User's Manual **PERFECTRON**

SCH-3X1

IEC-61850-3, IEEE-1613 Substation Fanless System



www.perfectron.com



Safety Information

Electrical safety

- To prevent electrical shock hazard, disconnect the power cable from the electrical outlet before relocating the system.
- When adding or removing devices to or from the system, ensure that the power cables for the devices are unplugged before the signal cables are connected. If possible, disconnect all power cables from the existing system before you add a device.
- Before connecting or removing signal cables from the motherboard, ensure that all power cables are unplugged.
- Seek professional assistance before using an adapter or extension cord. These devices could interrupt the grounding circuit.
- Make sure that your power supply is set to the correct voltage in your area.
- If you are not sure about the voltage of the electrical outlet you are using, contact your local power company.
- If the power supply is broken, do not try to fix it by yourself. Contact a qualified service technician or your local distributor.

Operation safety

- Before installing the motherboard and adding devices on it, carefully read all the manuals that came with the package.
- Before using the product, make sure all cables are correctly connected and the power cables are not damaged. If you detect any damage, contact your dealer immediately.
- To avoid short circuits, keep paper clips, screws, and staples away from connectors, slots, sockets and circuitry.
- Avoid dust, humidity, and temperature extremes. Do not place the product in any area where it may become wet.
- Place the product on a stable surface.
- If you encounter any technical problems with the product, contact your local distributor

Statement

- All rights reserved. No part of this publication may be reproduced in any form or by any means, without prior written permission from the publisher.
- All trademarks are the properties of the respective owners.
- All product specifications are subject to change without prior notice



Revision History

Revision	Date (yyyy/mm/dd)	Changes
V1.0	2022/01/20	First release
V1.1	2024/04/10	Modify Power connector pin define

Packing list

ltem	Description	Q'ty
1	SCH-3X1 Embedded System	1
2	SSD Tray Key	1
3	Driver CD	1
4	Rackmount Bracket + Screw	1 set

Ordering information

Model	Description
SCH-3X1	IEC-61850-3, IEEE-1613 Substation Fanless Computer with Intel® Core™ i7-9700TE, 2 x 2.5" Easy swap SSD Tray, 2 x PCIe expansion slot, 2 x RJ45 LAN , 6 x USB 3.0 , 2 x USB 2.0 , 1 x PS/2, 1 x DP , 1x DVI,1 x HDMI , 2 x COM(RS232/422/485), 1 x Mic-in / 1 x Line-out, 9~48V DC-IN, Extend Temp -20 to 60°C



RoHS Compliance



Perfectron RoHS Environmental Policy and Status Update

Perfectron is a global citizen for building the digital infrastructure. We are committed to providing green products and services, which are compliant with

European Union RoHS (Restriction on Use of Hazardous Substance in Electronic Equipment) directive **2011/65/EU**, to be your trusted green partner and to protect our environment.

In order to meet the RoHS compliant directives, Perfectron has established an engineering and manufacturing task force to implement the introduction of green products. The task force will ensure that we follow the standard Perfectron development procedure and that all the new RoHS components and new manufacturing processes maintain the highest industry quality levels for which Perfectron are renowned.

The model selection criteria will be based on market demand. Vendors and suppliers will ensure that all designed components will be RoHS compliant.



Safety Information	1
Electrical safety	
Operation safety	
Statement	
Revision History	2
Packing list	2
Chapter 1 : Production Introduction	5
1.1 Specifications	
1.2 Front Panel I/O Placement	7
1.3 Rear Panel I/O Placement	7
1.4 Mechanical Dimensions	8
Chapter 2 : Connectors Pin Define	9
2.1 External Connector Pin Definition	9
Chapter 3: AMI BIOS UTILITY	11
3.1 Starting	
3.2 Navigation Keys	
3.3 Main Setup	
3.4 Advanced Page	
3.4.1 Onboard Device	
3.4.2 CPU Configuration	
3.4.3 Trusted Computing	
3.4.4 WatchDog	
3.4.5 Super IO Configuration	
3.4.6 NCT6116D HW Monitor	
3.4.7 S5 RTC Wake Setting	
3.4.8 Network Stack Configuration	
3.4.9 NVMe Configuration	
3.5 Security Page	
3.5.1 Secure Boot	
3.5.2 BIOS Update	
3.6 Boot Page	
3.7 Save & Exit Page	



Chapter 1 : Production Introduction

1.1 Specifications

System		
CPU Type	Intel 9th ® Core i7-9700TE, 8C, 1.8/3.8GHz, 12MB cache, TDP 35W	
Chipset	Intel® C246	
Memory Type	DDR4 2666MHz, 2 x 260-pin SO-DIMM, Max. 64GB	
Expansion Slot	2 x PCle 3.0 x 8	
Storage Device	2 x 2.5" Easy swap tray	
Front I/O		
Power Button	1 x Power Button w/Indicator LED	
LED	1 x PWR LED ; 1 x HDD LED	
HDMI	1 x HDMI 1.4	
USB	2 x USB 3.0	
Rear I/O		
СОМ	2 x RS232 / 422 / 485 (Support Power 5V / 12V)	
Ethernet	2 x RJ45	
USB	4 x USB 3.0, 2 x USB 2.0	
PS/2	1	
DisplayPort	1 x DP1.2	
DVI-I	1 x DVI-I	
Terminal Block	1 x 2Pin Terminal Block Remote Power ON/OFF 1 x 2Pin Terminal Block Remote Reset 1 x 4Pin Terminal Block External FAN Connector 1 x 3Pin Terminal Block Power Input	
Audio	1 x Mic-in, 1 x Line-out	
DC-IN	1 x 9~48V	
Mechanical and Evvironmental		
Dimension (W x H x D)	170 x 264 x 250 mm(W x D x H)	
System Design	Fanless	
Mounting	Rackmount Cube	
Operating Temp.	-20°C to 60°C (35W CPU)	



(ambient with airflow)	
Storage Temp.	-40°C to +85°C
Relative Humidity	5% to 95%, non-condensing
OS support list	
Windows	Windows 10 x64
Linux	Ubuntu, Red Hat
Certification	
EMC	CE, FCC Certification
Green Product	RoHS , WEEE compliance



1.2 Front Panel I/O Placement



1.3 Rear Panel I/O Placement





1.4 Mechanical Dimensions









Chapter 2 : Connectors Pin Define

2.1 External Connector Pin Definition

3-Pin terminal block for DC Input



Pin	Signal
1	+
2	GND
3	-

4-pin Terminal Blcok for PWM Fan



Pin	Signal
1	Ground
2	+12V
3	System_FAN_TACH
4	SYSTEM_FAN_CTRL

2-pin Terminal Blcok for Remote Power ON/OFF and Reset



Pin	Signal
1	Ground
2	EXT Reset
3	Ground
4	EXT_PWRBT_ON/OFF



COM Pin definition



Pin No	RS-232	RS-422	RS-485
1	DCD	TX-	DATA-
2	RX	TX+	DATA+
3	RTX	RX-	NC
4	DTR	RX+	NC
5	GND	GND	GND
6	DSR	NC	NC
7	RTS	NC	NC
8	CTS	NC	NC
9	RI	NC	NC



Chapter 3: AMI BIOS UTILITY

This chapter provides users with detailed descriptions on how to set up a basic system configuration through the AMI BIOS setup utility.

3.1 Starting

To enter the setup screens, perform the following steps:

• Turn on the computer and press the key immediately.

• After the key is pressed, the main BIOS setup menu displays. Other setup screens can be accessed from the main BIOS setup menu, such as the Chipset and Power menus.

3.2 Navigation Keys

The BIOS setup/utility uses a key-based navigation system called hot keys. Most of the BIOS setup utility hot keys can be used at any time during the setup navigation process. Some of the hot keys are <F1>, <F10>, <Enter>, <ESC>, and <Arrow> keys.

(Berry)	
Left/Right	The Left and Right <arrow> keys moves the cursor to select a</arrow>
	menu.
Up/Down	The Up and Down <arrow> keys moves the cursor to select a</arrow>
	setup screen or sub-screen.
+- Plus/Minus	The Plus and Minus < Arrow> keys changes the field value of a
	particular setup setting.
Tab	The <tab> key selects the setup fields.</tab>
F1	The <f1> key displays the General Help screen.</f1>
F10	The <f10> key saves any changes made and exits the BIOS setup</f10>
	utility.
Esc	The <esc> key discards any changes made and exits the BIOS</esc>
	setup utility.
Enter	The <enter> key displays a sub-screen or changes a selected or</enter>
	highlighted option in each menu.

Some of the navigation keys may differ from one screen to another.



3.3 Main Setup

The Main menu is the first screen that you will see when you enter the BIOS Setup Utility.

Aptio Setup Utili [.] Main Advanced Security Boot	ty – Copyright (C) 2019 Americ Save & Exit	can Megatrends, Inc.	
BIOS Version Build Date	D8050X06 07/09/2019 16:43:29	▲ Set the Date. Use Tab to switch between Date elements. Default Ranges:	
ME(TXE) FW Version	12.0.40.1433	Year: 2005–2099 Months: 1–12	
Processor Information		Days: dependent on month	
Processor Type	Intel(R) Xeon(R) E–2176G CPU @ 3.70GHz		
Microcode Version	B4		
Memory Information			
Total Memory	8192 MB		
Memory Solt1	8192 MB (DDR4)		
Memory Solt2	0 MB (DDR4)	++: Select Screen	
Memory Speed	2133 MHz	¶↓: Select Item	
		Enter: Select	
Serial ATA Port 1	Empty	+/-: Change Opt.	
Serial ATA Port 2	Empty	F1: General Help	
Serial ATA Port 3	Empty	F2: Previous Values	
Serial ATA Port 4(M.2)	Empty	F3: Uptimized Defaults	
Serial Ala Port 5(mSAIA)	Empty	F4: Save & Reset	
Serial Ala Port 6(MSAIA)	Empty	ESU: EXIT	
System Date	[Tue 10/15/2267]		
System Time	[06:43:25]	•	
Version 2.20.1275. Copyright (C) 2019 American Megatrends. Inc.			

• System Date

Use this function to change the system date.

Select System Date using the Up and Down <Arrow> keys. Enter the new values through the keyboard. Press the Left and Right <Arrow> keys to move between fields. The date setting must be entered in MM/DD/YY format.

System Time

Use this function to change the system time.

Select System Time using the Up and Down <Arrow> keys. Enter the new values through the keyboard. Press the Left and Right <Arrow> keys to move between fields.

The time setting is entered in HH:MM:SS format.

Note: The time is in 24-hour format. For example, 5:30 A.M. appears as 05:30:00, and 5:30 P.M. as 17:30:00.

Access Level

Display the access level of the current user in the BIOS.



3.4 Advanced Page The Advanced Menu allows you to configure your system for basic operation. Some entries are defaults required by the system board, while others, if enabled, will improve the performance of your system or let you set some features according to your preference. <u>Setting incorrect field values may cause the system</u> to malfunction.

	Aptio Setup Utility – Copyright (C) 2016 Americ Main Advanced Chipset Security Boot Save & Ex	can Megatrends, Inc. kit
<u> </u>	Trusted Computing CPU Configuration ACPI Settings PCH-FW Configuration SMART Settings F81866 Super IO Configuration Hardware Monitor Platform Function Serial Port Console Redirection	Trusted Computing Settings
	USB Configuration CSM Configuration SATA Configuration	<pre> Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit </pre>
	Version 2.17.1255, Convright (C) 2016 American	n Megatrends, Inc.

Advanced	Description
Onboard Devices	Onboard Device Configuration
CPU Configuration	CPU Configuration Parameters
 Trusted Computing 	Trusted Computing Settings
► WatchDog	WatchDog Configuration
Super IO Configuration	System Super IO Chip Parameters.
NCT6116D HW Monitor	Monitor hardware status
S5 RTC Wake Setting	Enable System to wake from S5 using RTC
	alarm
Network Stack Configuration	Network Stack Settings
NVMe Configuration	NVMe Device Options Settings

AB



3.4.1 Onboard Device

Advanced		
Turbo Mode State After G3 DVMT Pre-Allocated DVMT Total Gfx Mem SATA Mode Selection Wake on LAN Enable HD Audio	[Enabled] [S5 State] [64M] [256M] [AHCI] [Enabled] [Enabled]	Enable/Disable processor Turbo Mode (requires Intel Speed Step or Intel Speed Shift to be available and enabled).
		<pre>++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit</pre>
Vension 0.00.11	DTE Comunicati (C) 2010 Ame	nicon Horatoondo Too

Onboard	Value	Onboard Device Configuration
Devices		
Turbo Mode	Disabled / [Enabled]	Enable/Disable processor Turbo Mode (requires Intel Speed Step or Intel Speed Shift to be available and enabled).
State After G3	S0 State / [S5 State]	Specify what state to go to when power is re- applied after a power failure (G3 state).
DVMT Pre-Allocated	[64M] / 32M/F7 / 36M / 40M / 44M / 48M / 52M / 56M / 60M	Select DVMT 5.0 Pre-Allocated(Fixed) Graphics Memory size used by the Internal Graphics Device.
DVMT Total Gfx Mem	128MB / [256MB] /Max	Select DVMT5.0 Total Graphic Menory size used by the Internal Graphics Device.
SATA Mode Selection	[AHCI] / Intel RST Premium With Intel Optane System Acceleration	Determines how SATA controller(s) operate.
Wake on LAN Enable	[Enabled] / Disabled	Enable/Disable integrated LAN to wake the system.
HD Audio	Disabled / [Enabled]	Control Detection of the HD-Audio device. Disable = HAD will be unconditionally disabled Enabled = HAD will be unconditionally enabled.



3.4.2 CPU Configuration

Aptio Setup Utility - Advanced	Copyright (C) 2019 American	Megatrends, Inc.
CPU Configuration		Enables utilization of additional hardware
Type ID Speed L1 Data Cache L1 Instruction Cache L2 Cache L3 Cache L4 Cache	Intel(R) Xeon(R) E-2176G CPU @ 3.70GHz 0x906EA 3700 MHz 32 KB x 6 32 KB x 6 256 KB x 6 12 MB N/A	capabilities provided by Intel (R) Trusted Execution Technology. Changes require a full power cycle to take effect.
VMX SMX/TXT	Supported Supported	
Intel Trusted Execution Technology	[Disabled]	<pre>++: Select Screen fl: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit</pre>

CPU Configuration	Value	CPU Configuration Parameters
CPU Configuration		
Туре	Intel® xxxx® xxxxxx xxxxxxx	
ID	0xXXXX	
Speed	XXXX MHz	
L1 Data Cache	EX. 32KB x 2	
L1 Instruction Cache	EX. 32KB x 2	
L2 Cache	EX. 256KB x 2	
L3 Cache	EX. 3MB	
L4 Cache		
VMX	Supported	
SMX/TXT	Supported	
Intel Trusted		Enables utilization of additional
Execution Technology		hardware capabilities provided by
	[Enabled] / Disabled	Intel® Trusted Execution
		Technology.
		Changes require a full power cycle
		to take effect.



3.4.3 Trusted Computing

Aptio Setup Advanced	Utility – Copyright (C) 2019 American Megatrends, Inc.
TPM20 Device Found Firmware Version: Vendor: Security Device Support Pending operation	7.2 NTC [Enable] [None]	Enables or Disables BIOS support for security device. O.S. will not show Security Device. TCG EFI protocol and INT1A interface will not be available.
		++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit
Vencion 2.2	0 1275 Conunight (C)	2019 Amonican Wagataanda Inc

Trusted Computing	Value	Trusted Computing Settings
TPM20 Device Found		
Firmware Version:	x.x	
Vendor:	XXXXXX	
Security Device Support	[Disabled] / Enabled	Enables or Disables BIOS support for security device. O.S. will not show Security Device. TCG EFI protocol and INT1A interface will not be available.
Pending operation	[None] / TPM Clear	Schedule an Operation for the Security Device. NOTE: Your Computer will reboot during restart in order to change State of Security Device.



3.4.4 WatchDog

Aptio Setup Advanced	Utility – Copyright (C) 2019 A	merican Megatrends, Inc.
WatchDog	[Disabled]	Enables or disables WatchDog function.
		<pre>++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit</pre>
Version 2.2	0.1275. Copyright (C) 2019 Ame	rican Megatrends, Inc.

WatchDog	Value	WatchDog Configuration
WatchDog	[Disabled] / Enabled	Enables or Ddisables WatchDog
		function.



3.4.5 Super IO Configuration

Aptio Setup Utilit Advanced	ty – Copyright (C) 2019 Ame	erican Megatrends, Inc.
Super IO Configuration		Set Parameters of Serial Port
Super IO Chip Serial Port 1 Configuration Serial Port 2 Configuration	NCT6116D	
		<pre>++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit</pre>
Vencion 2, 20, 427	- Penunisht (D) 2010 Areni	icon Marataondo Tao

Super IO Configuration	Value	System Super IO Chip Parameters.
Super IO Configuration		
Super IO Chip	NCT6116D	
 Serial Port 1 Configuration 	Value	Set Parameters of Serial Port 1 (COMA)
Serial Port 1 Configuration		
Serial Port	Disabled / [Enabled]	Enable or Disable Serial Port (COM)
Device Settings	IO=3F8h; IRQ=4	
Change settings	[Auto] / IO=3F8h; IRQ=4 / IO=3F8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12 / IO=2F8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12 / IO=3E8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12 / IO=2E8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12	Select an optimal settings for Super IO Device
Mode Configuration	[RS232] / RS485 / RS422	Configure serial port as



		RS232/RS422/RS485.
Serial Port 2	Value	Set Parameters of Serial Port 2
Configuration		(COMB)
Serial Port 2 Configuration		
Serial Port	Disabled / [Enabled]	Enable or Disable Serial Port (COM)
Device Settings	IO=2E8h; IRQ=4	
Change settings	[Auto] / IO=2E8h; IRQ=7 / IO=3E8h; IRO=3_4_5_6_7_9	Select an optimal settings for
	10, 11, 12	
	/ IO=2E8h; IRQ=3, 4, 5, 6, 7, 9,	
	10, 11, 12	
	10, 11, 12	
	/ IO=2E0h; IRQ=3, 4, 5, 6, 7, 9,	
	10, 11, 12	
Mode Configuration	[RS232] / RS485 / RS422	Configure serial port as RS232/RS422/RS485.

3.4.6 NCT6116D HW Monitor

Aptio Setup Utility Advanced	– Copyright (C) 2019 Americar	n Megatrends, Inc.
PC Health Status		If Enabled, POST monitors voltage, temperature, and fan
Hardware Monitor Alert Enable	[Disabled]	status. If these values are out of range, BIOS display
CPU Temperature	: +54 °c	warning message and turn on
CPU VR Temperature	: +32 °c	beep sound.
DIMM Temperature	: +31 °c	
System Fan_Internal Speed	: 1831 RPM	
System Fan_External Speed	: N/A	
VCORE	: +1.136 V	
PCH IO volt	: +1.048 V	
System Memory	: +1.200 V	
AVSB	: +3.344 V	
VSB3V	: +3.296 V	++: Select Screen
		I+: Select Item
		Enter: Select
		F1: Concent Help
		E2: Provinus Values
		E3. Ontimized Defaults
		F4: Save & Reset
		ESC: Exit
		COOP ENTE
Version 2.20.1275.	Copyright (C) 2019 American M	legatrends, Inc.



NCT6116D HW Monitor	Value	Monitor hardware status
PC Health Status		
Hardware Monitor Alert Enable	[Disabled] / Enabled	If Enabled, POST monitors voltage, temperature, and fan status. If these values are out of range, BIOS display warning message and turn on beep sound.
CPU Temperature	xx °C	
CPU VR Temperature	xx °C	
DIMM Temperature	xx °C	
System Fan_Internal Speed	xx RPM	
System Fan_External Speed	xx RPM	
VCORE	xx V	
PCH IO volt	xx V	
System Memory	xx V	
AVSB	xx V	
VSB3V	xx V	

3.4.7 S5 RTC Wake Setting

Aptio Setup U Advanced	tility – Copyright (C) 2019 A	merican Megatrends, Inc.
Wake system from S5	[Disabled]	Enable or disable System wake on alarm event. Select FixedTime, system will wake on the hr::min::sec specified. Select DynamicTime , System will wake on the current time + Increase minute(s)
		<pre>++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit</pre>
Version 2.20	.1275. Copyright (C) 2019 Ame	rican Megatrends, Inc.



S5 RTC Wake Setting	Value	Enable System to wake from S5 using RTC alarm
Wake System with Fixed Time from S5	[Disabled] / Fixed Time / Dynamic Time	Enable or disable System wake on alarm event. Select FixedTime, system will wake on the hr::min::sec specified. Select DynamicTime, System will wake on the current time + Increase minute(s)

3.4.8 Network Stack Configuration

Aptio Setup Advanced	Utility – Copyright (C) 2019 American	Megatrends, Inc.
Network Stack	[Disabled]	Enable/Disable UEFI Network Stack
		<pre>++: Select Screen fl: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit</pre>
Version 2.	20.1275. Copyright (C) 2019 American M	egatrends, Inc.

 Network Stack Configuration 	Value	Network Stack Settings
Network Stack	[Disabled] / Enabled	Enable/Disable UEFI Network Stack



3.4.9 NVMe Configuration

Aptio Setup Utility – Copyright (C) 2019 American Advanced	Megatrends, Inc.
NVMe Configuration	
No NVME Device Found	
	++: Select Screen
	Enter: Select
	F1: General Help
	F2: Previous values F3: Optimized Defaults
	ESC: Exit
Version 2.20.1275. Copyright (C) 2019 American M	egatrends, Inc.



3.5 Security Page

Aptio Setup Utilit Main Advanced Security Boot	y <mark>– Copyright (C) 2019 A</mark> Save & Exit	merican Megatrends, Inc.
Password Description		Set Administrator Password
If ONLY the Administrator's pass then this only limits access to only asked for when entering Set If ONLY the User's password is s is a power on password and must boot or enter Setup. In Setup th have Administrator rights. The password length must be in the following range: Minimum length Maximum length	word is set, Setup and is up. et, then this be entered to e User will 3 20	
Administrator Password User Password		++: Select Screen †↓: Select Item Enter: Select +/-: Change Opt. F1: General Help
▶ Secure Boot		F2: Previous Values
▶ BIOS Update		F3: Optimized Defaults F4: Save & Reset ESC: Exit
Vancian 2 20 1275	Conunight (C) 2019 Amor	aican Wagathanda The

Security	Value	Description
Password Description		
Administrator Password	XXXX	Set Administrator Password
User Password	XXXX	Set User Password
► HDD Security drive(EX:		HDD Security Configuration
XXXXXXXXXXXXXX)		for selected drive
Secure Boot		Secure Boot configuration
► BIOS Update		BIOS Update support



3.5.1 Secure Boot

Aptio Setup Security	Utility – Copyright (C) 2019 Amer	rican Megatrends, Inc.
System Mode	User	Secure Boot feature is Active
Secure Boot	[Disabled] Not Active	Platform Key(PK) is enrolled and the System is in User mode. The mode change requires
Secure Boot Mode ▶ Restore Factory Keys ▶ Reset To Setup Mode	[Custom]	platform reset
▶ Key Management		
		++: Select Screen f4: Select Item Foton: Select
		+/-: Change Opt. F1: General Help
		F3: Optimized Defaults F4: Save & Reset ESC: Exit
Version 2.2	0.1275. Copyright (C) 2019 Americ	can Megatrends, Inc.

Security	iity – copyright (c) 2019 American	Megatrenus, Inc.
Vendor Keys	Modified	Install factory default Secure Boot keys after the platform
Factory Key Provision Restore Factory Keys Reset To Setup Mode Export Secure Boot variables Enroll Efi Image	[Disabled]	reset and while the System is in Setup mode
Device Guard Ready Remove 'UEFI CA' from DB Restore DB defaults		
Secure Boot variable Size Platform Key(PK) 835 Key Exchange Keys 1560 Authorized Signatures 3143 Forbidden Signatures 3724 Authorized TimeStamps 0 OsRecovery Signatures 0	Keys Key Source 1 Factory 2 Factory 77 Factory 0 No Keys 0 No Keys	<pre>++: Select Screen f4: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Reset ESC: Exit</pre>
Version 2.20.1	275. Copyright (C) 2019 American M	egatrends, Inc.

Secure Boot	Value	Secure Boot configuration
System Mode	XXXX	
Secure Boot	[Disabled] / Enabled	Secure Boot feature is Active if Secure Boot is Enable, Platform Key(PK) is enrolled and the System is in User mode. The mode change requires platform reset
Secure Boot Mode	Standard / [Customer]	Secure Boot mode options: Standard or Custom. In Custom mode, Secure Boot Policy variables
		can be configured by a physically present user without full aythentication
 Restore Factory Keys 	[Yes] / No	Force System to User Mode. Install factory default Secure Boot key database
Reset To Setup Mode	[Yes] / No	Delete all Secure Boot key databases from NVRAM
Key Management		Enables expert users to modify Secure Boot Policy variables without full authentication
Vendor Keys	Invalid / Valid	
Factory Key Provision	[Disabled] / Enabled	Install factory default Secure Boot keys after the platform reset and while the System is in Setup mode
Restore Factory Keys	[Yes] / No	Force System to User Mode. Install factory default Secure Boot key database







 Reset To Setup Mode 	[Yes] / No	Delete all Secure Boot key databases from NVRAM
 Export Secure Boot variables 	Drive: \Path	Copy NVRAM content of Secure Boot variables to files in a root folder on a file system device
► Enroll Efi Image	*****	Allow the image to run in Secure Boot mode
	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	Enroll SHA256 Hash cortificate of a DE image
		inte Authorized Cignoture Database (db)
		into Authorized Signature Database (db)
Device Guard ready		
Remove 'UEFI CA'		Device Guard ready system must not list
from DB		'Microsoft UEFI CA' Certificate in Authorized
		Signature database (db)
Remove DB defaults	[Yes] / No	Restore DB variable to factory defaults
Secure Boot variables	Size   Keys   Key	
Source		
Platform Key(PK)	[Details] / Export /	Enroll Factory Defaults or load certificates from
	Update / Delete	a file:
		1.Public Key Certificate:
		a)EFI_SIGNATURE_LIST
		b)EFI CERT X509 (DER)
		cĺEFI CERT RSA2048 (bín)
		d)EFI_CERT_SHAXXX
		2 Authenticated LIFEL Variable
		3 EEI DE/COEE Image/SHA256)
		S. ETTPE/COTT IIIage(STA250)
		Rey Source.
N Kara Frank and a Kara		Factory, External, Mixed
Key Exchange Keys	[Details] / Export /	Enroll Factory Defaults or load certificates from
	Update / Append /	
	Delete	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
Authorized	[Details] / Export /	Enroll Factory Defaults or load certificates from
Signatures	Update / Append /	a file:
	Delete	1.Public Key Certificate:
		a)EFI SIGNATURE LIST
		b)EFI CERT X509 (DER)
		c)EFI_CERT_RSA2048 (bin)
		d)EFI CERT SHAXXX
		2 Authenticated UFFI Variable
		3. EFI PE/COFF Image(SHA256)
		Key Source:
		Factory, External Mixed
Forbidden Signatures	[Details] / Export /	Enroll Factory Defaults or load certificates from
	Update / Append /	a file:
	Delete	1.Public Key Certificate:
		a)FEL SIGNATURE LIST
		h)FFL CERT X509 (DER)
		c)FEL CERT RSA2048 (bin)
		2 Authoritostad UEELVariable
		Z.Authenticated DEFT Variable



		3. EFI PE/COFF Image(SHA256)
		Key Source:
		Factory, External,Mixed
<ul> <li>Authorized</li> </ul>	[Details] / Export /	Enroll Factory Defaults or load certificates from
TimeStamps	Update / Append /	a file:
	Delete	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
<ul> <li>OsRecovery</li> </ul>	[Details] / Export /	Enroll Factory Defaults or load certificates from
Signatures	Update / Append /	a file:
	Delete	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



#### 3.5.2 BIOS Update

Aptio Setup Utility – Copyright (C) 2019 American Security	Megatrends, Inc.
▶ Path for ROM Image Notice : ROM Image must in the root folder of storage device. File name must match with current BIOS project.	Enter the path to the BIOS update option
	<pre>++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Reset ESC: Exit</pre>
Version 2.20.1275. Copyright (C) 2019 American Me	gatrends, Inc.



#### 3.6 Boot Page

Aptio Setup Utility – Copyright (C) 2019 American Megatrends, Inc. Main Advanced Security <mark>Boot</mark> Save & Exit		
Boot Configuration Setup Prompt Timeout Bootup NumLock State	<mark>1</mark> [Off]	Number of seconds to wait for setup activation key. 65535(0xFFFF) means indefinite waiting.
FIXED BOOT ORDER Priorities Boot Option #1 Boot Option #2 Boot Option #3 Boot Option #4 Boot Option #5 Boot Option #6 Boot Option #7 • UEFI USB Key Drive BBS Priorities	[USB Floppy] [CD/DVD] [USB CD/DVD] [Hard Disk] [USB Key] [USB Hard Disk] [Network]	<pre>++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Reset ESC: Exit</pre>

Version 2.20.1275. Copyright (C) 2019 American Megatrends, Inc.

Boot	Value	Description
Setup Prompt Timeout	1	Number of seconds to wait for setup activation key. 65535(0xFFFF) means indefinite waiting.
Bootup NumLock State	On / [Off]	Select the keyboard NumLock state
FIXED BOOT ORDER Priorities		
Boot Optoin #1	[USB Floppy] / CD/DVD / USB CD/DVD / Hard Disk / USB Key / USB Hard Disk / Network / Disable	Sets the system boot orfer
Boot Optoin #2	USB Floppy / [CD/DVD] / USB CD/DVD / Hard Disk / USB Key / USB Hard Disk / Network / Disable	Sets the system boot orfer
Boot Optoin #3	USB Floppy / CD/DVD / [USB CD/DVD] / Hard Disk / USB Key / USB Hard Disk / Network /	Sets the system boot orfer



	Disable	
Boot Optoin #4	USB Floppy / CD/DVD / USB CD/DVD / [Hard Disk] / USB Key / USB Hard Disk / Network / Disable	Sets the system boot orfer
Boot Optoin #5	USB Floppy / CD/DVD / USB CD/DVD / Hard Disk / [USB Key] / USB Hard Disk / Network / Disable	Sets the system boot orfer
Boot Optoin #6	USB Floppy / CD/DVD / USB CD/DVD / Hard Disk / USB Key / [USB Hard Disk] / Network / Disable	Sets the system boot orfer
Boot Optoin #7	USB Floppy / CD/DVD / USB CD/DVD / Hard Disk / USB Key / USB Hard Disk / [Network] / Disable	Sets the system boot orfer



#### 3.7 Save & Exit Page

Aptio Setup Utility – Copyright (C) 2019 American Main Advanced Security Boot <mark>Save &amp; Exit</mark>	Megatrends, Inc.
Save Options Save Changes and Reset Discard Changes and Reset Load Optimized Defaults	Reset the system after saving the changes.
	<pre>++: Select Screen f↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Reset ESC: Exit</pre>
Version 2.20.1275. Copyright (C) 2019 American Mo	egatrends, Inc.

Save & Exit	Description
Save Changes and Reset	Reset the system after saving the changes.
Discard Changes and Reset	Reset system setup without saving any changes.
Load Optimized Defaults	Restore/Load Default values for all the setup options.