



LPC-2Tx Series P-cap Panel PC With 11th Gen., Core-i7/5/3 User Manual

Published in Taiwan Release Date : Feb 2024 Revision : V0.1

Warning!

This equipment generates, uses and can radiate radio frequency energy and if not installed and used in accordance with the instruction's manual, it may cause interference to radio communications. It has been tested and found to comply with the limits for a Class A computing device pursuant to FCC Rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference in which case the user at his own expense will be required to take whatever measures may be required to correct the interference.

Electric Shock Hazard – Do not operate the machine with its back cover removed. There are dangerous high voltages inside.

Disclaimer

This information in this document is subject to change without notice. In no event shall ELGENS Co., Ltd. be liable for damages of any kind, whether incidental or consequential, arising from either the use or misuse of information in this document or in any related materials.

Packing List



Safety Precautions

Follow the messages below to avoid your systems from damage:

- Avoid your system from static electricity on all occasions.
- Prevent electric shock. Don't touch any components of this card when the card is power-on. Always disconnect power when the system is not in use.
- Disconnect power when you change any hardware devices. For instance, when you connect a jumper or install any cards, a surge of power may damage the electronic components or the whole system.

Table of Contents

Warn	ing!	2
Disc Pack Safe	claimer king List ty Precautions	
Chapt	ter 1 Getting Started	4
1.1	Brief Description of LPC P-cap Series	4
1.2	System Specifications	4
1.3	Naming Rule	6
1.4	Dimension	8
1.5	General Rear IO Placement	
1.6	Front View of LPC- 2Tx Series	
1.7	Rear View of LPC- 2Tx Series	
1.8	Top / Bottom IO View	14
1.9	Installation of HDD	14
~		

Chapter 2Installation15

2.1	Remove Heatsink	.15
2.2	Install DRAM Modules	.16
2.3	Install Nano SIM Card	.17
2.4	Install M.2 Expansion Modules	.18
2.5	Install M.2 NVME SSD	.19

3.1	Entering Setup	20
3.2	The Menu Bar	22
3.3	Main	23
3.4	Advanced	24
3.5	Boot	30
3.6	Security	30
3.7	Chipset	41
3.8	Power	42
3.9	Save & Exit	43

Chapter 1 Getting Started

1.1 Brief Description of LPC P-cap Series

The LPC P-cap 2Tx series is a power-optimized and delivers robust performance-per-watt for embedded HMI, powered by an Intel 11th Gen., TigerLake-UP3 Core-i7/i5/i3 processors. It comes with a Bezel-Free design, M.2(NVME) slot and a SATA 2.5-inch lockable HDD tray, up to 64GB DDR4 memory, audio jack, 2 Ethernet, and 4 USB 3.2 ports. The unit supports Windows 10 / Windows 11 operation system.

The Elgens' fanless touch panel computer is ideal for use as Web Browser, Terminal, HMI at all levels of automation control or a high-performance system that working on rash environment.

Model Number	LPC-P150S-2Tx	LPC-P156W-2Tx	LPC-P170S-2Tx	LPC-P185W-2Tx		
Max Resolution	1024*768	1920*1080	1280*1024	1920*1080		
Color	16.2M	16.2M	16.7M	16.7M		
Luminance	350 nits	450 nits	350 nits	350 nits		
View Angle (H/V)	160/140	170/170	160/140	178/178		
Contrast Ratio	700	800	800	1000		
Computing						
Processor	Intel [®] TGL-UP	3 i7-1185G7E/i5-1145G	67E/i3-1115G4E Proc	essors		
System Memory	2 x DDR4 SO-I	DIMM, up to 64GB				
Storage	1 x 2.5" Stora	ge Bay				
	1 x M.2 M-key	1 x M.2 M-key (NVME) 2280 Socket				
External I/O Port	4 x USB 3.2 G	4 x USB 3.2 Gen2 Ports				
	2 x RJ45 GbE	2 x RJ45 GbE LAN (Intel [®] I225-LM supports 2.5GbE LAN)				
	1 x Display Po	1 x Display Port				
	1 x HDMI					
	4 x RS-232/42	2/485				
	1 x Audio out					
	1 x Power pre	1 x Power press button				
	1 x 3-Pin Pow	er Input				
Expansion Slots	1 x M.2 B-key	1 x M.2 B-key 2242/3042 (SATA 3.0, PCle x1, USB 2.0)				
	1 x M.2 E-key	2230 (PCIe x1, USB 2.0))			
OS support	Windows 10 I	Windows 10 IoT Enterprise 2021 LTSC (64-bit, 21H2)				
	Windows 11 I	oT Enterprise (64-bit, 2	1H2, Pre-scan)			
	Linux Ubuntu	22.04 (64-bit, by reque	st)			

1.2 System Specifications

	Linux Yocto Project 3.1 (64-bit, by request)		
Touch Screen			
Туре	USB P-cap Touch		
Light Transmission	90%		
Power Supply			
Power Input	DC12~24V Wide Range Power Input		
	3-Pin Terminal Block		
Mechanical			
Construction	Aluminum Heatsink for 35W		
IP Rating	Front Panel compliant IP65		
Mounting	Panel/VESA		
Environmental			
Operating Temperature	-40~70 °C		
Storage Temperature	-40~70 °C		
Storage Humidity	10~90% @40 °C non-condensing		

1.3 Naming Rule



Order Code		
LPC-PxxxS/W	-H / -OB / -AG / -AR / -B / -V	
P = P-Cap touch		
B = Glass without touch		
xxx = size, For example,	10.1" = 101	
S = Dimension Ratio Square = 4:3 or 5:4		
W= Dimension Ration Wide = 16:9 or 16:10		
H = High Brightness 100	0 nits LED backlight (Optional, up to 1600 nits backlight)	
OB = Optical Bonding (C	ptional)	
AG = Anti-Glare (Option	al)	
AR = Anti-Reflection (Op	otional)	
V = Vandal Proof Glass (Optional)		

1.4 Dimension



LPC-P150S-2Tx Drawing



LPC-P156W-2Tx Drawing



ELGENS CO., LTD LPC P-cap 2Tx Series User Manual



LPC-P185W-2Tx Drawing

1.5 General Rear IO Placement



The default setting of COM ports is RS-232 as below pin definition, adjustable to RS-RS422/485 by BIOS.

Pin No	Color	RS-232	RS-422	RS-485
1	Brown	DCD	422 TXD-	485 TXD-
2	Red	SIN	422 TXD+	485 TXD+
3	Orange	SOUT	422 RXD+	NC
4	Yellow	DTR	422 RXD-	NC
5	Black	GND	GND	GND
6	Green	DSR	NC	NC
7	Blue	RTS	NC	NC
8	Purple	CTS	NC	NC
9	Grey	VCC	VCC	VCC

COM 1



Power input terminal block pin definition is as below.



1.6 Front View of LPC- 2Tx Series



1.7 Rear View of LPC- 2Tx Series



1.8 Top / Bottom IO View



Top IO



Bottom IO

1.9 Installation of HDD



Chapter 2 Installation

The LPC 2Tx series is a panel pc with 3.5" motherboard. Before you install the accessories on motherboard, study the installation guide to ensure that the accessories be secured.

2.1 Remove Heatsink

The heatsink cover is secured onto the chassis with 18 M3*5 zinc-coated screws located at 4 sides. Use a Phillips screwdriver to unscrew them.

Step 1. Loosen screws as below picture



Step 2. You can access internal accessories while you pull-up the heatsink.



- 1. Remove all power source before you start to remove heatsink.
- It is easy to cause damage after the heatsink been removed. Please be carefully do not drop tools and/or parts on it while heatsink had removed.
- not drop tools and/or parts on it while neatsink had removed.
- 3. Make sure all parts and screws are secured before you cover up.

2.2 Install DRAM Modules

Step 1. Following CH2.1 to remove heatsink.

Step 2. Align a SO-DIMM on the slot such that the notch on the SO-DIMM matches the break on the slot.







1. Always insert memory modules in the DIMM1 slot first.



- The SO-DIMM only fits in one correct orientation. It will cause permanent damage to the motherboard and the SO-DIMM if you force the SO-DIMM into the slot at incorrect orientation.
- 3. Please do not intermix different voltage SO-DIMMs on this motherboard.

Step 3. Firmly insert the SO-DIMM into the slot until the retaining clips at both ends fully snap back in place and the SO-DIMM is properly seated.

2.3 Install Nano SIM Card



Step 1. Following CH2.1 to remove heatsink.

Step 2. Install USIM1-Nano SIM Holder.

This holder is provided for 3G, 4G, LTE, 5G Nano SIM cards.



2.4 Install M.2 Expansion Modules



Step 1. Following CH2.1 to remove heatsink.

Step 2. Install M.2 expansion modules.

Please install the Wi-Fi/ Bluetooth card into the M2_E1 M.2 slot.

Please install the WWAN Card/ solid-state drive (SATA SSD) into the M2_B1 M.2 slot.



2. M2_B1 slot supports PCIe x 1, SATA 3.0, USB 2.0 signal.

2.5 Install M.2 NVME SSD

Step 1. Following CH2.1 to remove heatsink.

Step 2. Please install the M.2 solid-state drive (NVME SSD) into the M.2 slot as shown below.



Chapter 3 BIOS Setup

This chapter provides information on the BIOS Setup program and allows users to configure the system for optimal use.

Users may need to run the Setup program when:

- An error message appears on the screen at system startup and requests users to run SETUP.
- Users want to change the default settings for customized features.

Important

- Please note that BIOS update assumes technician-level experience.
- As the system BIOS is under continuous update for better system performance, the illustrations in this chapter should be held for reference only.

3.1 Entering Setup

Power on the computer and the system will start POST (Power On Self Test) process. When the message below appears on the screen, press or <F2> key to enter Setup.

Press or <F2> to enter SETUP

If the message disappears before you respond and you still wish to enter Setup, restart the system by turning it OFF and On or pressing the RESET button. You may also restart the system by simultaneously pressing <Ctrl>, <Alt>, and <Delete> keys.

Important

The items under each BIOS category described in this chapter are under continuous update for better system performance. Therefore, the description may be slightly different from the latest BIOS and should be held for reference only.

Control Keys

$\leftrightarrow \rightarrow$	Select Screen	
$\wedge \downarrow$	Select Item	
Enter	Select	
+ -	Change Value	
Esc	Exit	
F1	General Help	
F7	Previous Values	
F9	Optimized Defaults	
F10	Save & Reset*	
F12	Screenshot capture	
<k></k>	Scroll help area upwards	
<m></m>	Scroll help area downwards	

Getting Help

After entering the Setup menu, the first menu you will see is the Main Menu.

Main Menu

The main menu lists the setup functions you can make changes to. You can use the arrow keys ($\uparrow \downarrow$) to select the item. The on-line description of the highlighted setup function is displayed at the bottom of the screen.

Sub-Menu

If you find a right pointer symbol appears to the left of certain fields that means a sub-menu can be launched from this field. A sub-menu contains additional options for a field parameter. You can use arrow keys ($\uparrow \downarrow$) to highlight the field and press <Enter> to call up the sub-menu. Then you can use the control keys to enter values and move from field to field within a sub-menu. If you want to return to the main menu, just press the <Esc >.

General Help <F1>

The BIOS setup program provides a General Help screen. You can call up this screen from any menu by simply pressing <F1>. The Help screen lists the appropriate keys to use and the possible selections for the highlighted item. Press <Esc> to exit the Help screen.

3.2 The Menu Bar



» Main

Use this menu for basic system configurations, such as time, date, etc.

» Advanced

Use this menu to set up the items of special enhanced features.

» Boot

Use this menu to specify the priority of boot devices.

» Security

Use this menu to set supervisor and user passwords.

» Chipset

This menu controls the advanced features of the onboard chipsets.

» Power

Use this menu to specify your settings for power management.

» Save & Exit

This menu allows you to load the BIOS default values or factory default settings into the BIOS and exit the BIOS setup utility with or without changes.

3.3 Main

Main Advanced Boot Security	Aptio Setup – AMI Chipset Power Save & Exi	it
System Date System Time	[Wed 08/17/2022] [17:08:32]	Set the Date. Use Tab to switch between Date elements.
SATA_1 SATA_2 M.2	Not Present Not Present Not Present	Vear: 2000-2099 Months: 1-12 Days: Dependent on month Range of Vears may vary
SATA Mode Selection	[AHCI]	
USB Devices: 1 Drive, 1 Keyboard		
BIOS Version E98M3IMS.100		++: Select Screen
11th Gen Intel(R) Core(TM) i3–11 Processor ID	15GRE @ 3.00GHz 0x806C1	Enter: Select +/-: Change Opt.
Build Type Total Memory	64 3968 MB (DDR4)	ESC: Exit F1: General Help
		F7: Previous values F9: Optimized Defaults F10: Save & Reset Setup
		F12: Screenshot capture <k>: Scroll help area upwards</k>
		<m>: Scroll help area downwards</m>
HDD Information		
• RAID (VMD) Disabled: Disp	olay HDD information as p	olugging in status.
RAID (VMD) Enabled: Disp	lay "Not Present" only.	

» System Date

This setting allows you to set the system date. The date format is <Day>, <Month>, <Date>, <Year>.

» System Time

This setting allows you to set the system time. The time format is <Hour> <Minute> <Second>.

» SATA Mode Selection

This setting specifies the SATA controller mode.

[AHCI]	AHCI (Advanced Host Controller Interface), is a technical standard for an interface that allows the software to communicate with Serial ATA (SATA) devices. It offers advanced SATA features such as Native Command Queuing (NCQ) and hot-plugging.
[RAID]	RAID (Redundant Array of Independent Disks) is a virtual disk storage technology that combines multiple physical disks into one unit for data redundancy, performance improvement, or both.

3.4 Advanced

Main Advanced Boot Security Chi	Aptio Setup – AMI pset Power Save & Exit	
Full Screen Logo Display Bootup NumLock State Configurable TDP Boot Mode CPU Configuration Memory Configuration Super IO Configuration H/W Monitor Smart Fan Configuration Network Stack Configuration PCL/PCIE Device Configuration GPIO Group Configuration TSN GBE Configuration Intel(R) Time Coordinated Computing	[Disabled] [On] [Up]	Enables or disables Full Screen Logo Display option
		<pre>++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. ESC: Exit F1: General Help F7: Previous Values F9: Optimized Defaults F10: Save & Reset Setup F12: Screenshot capture <k>: Scroll help area upwards <h>: Scroll help area downwards</h></k></pre>
Version 2	.22.1282 Copyright (C) 2022	AMI

» Full Screen Logo Display

This BIOS feature determines if the BIOS should hide the normal POST messages with the motherboard or system manufacturer's full-screen logo.

[Enabled]	BIOS will display the full-screen logo during the boot-up sequence,
	hiding normal POST messages.
[Disabled]	BIOS will display the normal POST messages, instead of the full-screen logo.

Please note that enabling this BIOS feature often adds 2-3 seconds of delay to the booting sequence. This delay ensures that the logo is displayed for a sufficient amount of time. Therefore, it is recommended that you disable this BIOS feature for a faster boot-up time.

» Bootup NumLock State

This setting is to set the Num Lock status when the system is powered on.

[On]	Turn on the Num Lock key when the system is powered on.
[Off]	Allow users to use the arrow keys on the numeric keypad.

» Configurable TDP Boot Mode

This feature allows you sets the TDP (Thermal Design Power) Boot mode to either Nominal, Down or Up.

TDP Power Spec			
Processor Family	Nominal	Down	Up
Intel® Core™ Processors	28W	12W	15W
Intel [®] Celeron [®] Processors	15W	N/A	N/A

3.4.1 CPU Configuration

Advanced		
CPU Configuration 11th Gen Intel(R) Core(TM) i3-1115GRE @ 3.00GHz Processor ID Processor Speed L2 Cache L3 Cache Intel (VMX) Virtualization Technology	0×806C1 2200 MHz 1280 KB × 2 6 MB [Enabled]	When enabled, a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology.
Active Processor Cores Hyper-Threading Intel(R) SpeedStep(tm) C states	[A11] [Enabled] [Disabled] [Enabled]	<pre>++: Select Screen t4: Select Item Enter: Select +/-: Change Opt. ESC: Exit F1: General Help F7: Previous Values F9: Optimized Defaults F10: Save & Reset Setup F12: Screenshot capture <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

» Intel (VMX) Virtualization Technology

Virtualization enhanced by Intel Virtualization Technology will allow a platform to run multiple operating systems and applications in independent partitions. With Virtualization, one computer system can function as multiple "virtual" systems.

» Active Processor Cores

This setting specifies the number of active processor cores.

» Hyper-Threading

The processor uses Hyper-Threading technology to increase transaction rates and reduces end-user response times. The technology treats the two cores inside the processor as two logical processors that can execute instructions simultaneously. In this way, the system performance is highly improved. If you disable the function, the processor will use only one core to execute the instructions. **Please disable this item if your operating system doesn't support HT Function**, or unreliability and instability may occur.

» Intel[®] SpeedStep[™]

EIST (Enhanced Intel SpeedStep Technology) allows the system to dynamically adjust processor voltage and core frequency, which can result in decreased average power consumption and decreased average heat production.

When disabled, the processor will return the actual maximum CPUID (CPU Identification) input value of the processor when queried.

» Turbo Mode

Enables or disables the Turbo Mode. This feature only display when Intel[®] SpeedStep[™] is enabled.

[Enabled]	Enables this function to boost CPU performance automatically over
	specification when system request the highest performance state.
[Disabled]	Disables this function.

» C-States

This setting controls the C-States (CPU Power states).

[Enabled]	Detects the idle state of system and reduce CPU power consumption accordingly.
[Disabled]	Disables this function.

3.4.2 Memory Configuration

Advanced		
Memory Configuration		Enable/Disable In-Band ECC. Either the IBECC or the TME
In–Band ECC Support	[Enabled]	can be enabled.
In-Band ECC Error Injection	[Disabled]	
In-Band ECC Operation Mode	[2]	

» In-Band ECC Support

Enables or disables In-Band ECC(Error-Correcting Code) Support.

[Enabled]	When enabled this function, a portion(1/32) of memory space will be
	reserved to store ECC data.
[Disabled]	Disables this function.

► In-Band ECC Error Injection

Enables or disables In-Band ECC Error Injection. This feature only display when In-Band ECC Support is enabled.

► In-Band ECC Error Operation Mode

Select an operation mode from 0-2. This feature only display when In-Band ECC Support is enabled.

3.4.3 Super IO Configuration

Huvanceu		
Super IO Configuration		Enable or Disable Serial Port (COM)
Serial Port 1	[Enabled]	
Device Settings	IO=3F8h; IRQ=4;	
Change Settings	[Auto]	
Mode Select	[RS232]	
Serial Port 2	[Enabled]	
Device Settings	IO=2F8h; IRQ=3;	
Change Settings	[Auto]	
Mode Select	[RS232]	
Serial Port 3	[Enabled]	
Device Settings	IO=3E8h; IRQ=7;	
Change Settings	[Auto]	
Mode Select	[RS232]	++: Select Screen
Serial Port 4	[Enabled]	14: Select Item
Device Settings	10=2E8n; IRQ=/;	Enter: Select
Unange Settings	[AUTO]	+/-: Unange Upt.
Mode Select	[RS232]	ESU: EXIT
ETED Mode	[100 buto]	F1: General Help
Shaped IRO Mede	[IZO-Dyte]	F7: Previous values
Hatch Dog Timon	[Displad]	F10: Soup & Papet Setup
watch bog iimer	[DISADIEU]	F10: Save & Reset Setup
		/K: Scholl bein anea unwands
		(M): Scholl help area downwards
		the of orr herp area downwards

» Serial Port 1/ 2/ 3/ 4/ 5/ 6

This setting enables/disables the specified serial port.

Change Settings

This setting is used to change the address & IRQ settings of the specified serial port.

Mode Select

Select an operation mode for the specified serial port.

» FIFO Mode

This setting controls the FIFO data transfer mode.

» Shared IRQ Mode

This setting provides the system with the ability to share interrupts among its serial ports.

» Watch Dog Timer

You can enable the system watch-dog timer, a hardware timer that generates a reset when the software that it monitors does not respond as expected each time the watch dog polls it.

3.4.4 H/W Monitor

These items display the status of all monitored hardware devices/components such as voltages, temperatures, and all fans' speeds.

Huvanceu		
Pc Health Status		Thermal Shutdown
Thermal Shutdown	[Disabled]	
System temperature CPU temperature	: +38 C : +38 C	
SYSFAN	: N/A	
VCC_CORE VCC3 VCC5 +12V VCC3V VSB3V VSB3V VSB5V VBAT	: +1.264 V : +3.288 V : +5.087 V : +12.144 V : +3.312 V : +3.296 V : +4.968 V : +3.040 V	<pre>++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. ESC: Exit F1: General Help F7: Previous Values F9: Optimized Defaults F10: Save & Reset Setup F12: Screenshot capture <k>: Scroll help area upwards <h>: Scroll help area downwards</h></k></pre>

» Thermal Shutdown

This setting enables/disables the Thermal Shutdown function. It will automatically shut down when the internal temperature reaches the critical level.

3.4.5 Smart Fan Configuration

Advanced		
Configuration Smart FAN		Disabled/Enabled Smart FAN Function
SYSFAN	[Disabled]	

» SYSFAN

This setting enables/disables the Smart Fan function. Smart Fan is an excellent feature which will adjust the CPU/system fan speed automatically depending on the current CPU/system temperature, avoiding the overheating to damage your system.

3.4.6 Network Stack Configuration

Advanced		
Network Stack	[Disabled]	Enable/Disable UEFI Network Stack

» Network Stack

This menu provides Network Stack settings for users to enable network boot (PXE) from BIOS. The following items will display when Network Stak is enabled.

3.4.7 PCI/PCIE Device Configuration

Advanced		
Audio Controller	[Enabled]	Control Detection of the Audio Controller. Disabled = Audio Controller will be unconditionally disabled. Enabled = Audio Controller will be unconditionally Enabled.

» Audio Controller

This setting enables/disables the onboard audio controller.

3.4.8 GPIO Group Configuration

Advanced		
GPOO	[Low]	Set GPOO to output High/Low
GP01	[Low]	
GP02	[Low]	
GP03	[Low]	
GP04	[Low]	
GP05	[Low]	
GP06	[Low]	
GP07	[Low]	

» GPO0 ~ GPO7

These settings control the operation mode of the specified GPIO.

3.5 Boot

Aptio Setup – AMI Main Advanced <mark>Boot</mark> Security Chipset Power Save & Exit		
Boot Option Priorities Boot Option #1	[UEFI: KingstonDataTraveler 3.0, Partition 1 (KingstonDataTraveler 3.0)]	Sets the system boot order
BOOT Uption #2	(UEF1: Built-in EFI Shell]	

» Boot Option Priorities

This setting allows users to set the sequence of boot devices where BIOS attempts to load the disk operating system.

3.6 Security

Main Advanced Boot Security C	Aptio Setup – AMI hipset Power Save & Exit	
Administrator Password User Password		Set Administrator Password
Intel BIOS Guard Support	[Disabled]	
▶ PCH-FW Configuration		
AMT Configuration		
 Trusted Computing 		
Serial Port Console Redirection		

» Administrator Password

Administrator Password controls access to the BIOS Setup utility.

» User Password

User Password controls access to the system at boot and to the BIOS Setup utility.

» Intel Trusted Execution Technology

Intel Trusted Execution Technology provides highly scalable platform security in physical and virtual infrastructures.

3.6.1 PCH-FW Configuration

Security		
ME Firmware Version ME Firmware Mode ME Firmware SKU ME Firmware Status 1 ME Firmware Status 2	15.0.35.1951 Normal Mode Consumer SKU 0×90000255 0×39850106	When Disabled ME will be put into ME Temporarily Disabled Mode.
ME State ME Unconfig on RTC Clear Comms Hub Support JHI Support Core Bios Done Message	[Enabled] [Enabled] [Disabled] [Disabled] [Enabled]	
 Firmware Update Configuration PIT Configuration 		the Salast Sanaan
ME Debug Configuration		14: Select Item
▶ Anti-Rollback SVN Configuration		Enter: Select
		+/-: Change Opt.
		ESC: Exit
		F1: General Help
		F9: Ontimized Defaults
		F10: Save & Reset Setup
		F12: Screenshot capture
		<k>: Scroll help area upwards</k>
		<m>: Scroll help area downwards</m>

» ME Firmware Version, ME Firmware Mode, ME Firmware SKU, System Integrity Value, ME Firmware Status 1, ME Firmware Status 2, NFC Sup-port

These settings show the firmware information of the Intel ME (Management Engine).

» ME Status

This setting enables/disables the ME status.

» ME Unconfig on RTC Clear

This setting enables/disables ME Firmware Un-configure on RTC clear state.

» Comms Hub Support

This setting enables/disables Communications Hub Support.

» JHI Support

This setting enables/disables support for Intel Dynamic Application Loader Host Interface (JHI).

» Core BIOS Done Message

This setting enables/disables Core BIOS Done Message sent to ME.

3.6.1.1 Firmware Update Configuration

Securi	ty	
Me FW Image Re-Flash	[Disabled]	Enable/Disable Me FW Image
FW Update	[Enabled]	Re—Flash function.

» ME FW Image Re-Flash

This setting enables/ disables the ME FW (Firmware) image re-flash.

» FW Update

This setting enables/ disables the FW (Firmware) update.

3.6.1.2 PTT Configuration

Intel Platform Trust Technology (PTT) is a platform functionality for credential storage and key management used by Microsoft Windows.

Securit	y .	
PTT Capability / State	1 / 0	Selects TPM device: PTT or dTPM. PTT – Enables PTT in
TPM Device Selection TPM 1.2 Deactivate	[dTPM] [Disabled]	SkuMgr dTPM 1.2 – Disables PTT in SkuMgr Warning ! PTT/dTPM will be disabled and all data saved on it will be lost.

» TPM Device Selection

Select TPM (Trusted Platform Module) devices from PTT or dTPM (Discrete TPM).

[PTT]	Enables PTT in SkuMgr.
[dTPM]	Disables PTT in SkuMgr. Warning! PTT/ Discrete TPM will be disabled and all data saved on it will be lost.

3.6.1.3 ME Debug Configuration

Security		
HECI Timeouts	[Enabled]	Enable/Disable HECI Send/Receive Timeouts.
Force ME DID Init Status	[Disabled]	
CPU Replaced Polling Disable	[Disabled]	
HECI Message check Disable	[Disabled]	
MBP HOB Skip	[Disabled]	
HECI2 Interface Communication	[Disabled]	
KT Device	[Enabled]	
End Of Post Message	[Send in DXE]	
DOI3 Setting for HECI Disable	[Disabled]	
MCTP Broadcast Cycle	[Disabled]	

» HECI Timeouts

This setting enables/ disables the HECI (Host Embedded Controller Interface) send/receive timeouts.

» Force ME DID Init Status

Forces the DID initialization status value.

» CPU Replaced Polling Disable

Setting this option disables the CPU replacement polling loop.

» HECI Message Check Disable

This setting disables message check for BIOS boot path when sending messages.

» MBP HOB Skip

Setting this option will skip MBP HOB.

» HECI2 Interface Communication

This setting Adds/ Removes HECI2 device from PCI space.

» KT Device

This setting enables/ disables KT Device.

» End of Post Message

This setting enables/ disables End of Post Message sent to ME.

» DOI3 Setting for HECI Disable

Setting this option disables setting DOI3 bit for all HECI devices.

» MCTP Broadcast Cycle

This setting enables/ disables Management Component Transport Protocol (MCTP) Broadcast Cycle.

3.6.1.4 Anti-Rollback SVN Configuration

Security		
Minimal Allowed Anti-Rollback SVN	0	When enabled,
Automatic HW-Enforced	¶ [Disabled]	Anti-Rollback mechanism is
Set HW-Enforced Anti-Rollback for Current SVN	[Disabled]	ME FW was successfully run on a platform, FW with lower ARB-SVN will be blocked from execution

» Automatic HW-Enforced Anti-Rollback SVN

Setting this option enables will automatically activate the hardware-enforced Anti-Rollback security version (HW ERB SVN). Once ME FW was successfully run on a platform, FW with lower ARB-VN will be blocked from execution.

» Set HW-Enforced Anti-Rollback for Current SVN

Enable HW ERB mechanism for current ARB SVN value. FW with lower ARB-SVN will be blocked from execution. The value will be restored to disable after the command is sent.

3.6.2 AMT Configuration

occurry		
USB Provisioning of AMT CIRA Configuration ASF Configuration Secure Erase Configuration DEM Flags Settings MEBx Resolution Settings	[Disabled]	Enable/Disable of AMT USB Provisioning. ++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. ESC: Exit F1: General Help F7: Previous Values F9: Optimized Defaults F10: Save & Reset Setup F12: Screenshot capture <k>: Scroll help area upwards <h>: Scroll help area downwards</h></k>

» USB Provisioning of AMT

Enables or disable USB Provisioning of AMT.

3.6.2.1 CIRA Configuration

Security		
Activate Remote Assistance Process CIRA Timeout	[Disabled] O	Trigger CIRA boot Note: Network Access must be activated first from MEBx Setup.

» Activate Remote Assistance Process

Setting this option enables will trigger CIRA boot.

» CIRA Timeout

This item displays CIRA Timeout.

3.6.2.2 ASF Configuration

Secur.		
PET Progress WatchDog OS Timer BIOS Timer ASF Sensors Table	[Enabled] [Disabled] 0 0 [Disabled]	Enable/Disable PET Events Progress to receive PET Events.

» PET Progress

Setting this option enables/ disables to receive PET Events.

» WatchDog

This setting enables/ disables the watchdog timer.

» OS Timer

This item displays OS Timer.

» **BIOS Timer**

This item displays BIOS Timer.

» ASF Sensor Table

This setting enables/ disables Alert Standard Format(ASF) Sensor Table.

3.6.2.3 Secure Erase Configuration

Security			
Secure Erase mode Force Secure Erase	[Simulated] [Disabled]	Change Secure Erase module behavior: Simulated: Performs SE flow without erasing SSD Real: Erase SSD.	

» Secure Erase Mode

This setting changes Secure Erase module behavior.

[Simulated]	Performs SE flow without erasing SSD.
[Real]	Erase SSD.

» Force Secure Erase

Setting this option enables/ disables to force Secure Erase on next boot.

3.6.2.40EM Flag Setting

Security		
MEBx hotkey Pressed MEBx Selection Screen	[Disabled] [Disabled]	OEMFLag Bit 1: Enable automatic MEBx hotkey
Hide Unconfigure ME Confirmation Prompt	[Disabled]	press.
MEBX OEM Debug Menu Enable Unconfigure ME	[Disabled] [Disabled]	

» MEBx hotkey Pressed

This setting enables/ disables the management Engine BIOS Extension (MEBx) hotkey Pressed.

» MEBx Selection Screen

This setting enables/ disables the MEBx Selection Screen.

» Hide Unconfigure ME Confirmation Prompt

This setting enables/ disables the Hide Unconfigure ME Confirmation Prompt.

» MEBx OEM Debug Menu Enable

This setting enables/ disables the MEBx OEM Debug Menu.

» Unconfigure ME

This setting enables/ disables the Unconfigure ME.

3.6.2.5 MEBx Resolution Setting

Security		
Non-UI Mode Resolution UI Mode Resolution Graphics Mode Resolution	(Auto) (Auto) (Auto)	Resolution for non–UI text mode.

» Non-UI Mode Resolution

Resolution for non-UI text mode.

» UI Mode Resolution

Resolution for UI text mode.

» Graphic Mode Resolution

Resolution for graphics mode.

3.6.3 Trusted Computing

TPM 2.0 Device FoundEnables or Disables BIOSFirmware Version:7.85Vendor:IFXSecurity Device Support[Enable]Active PCR banksSHA256Available PCR banksSHA256SHA256 PCR Bank[Enabled]Pending operation[None]Platform Hierarchy[Enabled]Physical Presence Spec Version[1.3]TPM 2.0 InterfaceType[TIS]PH Randomization[Enabled]PH Randomization[Enabled]Device Select[TPM 2.0]Enabled]#*: Select ItemFT 2.0][Enabled]FT 2.0][Enabled]PH Randomization[Enabled]PH Randomization[Enabled]Device Select[TPM 2.0]F2: Screenshot CaptureK: Scroll help area upwardsWei Scroll help area upwardsWei Scroll help area downwards

» Security Device Support

This setting enables/disables BIOS support for security device. When set to [Disable], the OS will not show security device. TCG EFI protocol and INT1A interface will not be available.

» SHA256 PCR Bank

These settings enable/disable the SHA-1 PCR Bank and SHA256 PCR Bank.

» Pending Operation

When Security Device Support is set to [Enable], Pending Operation will appear. Set this item to [TPM Clear] to clear all data secured by TPM or [None] to discard the selection. It is advised that users should routinely back up their TPM secured data.

» Platform Hierarchy, Storage Hierarchy, Endorsement Hierarchy

These settings enable/disable the Platform Hierarchy, Storage Hierarchy and Endorsement Hierarchy.

» Physical Presence Spec Version

This setting show the Physical Presence Spec Version.

» TPM 2.0 Interface Type

This setting shows the TPM 2.0 Interface Type.

» PH Randomization

This setting enables/disables PH Randomization.

» Device Select

Select your TPM device through this setting.

3.6.4 Serial Port Console Redirection

Security	Aptio Setup – AMI	
COM1 Console Redirection Console Redirection Settings Serial Port for Out-of-Band Managemen Windows Emergency Management Services Console Redirection EMS Console Redirection Settings	[Disabled] ht∕ s (EMS) [Disabled]	Console Redirection Enable or Disable.
		++: Select Screen t4: Select Item Enter: Select +/-: Change Opt. ESC: Exit F1: General Help F7: Previous Values F9: Optimized Defaults F10: Save & Reset Setup F12: Screenshot capture <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k>

» Console Redirection

Console Redirection operates in host systems that do not have a monitor and keyboard attached. This setting enables/disables the operation of console redirection. When set to [Enabled], BIOS redirects and sends all contents that should be displayed on the screen to the serial COM port for display on the terminal screen. Besides, all data received from the serial port is interpreted as keystrokes from a local keyboard.

3.6.4.1 Console Redirection Settings (COM1)

Security		
COM1 Console Redirection Settings		Emulation: ANSI: Extended
Terminal Tune	[ANST]	char set. VT100Plus: Extends
Bits per second	[115200]	function keys, etc. VT-UTF8:
Parity	[8] [None]	Unicode chars onto 1 or more
Stop Bits Flow Control	[1] [None]	bytes.
VT–UTF8 Combo Key Support Recorder Mode	[Enabled]	
Resolution 100x31	[Disabled]	
Putty KeyPad	[VT100]	

» Terminal Type

To operate the system's console redirection, you need a terminal supporting ANSI terminal protocol and a RS-232 null modem cable connected between the host system and terminal(s). You can select emulation for the terminal from this setting.

[ANSI]	Extended ASCII character set.
[VT100]	ASCII character set.
[VT100Plus]	Extends VT100 to support color, function keys, etc.
[VT-UTF8]	Uses UTF8 encoding to map Unicode characters onto one or more
	bytes.

» Bits per second, Data Bits, Parity, Stop Bits

This setting specifies the transfer rate (bits per second, data bits, parity, stop bits) of Console Redirection.

» Flow Control

Flow control is the process of managing the rate of data transmission between two nodes. It's the process of adjusting the flow of data from one device to another to ensure that the receiving device can handle all the incoming data. This is particularly important where the sending device can send data much faster than the receiving device can receive it.

» VT-UTF8 Combo Key Support

This setting enables/disables the VT-UTF8 combination key support for ANSI/VT100 terminals.

» Recorder Mode, Resolution 100x31

These settings enable/disable the recorder mode and the resolution 100x31.

» Putty Keypad

PuTTY is a terminal emulator for Windows. This setting controls the numeric keypad for use in PuTTY.

3.6.4.2 Console Redirection Settings (Out-of-Band Management)

Security		
Out-of-Band Mgmt Port Terminal Type EMS Bits per second EMS Flow Control EMS Data Bits EMS Parity EMS Stop Bits EMS	COM1 [VT-UTF8] [115200] [None] 8 None 1	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 Tupe/Emulation.

» Out-of-Band Mgmt Port

This setting specifies the Out-of-Band Management Port.

» Terminal Type EMS (Windows Emergency Management Service)

You can select the type of terminal device for console redirection from this setting.

[VT-UTF8] is the preferred terminal type for the out-of-band management. The next best choice is **[VT100+]** and then **[VT100]**. See above in **Console Redirection Setting** page for more help with Terminal Type/ Emulation.

Flow Control EMS (Windows Emergency Management Service)

Flow control is the process of managing the rate of data transmission between two nodes. It's the process of adjusting the flow of data from one device to another to ensure that the receiving device can handle all of the incoming data. This is particularly important where the sending device is capable of sending data much faster than the receiving device can receive it.

» Bits per second EMS, Data Bits EMS, Parity EMS, Stop Bits EMS

This setting specifies the transfer rate of Console Redirection.

3.7 Chipset

Main Advanced Boot Security	Aptio Setup – AMI Chipset Power Save & Exit	
DVMT Total Gfx Mem Panel 1 function	[256M] [Enabled]	Select DVMT5.0 Total Graphic Memory size used by the Internal Graphics Device.
LCD Panel Type Panel 1 Backlight Control	[LVDS] [1024 × 768 & 24bit] [Level 3]	
Panel 2 function Panel 2 Type Select LCD Panel Type Panel 2 Backlight Control	[Enabled] [LVDS] [1024 × 768 & 24bit] [Level 3]	

» DVMT Total Gfx Mem

This setting specifies the memory size for DVMT.

» Panel 1/ 2 Function

This setting enables/disables Panel 1 Function.

Type Select

Set your video signal interface as LVDs or eDP. This item will display when Panel 1 Function is enabled.

LCD Panel Type

This setting specifies the LCD Panel's resolution and distribution formats. The item will display when Panel 1 Type is set to LVDs.

» Panel 1/ 2 Backlight Control

This setting controls the intensity of the LED's backlight output. When lighting conditions are brighter, set it high for a clearer image and low when it is darker.

LED's backlight output		
[Level 1]	20%	
[Level 2]	40%	
[Level 3]	60%	
[Level 4]	80%	
[Level 5]	100%	

3.8 Power

Main Advanced Boot Security	Aptio Setup – AMI Chipset Power Save & Exit	
Restore AC power Loss Deep Sleep Mode	[Last State] [S5]	Select AC power state when power is re-applied after a power failure.
Advanced Resume Events Control		
OnChip USB	[Enabled]	
LAN Wake	[Enabled]	
PCIE PME	[Disabled]	
RTC	[Disabled]	

» Restore AC Power Loss

This setting specifies whether your system will reboot after a power failure or interrupt occurs. Available settings are:

[Power Off]	Leaves the computer in the power off state.
[Power On]	Leaves the computer in the power on state.
[Last State]	Restores the system to the previous status before
	power failure or interrupt occurred.

» Deep Sleep Mode

The setting enables/disables the Deep S5 power saving mode. S5 is almost the same as G3 Mechanical Off, except that the PSU still supplies power, at a minimum, to the power button to allow return to S0. A full reboot is required. No previous content is retained. Other components may remain powered so the computer can "wake" on input from the keyboard, clock, modem, LAN, or USB device.

** Advanced Resume Events Control **

» Onchip GbE / USB

The item allows the activity of the OnChip GbE/USB device to wake up the system from S3/S4 sleep state.

» PCIE PME

This field specifies whether the system will be awakened from power saving modes when activity or input signal of onboard PCIE PME is detected.

» RTC

When [Enabled], you can set the date and time at which the RTC (real-time clock) alarm awakens the system from suspend mode.

3.9 Save & Exit

Aptio Setup – AMI Main Advanced Boot Security Chipset Power Save & Exit	
Save Changes and Reset Discard Changes and Exit Discard Changes	Reset the system after saving the changes.
Load Optimized Defaults Save as User Defaults Restore User Defaults	
Launch EFI Shell from filesystem device	

» Save Changes and Reset

Save changes to CMOS and reset the system.

» Discard Changes and Exit

Abandon all changes and exit the Setup Utility.

» Discard Changes

Abandon all changes.

» Load Optimized Defaults

Use this menu to load the default values set by the motherboard manufacturer specifically for optimal performance of the motherboard.

» Save as User Defaults

Save changes as the user's default profile.

» Restore User Defaults

Restore the user's default profile.

» Launch EFI Shell from filesystem device

This setting helps to launch the EFI Shell application from one of the available file system devices.



Revision	Date	Modification	Note