

SIEMENS

SIMATIC

Industrial PC Firmware/BIOS description SIMATIC IPC627E, IPC677E, IPC647E, IPC847E

Operating Instructions




Important information

<u>Using the firmware selection menu</u>	1
<u>Configure firmware</u>	2
<u>Configuring Intel® Management Engine BIOS Extension (MEBx)</u>	3
<u>Configuring Intel® AMT</u>	4
<u>Update firmware</u>	5
<u>Booting from USB stick</u>	6
<u>Enable Trusted Platform Module (TPM)</u>	7
<u>Configuring automatic switch-on of device</u>	8
<u>Configuring multi-monitoring</u>	9

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

 DANGER
indicates that death or severe personal injury will result if proper precautions are not taken.
 WARNING
indicates that death or severe personal injury may result if proper precautions are not taken.
 CAUTION
indicates that minor personal injury can result if proper precautions are not taken.
NOTICE
indicates that property damage can result if proper precautions are not taken.


If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

 WARNING
Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Important information

Basic knowledge requirements

This firmware / BIOS description is intended for the following qualified personnel:

- Programmers and testers who commission the device themselves and connect it to an automation system.
- Service and maintenance technicians who install enhancements or conduct fault analyzes.

A solid background in personal computers is required to understand this manual. General knowledge in the field automation control engineering is recommended.

Scope of validity

This firmware/BIOS description applies to the following SIMATIC IPCs:

- SIMATIC IPC627E
- SIMATIC IPC677E
- SIMATIC IPC647E
- SIMATIC IPC847E

History

The following versions of this firmware/BIOS description have been published previously:

Edition	Comment
10/2018	First Edition

Firmware/BIOS

The firmware (BIOS) is located in a FLASH block on the motherboard.

The firmware selection menu can be opened after the device has been started. You can then configure the firmware settings of your device.

Change firmware settings

The firmware settings are preset for working with the included software. You should only change the default firmware settings if technical changes to your device require other settings.

NOTICE

Malfunctions can occur with running software CPU

If a PC firmware/BIOS update is being performed while a SIMATIC software controller, such as a SIMATIC WinAC, is running, the software CPU can malfunction, resulting in communication interruptions or failures, among other things. Other actions that put a heavy load on the PC hardware, for example, running hardware tests such as benchmarks, can result in malfunctions of the software CPU.

Do not run a firmware/BIOS update or other actions that would put a heavy load on the hardware during operation of a software CPU.

Switch the software CPU to "STOP" before you run a firmware/BIOS update or perform other critical actions.

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit (<http://www.siemens.com/industrialsecurity>).

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customers' exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under (<http://www.siemens.com/industrialsecurity>).

Disclaimer for third-party software updates

This product includes third-party software. Siemens AG only provides a warranty for updates/patches of the third-party software, if these have been distributed as part of a Siemens software update service contract or officially released by Siemens AG. Otherwise, updates/patches are undertaken at your own risk. You can find more information about our Software Update Service offer on the Internet at Software Update Service (<http://www.automation.siemens.com/mcms/automation-software/en/software-update-service>).

Table of contents

	Important information	3
1	Using the firmware selection menu	7
1.1	Open firmware selection menu.....	7
1.2	Firmware selection menu options.....	7
2	Configure firmware	8
2.1	Starting the Setup Utility.....	8
2.2	Keyboard inputs in Setup Utility.....	8
2.3	"Main" tab.....	9
2.3.1	"Main tab" level.....	9
2.4	"Advanced" tab.....	11
2.4.1	"Boot Configuration".....	11
2.4.2	"Peripheral Configuration".....	12
2.4.3	"SATA Configuration".....	15
2.4.4	"CPU Configuration".....	16
2.4.5	"Power & Performance".....	17
2.4.5.1	"CPU - Power Management Control".....	17
2.4.6	"Memory Configuration".....	18
2.4.7	"System Agent (SA) Configuration".....	19
2.4.7.1	"Graphics Configuration".....	19
2.4.7.2	"PEG Port Configuration".....	20
2.4.7.3	Level: "System Agent (SA) Configuration".....	21
2.4.8	"PCH-IO Configuration".....	22
2.4.8.1	"PCI Express Configuration".....	22
2.4.8.2	"SATA And RST Configuration".....	23
2.4.8.3	"HD Audio Configuration".....	25
2.4.8.4	Level: "PCH-IO Configuration".....	25
2.4.9	"PCH-FW Configuration".....	26
2.4.9.1	Level: "PCH-FW Configuration".....	26
2.4.9.2	"AMT Configuration".....	27
2.4.10	"Fan Control Configuration".....	28
2.4.11	Level: "Advanced" tab.....	29
2.5	"Security" tab.....	30
2.5.1	Level: "Security" tab.....	30
2.6	"Power" tab.....	34
2.6.1	Level: "Power" tab.....	34
2.7	"Boot" tab.....	41
2.7.1	Level: "Boot" tab.....	41
2.7.2	"EFI".....	42
2.8	"Exit" tab.....	43
2.8.1	Level: "Exit" tab.....	43

3	Configuring Intel® Management Engine BIOS Extension (MEBx)	44
3.1	Logging onto MEBx (assigning password)	44
3.2	Options of the MEBx	45
4	Configuring Intel® AMT	48
5	Update firmware	49
6	Booting from USB stick.....	50
7	Enable Trusted Platform Module (TPM).....	51
8	Configuring automatic switch-on of device.....	52
9	Configuring multi-monitoring	53
	Index.....	54

Using the firmware selection menu

1.1 Open firmware selection menu

Procedure

1. Switch on the device or restart the device.

Note

The following message appears briefly after the device is switched on:

```
Press ESC for boot options
```

2. Immediately after switching on the device, press the <Esc> button and hold it down.

Result

The "Main Page" with the Firmware selection menu options (Page 7) is open.

1.2 Firmware selection menu options

The number of available options in the firmware selection menu depends on your device version.

The following options are available:

Option	Function
Continue	Exit firmware selection menu Continue the boot procedure.
Boot Manager	Specify the boot media from which to start, for example: <ul style="list-style-type: none"> • Drive • USB stick
Setup Utility	Start firmware configuration menu.
Device Management	Start device manager for UEFI boot media.
Boot From File	Boot from an *.EFI file.
Administer Secure Boot	Configure device startup in "Secure Boot Modus".
BIOS Update	Perform BIOS update. You can find more detailed information under "Update firmware (Page 49)".
Intel(R) Management Engine BIOS Extension	Start Intel® Management Engine BIOS Extension (MEBx) so that the hardware can be configured for use of Intel® Active Management Technology (iAMT).

Configure firmware

2.1 Starting the Setup Utility

You configure important firmware settings of your device using the firmware configuration menu "Setup Utility".

Procedure

1. Open the firmware selection menu (Page 7).
2. Select the "Setup Utility" option on the "Main Page" with the arrow keys.
3. Confirm your selection with the <Return> button.

2.2 Keyboard inputs in Setup Utility

Button	Function
<F1>	Call help function.
<F5> or <F6>	Change firmware settings. The <F5> key is used to take the previous setting possibility or value. The <F6> key is used to take the next setting possibility or value.
<F9>	Load Optimal Defaults: The firmware settings are reset to the safe default values. The delivery state is restored. NOTICE: All current firmware settings are overwritten.
<F10>	Exit Saving Changes: All changes are saved. The device is restarted with the changed firmware settings.
<Return>	A submenu previously selected with the arrow keys opens. The value of a firmware setting previously selected with the arrow keys can be changed.
[←] [→]	Navigate to a tab.
[↑] [↓]	Navigate to a submenu or a firmware setting. Confirm your selection with the <Return> button.
<Esc>	A submenu or tab or the Setup Utility is exited. If the Setup Utility is closed after the confirmation prompt, changes to the firmware settings are discarded.

2.3 "Main" tab

2.3.1 "Main tab" level

Calling "Main" tab

Select: "Setup Utility (Page 8)" > "Main".

Device information

You can find important device information at the top of the "Main" tab.

Device information	Explanation
SIMATIC	Device version.
BIOS Version	Current firmware version.
BIOS Number	Article number of the current firmware version.
CPU Type	CPU type.
Cache RAM	L2 cache size total.
Total Memory	Total memory size.
CPU Speed	CPU speed.
CPU Stepping	CPU version.
L2 Cache	L2 cache size (size per processor core x number of processor cores).
L3 Cache	L3 cache size.
Number Of Processors	Number of processor cores. Number of threads.
Microcode Rev	Microcode version.
PCH Rev / SKU	Platform Controller Hub (PCH) version.
GOP Ver	Version of the Graphics Output Protocol (GOP) driver.
Board ID	ID of the motherboard
Intel ME Version / SKU	Version of the Intel® Management Engine (ME).
CPB Ver	Version of the Siemens Command Parameter Block (CPB).
TPM Ver	Firmware version of the Trusted Platform Module (TPM).

Calling "System Time" and "System Date"

Date and time settings.

Select: "Setup Utility (Page 8)" > "Main" > "System Time" and "System Date".

Firmware setting	Explanation
System Time	Set current device time in the format [Hour:Minute:Second].
System Date	Set current device date in the format [Month/Day/Year].

Key functions for setting the numeric time and date values

Button	Function
<Return>	Switch between the setting options within a firmware setting, e.g. from hour to minute.
[+] [-]	Increase or decrease desired value.
[0] - [9]	Enter desired value.

2.4 "Advanced" tab

2.4.1 "Boot Configuration"

Basic display and input options during the boot procedure

Calling "Boot Configuration"

Select: "Setup Utility (Page 8)" > "Advanced" > "Boot Configuration".

Firmware setting	Value	Setting in delivery state		Meaning
		IPC627E IPC677E	IPC647E IPC847E	
Numlock	Off			Numerical keypad is switched off after starting the device.
	On	x	x	Numerical keypad is switched on off after starting the device.
POST Errors	Never halt on errors			Boot procedure is continued when errors occur.
	Halt on all errors			Boot procedure is interrupted when errors occur.
	All without key-board	x	x	Boot procedure is interrupted when errors occur, except keyboard errors.
	All without kb/smart			The boot procedure is canceled when errors occur, except for keyboard errors and S.M.A.R.T. errors (self-monitoring, analysis and reporting technology) which can occur with the storage media.

2.4.2 "Peripheral Configuration"

Configuration of the interfaces.

Calling "Peripheral Configuration"

Select: "Setup Utility (Page 8)" > "Advanced" > "Peripheral Configuration".

Firmware setting	Value	Setting in delivery state		Meaning
		IPC627E IPC677E	IPC647E IPC847E	
Internal COM 1	Disabled			The COM1 port is enabled and the resources it used are freed up.
	Enabled	x	x	The COM1 port is enabled. You can then set the I/O base address and thus the interrupt.
<ul style="list-style-type: none"> Base I/O Address (only if "Internal COM 1" = Enabled) 	2E8			The I/O basic address of the COM1 port is set with this value.
	2F8			
	3E8			
	3F8	x	x	
<ul style="list-style-type: none"> Interrupt (only if "Internal COM 1" = Enabled) 	IRQ3			The interrupt of the COM1 port is set with this value.
	IRQ4	x	x	
<ul style="list-style-type: none"> Internal COM 2 • Only with: IPC647E IPC847E 	Disabled		(depending on the device configuration)	The COM2 port is disabled and the resources it used are freed.
	Enabled		(depending on the device configuration)	The COM2 port is enabled. You can then set the I/O base address and thus the interrupt.
<ul style="list-style-type: none"> Base I/O Address (only if "Internal COM 2" = Enabled) • Only with: IPC647E IPC847E 	2E8			The I/O basic address of the COM2 port is set with this value.
	2F8		x	
	3E8			
	3F8			

Firmware setting	Value	Setting in delivery state		Meaning
		IPC627E IPC677E	IPC647E IPC847E	
<ul style="list-style-type: none"> Interrupt (only if "Internal COM 2" = Enabled) Only with: IPC647E IPC847E 	IRQ3		x	The interrupt of the COM2 port is set with this value.
	IRQ4			
Onboard Ethernet 1 (LAN 1, X1 P1)	Disabled			The onboard Ethernet interface "X1 P1" is disabled.
	Enabled	x	x	The onboard Ethernet interface "X1 P1" is enabled.
Onboard Ethernet 2 (LAN 2, X2 P1)	Disabled			The onboard Ethernet interface "X2 P1" is disabled.
	Enabled	x	x	The onboard Ethernet interface "X2 P1" is enabled.
Onboard Ethernet 3 (LAN 3, X3 P1)	Disabled			The onboard Ethernet interface "X3 P1" is disabled.
	Enabled	x	x	The onboard Ethernet interface "X3 P1" is enabled.
USB Port 1 (USB Slot Adapter Bottom)	Disabled			USB 1 (USB Slot Adapter Bottom) port is disabled.
	Enabled	x	x	USB 1 (USB Slot Adapter Bottom) port is enabled.
USB Port 2 (X65)	Disabled			USB 2 (X65) port is disabled.
	Enabled	x	x	USB 2 (X65) port is enabled.
USB Port 3 (USB Slot Adapter Top)	Disabled			USB 3 (USB Slot Adapter Top) port is disabled.
	Enabled	x	x	USB 3 (USB Slot Adapter Top) port is enabled.
USB Port 4 (X61)	Disabled			USB 4 (X61) port is disabled.
	Enabled	x	x	USB 4 (X61) port is enabled.
USB Port 5 (X63)	Disabled			USB 5 (X63) port is disabled.
	Enabled	x	x	USB 5 (X63) port is enabled.
USB Port 6 (X62)	Disabled			USB 6 (X62) port is disabled.
	Enabled	x	x	USB 6 (X62) port is enabled.
USB Port 7 (X64)	Disabled			USB 7 (X64) port is disabled.
	Enabled	x	x	USB 7 (X64) port is enabled.
USB Port 8 (USB2 P8, internal)	Disabled			USB 8 (USB2 P8, internal) port is disabled.
	Enabled	x	x	USB 8 (USB2 P8, internal) port is enabled.

Firmware setting	Value	Setting in delivery state		Meaning
		IPC627E IPC677E	IPC647E IPC847E	
USB Port 9 (Front Top) • Only with: IPC647E IPC847E	Disabled			USB 9 (Front Top) port is disabled.
	Enabled		x	USB 9 (Front Top) port is enabled.
USB Port 9 (USB2 P9, WFP) • Only with: IPC627E IPC677E	Disabled			USB 9 (USB2 P9, WFP) port is disabled.
	Enabled	x		USB 9 (USB2 P9, WFP) port is enabled.
USB Port 10 (USB3 P7, internal) • Only with: IPC647E IPC847E	Enabled		x	USB 10 (USB3 P7, internal) port is enabled. To ensure that this internal USB port is always enabled, this setting cannot be changed.
USB Port 11 (USB3 P7, internal) • Only with: IPC627E IPC677E	Enabled	x		USB 11 (USB3 P7, internal) port is enabled. To ensure that this internal USB port is always enabled, this setting cannot be changed.
USB Port 12 (USB2 P12, internal)	Disabled			USB port 12 (USB3 P7, internal) is disabled.
	Enabled	x	x	USB 12 (USB3 P7, internal) port is enabled.
USB Port 13 (Front Bottom) • Only with: IPC647E IPC847E	Disabled			USB 13 (Front Bottom) port is disabled.
	Enabled		x	USB13 (Front Bottom) port is enabled.
USB Port 13 (USB2 P13, WFP) • Only with: IPC627E IPC677E	Disabled			USB 13 (USB2 P13, WFP) port is disabled.
	Enabled	x		USB 13 (USB2 P13, WFP) port is enabled.
USB Port 14 (X60)	Disabled			USB 14 (X60) port is disabled.
	Enabled	x	x	USB 14 (X60) port is enabled.

2.4.3 "SATA Configuration"

Calling "SATA Configuration"

Select: "Setup Utility (Page 8)" > "Advanced" > "SATA Configuration".

Here you will find information about (depending on the device type, only a subset of these SATA ports may be visible):

- Serial ATA Port 0
- Serial ATA Port 1
- Serial ATA Port 2
- Serial ATA Port 3
- Serial ATA Port 4
- Serial ATA Port 5

2.4.4 "CPU Configuration"

Calling "CPU Configuration"

Select: "Setup Utility (Page 8)" > "Advanced" > "CPU Configuration".

Firmware setting	Value	Setting in delivery state		Meaning
		IPC627E IPC677E	IPC647E IPC847E	
Software Guard Extensions (SGX)	Disabled			The use of Software Guard Extensions (SG) is disabled.
	Enabled			The use of Software Guard Extensions (SG) is enabled.
	Software Controlled	x	x	The use of Software Guard Extensions (SG) is controlled by the software.
Select Owner EPOCH input type	No Change in Owner EPOCHs	x	x	The EPOCH values are not changed.
	Change to New Random Owner EPOCHs			The EPOCH values are changed to randomly generated values. After creating new EPOCH values using "Change to New Random Owner EPOCHs", the selection is reset to "No Change in Owner EPOCH" to ensure that the EPOCH values remain the same in all Sx states.
Intel (VMX) Virtualization Technology	Disabled			The virtualization functionality of Intel® is locked.
	Enabled	x	x	The virtualization functionality of Intel® is released. VMM systems (virtual machine monitor) can use the processor support for virtualization purposes (virtual machine extensions VMX) and additional performance features of the Vanderpool Technology hardware (VT).
Active Processor Cores	All	x	x	All cores of the processor are active and used.
	1			Number of processor cores used provided they do not exceed the actual number of cores. The remaining processor cores are inactive and are hidden from the operating system. This can resolve certain problems with software.
	2			
	3			
	4			
5				
Hyper-Threading (only if the processor type used supports Hyper-Threading)	Disabled			Hyper-Threading is disabled.
	Enabled	x	x	Hyper-Threading is enabled (for Windows® and Linux operating systems).
AES	Disabled			The secure encryption method AES (Advanced Encryption Standard) is not supported by hardware.
	Enabled	x	x	The secure encryption method AES (Advanced Encryption Standard) is supported by hardware. Encryption and decryption are accelerated.

2.4.5 "Power & Performance"

2.4.5.1 "CPU - Power Management Control"

Calling "CPU - Power Management Control"

Select: "Setup Utility (Page 8)" > "Advanced" > "Power & Performance" > "CPU - Power Management Control".

Firmware setting	Value	Setting in delivery state		Meaning
		IPC627E IPC677E	IPC647E IPC847E	
Intel(R) Speed-Step(tm)	Disabled			The use of more than two frequency ranges is disabled.
	Enabled	x ¹⁾	x ¹⁾	The use of more than two frequency ranges is enabled.
Intel(R) Speed Shift Technology	Disabled			Intel® Speed Shift Technology is disabled.
	Enabled	x ¹⁾	x ¹⁾	Intel® Speed Shift Technology is enabled.
HDC Control	Disabled			HDC Control (Hardware Duty Cycle Control) is disabled.
	Enabled	x	x	HDC Control (Hardware Duty Cycle Control) is enabled (if supported by the operating system).
<ul style="list-style-type: none"> Turbo Mode (only if the processor type used supports turbo mode) (only if "Intel (R) SpeedStep (tm)" = Enabled or "Intel (R) Speed Shift Technology" = Enabled)	Disabled	x ¹⁾		Turbo mode is disabled.
	Enabled		x ¹⁾	Turbo mode is enabled. When the operating system requires more power, the processor can use Intel® Turbo Boost Technology to increase the clock speed. To use turbo mode effectively, the performance modes of the "Intel(R) SpeedStep(tm)"/"Intel (R) Speed Shift Technology" processor and the power saving modes of the "C states" processor must be enabled.
C states	Disabled			The energy-saving modes of the "C states" processor are disabled.
	Enabled	x ¹⁾	x ¹⁾	The energy-saving modes of the "C states" processor are enabled.

1) Depending on the device type, the device configuration and other firmware settings, if applicable, the setting on delivery may deviate from the specified value.

2.4.6 "Memory Configuration"

Calling "Memory Configuration"

Select: "Setup Utility (Page 8)" > "Advanced" > "Memory Configuration".

Firmware setting	Value	Setting in delivery state		Meaning
		IPC627E IPC677E	IPC647E IPC847E	
ECC Support	Disabled			ECC (Error Correction Code) is disabled.
	Enabled	x	x	ECC (Error Correction Code) is enabled, if possible (the processor used and the memory modules must actually support ECC).
Max TOLUD	Dynamic	x	x	The maximum value of TOLUD (Top Of Low Usable DRAM) is set. With the "Dynamic" setting, TOLUD is automatically adjusted based on the longest MMIO length of the installed graphics controller.
	1 GB			
	1.25 GB			
	1.5 GB			
	1.75 GB			
	2 GB			
	2.25 GB			
	2.5 GB			
2.75 GB				

2.4.7 "System Agent (SA) Configuration"

2.4.7.1 "Graphics Configuration"

Calling "Graphics Configuration"

Select: "Setup Utility (Page 8)" > "Advanced" > "System Agent (SA) Configuration" > "Graphics Configuration".

Firmware setting	Value	Setting in delivery state		Meaning
		IPC627E IPC677E	IPC647E IPC847E	
Primary Display	Auto			During the boot procedure, the system automatically detects whether the device has a graphics card. Messages during the boot procedure are then issued via the graphics card. If no graphics card is available, messages are generated during the boot process via the integrated onboard graphics interface (Internal Graphics Device = IGFX).
	IGFX	x	x	Messages are output exclusively via the integrated onboard graphics interface (Internal Graphics Device = IGFX) during the boot process.
	PEG			During the boot procedure, the system automatically detects whether the device has a PEG graphics card. Messages during the boot procedure are then issued via the PEG graphics card. If no graphics card is available, messages are generated during the boot process via the integrated onboard graphics interface (Internal Graphics Device = IGFX).
Internal Graphics	Auto			The integrated onboard graphics interface (Internal Graphics Device = IGFX) is deactivated when an external graphics is detected.
	Disabled			The integrated onboard graphics interface (Internal Graphics Device = IGFX) is disabled.
	Enabled	x	x	The integrated onboard graphics interface (Internal Graphics Device = IGFX) is enabled.

2.4.7.2 "PEG Port Configuration"

The following information applies to the following PEG slots (depending on the device type and device configuration, only a subset of these PEG slots may be visible):

- PEG-Slot 0:1:0
- PEG-Slot 0:1:1
- PEG-Slot 0:1:2

Calling "PEG Port Configuration"

Select: "Setup Utility (Page 8)" > "Advanced" > "System Agent (SA) Configuration" > "PEG Port Configuration".

Firmware setting	Value	Setting in delivery state		Meaning
		IPC627E IPC677E	IPC647E IPC847E	
Enable Root Port for PEG slot #	Disabled			PEG slot # is disabled.
	Enabled	x	x	PEG slot # is enabled.
Max Link Speed for PEG slot #	Auto	x	x	For PEG slot # , the maximum speed is set automatically or set to Gen1, Gen2 or Gen3.
	Gen1			
	Gen2			
	Gen3			

2.4.7.3 Level: "System Agent (SA) Configuration"

Calling "System Agent (SA) Configuration"

Select: "Setup Utility (Page 8)" > "Advanced" > "System Agent (SA) Configuration".

Firmware setting	Value	Setting in delivery state		Meaning
		IPC627E IPC677E	IPC647E IPC847E	
VT-d	Disabled			Hardware support for shared use of input/output devices across multiple virtual machines (VT-d; Intel® Virtualization Technology for Directed I/O) is disabled.
	Enabled	x	x	Hardware support for shared use of input/output devices across multiple virtual machines (VT-d; Intel® Virtualization Technology for Directed I/O) is enabled.

2.4.8 "PCH-IO Configuration"

2.4.8.1 "PCI Express Configuration"

"PCI Express Root Port #"

The following information applies to the following root ports (depending on the device type and device configuration, only a subset of these root ports may be visible):

- PCI Express Root Port 8
- PCI Express Root Port 9
- PCI Express Root Port 19
- PCI Express Root Port 20
- PCI Express Root Port 21

Calling "PCI Express Root Port #"

Select: "Setup Utility (Page 8)" > "Advanced" > "PCH-IO Configuration" > "PCI Express Configuration" > "PCI Express Root Port #".

Firmware setting	Value	Setting in delivery state		Meaning
		IPC627E IPC677E	IPC647E IPC847E	
PCIe Speed	Auto	x	x	Automatically determines the optimum speed for the PCIe expansion cards connected to PCIe-Root-Port # .
	Gen1			Compatibility setting for PCIe expansion cards that do not react stably according to specification. The speed is throttled to Gen1 according to specification.
	Gen2			Compatibility setting for PCIe expansion cards that do not react stably according to specification. The speed is throttled to Gen2 according to specification.
	Gen3			Compatibility setting for PCIe expansion cards that do not react stably according to specification. The speed is throttled to Gen3 according to specification.
Detect Timeout	0..65535	0	0	Time period in ms before the port is disabled if no feedback is received.

2.4.8.2 "SATA And RST Configuration"

Calling "SATA And RST Configuration"

Select: "Setup Utility (Page 8)" > "Advanced" > "PCH-IO Configuration" > "SATA And RST Configuration".

Firmware setting	Value	Setting in delivery state		Meaning
		IPC627E IPC677E	IPC647E IPC847E	
SATA Mode Selection	AHCI			The SATA controller works with the AHCI mode.
	Intel RST Premium With Intel Optane System Acceleration	x	x	The SATA controller works with the Intel® SATA driver.
PCIe Storage Dev On Port 21 (only if "SATA Mode Selection" = "Intel RST Premium With Intel Optane System Acceleration")	RST Controlled	x	x	Intel RST (Rapid Storage Technology) PCIe Storage Remapping is enabled for PCH Root Port 21.
	Not RST Controlled			Intel RST (Rapid Storage Technology) PCIe Storage Remapping is disabled for PCH Root Port 21.
Hot Plug for SATA Port 0 • Only with: IPC647E IPC847E	Disabled			The Hot-Plug-capability for SATA Port 0 is disabled.
	Enabled		x	The Hot-Plug capability for SATA Port 0 is enabled.
Hot Plug for SATA Port 1 • Only with: IPC647E IPC847E	Disabled			The Hot-Plug-capability for SATA Port 1 is disabled.
	Enabled		x	The Hot-Plug capability for SATA Port 1 is enabled.
Hot Plug for SATA Port 2 • Only with: IPC627E IPC677E IPC847E	Disabled			The Hot-Plug capability for SATA Port 2 is disabled.
	Enabled	x	x	The Hot-Plug-capability for SATA Port 2 is enabled.

Firmware setting	Value	Setting in delivery state		Meaning
		IPC627E IPC677E	IPC647E IPC847E	
Hot Plug for SATA Port 3 <ul style="list-style-type: none"> Only with: IPC627E IPC677E IPC847E 	Disabled			The Hot-Plug-capability for SATA Port 3 is disabled.
	Enabled	x	x	The Hot-Plug-capability for SATA Port 3 is enabled.
Hot Plug for SATA Port 4 <ul style="list-style-type: none"> Only with: IPC627E IPC677E IPC847E 	Disabled			The Hot-Plug capability for SATA Port 4 is disabled.
	Enabled	x	x	The Hot-Plug-capability for SATA Port 4 is enabled.
Hot Plug for SATA Port 5	Disabled			The Hot-Plug-capability for SATA Port 5 is disabled.
	Enabled	x	x	The Hot-Plug-capability for SATA Port 5 is enabled.

2.4.8.3 "HD Audio Configuration"

Calling "HD Audio Configuration"

Select: "Setup Utility (Page 8)" > "Advanced" > "PCH-IO Configuration" > "HD Audio Configuration".

Firmware setting	Value	Setting in delivery state		Meaning
		IPC627E IPC677E	IPC647E IPC847E	
HD Audio • Only with: IPC647E IPC847E	Disabled			The onboard High Definition Audio Controller is disabled.
	Enabled		x	The onboard High Definition Audio Controller is enabled.

2.4.8.4 Level: "PCH-IO Configuration"

Calling "PCH-IO Configuration"

Select: "Setup Utility (Page 8)" > "Advanced" > "PCH-IO Configuration".

Firmware setting	Value	Setting in delivery state		Meaning
		IPC627E IPC677E	IPC647E IPC847E	
State After G3	S5 State			Following power failure (state: G3) and subsequent voltage restoration, the device remains switched off.
	S0 State	x	x	Following power failure (state: G3) and subsequent voltage restoration, the device switches on automatically.

2.4.9 "PCH-FW Configuration"

2.4.9.1 Level: "PCH-FW Configuration"

Calling "PCH-FW Configuration"

Select: "Setup Usability (Page 8)" > "Advanced" > "PCH-FW Configuration".

Firmware setting	Value	Setting in delivery state		Meaning
		IPC627E IPC677E	IPC647E IPC847E	
Manageability Features State	Disabled	x	x	The Intel® Manageability functions are disabled.
	Enabled			The Intel® Manageability functions are enabled.
<ul style="list-style-type: none"> AMT BIOS Features (only if "Manageability Features State" = Enabled)	Disabled			Intel® Management Engine BIOS Extension (MEBx) is disabled.
	Enabled	x	x	Intel® Management Engine BIOS Extension (MEBx) is enabled and can be used to configure the Intel® Active Management Technology (iAMT) hardware.

2.4.9.2 "AMT Configuration"

Calling "AMT Configuration"

Select: "Setup Usability (Page 8)" > "Advanced" > "PCH-FW Configuration" > "AMT Configuration".

Firmware setting	Value	Setting in delivery state		Meaning
		IPC627E IPC677E	IPC647E IPC847E	
ASF Support	Disabled			ASF support (Alert Standard Format) is disabled.
	Enabled	x	x	ASF support (Alert Standard Format) is enabled.
USB Provisioning of AMT	Disabled	x	x	The USB configuration (USB Provisioning) from Intel® Active Management Technology (iAMT) is disabled.
	Enabled			The USB configuration (USB Provisioning) from Intel® Active Management Technology (iAMT) is enabled.

"CIRA Configuration"

Calling "CIRA Configuration"

Select: "Setup Usability (Page 8)" > "Advanced" > "PCH-FW Configuration" > "AMT Configuration" > "CIRA Configuration".

Firmware setting	Value	Setting in delivery state		Meaning
		IPC627E IPC677E	IPC647E IPC847E	
Activate Remote Assistance Process	[Option disabled]	x	x	CIRA (Client Initiated Remote Access, "Fast Call For Help") is disabled.
	[Option enabled]			CIRA (Client Initiated Remote Access, "Fast Call For Help") is enabled. CIRA allows AMT maintenance even if the AMT PC is not in the intranet. ("Network Access" must be enabled in the Intel® Management Engine BIOS Extension (MEBx).)
CIRA Timeout	0..255	0	0	CIRA Timeout in seconds for connection setup with MPS (Manageability Presence Server) 0 = A default value of 60 seconds is taken for CIRA Timeout. 255 = The Intel® Management Engine BIOS Extension (MEBx) waits until the connection is established.

"OEM Flags Settings"

Calling "OEM Flag Settings"

Select: "Setup Usability (Page 8)" > "Advanced" > "PCH-FW Configuration" > "AMT Configuration" > "OEM Flags Settings".

Firmware setting	Value	Setting in delivery state		Meaning
		IPC627E IPC677E	IPC647E IPC847E	
Hide Unconfigure ME Confirmation Prompt	[Option disabled]	x	x	On resetting with Unconfigure, a confirmation prompt is shown.
	[Option enabled]			On resetting with Unconfigure, NO confirmation prompt is shown.
Unconfigure ME	[Option disabled]	x	x	All values of the Intel® Management Engine BIOS Extension (MEBx) remain unchanged.
	[Option enabled]			If the "Hide Unconfigure ME Confirmation Prompt" option is disabled, a confirmation prompt for performing the "Unconfigure ME" action is displayed at the next startup. If you perform this action, all values of the Intel® Management Engine BIOS Extension (MEBx) including the MEBx password are reset to default values.

2.4.10 "Fan Control Configuration"

Calling "Fan Control Configuration"

Select: "Setup Utility (Page 8)" > "Advanced" > "Fan Control Configuration".

Firmware setting	Value	Setting in delivery state		Meaning
		IPC627E IPC677E	IPC647E IPC847E	
Fan Control Mode	Enhanced			At high temperatures, the fan speed is automatically increased to maintain processor performance through cooling.
	Standard	x	x	The fan speed is automatically adjusted. Cooling and processor performance are balanced in this case.
	Silent			In case of temperature fluctuations, the processor performance is automatically adjusted to the temperature before the fan speed is adjusted. The fans are quieter, but the processor performance also decreases.
	Disabled			Fan speed control is disabled. The fans always run at full speed.

2.4.11 Level: "Advanced" tab

Calling "Advanced"

Select: "Setup Utility (Page 8)" > "Advanced".

Firmware setting	Value	Setting in delivery state		Meaning
		IPC627E IPC677E	IPC647E IPC847E	
HPET - HPET Support	Disabled			The high-precision event timer for multimedia HPET (High Precision Event Timer) is disabled.
	Enabled	x	x	The high-precision event timer for multimedia HPET (High Precision Event Timer) is enabled.

2.5 "Security" tab

2.5.1 Level: "Security" tab

Calling "Security" tab

Select: "Setup Utility (Page 8)" > "Security".

Firmware setting	Value	Setting in delivery state		Meaning
		IPC627E IPC677E	IPC647E IPC847E	
TPM Availability (only if TPM is present in the hardware)	Available	x	x	The TPM (Trusted Platform Module) is visible in the operating system.
	Hidden			The TPM (Trusted Platform Module) is not visible in the operating system.
TPM Operation (only if TPM is present in the hardware)	No Operation	x	x	The status of the TPM (Trusted Platform Module) is not changed.
	Enable			The status of the TPM (Trusted Platform Module) is changed dependent on the selected action.
	SetPCRBanks (Algorithm)			The status of the TPM (Trusted Platform Module) is changed dependent on the selected action. Note: <ul style="list-style-type: none"> • PP = Physical Presence • PCRs = Platform Configuration Registers • EPS = Endorsement Primary Seed
	LogAllDigests			
	SetPPRe-quiredFor-Clear_True			
	SetPPRe-quiredFor-Clear_False			
	SetPPRe-quiredFor-TurnOn_False			
	SetPPRe-quiredFor-TurnOn_True			
	SetPPRe-quiredFor-TurnOff_False			
	SetPPRe-quiredFor-TurnOff_True			

Firmware setting	Value	Setting in delivery state		Meaning
		IPC627E IPC677E	IPC647E IPC847E	
TPM Operation (only if TPM is present in the hardware)	SetPPRequiredForChangePCRs_False			
	SetPPRequiredForChangePCRs_True			
	SetPPRequiredForChangeEPS_False			
	SetPPRequiredForChangeEPS_True			
	ChangeEPS			
Clear TPM (only if TPM is present in the hardware)	[Option disabled]	x	x	The content of the TPM (Trusted Platform Module) remains unchanged.
	[Option enabled]			The content of the TPM (Trusted Platform Module) is deleted.
Password Management Interface	Enabled	x	x	The interface for password configuration is enabled. The password settings can be configured via the software. You need the current password to make changes.
	Disabled			The interface for password configuration is disabled. The password settings can only be configured via the firmware settings.

Firmware setting	Value	Setting in delivery state		Meaning
		IPC627E IPC677E	IPC647E IPC847E	
Set Supervisor Password				<p>Here you can set a general password for full access to the firmware settings.</p> <p>A password prompt then appears before the firmware is opened. After correct entry of the general password, it can be changed by entering a new one. If no password is entered and only the <Return> key is pressed, the configured general password is deleted, thereby disabling the password prompt again.</p> <p>NOTICE:</p> <p>If you lose the general password that you defined during firmware setup, the device must be reset by the manufacturer.</p> <ul style="list-style-type: none"> • Make a note of the general password and keep it in a safe place. • Protect the general password from unauthorized access.
<ul style="list-style-type: none"> • Power on Password <p>(only if a "Supervisor Password" was set up)</p>	Enabled			A password prompt is displayed for every boot procedure. The general password or a user password must be entered.
	Disabled	x	x	A password prompt appears only when the setup utility is opened. The general password or a user password must be entered.
<ul style="list-style-type: none"> • User Access Level <p>(only if a "Supervisor Password" was set up)</p>	View Only			Only read access to Setup utility is permitted. Firmware settings cannot be changed.
	Limited			Restricted write access to Setup utility is permitted. Only certain firmware settings can be changed.
	Full	x	x	Unrestricted write access to the Setup utility is permitted. All firmware settings except the general password (Supervisor Password) can be changed.
<ul style="list-style-type: none"> • User Boot Manager Access <p>(only if a "Supervisor Password" was set up)</p>	Disabled	x	x	The general password is required to enter the Boot Manager.
	Enabled			A user password is sufficient to start the Boot Manager.

Firmware setting	Value	Setting in delivery state		Meaning
		IPC627E IPC677E	IPC647E IPC847E	
Set User Password				Here you can set a user password for limited access to the firmware settings. After correct entry of the user password, it can be changed by entering a new one. If no password is entered and only the <Return> key is pressed, the configured user password is deleted.
<ul style="list-style-type: none"> • Clear User Password (only if a "User Password" was set up) 				Here you can delete the user password.

2.6 "Power" tab

2.6.1 Level: "Power" tab

Device behavior after a power failure and after a "wake event".

Calling "Power" tab

Select: "Setup Utility (Page 8)" > "Power".

Firmware setting	Value	Setting in delivery state		Meaning
		IPC627E IPC677E	IPC647E IPC847E	
Wake on PME	Disabled			If a power management event occurs, the device does not switch on.
	Enabled	x	x	If a power management event occurs, the device switches on.
Auto Wake on S5	Disabled	x	x	The device does not switch on when it is in the S5 (= Soft Off) operating state.
	By Every Day			The device switches on each day when it is in the S5 operating state. You set the time for switching on the device with "Wake on S5 Time".
	By Day of Month			The device switches on each month when it is in the S5 operating state. You set the time for switching on the device with "Wake on S5 Time". You set the day of the month for switching on the device with "Day of Month".
<ul style="list-style-type: none"> Wake on S5 Time (only if "Auto Wake on S5" = "By Every Day" or "By Day of Month") 	00:00:00 23:59:59	00:00:00	00:00:00	You set the time for switching on the device with "Wake on S5 Time". Format: [Hour:Minute:Second] You can use the <Enter> key to move within a format, for example, from hour to minute. Set the desired time values with the [+] and [-] buttons. You can also enter the numbers directly.
<ul style="list-style-type: none"> Day of Month (only if "Auto Wake on S5" = "By Day of Month") 	1..31	1	1	You set the day of the month for switching on the device with "Day of Month". Format: Numbers from 1 to 31 Set the desired day with the [+] and [-] buttons. You can also enter the number directly with <Return>.

Firmware setting	Value	Setting in delivery state		Meaning
		IPC627E IPC677E	IPC647E IPC847E	
Wake on LAN 1 (X1 P1)	Disabled			The LAN controller of the onboard Ethernet interface "X1 P1" cannot switch on the device.
	Enabled	x	x	The LAN controller of the onboard Ethernet interface "X1 P1" can switch on the device.
Wake on LAN 2 (X2 P1)	Disabled			The LAN controller of the onboard Ethernet interface "X2 P1" cannot switch on the device.
	Enabled	x	x	The LAN controller of the onboard Ethernet interface "X2 P1" can switch on the device. Requirement: The firmware setting "Wake on PME" must be set to "Enabled".
Wake on LAN 3 (X3 P1)	Disabled			The LAN controller of the onboard Ethernet interface "X3 P1" cannot switch on the device.
	Enabled	x	x	The LAN controller of the onboard Ethernet interface "X3 P1" can switch on the device. Requirement: The firmware setting "Wake on PME" must be set to "Enabled".
USB Ports 1/3 (USB Slot Adapter) powered	Disabled			The respective USB port is not supplied with voltage during operation.
	Enabled	x	x	The respective USB port is supplied with voltage during operation. When "Wake Capability" is selected as well (Enabled), the USB port is also supplied with voltage in sleep mode.
<ul style="list-style-type: none"> USB Ports 1/3 (USB Slot Adapter) Wake Cap (only if "USB Ports 1/3 (USB Slot Adapter) powered" = Enabled)	Disabled	x	x	The respective USB port cannot switch on the device.
	Enabled			The respective USB port can switch on the device.

Firmware setting	Value	Setting in delivery state		Meaning
		IPC627E	IPC647E	
		IPC677E	IPC847E	
USB Ports 2/7 (X65/X64) powered	Disabled			The respective USB port is not supplied with voltage during operation.
	Enabled	x	x	The respective USB port is supplied with voltage during operation. When "Wake Capability" is selected as well (Enabled), the USB port is also supplied with voltage in sleep mode.
<ul style="list-style-type: none"> USB Ports 2/7 (X65/X64) Wake Capability (only if "USB Ports 2/7 (X65/X64)" = Enabled)	Disabled	x	x	The respective USB port cannot switch on the device.
	Enabled			The respective USB port can switch on the device.
USB Port 4 (X61) powered	Disabled			The respective USB port is not supplied with voltage during operation.
	Enabled	x	x	The respective USB port is supplied with voltage during operation. When "Wake Capability" is selected as well (Enabled), the USB port is also supplied with voltage in sleep mode.
<ul style="list-style-type: none"> USB Port 4 (X61) Wake Capability (only if "USB Port 4 (X61) powered" = Enabled)	Disabled	x	x	The respective USB port cannot switch on the device.
	Enabled			The respective USB port can switch on the device.
USB Port 5 (X63) powered	Disabled			The respective USB port is not supplied with voltage during operation.
	Enabled	x	x	The respective USB port is supplied with voltage during operation. When "Wake Capability" is selected as well (Enabled), the USB port is also supplied with voltage in sleep mode.
<ul style="list-style-type: none"> USB Port 5 (X63) Wake Capability (only if "USB Port 5 (X63) powered" = Enabled)	Disabled	x	x	The respective USB port cannot switch on the device.
	Enabled			The respective USB port can switch on the device.

Firmware setting	Value	Setting in delivery state		Meaning
		IPC627E IPC677E	IPC647E IPC847E	
USB Port 6 (X62) powered	Disabled			The respective USB port is not supplied with voltage during operation.
	Enabled	x	x	The respective USB port is supplied with voltage during operation. When "Wake Capability" is selected as well (Enabled), the USB port is also supplied with voltage in sleep mode.
<ul style="list-style-type: none"> USB Port 6 (X62) Wake Capability (only if "USB Port 6 (X62) powered" = Enabled) 	Disabled	x	x	The respective USB port cannot switch on the device.
	Enabled			The respective USB port can switch on the device.
USB Ports 8/12 (USB2 P8/P12) powered	Disabled			The respective USB port is not supplied with voltage during operation.
	Enabled	x	x	The respective USB port is supplied with voltage during operation. When "Wake Capability" is selected as well (Enabled), the USB port is also supplied with voltage in sleep mode.
<ul style="list-style-type: none"> USB Ports 8/12 (USB2 P8/P12) Wake Cap (only if "USB Port 8/12 (USB2 P8/P12) powered" = Enabled) 	Disabled	x	x	The respective USB port cannot switch on the device.
	Enabled			The respective USB port can switch on the device.

Firmware setting	Value	Setting in delivery state		Meaning
		IPC627E IPC677E	IPC647E IPC847E	
USB Ports 9/13 (Front) powered <ul style="list-style-type: none"> Only with: IPC647E IPC847E 	Disabled			The respective USB port is not supplied with voltage during operation.
	Enabled		x	The respective USB port is supplied with voltage during operation. When "Wake Capability" is selected as well (Enabled), the USB port is also supplied with voltage in sleep mode.
<ul style="list-style-type: none"> USB Ports 9/13 (Front) Wake Capability (only if "USB Ports 9/13 (Front) powered" = Enabled) Only with: IPC647E IPC847E 	Disabled		x	The respective USB port cannot switch on the device.
	Enabled			The respective USB port can switch on the device.
USB Ports 9/13 (USB2 P9/P13) powered <ul style="list-style-type: none"> Only with: IPC627E IPC677E 	Disabled			The respective USB port is not supplied with voltage during operation.
	Enabled	x		The respective USB port is supplied with voltage during operation. When "Wake Capability" is selected as well (Enabled), the USB port is also supplied with voltage in sleep mode.
<ul style="list-style-type: none"> USB Ports 9/13 (USB2 P9/P13) Wake Cap (only if "USB Ports 9/13 (USB2 P9/P13) powered" = Enabled) Only with: IPC627E IPC677E 	Disabled	x		The respective USB port cannot switch on the device.
	Enabled			The respective USB port can switch on the device.

Firmware setting	Value	Setting in delivery state		Meaning
		IPC627E IPC677E	IPC647E IPC847E	
USB Port 10 (USB3 P7) powered • Only with: IPC647E IPC847E	Disabled			The respective USB port is not supplied with voltage during operation.
	Enabled		x	The respective USB port is supplied with voltage during operation. When "Wake Capability" is selected as well (Enabled), the USB port is also supplied with voltage in sleep mode.
• USB Port 10 (USB3 P7) Wake Capability (only if "USB Port 10 (USB3 P7) powered" = Enabled) • Only with: IPC647E IPC847E	Disabled		x	The respective USB port cannot switch on the device.
	Enabled			The respective USB port can switch on the device.
USB Port 11 (USB3 P7) powered • Only with: IPC627E IPC677E	Disabled			The respective USB port is not supplied with voltage during operation.
	Enabled	x		The respective USB port is supplied with voltage during operation. When "Wake Capability" is selected as well (Enabled), the USB port is also supplied with voltage in sleep mode.
• USB Port 11 (USB3 P7) Wake Capability (only if "USB Port 11 (USB3 P7) powered" = Enabled) • Only with: IPC627E IPC677E	Disabled	x		The respective USB port cannot switch on the device.
	Enabled			The respective USB port can switch on the device.

Firmware setting	Value	Setting in delivery state		Meaning
		IPC627E IPC677E	IPC647E IPC847E	
USB Port 14 (X60) powered	Disabled			The respective USB port is not supplied with voltage during operation.
	Enabled	x	x	The respective USB port is supplied with voltage during operation. When "Wake Capability" is selected as well (Enabled), the USB port is also supplied with voltage in sleep mode.
<ul style="list-style-type: none"> USB Port 14 (X60) Wake Capability (only if "USB Port 14 (X60) powered" = Enabled) 	Disabled	x	x	The respective USB port cannot switch on the device.
	Enabled			The respective USB port can switch on the device.

2.7 "Boot" tab

2.7.1 Level: "Boot" tab

Boot behavior of the device, bootable device components (boot media) and boot order.

Calling "Boot" tab

Select: "Setup Utility (Page 8)" > "Boot".

Firmware setting	Value	Setting in delivery state		Meaning	
		IPC627E IPC677E	IPC647E IPC847E		
Quick Boot	Enabled	x	x	Quick start of the device is enabled. During the boot procedure, various hardware function tests are skipped. This shortens the boot procedure.	
	Disabled			Quick start of the device is disabled.	
Quiet Boot	Enabled	x	x	The boot logo is displayed during the self-test.	
	Disabled			Start information appears in text mode during the self-test.	
Network Stack	Disabled	x	x	The UEFI Network Stack for network access under UEFI is not available. For example, UEFI installation via PXE (Preboot Executable Environment) is not possible.	
	Enabled			The UEFI Network Stack for network access under UEFI is available.	
<ul style="list-style-type: none"> PXE Boot capability (only if "Network Stack" = Enabled)	Disabled	x	x	Booting via PXE (Preboot Executable Environment) is disabled. Only UEFI Network Stack is supported.	PXE = Preboot Executable Environment Controls the booting of a boot image that can be loaded over the network.
	UEFI:IPv4			Only UEFI boot media that support Internet protocol version 4 are considered as PXE boot media.	
	UEFI:IPv6			Only UEFI boot media that support Internet protocol version 6 are considered as PXE boot media.	
	UEFI:IPv4/IPv6			Only UEFI boot media that support Internet protocol version 4 or version 6 are considered as PXE boot media.	

Firmware setting	Value	Setting in delivery state		Meaning
		IPC627E IPC677E	IPC647E IPC847E	
Add Boot Options	First			Newly detected boot media are placed at the top of the boot order.
	Auto	x	x	Newly detected boot media are placed automatically in the boot order, e.g. dependent on the device path for UEFI boot media.
	Last			Newly detected boot media are placed at the bottom of the boot order.
USB Boot	Enabled			Booting from USB devices is permitted.
	Disabled	x	x	Booting from USB devices is not permitted.
SATA Boot	Enabled	x	x	Booting from SATA devices is permitted.
	Disabled			Booting from SATA devices is not permitted.
Timeout	0..10	0	0	Delay time in seconds during booting so that the user has time to press the hotkey to open the firmware selection menu.

2.7.2 "EFI"

List of boot media.

Calling "EFI"

Select: "Setup Utility (Page 8)" > "Boot" > "EFI".

- If "Add Boot Options" = "Auto", the boot media is grayed out and cannot be changed.
- If "Add Boot Options" = "First" or "Last", the following can be changed:
 - Sequence of the boot media: <F6>, <F5> or <+>, <-> keys
 - List of valid boot media: <Return> button

2.8 "Exit" tab

2.8.1 Level: "Exit" tab

Exit the Setup utility. You have the following options for saving or discarding the changes you made:

Calling "Exit"

Choose: "Setup Utility (Page 8)" > "Exit".

Firmware setting	Meaning
Exit Saving Changes	All changes are saved. The device is restarted with the changed firmware settings.
Save Change Without Exit	All changes are saved. Setup utility remains open.
Exit Discarding Changes	Setup Utility is closed. All changes are discarded.
Load Optimal Defaults	The firmware settings are reset to the safe default values. The delivery state is restored. NOTICE: All current firmware settings are overwritten.
Load Custom Defaults	The user-specific profile with the user-specific firmware settings is loaded. Requirement: The firmware settings were previously saved as user-specific profile with "Save Custom Defaults". NOTICE: All current firmware settings are overwritten when loading the user-specific profile with "Load Custom Defaults".
Save Custom Defaults	The current firmware settings are saved as a user-specific profile (see also "Load Custom Defaults").
Discard Changes	All changes to the firmware settings are discarded.
Save setup settings to file	The current firmware settings are written to a file.
Load setup settings from file	Firmware settings are loaded from a file.

Configuring Intel® Management Engine BIOS Extension (MEBx)

3

3.1 Logging onto MEBx (assigning password)

Procedure

1. Open the firmware selection menu (Page 7).
2. Select the "Intel(R) Management Engine BIOS Extension" option on the "Main Page" with the arrow keys.
3. Confirm your selection with the <Return> key.
4. In the "MAIN MENU" of the MEBx, select the "MEBx Login" option.
5. Enter the following "**Intel(R) ME Password**" when logging on the first time:
admin
6. Afterwards, change the password immediately.

The new password must contain the following characters:

- A total of at least eight characters
- An upper case letter
- A lower case letter
- A number
- A special character . ! @ # \$ % ^ & *

Note

The underscore and blank space are valid password characters but do not increase password complexity.

3.2 Options of the MEBx

Use "Intel® Management Engine BIOS Extension" (MEBx) to configure important firmware settings of your device to use Intel® AMT functions and the Intel® Management Engine (ME). The following options are available for Intel® AMT-enabled devices:

- Intel(R) ME General Settings
- Intel(R) AMT
- Intel(R) AMT Configuration
- MEBx Exit

Requirement for the use of "Intel® Management Engine BIOS Extension" (MEBx)

- The firmware setting "AMT BIOS Features" is assigned the value "Enabled". You can find information on this under Level: "PCH-FW Configuration" (Page 26).

Note

The MEBx setting options depend on whether or not your device supports Intel® AMT.

Intel(R) ME General Settings

MEBx setting	Meaning
Change ME Password	Here, you can change the current password for logging onto MEBx. You can find information on this under "Logging onto MEBx (assigning password) (Page 44)".
FW Update	Firmware updates of the "Intel® Management Engine" (ME) can be installed, not installed or only installed after entering the password.

Intel(R) AMT

MEBx setting	Meaning
Intel(R) AMT	When Intel® Active Management Technology (iAMT) is disabled, all network settings are reset to the settings in the delivery state.

Intel(R) AMT Configuration

MEBx setting	Meaning
Manageability Feature Selection	Intel® AMT functions are enabled or disabled. In the delivery state, "Manageability Feature Selection" = Disabled.
SOL/Storage Redirection/KVM (only if "Manageability Feature Selection" = Enabled)	Enabling and disabling of the Intel® AMT functions: <ul style="list-style-type: none"> • SOL • Storage Redirection • KVM Feature Selection
User Consent (only if "Manageability Feature Selection" = Enabled)	User Consent settings. Forces the following additional security behavior: When a user attempts to establish a KVM connection remotely, a six-digit number is displayed on the AMT PC. The remote user must enter this number on the help desk PC before the KVM connection can be opened.
Password Policy (only if "Manageability Feature Selection" = Enabled)	Password policy that specifies the conditions under which the password is permitted to be changed remotely. The following options can be selected: <ul style="list-style-type: none"> • Default Password Only • During Setup And Configuration • Anytime
Network Setup (only if "Manageability Feature Selection" = Enabled)	The following network settings can be configured: Intel(R) ME Network Name Settings <ul style="list-style-type: none"> • Host Name • Domain Name • Shared/Dedicated FQDN • Dynamic DNS Update TCP/IP Settings > Wired LAN IPV4 Configuration <ul style="list-style-type: none"> • DHCP mode
Activate Network Access (only if "Manageability Feature Selection" = Enabled)	Enables the network interface. This MEBx setting is only available when the network is not enabled.
Unconfigure Network Access (only if "Manageability Feature Selection" = Enabled)	Disables the network interface and resets the network settings to their default values.
Remote Setup And Configuration (only if "Manageability Feature Selection" = Enabled)	Displays the current provisioning settings.
Power Control (only if "Manageability Feature Selection" = Enabled)	Specifies the power states (S0, S3, S4, S5) of the computer in which MEBx is enabled.

MEBx Exit

Exiting MEBx. The changes are saved.

Further information

More information about MEBx can be found here: Intel® website (<https://www.intel.com>).

Configuring Intel® AMT

To make use of "Intel® Active Management Technology ", proceed as follows:

- First, enable the Intel® AMT functions in the firmware settings of the Setup Utility.
- Then, configure the Intel® AMT functions with Intel® Management Engine BIOS Extension

Enabling and configuring Intel® AMT functions

1. Open "Setup Utility (Page 8)".
2. Assign the "Enabled" value to the firmware setting "AMT BIOS Features". You can find information on this under "Level: "PCH-FW Configuration" (Page 26)".
3. Press the <ESC> key to return to the firmware selection menu.
4. Select the "Intel(R) Management Engine BIOS Extension" option and configure the Intel® AMT functions again. You can find information on this under "Options of the MEBx (Page 45)".

Reset Intel® AMT functions to default settings and disabling iAMT

One effect of resetting to the default settings is that Intel® AMT is disabled.

1. Open "Setup Utility (Page 8)".
2. Enable the firmware setting "Unconfigure ME". You can find information on this under "OEM Flags Settings" (Page 28).

If the "Hide Unconfigure ME Confirmation Prompt" option is disabled, a confirmation prompt for performing the "Unconfigure ME" action is displayed at the next startup. If you perform this action, all values of the Intel® Management Engine BIOS Extension (MEBx) including the MEBx password are reset to default values.

Disabling Intel® AMT access to the firmware/BIOS settings

You can prevent access to firmware/BIOS settings with Intel® AMT

This may be necessary, for example, in the following cases:

- When you are no longer using Intel® AMT.
- You want to ensure that Intel® AMT is not used without authorization.

For this, you need to disable iAMT as described in the previous section.

All Intel® AMT functions are thereby reset to default settings.

Update firmware

Firmware/BIOS updates are regularly available for your device. You can download these from the Internet.

Backing up firmware settings before updating the firmware

NOTICE

Risk of irretrievable loss of data

After a firmware/BIOS update all firmware settings are deleted.

This can put the system in an undefined state. The consequence may be damage to the device or system.

- Before updating your firmware, back up the current firmware settings by writing them to a file.

You can find information on this under "Level: "Exit" tab (Page 43)".

Procedure

1. Open the "SIEMENS Industry Online Support (<https://support.industry.siemens.com/cs/ww/en/view/75842768>)" page.
2. Navigate to your device in the area "Online Support; Drivers and BIOS Updates for download".
3. Download the current firmware/BIOS version in the download area.
Registration is required for this.
4. Install the current firmware/BIOS update on your device following the instructions accompanying the download.
5. Change the firmware settings as required for your application. If necessary, use the previously created file with the previous firmware settings for this.
6. Save the firmware settings.

Booting from USB stick

Note

The "USB Boot" option has to be set to "Enabled" in the "Boot" tab so that the device can boot from the USB stick.

1. Connect the USB stick to the device.
2. Open the firmware selection menu (Page 7).
3. Select "Boot-Manager."
4. Select the USB medium in the "Boot-Manager" and confirm the entry.

Enable Trusted Platform Module (TPM)

Depending on the ordered configuration, your device may have a Trusted Platform Module. The Trusted Platform Module is a chip that enhances your device with security functions. This provides improved protection against device manipulation.

You enable use of the Trusted Platform Module in the firmware settings.

NOTICE
Import restrictions for the Trusted Platform Module
Use of the Trusted Platform Module is subject to legal restrictions in some countries and is not permitted in these countries.
<ul style="list-style-type: none">• Always observe the import restrictions of the country in which the device will be operated.

Procedure

1. Check your order documents to find out whether a Trusted Platform Module is present on your device.
2. Open the "Security" tab. You can find information on this under "Level: "Security" tab (Page 30)".
3. Ensure that the "Available" value is assigned to firmware setting "TPM Availability".
4. Save the changes you made before closing the Setup Utility. You can find information on this under ""Exit" tab (Page 43)".

Configuring automatic switch-on of device

You can specify that the device should automatically switch on again after disconnection from the supply voltage lasting at least 20 ms as soon as the supply voltage is available again. The exact minimum supply voltage failure time that is required is dependent on the device equipment and the application.

 **CAUTION**

Danger from undesired startup of device after power failure

Automatic startup of the device, for example, after a power failure, can result in undesired reactions of the machine or system and endanger operation.

During system planning, check whether this automatic startup of your machine or system poses a safety risk and then change the device behavior appropriately.

Procedure

1. Call "PCH-IO Configuration". You can find information on this under "Level: "PCH-IO Configuration" (Page 25)".
2. Assign the value "S0 State" to the firmware setting "State After G3".
3. Save the changes you made before closing the Setup Utility. You can find information on this under "Level: "Exit" tab (Page 43)".

Configuring multi-monitoring

You can operate several monitors on one device at the same time.

For multi-monitoring you can use the integrated onboard graphics interface (Internal Graphics Device = IGFX) and the graphics interface of the external graphics card (PEG graphics card) at the same time.

Under "Graphics Configuration" (Page 19), assign the following values to the corresponding firmware settings. These settings are already configured as defaults in the delivery state.

Firmware setting	Value
Primary Display	IGFX
Internal Graphics	Enabled

Index

"

- "Advanced" tab, 29
 - PCH-FW Configuration, 26
 - Boot Configuration, 11
 - PCH-FW Configuration; AMT Configuration, 27
 - Power & Performance, CPU Configuration, 16
 - Fan Control Configuration, 28
 - System Agent (SA) Configuration, 21
 - PCH-IO Configuration, 25
 - Memory Configuration, 18
 - PCH-FW Configuration; AMT Configuration, 27
 - PCH-FW Configuration, 26
 - PCH-IO Configuration, 25
 - PCH-IO Configuration; PCI Express Configuration, System Agent (SA) Configuration, 21
 - Peripheral Configuration, 12
 - PCH-IO Configuration, 25
 - SATA Configuration, 15
 - System Agent (SA) Configuration, 21
- "Boot" tab, 41
- "Exit" tab, 43
- "Main" tab
 - Device information, 9
 - System Time and System Date, 10
- "Power" tab, 34
- "Security" tab, 30

A

- Activate Network Access, 46
- Activate Remote Assistance Process, 27
- Active Processor Cores, 16
- Add Boot Options, 42
- Administer Secure Boot, 7
- Advanced Encryption Standard, (AES) AES, 16
- AMT BIOS Features, 26
- AMT Configuration, 27
- ASF Support, 27
- Auto Wake on S5, 34

B

- Base I/O Address
 - COM1 port, 12
 - COM2 port, 12
- BIOS Number, (Firmware version > Article number)
- BIOS Setup, 3
- BIOS update, 7
- BIOS Version, (Firmware version)
- Board ID, 9
- Boot behavior
 - Configuring, 41
- Boot Configuration, 11
- Boot From File, 7
- Boot Manager, 7
- Boot media, 41
- Boot order, 41
- Boot procedure
 - Configuring, 11

C

- C states, 17
- Cache RAM, 9
- Change ME Password, 45
- CIRA Configuration, 27
- CIRA Timeout, 27
- Clear TPM, 31
- Clear User Password, 33
- COM1 port
 - Configuring, 12
 - I/O basic address, 12
 - Interrupt, 12
- COM2 port
 - Configuring, 12
 - I/O basic address, 12
 - Interrupt, 13
- Configure security settings, 30
- Configuring multi-monitoring, 53
- Configuring power supply of the device, 34
- CPB Ver, 9
- CPU - Power Management Control, 17
- CPU Type, 9
- CPU Configuration, 16
- CPU speed, 9
- CPU Speed, 9

CPU Stepping, 9
 CPU type, 9
 CPU version, 9

D

Day of Month, 34
 Default values
 Restoring, (Delivery state), (Delivery state), (Delivery state), (Delivery state)
 Delivery state
 Restoring, 8, 43
 Detect Timeout
 PCI Express Root Port 19, 22
 PCI Express Root Port 20, 22
 PCI Express Root Port 21, 22
 PCI Express Root Port 8, 22
 PCI Express Root Port 9, 22
 Device date
 Setting, 10
 Device information, 9
 Device Management, 7
 Device Manager, (Device Management)
 Device time
 Setting, 10
 Discard Changes, 43

E

ECC Support, 18
 EFI, 42
 Enable Root Port, 20
 EPOCH, 16
 Error Correction, 18
 Exit Discarding Changes, 43
 Exit Saving Changes, 43

F

Fan Control Configuration, 28
 Fan Control Mode, 28
 Fan speed
 Configuring, 28
 Firmware configuration menu, (Setup Utility)
 Firmware selection menu
 Opening, 7
 Firmware selection menu
 Options, 7
 Firmware version, 9, (Article number)
 FW Update, 45

G

General password
 Setting up, 32
 GOP Ver, 9
 Graphics Configuration, 19

H

HD Audio, 25
 HD Audio Configuration, 25
 HDC Control, 17
 Hide Unconfigure ME Confirmation Prompt, 28
 High Precision Event Timer, (HPET)
 HPET - HPET Support, 29
 Hyper-Threading, 16

I

Intel (VMX) Virtualization Technology, 16
 Intel ME Version / SKU, 9
 Intel(R) AMT, 45
 Intel(R) AMT Configuration, 46
 Intel(R) Management Engine BIOS Extension, 7
 Intel(R) ME General Settings, 45
 Intel(R) ME Password, 44
 Intel(R) Speed Shift Technology, 17
 Intel(R) SpeedStep(tm), 17
 Intel® Active Management Technology, 48
 Intel® Virtualization Technology for Directed I/O, 21
 Interfaces
 Configuring, 12
 Internal COM 1, 12
 Internal COM 2, 12
 Internal Graphics, 19
 Interrupt
 COM1 port, 12
 COM2 port, 13

K

KVM Feature Selection, 46

L

L2-Cache, 9
 L3-Cache, 9
 Load Custom Defaults, 43
 Load Optimal Defaults, 43
 Load setup settings from file, 43

- M**
 - Manageability Feature Selection, 46
 - Manageability Features State, 26
 - Max Link Speed, 20
 - Max TOLUD, 18
 - MEBx, (Intel® Management Engine BIOS Extension)
 - MEBx Exit, 47
 - Memory Configuration, 18
 - Microcode Rev, 9
 - Microcode version, 9

- N**
 - Network Setup, 46
 - Network Stack, 41
 - Number Of Processors, 9
 - Numerical keypad
 - Configure after starting the device, 11
 - Numlock, 11

- O**
 - OEM Flag Settings, 28
 - Onboard Ethernet 1 (LAN 1, X1 P1), 13
 - Onboard Ethernet 2 (LAN 2, X2 P1), 13
 - Onboard Ethernet 3 (LAN 3, X3 P1), 13

- P**
 - Password Management, 31
 - Password Management Interface, 31
 - Password Policy, 46
 - PCH Rev / SKU, 9
 - PCH-FW Configuration, 26
 - PCH-IO Configuration, 25
 - PCI Express Root Port #, 22
 - PCI Express Root Port 19, 22
 - PCI Express Root Port 20, 22
 - PCI Express Root Port 21, 22
 - PCI Express Root Port 8, 22
 - PCI Express Root Port 9, 22
 - PCIe Speed
 - PCI Express Root Port 19, 22
 - PCI Express Root Port 20, 22
 - PCI Express Root Port 21, 22
 - PCI Express Root Port 8, 22
 - PCI Express Root Port 9, 22
 - PCIe Storage Dev On Port 21, 23
 - PEG Port Configuration, 20
 - PEG-Slot 0:1:0, 20
 - PEG-Slot 0:1:1, 20
 - PEG-Slot 0:1:2, 20
 - Peripheral Configuration, 12
 - POST Errors, 11
 - Power Control, 46
 - Power failure
 - Configuring device behavior after power failure, 34
 - Power on Password, 32
 - Primary Display, 19
 - Processor cores, 9
 - PXE Boot capability, 41

- Q**
 - Quick Boot, 41
 - Quick start, 41
 - Quiet Boot, 41

- R**
 - Remote Setup And Configuration, 46

- S**
 - SATA And RST Configuration, 23
 - SATA Boot, 42
 - SATA Configuration, 15
 - SATA Mode Selection, 23
 - Save Change Without Exit, 43
 - Save Custom Defaults, 43
 - Save setup settings to file, 43
 - Select Owner EPOCH input type, 16
 - Set User Password, 33
 - Setup Utility, 7
 - Keyboard inputs, 8
 - Starting, 8
 - SGX, 16
 - Software Guard Extensions (SGX), 16
 - SOL, 46
 - State After G3, 25
 - Storage Redirection, 46
 - Supervisor Password, 32
 - Switching on the device
 - Configuring automatic startup, 52
 - System Agent (SA) Configuration, 21
 - System Date, 10
 - System Time, 10

T

Threads, 9
 Timeout, 42
 Total Memory, 9
 TPM
 Configuring, 30
 TPM Availability, 30
 TPM Operation, 30
 TPM Ver, 9
 Turbo Mode, 17

U

UEFI Network Stack, 41
 Unconfigure ME, 28
 Unconfigure Network Access, 46
 Update
 Intel® Management Engine BIOS Extension (MEBx), 45
 USB Boot, 42
 USB Port 11 (USB3 P7) powered, 39
 USB Port 11 (USB3 P7) Wake Capability, 39
 USB Port 1 (USB Slot Adapter Bottom), 13
 USB Port 10 (USB3 P7) powered, 39
 USB Port 10 (USB3 P7) Wake Capability, 39
 USB Port 10 (USB3 P7, internal), 14
 USB Port 11 (USB3 P7, internal), 14, 38
 USB Port 12 (USB2 P12, internal), 14
 USB Port 13 (Front Bottom), 14
 USB Port 13 (USB2 P13, WFP), 14
 USB Port 14 (X60) powered, 40
 USB Port 14 (X60) Wake Capability, 40
 USB Port 14 (X60), 14
 USB Port 2 (X65), 13
 USB Port 3 (USB Slot Adapter Top), 13
 USB Port 4 (X61), 13
 USB Port 4 (X61) powered, 36
 USB Port 4 (X61) Wake Capability, 36
 USB Port 5 (X63) powered, 36
 USB Port 5 (X63) Wake Capability, 36
 USB Port 5 (X63), 13
 USB Port 6 (X62) powered, 37
 USB Port 6 (X62) Wake Capability, 37
 USB Port 6 (X62), 13
 USB Port 7 (X64), 13
 USB Port 8 (USB2 P8, internal), 13
 USB Port 9 (Front Top), 14
 USB Port 9 (USB2 P9, WFP), 14
 USB Ports 1/3 (USB Slot Adapter) powered, 35
 USB Ports 1/3 (USB Slot Adapter) Wake Cap, 35
 USB Ports 2/7 (X65/X64) powered, 36

USB Ports 2/7 (X65/X64) Wake Capability, 36
 USB Ports 8/12 (USB2 P8/P12) powered, 37
 USB Ports 8/12 (USB2 P8/P12) Wake Cap, 37
 USB Ports 9/13 (Front) powered, 38
 USB Ports 9/13 (Front) Wake Capability, 38
 USB Ports 9/13 (USB2 P9/P13) powered, 38
 USB Ports 9/13 (USB2 P9/P13) Wake Cap, 38
 USB Provisioning of AMT, 27
 User Access Level, 32
 User Boot Manager Access, 32
 User Consent, 46
 User password
 Setting up, 33
 User-specific firmware settings
 Downloading, 43
 Saving in a profile, 43

V

VT-d, 21

W

Wake event
 Configuring device behavior after a wake event, 34
 Wake on LAN 1 (X1 P1), 35
 Wake on LAN 2 (X2 P1), 35
 Wake on LAN 3 (X3 P1), 35
 Wake on PME, 34
 Wake on S5 Time, 34