled • **Disabled**
FRB-2 Timer	Enables or disables FRB-2 timer (POST timer).	• **Enabled** • Disabled
FRB-2 Timer timeout	Enter value Between 1 to 30 min for FRB-2 Timer Expiration.	10
FRB-2 Timer Policy	Configures how the system should respond if the FRB-2 Timer expires. Not available if FRB-2 Timer is disabled.	• **Do Nothing** • Reset • Power Down • Power Cycle
OS Watchdog Timer	If enabled, starts a BIOS timer which can only be shut off by Intel Management Software after the OS loads. Helps determine that the OS successfully loaded or follows the OS Boot Watchdog Timer policy.	• Enabled • **Disabled**
OS Wtd Timer Timeout	Enter the value Between 1 to 30 min for OS Boot Watchdog Timer Expiration. Not available if OS Boot Watchdog Timer is disabled.	10
OS Wtd Timer Policy	Configures how the system should respond if the OS Boot Watchdog Timer expires. Not available if OS Boot Watchdog Timer is disabled.	• Do Nothing • **Reset** • Power Down • Power Cycle
BMC Configured Power Control Policy	Power On	
Power Control Policy	Configures how the system should respond if AC Power is lost,Reset not required as selected Power policy will be set in BMC when policy is saved.	• Do not PowerUp • Last Power State • Powe Restore • **Unspecified**

Table 55. Server Mgmt

"System Event Log" on page 45	Press <Enter> to change the SEL event log configuration.
"BMC self test log" on page 45	BMC self test log is for logs the report returned by BMC self test command.
"BMC network configuration" on page 45	BMC network configuration is for configuring BMC network parameters.
"View System Event Log" on page 47	Press <Enter> to view the System Event Log Records.
"BMC User Settings" on page 47	Press <Enter> to add, delete and set privilege level for users.

Table 56. Server Mgmt

Item	Description
BMC Warm Reset	Press Enter to do warm reset BMC.

System Event Log

Press <Enter> to change the SEL event log configuration.

Table 57. System Event Log

Item	Description or instruction	Options
Enabling/Disabling Options		
SEL Components	Change this to enable or disable event Logging for error/precess codes during boot.	• Disabled • **Enabled**
Erasing Settings		
Erase SEL	Choose options for erasing SEL.	• **No** • Yes, On next reset • Yes, On every reset
When SEL is Full	Choose options for reactions to a full SEL.	• **Do Nothing** • Erase Immediately • Delete Oldest Record
Custom EFI Logging Options		
Log EFI Status Codes	Disables the logging of EFI Status Codes or log only error code or only progress code or both.	• Disabled • Both • **Error code** • Progress code

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

BMC self test log

BMC self test log is for logs the report returned by BMC self test command.

Table 58. BMC self test log

Item	Description	Options
Log area usage = 00 out of 20 logs		
Erase Log	Erases Log Options.	• **Yes, On every reset** • No
When log is Full	Selects the action to be taken when log is full.	• **Clear Log** • Do not log any more
Log Empty		

BMC network configuration

BMC network configuration is for configuring BMC network parameters.

Table 59. BMC network configuration

Item	Description	Options or value
Lan channel 1 (Dedicated NIC)		
Configuration Address source	Selects to configure LAN channel parameters statically or dynamically (by BIOS or BMC). Unspecified option will not modify any BMC network parameters during BIOS phase.	• **Keep Current Address Source** • Static • DynamicBmcDhcp
Current Configuration Address source	N/A	DynamicAddressBmcDhcp
Station IP address	N/A	xxx.xxx.xxx.xxx
Subnet mask	N/A	xxx.xxx.xxx.xxx
Station MAC address	N/A	xx-xx-xx-xx-xx-xx
Router IP address	N/A	xxx.xxx.xxx.xxx
Router MAC address	N/A	xx-xx-xx-xx-xx-xx

Table 60. BMC network configuration

Item	Description	Options
Lan channel 1 (Dedicated NIC)		
IPV6 Support	Enables or disables LAN1 IPV6 Support.	• **Enabled** • Disabled

Table 61. BMC network configuration

Item	Description	Options
Configuration Address source	Selects to configure LAN channel parameters statically or dynamically (by BIOS or BMC). Unspecified option will not modify any BMC network parameters during BIOS phase.	• **Keep Current Address Source** • Static • DynamicBmcDhcp
Current Configuration Address source	DynamicAddressBmcDhcp	N/A

Table 62. BMC network configuration

Item
IPV6 Router IP address
IPV6 Router Prefix Length
IPV6 Router Prefix Value

Table 62. BMC network configuration (continued)

Item
****
Lan channel 1 (Dedicated NIC)

Table 63. BMC network configuration

Item	**Description**	**Options or value**
VLAN Support	Enables VLAN Support to specify the 802.1q VLAN ID.	• **Enabled** • Disabled • Unspecified
VLAN ID	VLAN ID Range is from 1-4094. VLAN ID 0 & 4095 are reserved VLAN ID's.	0
VLAN Priority	Value ranges from 0 to 7. 7 is the highest priority for VLAN.	0

View System Event Log

Press <Enter> to view the System Event Log Records.

Table 64. View System Event Log

No. of log entries in SEL: 2828			
DATE	TIME	SENSOR TYPE	Message
mm:dd:yy	HH:MM:SS	Event Logging Disabled	HEX: 01 00 02 85 A3 FF 4E 20 00 04 10 F6 6F 02 FF FF Generator ID: BMC - LUN #0 (Channle #0) Sensor Number: 0xF6 OEM (Unknown) Event Description:Log Area Reset/Cleared. Record Type-0x02. Assertion Event

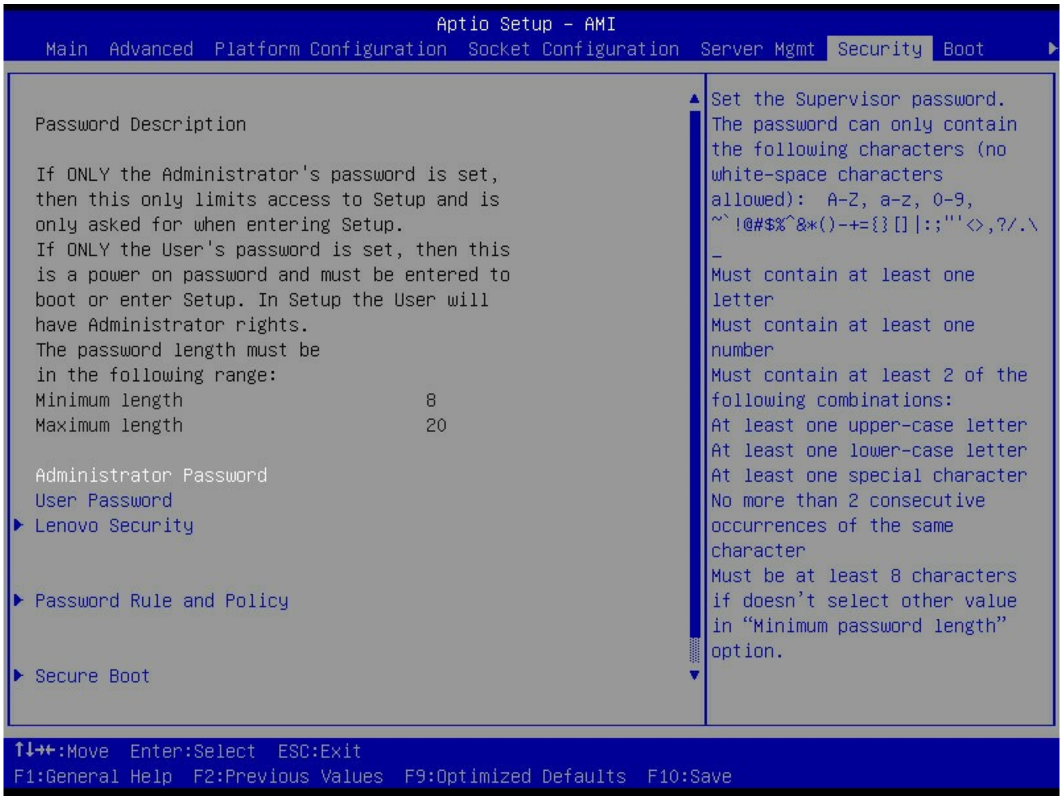
BMC User Settings

Press <Enter> to add, delete and set privilege level for users.

Item		Description or instruction	Options
Add User			
	BMC Add User Details		
	User Name	Enter BMC User Name.	N/A
	User Password	Enter BMC User Password.	N/A
	User Access	Enables or disables the BMC User's Access.	• Disable • Enable
	Channel No	Enter BMC Channel Number.	0
	User Privilege Limit	N/A	No Access
Delete User			
	BMC Delete User Details		
	User Name	Enter BMC User Name.	N/A
	User Password	Enter BMC User Password.	N/A
Change User Settings			
	BMC Change User Settings		
	User Name	Enter BMC User Name.	N/A
	User Password	Enter BMC User Password.	N/A
	Changer User Peassword	N/A	N/A
	User Access	N/A	• Enable • Disable
	Channel No	N/A	0
	User Privilege Limit	N/A	No Access

Chapter 7. Security

Security allows users to set up security parameters, including password setup, secure boot, etc.



```
Password Description

If ONLY the Administrator's password is set,
then this only limits access to Setup and is
only asked for when entering Setup.
If ONLY the User's password is set, then this
is a power on password and must be entered to
boot or enter Setup. In Setup the User will
have Administrator rights.
The password length must be
in the following range:
Minimum length                      8
Maximum length                      20

Administrator Password
User Password
▶ Lenovo Security


▶ Password Rule and Policy


▶ Secure Boot
```

```
Set the Supervisor password.
The password can only contain
the following characters (no
white-space characters
allowed):  A-Z, a-z, 0-9,
~`!@#$%^&*()-+={}[]|:;"'<>,?/.\
_
Must contain at least one
letter
Must contain at least one
number
Must contain at least 2 of the
following combinations:
At least one upper-case letter
At least one lower-case letter
At least one special character
No more than 2 consecutive
occurrences of the same
character
Must be at least 8 characters
if doesn't select other value
in "Minimum password length"
option.
```

Figure 8. Security

Password Description

If ONLY the Administrator's password is set, then this only limits access to Setup and is only asked for when entering Setup.

If ONLY the User's password is set, then this is a power on password and must be entered to boot or enter Setup. In Setup the User will have Administrator rights.

Table 65. Security

The password length must be in the following range:

Minimum length	8
Maximum length	20

Table 66. Security

Item	**Description**
Administrator Password	Set the Administrator password. The password can only contain the following characters (no white-space characters allowed): A-Z, a-z, 0-9,~`!@#$ %^&*()-+{}[]| : ; " '<>,?/._ Must contain at least one letter. Must contain at least one number. Must contain at least 2 of the following combinations: • At least one upper-case letter. • At least one lower-case letter. • At least one special character. • No more than 2 consecutive occurrences of the same character. • Must be at least 8 characters if doesn't select other value in "Minimum password length" option.
User Password	Set the User password. The password can only contain the following characters (no white-space characters allowed): A-Z, a-z, 0-9,~`!@#$ %^&*()-+{}[]| : ; " '<>,?/._ Must contain at least one letter. Must contain at least one number. Must contain at least 2 of the following combinations: • At least one upper-case letter. • At least one lower-case letter. • At least one special character. • No more than 2 consecutive occurrences of the same character. • Must be at least 8 characters if doesn't select other value in "Minimum password length" option.

Table 67. Security

"Lenovo Security" on page 50	Lenovo Security is for securing Flash Update support.
"Password Rule and Policy" on page 51	Password Rule and Policy lists the requirements of passwords and values for reference.
"Secure Boot" on page 52	See this section to view and set up Secure Boot configuration.
"Secure Flash Update" on page 55	See this section to view Secure Flash Update support.

Lenovo Security

Lenovo Security is for securing Flash Update support.

Table 68. Lenovo Security

Item	Description	Options
Security Freeze Lock	Enables or disables HDD Freeze lock.	• Enabled • **Disabled**

Password Rule and Policy

Password Rule and Policy lists the requirements of passwords and values for reference.

Table 69. Password Rule and Policy

Item	Description	Value
Minimum password length	The minimum number of characters that can be used to specify a valid password.	8
Password expiration period	The number of days a password may be used before it must be changed. If set to 0 the passwords never expire.	0
Password expiration warning period	The number of days before receiving a warning about the expiration of the password. If set to 0 the passwords never warned.	0
Minimum password change interval	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.	0
Minimum password reuse cycle	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.	0

Table 69. Password Rule and Policy (continued)

Item	Description	Value
Maximum number of login failures	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.	5
Lockout period after maximum login failures	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.	2

Secure Boot

See this section to view and set up Secure Boot configuration.

System Mode

Table 70. System Mode

Item	Description	Options
System Mode	User	
Secure Boot	N/A	• Disabled • **Enabled**
/	Not Active	N/A

Secure Boot Mode

Table 71. Secure Boot Mode

Item		**Description**	**Options**
Secure Boot Mode		Secures Boot mode options: Standard or Custom. In Custom mode Secure Boot Policy Variables can be configured by a physically present user without full authentication.	• Standard • **Custom**
	Restore Factory Keys	Force System to User Mode. Install factory default Secure Boot key databases.	N/A
	Restore to Setup Mode		

Key Management

Table 72. Key Management

Item	**Description**	**Options**
Key Management	Enables expert users to modify Secure Boot variables without full authentication.	
Vendor Keys	N/A	• **Valid** • Modified
Factory key Provision	Installs factory default Secure Boot keys when System is in Setup Mode.	• Disabled • **Enabled**
Restore Factory keys	Forces System to User Mode - install all Factory Default Secure Boot key databases.	N/A
Reset To Setup Mode	Deletes all Secure Boot key databases from NVRAM.	N/A
Export Secure Boot variables	Copies NVRAM content of Secure Boot variables to files in a root folder on a file system device.	N/A
Enroll Efi Image	Allows the image to run in Secure Boot mode. Enrolls SHA256 Hash certificate of a PE image into Authorized Signature Database (db).	N/A

<table>
<tr><th>Item</th><th>Description</th></tr>
<tr><td colspan="2">Secure Boot variable | Size | Keys | Key source</td></tr>
<tr><td>Platform Key(PK) | 300 | 1 | Facroty</td><td>Enrolls 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.</td></tr>
<tr><td>Key Exchange Keys(KEK) | 1860 | 2 | Facroty</td><td>Enrolls 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.</td></tr>
<tr><td>Authorized Signatures(db) | 5768 | 4 | Facroty</td><td>Enrolls 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.</td></tr>
<tr><td>Forbidden Signatures(dbx) | 10520 | 218 | Facroty</td><td>Enrolls 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.</td></tr>
</table>

Item	Description
Authorized TimeStamps(dbt) | 0 | 0 | No Keys	Enrolls 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.
0sRecovery Signatures(dbr) | 0 | 0 | No Keys	Enrolls 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.

Secure Flash Update

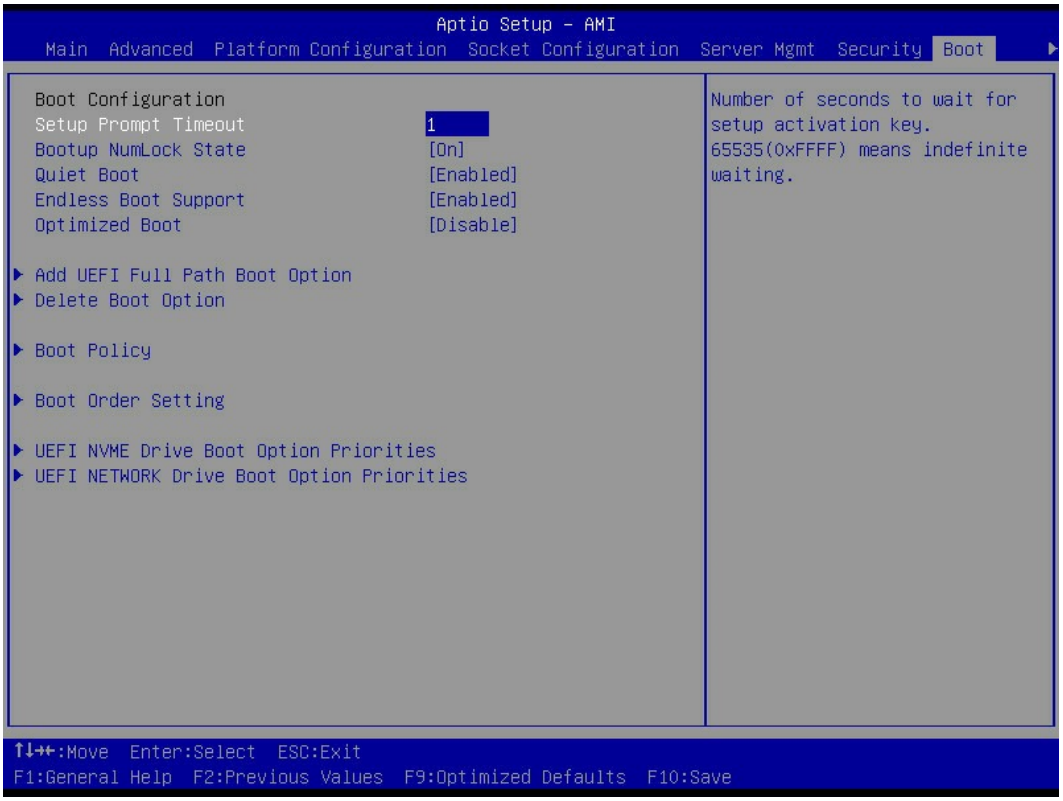
See this section to view Secure Flash Update support.

Table 73. Secure Flash Update

Item	Value
Signed BIOS Update	**Enabled**
FW Key Type	**SHA256**
FW Key Name	**OEM**
FW Update Method	**Runtime, Capsule, Recovery**
FW Rollback Protection	**Disabled**
Flash Write Protection	**Enabled**

Chapter 8. Boot

Boot lists configuration for boot, boot policy, add UEFI full path boot option. It also allows users to set boot order and specifies boot priority.



```
                          Aptio Setup - AMI
  Main  Advanced  Platform Configuration  Socket Configuration  Server Mgmt  Security  Boot

  Boot Configuration                                    Number of seconds to wait for
  Setup Prompt Timeout          1                       setup activation key.
  Bootup NumLock State          [On]                    65535(0xFFFF) means indefinite
  Quiet Boot                    [Enabled]               waiting.
  Endless Boot Support          [Enabled]
  Optimized Boot                [Disable]

▶ Add UEFI Full Path Boot Option
▶ Delete Boot Option

▶ Boot Policy

▶ Boot Order Setting

▶ UEFI NVME Drive Boot Option Priorities
▶ UEFI NETWORK Drive Boot Option Priorities

↑↓→←:Move  Enter:Select  ESC:Exit
F1:General Help  F2:Previous Values  F9:Optimized Defaults  F10:Save
```

Figure 9. Boot

Table 74. Boot Configuration

Item	Description	Options or value
Boot Configuration		
Setup Prompt Timeout	Number of seconds to wait for setup activation key. 65535(0xFFFF) means indefinite waiting.	1
Bootup NumLock State	Selects the keyboard NumLock state.	• **On** • Off
Quiet Boot	Enables or disables Quiet Boot option.	• Disabled • **Enabled**
Endless Boot Support	Enabled: Do endless boot. Disabled: each boot option boot one time.	• Disabled • **Enabled**

Table 74. Boot Configuration (continued)

Item	Description	Options or value
Boot Mode Select	Selects boot mode LEGACY/UEFI.	• Legacy • **UEFI**
Optimized Boot	N/A	• **Disabled** • Enabled

Boot Policy

Table 75. Boot Policy

Item	Description	Options or value
Boot Policy		
PXE Retry Count	Sets PXE Retry Count(0~50), Set 50 means always retry.	50
PXE Ports Retry Count	Sets PXE Ports Retry Count(0~3).	0
Boot Fail Policy	If all bootable device is retried and related controls are also applied but still fails, halt or reboot the system.	• **Halt** • Reboot

Add UEFI Full Path Boot Option

Table 76. Add UEFI Full Path Boot Option

Item		Description or instruction	Options or value
Add UEFI Full Path Boot Option			
Boot Option File Path		File path for newly created boot option.	50
Input the Description		Specifies name for the new boot option.	0
	Select Device Path Option	Select Device Path Option.	N/A
	Commit Changes and Exit	Save changes and exit.	N/A

Delete Boot Option

Table 77. Delete Boot Option

Item	Options
Delete Boot Option	• **Select one to Delete** • Build-in EFI Shell

Boot Order Setting

Table 78. Boot Order Setting

Item	Value
Option #1	[Hard Disk]
Option #2	[NVME]
Option #3	[CD/DVD]

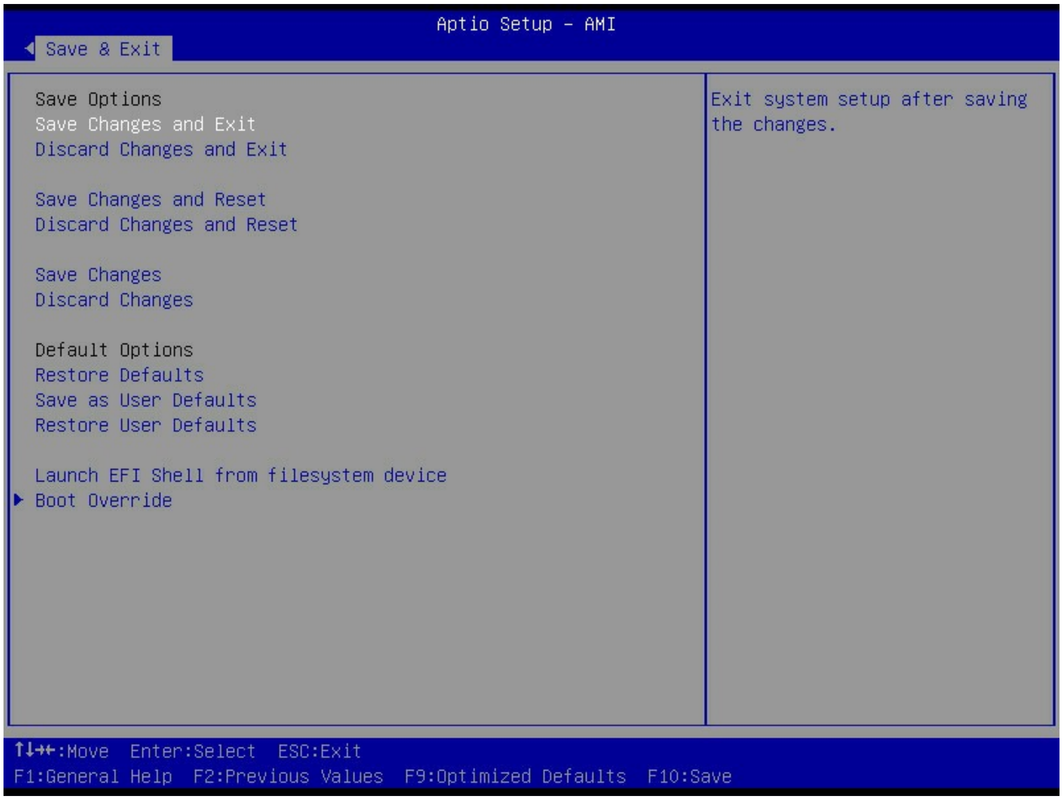
Table 78. Boot Order Setting (continued)

Item	Value
Option #4	[USB Device]
Option #5	[Network]
Option #6	[Other Device]

Item	Description
Hard Disk Drive Boot Option Priorities	Specifies the Boot Device Priority sequence from available Hard Disk Drives.
NETWORK Drive Boot Option Priorities	Specifies the Boot Device Priority sequence from available Network Drives.
CD/DVD Drive Boot Option Priorities	Specifies the Boot Device Priority sequence from available CD/DVD Drives.
USB Drive Boot Option Priorities	Specifies the Boot Device Priority sequence from available USB Drives.
Other Drive Boot Option Priorities	Specifies the Boot Device Priority sequence from Other Drives.

Chapter 9. Save & Exit

Save & Exit instructs users to handle changes made on BIOS and lists default options.



```
                              Aptio Setup - AMI
◀ Save & Exit

  Save Options                                       Exit system setup after saving
  Save Changes and Exit                              the changes.
  Discard Changes and Exit

  Save Changes and Reset
  Discard Changes and Reset

  Save Changes
  Discard Changes

  Default Options
  Restore Defaults
  Save as User Defaults
  Restore User Defaults

  Launch EFI Shell from filesystem device
▶ Boot Override

↑↓→←:Move  Enter:Select  ESC:Exit
F1:General Help  F2:Previous Values  F9:Optimized Defaults  F10:Save
```

Figure 10. Save & Exit

Save Options

Table 79. Save Options

Item	Description
Save Changes and Exit	Exits system setup after saving the changes. F10 Key can be used for this operation.
Discard Changes and Exit	Exits system setup without saving any changes. Esc key can be used for this operation.
Save Changes and Reset	Resets the system after saving the changes.
Discard Changes and Reset	Resets system setup without saving any changes.
Save Changes	Saves changes done so far to any of the setup options.
Discard Changes	Discards changes done so far to any of the setup options. F3 key can be used for this operation.

Default Options

Table 80. Default Options

Item		Description
Load UEFI Defaults		Loads UEFI Default values for all the setup options. F4 key can be used for this operation.
Save as User Defaults		Saves the changes done so far as User Defaults.
Restore User Defaults		Restores the User Defaults to all the setup options.
Launch EFI Shell from filesystem device		Attempts to Launch EFI Shell application(Shell.efi) from one of the available filesystem devices.
	Boot Override	Attempts to Launch one selected boot option from available boot option list.

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.