BIOS Setup

(For Skylake-W Platform)

User's Guide

Rev.1.1

Copyright

© 2017 GIGA-BYTE TECHNOLOGY CO., LTD. All rights reserved. The trademarks mentioned in this manual are legally registered to their respective owners.

Disclaimer

Information in this manual is protected by copyright laws and is the property of GIGABYTE. Changes to the specifications and features in this manual may be made by GIGABYTE without prior notice. No part of this manual may be reproduced, copied, translated, transmitted, or published in any form or by any means without GIGABYTE's prior written permission.

Documentation Classifications

In order to assist in the use of this product, GIGABYTE provides the following types of documentations:

For detailed product information, carefully read the User's Manual.

For more information, visit our website at:

http://b2b.gigabyte.com

You are a professional?

Get an access to our complete source of sales, marketing & technical materials at:

http://reseller.b2b.gigabyte.com

f

Table of Contents

Chapter 1	BIOS S	Setup	5
	1-1 T	The Main Menu	7
	1-2 A	Advanced Menu	9
	1-2-1	1 Intel RC Configuration	10
	1-	-2-1-1 Memory Topology	12
	1-	-2-1-2 Intel® VMD technology	13
	1-2-2	2 Trusted Computing	14
	1-2-3	3 SATA and RST Configuration	15
	1-2-4	4 Super IO Configuration	16
	1-	-2-4-1 Serial Port 1/2 Configuration	17
	1-2-5	5 Hardware Monitor	18
	1-2-6	3 S5 RTC Wake Settings	20
	1-2-7	7 CSM Configuration	21
	1-2-8	3 NVMe Configuration	22
	1-2-9	9 OffBoard SATA Controller	23
	1-2-1	10 Intel(R) I210 Gigabit Network Connection	24
	1-	-2-10-1 NIC Configuration	26
	1-3 C	Chipset Setup Menu	27
	1-4 S	Security Menu	
	1-4-1	1 Secure Boot	29
	1-	-4-1-1 Key Management	31
	1-5 B	Boot Menu	
	1-6 S	Save & Exit Menu	
	1-7 B	BIOS POST Beep code (AMI standard)	
	1-7-1	1 PEI Beep Codes	35
	1-7-2	2 DXE Beep Codes	
	1-8 E	BIOS Recovery Instruction	

Chapter 1 BIOS Setup

BIOS (Basic Input and Output System) records hardware parameters of the system in the EFI on the motherboard. Its major functions include conducting the Power-On Self-Test (POST) during system startup, saving system parameters and loading operating system, etc. BIOS includes a BIOS Setup program that allows the user to modify basic system configuration settings or to activate certain system features. When the power is turned off, the battery on the motherboard supplies the necessary power to the CMOS to keep the configuration values in the CMOS.

To access the BIOS Setup program, press the <F2> key during the POST when the power is turned on.



- BIOS flashing is potentially risky, if you do not encounter problems of using the current BIOS version, it is recommended that you don't flash the BIOS. To flash the BIOS, do it with caution. Inadequate BIOS flashing may result in system malfunction.
- It is recommended that you not alter the default settings (unless you need to) to prevent system
 instability or other unexpected results. Inadequately altering the settings may result in system's
 failure to boot. If this occurs, try to clear the CMOS values and reset the board to default values.
 (Refer to the Exit section in this chapter or introductions of the battery/clearing CMOS jumper in
 Chapter 1 for how to clear the CMOS values.)

BIOS Setup	Program	Function	Keys
------------	---------	----------	------

	-	
	<←><→>	Move the selection bar to select the screen
	<↑><↓>	Move the selection bar to select an item
	<+>	Increase the numeric value or make changes
	<->	Decrease the numeric value or make changes
	<enter></enter>	Execute command or enter the submenu
	<esc></esc>	Main Menu: Exit the BIOS Setup program
		Submenus: Exit current submenu
	<f1></f1>	Show descriptions of general help
	<f3></f3>	Restore the previous BIOS settings for the current submenus
	<f9></f9>	Load the Optimized BIOS default settings for the current submenus
	<f10></f10>	Save all the changes and exit the BIOS Setup program
-		

Main

This setup page includes all the items in standard compatible BIOS.

Advanced

This setup page includes all the items of AMI BIOS special enhanced features.

(ex: Auto detect fan and temperature status, automatically configure hard disk parameters.)

Chipset

This setup page includes all the submenu options for configuring the function of processor, network, North Bridge, South Bridge, and System event logs.

Security

Change, set, or disable supervisor and user password. Configuration supervisor password allows you to restrict access to the system and BIOS Setup.

A supervisor password allows you to make changes in BIOS Setup.

A user password only allows you to view the BIOS settings but not to make changes.

Boot

This setup page provides items for configuration of boot sequence.

Save & Exit

Save all the changes made in the BIOS Setup program to the CMOS and exit BIOS Setup. (Pressing <F10> can also carry out this task.)

Abandon all changes and the previous settings remain in effect. Pressing <Y> to the confirmation message will exit BIOS Setup. (Pressing <Esc> can also carry out this task.)

1-1 The Main Menu

Once you enter the BIOS Setup program, the Main Menu (as shown below) appears on the screen. Use arrow keys to move among the items and press <Enter> to accept or enter other sub-menu.

Main Menu Help

The on-screen description of a highlighted setup option is displayed on the bottom line of the Main Menu.

Submenu Help

While in a submenu, press <F1> to display a help screen (General Help) of function keys available for the menu. Press <Esc> to exit the help screen. Help for each item is in the Item Help block on the right side of the submenu.



When the system is not stable as usual, select the Restore Defaults item to set your system to its defaults.

The BIOS Setup menus described in this chapter are for reference only and may differ by BIOS version.

Aptio Setup Utility Main Advanced Chipset Securit	∣ <mark>– Copyright (C) 2017 America</mark> y Boot Save & Exit	n Megatrends, Inc.
BIOS Information Project Name BIOS Version Build Date and Time	MW51-HP0-00 F2 08/15/2017 10:10:50	Set the Date. Use Tab to switch between Date elements.
Onboard LAN Information LANI MAC Address LANZ MAC Address ME FW Version System Date System Time	E0-D5-5E-14-E1-E5 E0-D5-5E-14-E1-E6 11.10.0.1300 (Tue 05/19/2017) [17:02:52]	++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Frevious Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2 19 1266	Convergent (C) 2017 American	Megatrends. Inc.

- ☞ BIOS Information
- Project Name

Displays the project name information.

☞ BIOS Version

Displays version number of the BIOS setup utility.

☞ Build Date and Time

Displays the date and time when the BIOS setup utility was created.

- ∽ Onboard LAN Information
- LAN2 MAC Address^(Note)
 Displays LAN2 MAC address information.

∽ ME FW Version^(Note)

Displays ME firmware version information.

∽ System Date

Sets the date following the weekday-month-day-year format.

∽ System Time

Sets the system time following the hour-minute-second format.

⁽Note) Functions available on selected models.

1-2 Advanced Menu

The Advanced menu display submenu options for configuring the function of various hardware components. Select a submenu item, then press [Enter] to access the related submenu screen.



1-2-1 Intel RC Configuration

Aptio Setup Utility - Advanced	Copyright (C) 2017 Americar	n Megatrends, Inc.
Processor Configuration		Enable/Disable Intel® Virtualization Technology for
Processor BSP Revision	50654 - SKX U0	Directed I/O (VT-d) by
Processor ID	00050654*	reporting the I/O device
Processor Frequency	4.000GHz	assignment to VMM through DMAR
Processor Max Ratio	28H	ACPI Tables.
Processor Min Ratio	OCH	
Microcode Revision	02000022	
L1 Cache RAM	64KB	
L2 Cache RAM	1024KB	
L3 Cache RAM	8448KB	
Processor 0 Version	Intel(R) Xeon(R) W-2125 CPU @ 4.00GHz	
		++: Select Screen
		↑↓: Select Item
SpeedStep (Pstates)	[Enable]	Enter: Select
Hyper-Threading [ALL]	[Enable]	+/-: Change Opt.
Turbo Mode	[Enable]	F1: General Help
CPU C6 report	[Auto]	F2: Previous Values F3: Optimized Defaults
Memory Topology		F4: Save & Exit
Intel® VMD technology		ESC: Exit

∽ Processor Configuration

Displays the processor configurations.

∽ Intel® VT for Directed I/O (VT-d)

Select whether to enable the Intel Virtualization Technology function. VT allows a single platform to run multiple operating systems in independent partitions.

Options available: Enable/Disable. Default setting is **Enable**.

∽ SpeedStep (Pstates)

Conventional Intel SpeedStep Technology switches both voltage and frequency in tandem between high and low levels in response to processor load.

Options available: Enable/Disable. Default setting is **Enable**.

∽ Hyper-Threading [ALL]

The Hyper Threading Technology allows a single processor to execute two or more separate threads concurrently. When hyper-threading is enabled, multi-threaded software applications can execute their threads, thereby improving performance.

Options available: Enable/Disable. Default setting is **Enable**.

🗢 Turbo Mode

When this item is enabled, the processor will automatically ramp up the clock speed of 1-2 of its processing cores to improve its performance.

When this item is disabled, the processor will not overclock any of its core.

Options available: Enable/Disable. Default setting is Enable.

CPU C6 report

Allows you to determine whether to let the CPU enter C6 mode in system halt state. When enabled, the CPU core frequency and voltage will be reduced during system halt state to decrease power consumption. The C6 state is a more enhanced power-saving state than C1.

Options available: Enable/Disable/Auto. Default setting is Auto.

∽ Memory Topology

Press [Enter] for configuration of advanced items.

∽ Intel® VMD technology

Press [Enter] for configuration of advanced items.

1-2-1-1 Memory Topology



1-2-1-2 Intel® VMD technology



Aptio Setup Utility - Advanced	- Copyright (C) 2017 American	Megatrends, Inc.
VMD Config for PStack0		Enable/Disable Intel® Volume
Intel® VMD for Volume Management Device for PStack0 VMD Config for PStack1	[Disable]	in this Stack.
Intel® VMD for Volume Management Device for PStack1	(Disable)	++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
10000 0 10 1000	Conunight (C) 2017 Amonicon M	

∽ Intel® VMD technology

\backsim Intel® VMD for volume Management Device on Socket 0

Press [Enter] to enable/disable the Intel VMD support function.

☞ VMD Config for PStack0/PStack1

\backsim Intel® VMD for volume Management Device for PStack0/PStack1

Enable/Disable the Intel VMD technology in this stack. Options available: Enable/Disable. Default setting is **Disable**.

1-2-2 Trusted Computing

Aptio Setup Util: Advanced	ity – Copyright (C) 2017	American Megatrends, Inc.
TPM Device	[dTPM]	Selects TPM : dTPM will be disabled and all data saved on it will be lost.
Security Device Support ND Security Device Found	[Enable]	
		++: Select Screen T4: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit

→ TPM Device

Selects the TPM. Once selected, the dTPM will be disabled and all data saved on it will be lost. Default setting is **dTPM**.

∽ Configuration

∽ Security Device Support

Enable/Disable BIOS support for security device. When enabled, OS will not show Security Device. TCG EFI protocol and INT-1A interface will not be available.

Options available: Enable/Disable. Default setting is Enable.

1-2-3 SATA and RST Configuration

Aptio Setup Chipset	Utility – Copyright (C) 2017 A	merican Megatrends, Inc.
SATA And RST Configuration		Enable/Disable SATA Device.
SATA Controller(s) SATA Mode Selection	[Enabled] [AHCI]	
Serial ATA Port 0 Serial ATA Port 1 Serial ATA Port 2 Serial ATA Port 3 Serial ATA Port 4 Serial ATA Port 5 Serial ATA Port 6	Empty Empty Empty Empty Empty Empty Empty	
Serial ATA Port 7	Empty	++: Select Screen fl: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit

∽ SATA And RST Configuration

∽ SATA Controller(s)

Enable/Disable SATA controller.

Options available: Enabled/Disabled. Default setting is Enabled.

\curvearrowleft SATA Mode Selection

Determines how SATA controller(s) operate. Options available: AHCI/Intel RST Premium. Default setting is AHCI.

∽ Serial ATA Port 0/1/2/3/4/5/6/7

The category identifies SATA hard drives that are installed in the computer. System will automatically detect HDD type.

1-2-4 Super IO Configuration



∽ Super IO Configuration

Serial Port 1/2 Configuration
 Press [Enter] for configuration of advanced items.

1-2-4-1 Serial Port 1/2 Configuration



∽ Serial Port 1/2 Configuration

When enabled allows you to configure the serial port settings. When set to disabled, displays no configuration for the serial port.

Options available: Enabled/Disabled. Default setting is Enabled.

∽ Device Settings

Displays the specified Serial Port base I/O address and and IRQ.

1-2-5 Hardware Monitor

Press [Enter] to view the Hardware Monitor screen which displays a real-time record of the CPU/system temperature, and fan speed. Items on this window are non-configurable



→ PC Health Status

∽ CPU FAN Fail Warning

Enable/Disable a warning message when the CPU fan failure or disconnected. Options available: Enabled/Disabled. Default setting is **Enabled**.

System FAN 1/2/3/4/5 Fail Warning

Enable/Disable a warning message when the system fan failure or disconnected. Options available: Enabled/Disabled. Default setting is **Disabled**.

∽ CPU FAN Type

Selects the CPU fan type.

Options available: 3 Pins/4 Pins/Auto. Default setting is ${\ensuremath{\textbf{Auto}}}$.

System FAN 1/2/3/4/5 Type

Selects the system fan type. Options available: 3 Pins/4 Pins/Auto. Default setting is Auto.

∽ Chassis Opened Warning

Enable/Disable a warning message when the system chassis is opened. Options available: Enabled/Disabled/Clear. Default setting is **Disabled**.

∽ THRM EXT For FAN 4/5

Selects the THRM EXT function. This option is disabled by default. For Fan 4, selects TH1 for THRM1 EXT. For Fan 5, selects TH2 for THRM2 EXT. Options available: Disabled/THRM1/THRM2. Default setting is **Disabled**.

∽ CPU Temperature

Displays the current CPU fan temperature.

∽ System Temperature

Displays the current system fan temperature.

∽ CPU Fan Speed

Displays the current CPU fan speed (RPM).

∽ System Fan 1/2/3/4/5 Speed

Displays the current system fan speed (RPM).

1-2-6 S5 RTC Wake Settings

Aptio	Setup Utility – Copyright (C)	2017 American Megatrends, Inc.
Wake system from SS	(Disabled)	Enable or disable System wake on alarm event. Select FixedTime, system will wake on the hr::min::sec specified. ++: Select Screen 11: Select Item Enter: Select +/-: Charge Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Vers	ion 2,19,1266, Copyright (C) 2	017 American Megatrends, Inc.

∽ Wake system from S5

Enable/Disable System wake on alarm event. When enabled, System will wake on the hr:min:sec specified.

Options available: Disabled/Fixed Time. Default setting is **Disabled**.

1-2-7 CSM Configuration

Aptio Setup Utility Advanced	y – Copyright (C) 2017 Americ	can Megatrends, Inc.
CSM Support		Enable/Disable CSM Support.
LAN EFI driver	[Disabled]	
Storage	(UEFI)	
		→+: Select Screen
		t↓: Select Item Enter: Select
		+/-: Change Upt. F1: General Help
		F3: Optimized Defaults
		ESC: Exit

∽ CSM Support

Enable/Disable the Compatibility Support Module (CSM) support function Options available: Enabled/Disabled. Default setting is **Disabled**.

- Advanced items prompt and configurable when this item is set to Enabled.
- If the **CSM Support** is set to **Disabled**, the following five items will not be able to support Legacy mode.

∽ LAN EFI driver

Enable/Disable LAN EFI driver.

Options available: Enabled/Disabled. Default setting is **Disabled**.

Please note that this item is visible when CSM Support is set to Disabled.

∽ Storage

Controls the execution of UEFI and Legacy Storage Option ROM. Options available: Do not launch/UEFI/Legacy setting is **Disabled**. **Please note that this item is visible when CSM Support is set to Disabled**.

1-2-8 NVMe Configuration



∽ NVMe Configuration

Displays the NVMe devices connected to the system.

1-2-9 OffBoard SATA Controller



1-2-10 Intel(R) I210 Gigabit Network Connection



Aptio Setup Utility - Advanced	Copyright (C) 2017 American	Megatrends, Inc.
▶ NIC Configuration		Click to configure the network
Blink LEDs	0	device port.
UEFI Driver	Intel(R) PRO/1000	
Adapter PBA	130916-002	
Device Name	Intel(R) I210 Gigabit Network Connection	
Chip Type	Intel i210	
PCI Device ID	1533	
PCI Address	02:00:00	
Link Status	[Disconnected]	→+: Select Screen ↑↓: Select Item
MAC Address	E0:D5:5E:14:E1:E6	Enter: Select
		+/-: Change Opt.
		F1: General Help
		F2: Previous Values
		F3: Optimized Defaults
		F4: Save & Exit
		ESC: Exit
Vancian 0 40 4066 0	opunight (C) 2017 Amonicon M	orotoondo Too

∽ NIC Configuration

Press [Enter] for configuration of advanced items of the selected network device port.

Ilink LEDs

Identifies the physical network port by blinking the associated LED. Press the numeric keys to adjust desired values.

→ UEFI Driver

Displays the technical specifications for the Network Interface Controller.

Adapter PBA

Displays the technical specifications for the Network Interface Controller

∽ Device Name

Displays the technical specifications for the Network Interface Controller.

∽ Chip Type

Displays the technical specifications for the Network Interface Controller.

∽ PCI Device ID

Displays the technical specifications for the Network Interface Controller.

☞ PCI Address

Displays the technical specifications for the Network Interface Controller.

∽ Link Status

Displays the technical specifications for the Network Interface Controller

∽ MAC Address

Displays the technical specifications for the Network Interface Controller..

1-2-10-1 NIC Configuration

Aptio Se Advanced	etup Utility – Copyright (C) 2017 America	an Megatrends, Inc.
Link Speed Wake On LAN	[Auto Negotiated] [N/A]	
		++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit

그 Link Speed

Allows for automatic link speed adjustment. Default setting is Auto Negotiated.

・ Wake On LAN

Enable/Disable the Wake On LAN feature. Note that configuring Wake on LAN in the operating system does not change the value of this setting, but does override the behavior of Wake on LAN in OS controlled power states.

Options available: Enabled/Disabled/N/A. Default setting is N/A.

1-3 Chipset Setup Menu

Chipset Setup menu displays submenu options for configuring the function of the North Bridge. Select a submenu item, then press [Enter] to access the related submenu screen.

Aptio Setup Utility Main Advanced Chipset Security	 Copyright (C) 2017 American Boot Save & Exit 	Megatrends, Inc.
OnBoard Audio		Control Detection of the
AC Power loss	[Always Off]	HD-Audio device. Disabled = HDA will be
BIOS Lock	[Disabled]	unconditionally disabled Enabled = HDA will be
Onboard LAN1	[Enabled]	unconditionally enabled.
Onboard LAN2	[Enabled]	
		the Salast Sanaan
		14: Select Item
		Enter: Select
		+/-: Change Opt.
		F1: General Help
		F3: Optimized Defaults
		F4: Save & Exit
		ESC: Exit
Vancian 2 19 1266	Conunight (C) 2017 American M	eratrando Inc

OnBoard Audio

Enable/Disable the onboard audio controller. When enabled, HD audio will be unconditionally enabled. When disabled, HD audio will be unconditionally disabled

Options available: Enabled/Disabled. Default setting is **Enabled**.

→ AC Power Loss

Specifies what state to go to when the power is re-applied after a power failure. Options available: Always On/Always Off/Last State. Default setting is **Always Off**.

☞ BIOS Lock

Enable/Disable the PCH BIOS Lock Enable feature. Options available: Enabled/Disabled. Default setting is **Disabled**.

∽ Onboard LAN 1/2

Enable/Disable the onboard LAN 1/2 controller. Options available: Enabled/Disabled. Default setting is **Enabled**.

1-4 Security Menu

The Security menu allows you to safeguard and protect the system from unauthorized use by setting up access passwords.

Aptio Setup Main Advanced Chipset	Utility – Copyright (C) 201 Security Boot Save & Exit	7 American Megatrends, Inc.
Password Description		Set Administrator Password
If ONLY the Administrator' then this only limits acce only asked for when enter If ONLY the User's password boot or enter Setup. In Se have Administrator rights. The password length must b in the following range: Minimum length	s password is set, ss to Setup and is ng Setup. d is set, then this must be entered to tup the User will e 3	
Maximum length Administrator Password	20	<pre>++: Select Screen f↓: Select Item</pre>
user Passoord ▶ Secure Boot		HTTER: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2.1	9 1266 Conucient (C) 2017	American Megatrends Inc

There are two types of passwords that you can set:

Administrator Password

Entering this password will allow the user to access and change all settings in the Setup Utility.

User Password

Entering this password will restrict a user's access to the Setup menus. To enable or disable this field, a Administrator Password must first be set. A user can only access and modify the System Time, System Date, and Set User Password fields.

∽ Administrator Password

Press [Enter] to configure the administrator password.

∽ User Password

Press [Enter] to configure the user password.

∽ Secure Boot

Press [Enter] for configuration of advanced items.

1-4-1 Secure Boot



∽ System Mode

Displays the system is in User mode or Setup mode.

☞ Vendor Keys

Displays the Vendor Keys function is actived or not actived.

∽ Secure Boot Enable

Secure Boot activated when Platform Key (PK) is enrolled, System mode is User/Deployed, and CSM function is disabled.

When this option is set to **Enabled**, an "Platform in Setup Mode!" message will prompt to request reenroll Platform Key (PK).

Options available: Enabled/Disabled. Default setting is Disabled.

∽ Secure Boot Mode^(Note)

Secure Boot requires all the applications that are running during the booting process to be pre-signed with valid digital certificates. This way, the system knows all the files being loaded before Windows loads and gets to the login screen have not been tampered with.

When set to Standard, it will automatically load the Secure Boot keys form the BIOS databases.

When set to Custom, you can customize the Secure Boot settings and manually load its keys from the BIOS database.

Options available: Standard/Custom. Default setting is Custom.

Reset to Setup Mode

Press [Enter] to reset the system mode to Setup mode.

Please note that this item is configurable when System Mode is set to User Mode.

☞ Restore Factory Keys

Press [Enter] to restore all secure boot database to factory default keys. Please note that this item is configurable when Secure Boot Mode is set to Custom.

∽ Key Management

Press [Enter] for configuration of advanced items.

Please note that this item is configurable when Secure Boot Mode is set to Custom.

1-4-1-1 Key Management

Aptio S	etup Utility – Copyr Security	ight (C) 2017 American	Megatrends, Inc.
Provision Factory Def Reset To Setup Mode Restore Factory Keys Export Secure Boot va Enroll Efi Image Device Guard Ready Remove 'UEFI CA' from Restore DB defaults	aults (Dis riables DB	ab 1ed)	Provision factory default keys on next system re-boot while platform is in Setup Mode
Secure Boot variable > Platform Key(PK) > Key Exchange Keys > Authorized Signatures > Forbidden Signatures > Authorized TimeStamps > OsRecovery Signatures	Size Keys Keys So 0 0 No Key 0 0 No Key	urce S S S S S	<pre>++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>

∽ Provision Factory Defaults

Allows to provision factory default Secure Boot keys when system is in Setup Mode. Options available: Enabled/Disabled. Default setting is **Disabled**.

∽ Reset To Setup mode

Press [Enter] to reset the system to Setup mode.

Please note that this item is configurable when System Mode is in User Mode.

∽ Restore Factory Keys

Press [Enter] to restore all Secure Boot Keys and key variables to factory defaults.

Export Secure Boot variables

Press [Enter] to export all Secure Boot Keys and key variables.

∽ Enroll Efi Image

Press [Enter] to enroll SHA256 hash of the binary into Authorized Signature Database (DB).

→ Device Guard Ready

∽ Remove 'UEFI CA' from DB

Press [Enter] to remove Microsoft UEFI CA from Secure Boot DB.

Please note that this item is configurable when the system is not in Device Guard Ready state.

→ Restore DB defaults

Press [Enter] to restore all DB variables to factory defaults.

∽ Secure Boot variable

Displays the current status of the variables used for secure boot.

∽ Platform Key (PK)

Displays the current status of the Platform Key (PK). Press [Enter] to enroll the PK. Options available: Update.

∽ Key Exchange Keys (KEK)

Displays the current status of the Key Exchange Key Database (KEK). Press [Enter] to enroll a new KEK or load additional KEK from storage devices. Options available: Update/Append.

∽ Authorized Signatures (DB)

Displays the current status of the Authorized Signature Database. Press [Enter] to enroll a new DB or load additional DB from storage devices. Options available: Update/Append.

∽ Forbidden Signatures (DBX)

Displays the current status of the Forbidden Signature Database. Press [Enter] to enroll a new dbx or load additional dbx from storage devices. Options available: Update/Append.

∽ Authorized TimeStamps (DBT)

Displays the current status of the Authorized TimeStamps Database. Press [Enter] to enroll a new DBT or load additional DBT from storage devices. Options available: Update/Append.

∽ OsRecovery Signatures

Displays the current status of the OsRecovery Signature Database.

Press [Enter] to enroll a new OsRecovery Signature or load additional OsRecovery Signature from storage devices.

Options available: Update/Append.

1-5 Boot Menu

The Boot menu allows you to set the drive priority during system boot-up. BIOS setup will display an error message if the legacy drive(s) specified is not bootable.

Aptio Setup Main Advanced Chipset	Utility – Copyright (C) 2017 American Security Boot Save & Exit	Megatrends, Inc.
Main Advanced Chipset Full Screen LOGO Show Boot Option Priorities Boot Option #1	Security Boot Save & Exit [Enabled] [UEFI: Built-in EFI Shell]	Allows you to determine whether to display the Logo at system startup. Disabled skips the Logo when the system starts up. +*: Select Screen T4: Select Item Enter: Select
		47-: Unange Upt. Fl: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit

☞ Full Screen LOGO Show

Enable/Disable whether the Logo displays on the full screen when the system starts up. Options available: Enabled/Disabled. Default setting is **Enabled**.

∽ Boot Option Priorities

∽ Boot Option #1

Press [Enter] to configure the boot priority. It allows you to specify the boot device priority from the available UEFI applications during system boot-up.

Options available: UEFI: Built-in EFI Shell/Disabled. Default setting is UEFI: Built-in EFI Shell.

1-6 Save & Exit Menu

The Exit menu displays the various options to quit from the BIOS setup. Highlight any of the exit options then press **Enter**.

Aptio Setup Utility – Copyright (C) 2017 American Main Advanced Chipset Security Boot <mark>Save & Exit</mark>	Megatrends, Inc.
Save Options Save Changes and Reset Discard Changes and Reset	Reset the system after saving the changes.
Restore Defaults	
Boot Override UEFI: Built-in EFI Shell	++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Prevlous Values F3: Optimized Defaults F4: Save & Exit ES: Exit
Vencion 2 19 1266 Copunisht (C) 2017 American M	erstpende Inc

∽ Save Options

∽ Save Changes and Reset

Restarts the system after saving the changes made. Options available: Yes/No.

Discard Changes and Reset

Restarts the system without saving any changes.

Options available: Yes/No.

→ Restore Defaults

Loads the default settings for all BIOS setup parameters. Setup Defaults are quite demanding in terms of resources consumption. If you are using low-speed memory chips or other kinds of low-performance components and you choose to load these settings, the system might not function properly. Options available: Yes/No.

∽ Boot Override

Press [Enter] to configure the device as the boot-up drive.

1-7 BIOS POST Beep code (AMI standard)

1-7-1 PEI Beep Codes

# of Beeps	Description
1	Memory not Installed.
1	Memory was installed twice (InstallPeiMemory routine in PEI Core called
	twice)
2	Recovery started
3	DXEIPL was not found
3	DXE Core Firmware Volume was not found
4	Recovery failed
4	S3 Resume failed
7	Reset PPI is not available

1-7-2 DXE Beep Codes

# of Beeps	Description
1	Invalid password
4	Some of the Architectural Protocols are not available
5	No Console Output Devices are found
5	No Console Input Devices are found
6	Flash update is failed
7	Reset protocol is not available
8	Platform PCI resource requirements cannot be met

1-8 BIOS Recovery Instruction

The system has an embedded recovery technique. In the event that the BIOS becomes corrupt the boot block can be used to restore the BIOS to a working state. To restore your BIOS, please follow the instructions listed below:

Recovery Instruction:

- 1. Change xxx.ROM to 1AUCR009.rom.
- 2. Copy 1AUCR009.rom and AFUDOS.exe to USB diskette.
- 3. Setting BIOS Recovery jump to enabled status.
- 4. Boot into BIOS recovery.
- 5. Run Proceed with flash update.
- 6. BIOS update.

Main Advanced Chipset	Bios Setup Utility Security Server Mgmt Event Logs	Boot Save & Exit Recovery
ROM Image update allowed ROM Image Verification pa	ssed	Select this to start flash update
Flash Update Parameters Reset NVRAM Main Block Update • Proceed with flash update	[Enabled] [Enabled]	
		++: Select Screen T4: Select Item Enter: Select +/-: Change Opt. F1: General Help F3: Previous Values F9: Ortimized Oreaults F10: Save & Exit ESC: Exit