SIEMENS

SIMATIC

**Industrial PC
Firmware/BIOS description
SIMATIC IPC127E**

Operating Instructions

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 IPC127E

History

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

Edition	Comment
01/2019	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

Using the firmware selection menu

<div style="text-align: right; font-size: 3em;">1</div>

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.

Open firmware selection menu manually

> **Note**
>
> **Windows®10 operating systems: Alternative procedure for opening the firmware selection menu**
>
> If you do not open the firmware selection menu after starting the device with the <Esc> key, follow these steps:
> 1. Start Windows®10.
> 2. Press the <Shift> key and keep it pressed.
> 3. Select "Restart".
>   The "Chose an Option" window opens.
> 4. Select the "Troubleshoot" option.
> 5. Select "UEFI / Firmware Settings".
> 6. Click "Restart".

Result

The "Main Page" with the options of the firmware selection menu (Page 8) 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:
	• Drive
	• USB stick
Device Manager	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".
Setup Utility	Start firmware configuration menu.
BIOS Update	Perform BIOS update.
	You can find more detailed information under "Update firmware (Page 25)".

Configure firmware

<div style="text-align: right; font-size: 2em;">2</div>

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.

See also

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 9)" > "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.
Processor Type	CPU type.
Cache RAM	L2 cache size total.
Total Memory	Total memory size.
BXT SOC	
SIC Version	
MRC Version	
Microcode	Microcode version.
PMC FW	
PUNIT FW	
TXE FW	
GOP	Version of the Graphics Output Protocol (GOP) driver.

Calling "System Time" and "System Date"

Date and time settings.

Select: "Setup Utility (Page 9)" > "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 9)" > "Advanced" > "Boot Configuration".

Firmware setting	Value	Setting in delivery state	Meaning
		IPC127E	
Numlock	Off		Numerical keypad is switched off after starting the device.
	On	x	Numerical keypad is switched on off after starting the device.

2.4.2 "Peripheral Configuration"

Configuration of the interfaces.

Calling "Peripheral Configuration"

Select: "Setup Utility (Page 9)" > "Advanced" > "Peripheral Configuration".

Firmware setting	Value	Setting in delivery state	Meaning
		IPC127E	
Onboard Ethernet 1 (LAN 1, X1 P1)	Disabled		The onboard Ethernet interface "X1 P1" is disabled.
	Enabled	x	The onboard Ethernet interface "X1 P1" is enabled.
Onboard Ethernet 1 Address:		20:87:56:70:48:71 *	The Onboard Ethernet 1 address is defined with this value.
Onboard Ethernet 2 (LAN 2, X2 P1)	Disabled		The onboard Ethernet interface "X2 P1" is disabled.
	Enabled	x	The onboard Ethernet interface "X2 P1" is enabled.
Onboard Ethernet 2 Address:		20:87:56:70:48:72 *	The Onboard Ethernet 2 address is defined with this value.
Onboard Ethernet 3 (LAN 3, X3 P1)	Disabled		The onboard Ethernet interface "X3 P1" is disabled.
	Enabled	x	The onboard Ethernet interface "X3 P1" is enabled.
Onboard Ethernet 3 Address:		20:87:56:70:48:73 *	The Onboard Ethernet 3 address is defined with this value.

*The Ethernet addresses are merely an example.

2.4.3 "SATA Configuration"

Calling "SATA Drives"

Select: "Setup Utility (Page 9)" > "Advanced" > "SATA Drives".

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

- Serial ATA Port 0
- Serial ATA Port 1

Firmware setting	Value	Setting in delivery state	Meaning
		IPC127E	
Chipset SATA	Disabled		The Chipset SATA Controller is disabled.
	Enabled	x	The Chipset SATA Controller is enabled.
SATA Mode Selection	AHCI	AHCI	The SATA controller works with the AHCI mode.
• SATA Port 0	Not installed	Not installed	The SATA Port 0 is not installed.
• SATA Port 1			Displays the drive type at SATA interface no. 1.

2.4.4 "USB Configuration"

Calling "USB Configuration"

Select: "Setup Utility (Page 9)" > "Advanced" > "USB Configuration".

Firmware setting	Value	Setting in delivery state	Meaning
		IPC127E	
xHCI Mode	Disabled		The USB Configuration does not work in xHCI mode.
			When you disable the XHCI mode, USB devices are not recognized during booting and are not used in the operating system.
			Note:
			Do not disable the XHCI mode.
	Enabled	x	The USB Configuration works in xHCI mode.
			USB devices are recognized during booting and used in the operating system.
USB Per-Port Control	Disabled	x	The USB ports (0-3) are disabled.
	Enabled		The USB ports (0-3) are enabled.

2.4.5 "Miscellaneous Configuration"

Calling "Miscellaneous Configuration"

Select: "Setup Utility (Page 9)" > "Advanced" > "Miscellaneous Configuration".

Firmware setting	Value	Setting in delivery state	Meaning
		IPC127E	
High Precision Timer	Disabled		The High Precision Event Timer is disabled.
	Enabled	x	The High Precision Event Timer is enabled.

2.5 "Security" tab

2.5.1 Level: "Security" tab

Calling "Security" tab

Select: "Setup Utility (Page 9)" > "Security".

Firmware setting	Value	Setting in delivery state	Meaning
		IPC127E	
Current TPM Device	Not Detected	x	The TPM (Trusted Platform Module) was not recognized in the operating system. See also: "Enable Trusted Platform Module (TPM) (Page 27)".
Supervisor Password	Not Installed		The "Supervisor Password" function is not installed.
User Password	Not Installed		The "User Password" function is not installed.
Set Supervisor Password			Here you can set a general password for full access to the firmware settings. 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. **NOTICE**: If you lose the general password that you defined during firmware setup, the device must be reset by the manufacturer. • Make a note of the general password and keep it in a safe place. • Protect the general password from unauthorized access.
• Enter New Password: (only if a "Supervisor Password" was set up)			Here you define a "Supervisor Password".
• Enter New Password Again: (only if a "Supervisor Password" was set up)			Here you enter the previously defined "Supervisor Password" once again.

Firmware setting	Value	Setting in delivery state	Meaning
		IPC127E	
Password Management Interface	Enabled	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.
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.

2.6 "Power" tab

2.6.1 Advanced CPU Control

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

Calling "Advanced CPU Control" tab

Select: "Setup Utility (Page 9)" > "Power" > "Advanced CPU Control".

Firmware setting	Value	Setting in delivery state IPC127E	Meaning
VTX-2	Enabled	x	Support of the VTX-2 mode is enabled.
	Disabled		Support of the VTX-2 mode is disabled.
VT-d	Enabled		The VT-d function is enabled.
	Disabled	x	The VT-d function is disabled.
AES-NI	Enabled	x	The AES instruction set extension of modern Intel® processors is enabled.
	Disabled		The AES instruction set extension of modern Intel® processors is disabled. You can use this feature to remain compatible with older CPUs or if errors occur.
Active Processor Cores	Enabled	x	All cores of the processor are active and used.
	Disabled		All cores of the processor are disabled.
• **Core 0**	Enabled	x	The processor core "**Core 0**" is enabled.
	Disabled		
• **Core 1**	Enabled	x	The processor core "**Core 1**" is enabled.
	Disabled		The processor core "**Core 1**" is disabled.
• **Core 2**	Enabled	x	The processor core "**Core 2**" is enabled.
	Disabled		The processor core "**Core 2**" is disabled.
• **Core 3**	Enabled	x	The processor core "**Core 3**" is enabled.
	Disabled		The processor core "**Core 3**" is disabled.
C-States	Enabled	x	The energy saving modes of the processor are released.
	Disabled		The energy saving modes of the processor are locked.
• **Max Core C State**	Core C7	x	Prevent the processor from entering hibernation states that are too deep.
	Core C6		
	Core C1		The larger the number behind the "C", the deeper the hibernation state, the less the power consumption of the processor and the longer it takes for the device to switch on again from the hibernation state. **Example:** The settings C7, C6, C1 are available.

Firmware setting	Value	Setting in delivery state	Meaning
		IPC127E	
User Power Scenario	Max Performance		The settings "Max Performance", "Balanced" and "High Temperature" are available.
	Balanced	x	
	High Temperature		
Turbo Mode	Enabled	x	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 the Turbo mode effectively, the performance modes of the processor "PStates (IST)" and energy saving modes of the processor "C States" must be enabled.
	Disabled		Turbo mode is disabled.

2.6.2 Level: "Power" tab

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

Calling "Power" tab

Select: "Setup Utility (Page 9)" > "Power".

Firmware setting	Value	Setting in delivery state IPC127E	Meaning
Wake on PME	Disabled		If a power management event occurs, the device does not switch on.
	Enabled by OS		If a power management event occurs, the device switches on.
	Force Enabled	x	
Wake on RTC from S5	Disabled	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".
	By Sleep Time	5	The device does not switch on for 5 seconds when it is in the S5 operating state.
	By OS Utility	By OS Utility	The OS determines when the device is switched on when it is in the S5 operating state.
• **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	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.
• **Day of Month** (only if "Auto Wake on S5" = "By Day of Month")	1..31	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>.
• **By Sleep Time** (only if "Auto Wake on S5" = "By Sleep Time")	5 ~ 255	5	With "By Sleep Time" you specify after how many seconds the device switches on in the S5 operating state.
• **By OS Utility** (only if "Auto Wake on S5" = "By OS Utility")	By OS Utility	By OS Utility	With "By OS Utility" you specify when the OS can switch on the device in the S5 operating state.

Firmware setting	Value	Setting in delivery state	Meaning
		IPC127E	
USB Port X60 Wake Capability	Disabled	x	The device connected to USB port X60 cannot switch on the device.
	Enabled		The device connected to USB port X60 can switch on the device.
USB Port X61 Wake Capability	Disabled	x	The device connected to USB port X61 cannot switch on the device.
	Enabled		The device connected to USB port X61 can switch on the device.
USB Port X62/X63 Wake Capability	Disabled	x	The device connected to USB port X62/63 cannot switch on the device.
	Enabled		The device connected to USB port X62/63 can switch on the device.
Wake on LAN 1 (X1 P1)	Disabled		The LAN controller of the onboard Ethernet interface "X1 P1" cannot switch on the device.
	Enabled	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	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	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".

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 9)" > "Boot".

Firmware setting	Value	Setting in delivery state	Meaning	
		IPC127E		
Quick Boot	Enabled	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	The boot logo is displayed during the self-test.	
	Disabled		Start information appears in text mode during the self-test.	
Network Stack	Disabled	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.	
• **PXE Boot capability** (only if "Network Stack" = Enabled)	Disabled	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.	
Add Boot Options	First		Newly detected boot media are placed at the top of the boot order.	
	Auto	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.	

Firmware setting	Value	Setting in delivery state	Meaning
		IPC127E	
USB Boot	Enabled		Booting from USB devices is permitted.
	Disabled	x	Booting from USB devices is not permitted.
SATA Boot	Enabled	x	Booting from SATA devices is permitted.
	Disabled		Booting from SATA devices is not permitted.
Timeout	0..10	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 9)" > "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 9)" > "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.

Update firmware

3

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 24)".

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

<div style="text-align: right; font-size: large;">4</div>

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) 5

Depending on the ordered configuration, you 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. • 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 16)".

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 "AUTOHOTSPOT".

Automatic switching on of the device

6

The device always switches on when the supply voltage is applied.

⚠ 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.

See also

Level: "Exit" tab (Page 24)

Index