

# SIEMENS

## SIMATIC

Industrial PC  
SIMATIC IPC  
FirmwareManager V4.0.2

Operating Manual

Safety instructions

1

Hardware and software requirements

2

Functions of IPC FirmwareManager

3

# 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.

# Table of contents

<b>1</b>	<b>Safety instructions.....</b>	<b>5</b>
1.1	Industrial Security .....	5
1.2	Disclaimer for third-party software updates .....	5
1.3	Notes on protecting administrator accounts .....	5
<b>2</b>	<b>Hardware and software requirements .....</b>	<b>6</b>
2.1	IPC FirmwareManager.....	6
2.2	Hardware requirements .....	6
2.3	Software Requirements.....	7
<b>3</b>	<b>Functions of IPC FirmwareManager .....</b>	<b>8</b>
3.1	Starting IPC FirmwareManager.....	8
3.2	General command line options.....	9
3.3	Firmware information from the flash.....	9
3.4	Updating the firmware.....	10
3.5	BIOS data, OEM-specific SMBIOS fields .....	12
3.6	Boot behavior .....	13
3.6.1	Boot behavior: Command line options.....	13
3.6.2	Examples of boot behavior.....	15
3.6.2.1	Show boot order.....	15
3.6.2.2	Set boot device by index or name for next boot.....	15
3.6.2.3	Move boot entry by index or name in boot order .....	16
3.6.2.4	Sort boot order by type or name.....	17
3.7	SMBIOS.....	18
3.8	Password parameter (supervisor or user).....	18
3.8.1	Password parameter (supervisor or user): Command line options.....	18
3.8.2	Password-password (supervisor or user): Examples.....	20
3.8.2.1	Calling current status .....	20
3.8.2.2	Generating a hash.....	20
3.8.2.3	Setting a new password (none available yet) .....	20
3.8.2.4	Setting the user password .....	21
3.8.2.5	Removing a password .....	21
3.8.2.6	Setting password options.....	21
3.8.2.7	Saving password changes with certificate.....	22

3.9	Setup settings.....	23
3.9.1	Setup settings: Command line options .....	23
3.9.2	Setup settings: Examples .....	25
3.9.2.1	Showing current setup settings (combine flags) .....	25
3.9.2.2	Load setup settings from a file .....	27
3.9.2.3	Changing values of setup settings .....	28
3.9.2.4	Querying individual options .....	28
3.9.2.5	Showing SecureSetup information.....	28
3.9.2.6	Installing or deleting a new SecureSetup certificate.....	29
3.10	Boot Logo.....	30
3.11	Secure Boot .....	31
3.11.1	Secure Boot: Command line options.....	31
3.11.2	Secure Boot: Examples.....	32
3.11.2.1	Displaying Secure Boot settings.....	32
3.11.2.2	Loading Secure Boot defaults.....	36
3.11.2.3	Changing Secure Boot settings.....	36
3.11.2.4	Initialization with own Secure Boot settings .....	36

# Safety instructions

## 1.1 Industrial Security

### Industrial Security

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 only form one element of such a concept. Siemens' products and solutions only form one element of such a concept.

Customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.

Additionally, Siemens' guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit (<http://www.siemens.com/industrialsecurity>).

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

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

### See also

Technical support (<https://support.industry.siemens.com/cs/ww/en/>)

## 1.2 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>).

## 1.3 Notes on protecting administrator accounts

A user with administrator privileges has extensive access and manipulation options in the system.

Therefore, ensure there are adequate safeguards for protecting the administrator accounts to prevent unauthorized changes. To do this, use secure passwords and a standard user account for normal operation. Other measures, such as the use of security policies, should be applied as needed.

# **Hardware and software requirements**

**2**

## **2.1 IPC FirmwareManager**

With IPC FirmwareManager you can configure or replace the components of the firmware of your IPC.

## **2.2 Hardware requirements**

The following Siemens products are supported:

- SIMATIC IPC427D
- SIMATIC IPC477D
- SIMATIC IPC627D
- SIMATIC IPC677D
- SIMATIC IPC647D
- SIMATIC IPC827D
- SIMATIC IPC847D
- SIMATIC IPC127E
- SIMATIC IPC227E
- SIMATIC IPC277E
- SIMATIC IPC427E
- SIMATIC IPC477E
- SIMATIC IPC627E
- SIMATIC IPC677E
- SIMATIC IPC647E
- SIMATIC IPC847E
- SIMATIC IPC227G
- SIMATIC IPC277G
- SIMATIC IPC BX-39A
- SIMATIC IPC PX-39A
- SIMATIC Field PG M5
- SIMATIC Field PG M6
- SIMATIC ITP1000

## 2.3 Software Requirements

### IPC FirmwareManager version

IPC FirmwareManager as of version 4.0.1

### Operating system

- UEFI Shell
- Windows XP 32/64 bit
- Windows 7 32/64 bit
- Windows 10 64 bit
- Linux based (Kernel 3.x, 4.x, 5.x) 32/64 bit

# Functions of IPC FirmwareManager

3

## 3.1 Starting IPC FirmwareManager

### Requirement

You have administrator rights.

### Procedure

1. Open a command box on your IPC.
2. Go to the folder where the IPC FirmwareManager is located or always enter the complete path to the program in 3.
3. Depending on the operating system installed on your IPC, enter one of the following command line options.
  - UEFI Shell:  
`FwMgr <Command line option>`
  - Windows 32Bit:  
`FwMgrWin <Command line option>`
  - Windows 64Bit:  
`FwMgrWin64 <Command line option>`
  - Linux 32 Bit:  
`FwMgr32 <Command line option>`
  - Linux 64 Bit:  
`FwMgr64 <Command line option>`

---

### Note

The possible return values of the program can be displayed with the option -hh.

---

## 3.2 General command line options

### Procedure

1. Start the IPC FirmwareManager (Page 8) and enter one of the following command line options:

Command line option	Function
-h	Show command line options help.
-hh	Show extended help (Return codes).
-w	Wait for keypress after each page.
-W	Disable colors; Useful for in output to a file, see also command line option "-logfile <file> [html/text]".
-Wo	Disable text output on screen; Useful for in output to a file, see also command line option "-logfile <file> [html/text]".
-u	Enable unattended mode (no input required). Requires no user input for a BIOS update. All dialog boxes are automatically skipped.
-H	Enable Headless mode; Status codes are output via port 80 and LEDs (where available).
-logfile <file> [html/text]	Output to an HTML file (if the extension .htm is used) or text file (default). The format can also be forced with the "html" option or text.
-show <file> [Question]	Show text file with reading confirmation of type "y/n". The execution of the program continues only after successful read confirmation.

## 3.3 Firmware information from the flash

### Procedure

1. Start the IPC FirmwareManager (Page 8) and enter one of the following command line options:

Command line option	Function
-I	Show all information available.
-i	Show all information on the device and firmware version.

## 3.4 Updating the firmware

### Note

In order to apply the command line options and carry out the flash procedure, add the `-a` option to the respective command line.

### Procedure

1. Start the IPC FirmwareManager (Page 8) and enter one of the following command line options:

Command line option	Function
<code>-F &lt;directory&gt;</code>	Automatically searches the specified directory and subdirectories for matching BIOS update packages. The parameters required for the update are determined automatically.
<code>-f &lt;file&gt;</code>	Execute BIOS update from file.
<code>-fnr</code> (Support depends on the device)	BIOS update with <code>-f &lt;file&gt;</code> : Do <b>not</b> update recovery region.
<code>-fm</code>	BIOS update with <code>-f &lt;file&gt;</code> : Update also Intel® ME (ManagementEngine); after this a global reset is executed.
<code>-fe</code>	BIOS update with <code>-f &lt;file&gt;</code> : Update Intel® GbE (Gigabit Ethernet).
<code>-fx</code>	BIOS update with <code>-f &lt;file&gt;</code> : Update Intel® Expansion Image.

### Additional options for programming

Command line option	Function
<code>-nr</code>	Do not execute system resets automatically. (User is responsible for executing required resets!)
<code>-sr &lt;Type&gt;</code>	Perform a reset (type: Soft, Hard, Full, Global, S5) after closing the IPC FirmwareManager.
<code>-n</code>	BIOS update with <code>-f &lt;file&gt;</code> : If possible, the existing system settings are applied.
<code>-dg</code>	BIOS update with <code>-f &lt;file&gt;</code> : Downgrade without asking for permission.
<code>-c &lt;file&gt;</code>	Execute script to program the OEM-specific SM-BIOS fields 4.5 and 14.2 to 14.9. The script file is a text (ASCII) file with the following format (example): <pre>[PUT:1] 4.5.=My asset tag 14.2.=My OEM string 14.3.=My second OEM string</pre>

**Example: Automatic firmware update without user input**

There is a search in the specified folder (-F) for the latest matching BIOS version and the update is started. No user action is required during the update process (-u).

- FwMgr -u -F D:\Updates

**Example: Manual programming of the BIOS flash**

Programming the BIOS Flash with the contents of the F:\V180108.bin file while retaining the current BIOS settings:

- FwMgr -f F:\V180108.bin -n -a

---

**Note**

With this input, only the BIOS component in the Flash is updated.

---

## 3.5 BIOS data, OEM-specific SMBIOS fields

### Note

In order to apply the command line options and carry out the flash procedure, add the `-a` option to the respective command line.

### Procedure

1. Start the IPC FirmwareManager (Page 8) and enter one of the following command line options:

Command line option	Function
<code>-l</code>	Show OEM-specific SM-BIOS fields.
<code>-l -w</code>	Show OEM-specific SM-BIOS fields by page.
<code>-g &lt;[store/]group.entry.&gt; [[store/]group.entry.]</code>	Lists one or more BIOS data entries.
<code>-p &lt;[store/]group.entry.=value&gt;</code>	Updates one or more BIOS data entries.
<code>-p &lt;[store/]config:index=value&gt;</code>	Updates one or more BIOS data entries.
<code>-d &lt;[store/]group.entry.&gt; [[store/]group.entry.]</code>	Deletes one or more BIOS data entries.

### List of writeable fields

Entry	Description
<code>1/4.5.</code>	Asset tag in DMI Type 3 (Chassis)
<code>1/14.2.-14.8.</code>	OEM strings in DMI Type 11

### Example: Set an asset tag

- `FwMgr -p "1/4.5.=My asset tag" -a`

## 3.6 Boot behavior

### 3.6.1 Boot behavior: Command line options

---

#### Note

In order to apply the command line options and carry out the flash procedure, add the `-a` option to the respective command line.

---

#### Procedure

1. Start the IPC FirmwareManager (Page 8) and enter one of the following command line options:

Command line option	Function
<code>-b</code>	Show boot order.
<code>-bb</code>	Show boot order with UEFI DevicePaths.
<code>-bo &lt;Type/Name&gt; [...]</code>	<p>Sort boot order by: Type or name. Setup parameter "Boot/EFI Device First" has an influence on boot order. If this setup parameter is set to "Enabled", the EFI boot devices are automatically sorted upwards by the BIOS.</p> <p>The following types are available:</p> <ul style="list-style-type: none"> <li>• <b>HDD/SSD</b> All drives HDD and SSD (not: USB)</li> <li>• <b>DVD/CD</b> DVD and CD (not: USB)</li> <li>• <b>NET</b> Network/PXE boot</li> <li>• <b>USBHDD</b> USB HDD drives</li> <li>• <b>USBDVD</b> USB-DVD/CDROM drives</li> <li>• <b>USBFDD</b> USB floppy drives</li> <li>• <b>USB</b> USB drives: Order USBHDD, USBDVD, USBFDD</li> <li>• <b>FDD</b> Floppy drives (not: USB)</li> </ul>

---

3.6 Boot behavior

Command line option	Function
-bm <FromIndex/Name> <ToIndex/Name>	Move boot entry by index or name in boot order.
-bn <Index/Name>	Set boot device by index or name for next boot.
-bf <Index/Name> <Enable/Disable>	Enables or disables a boot entry. If it is disabled, it is no longer taken into account when booting, but is still present.
-R	Reset setup settings <b>without</b> boot order.
-Rb	Reset setup settings <b>and</b> boot order.
-Ra	Reset <b>all</b> settings <b>except</b> security settings.

### 3.6.2 Examples of boot behavior

#### 3.6.2.1 Show boot order

- FwMgr -b

#### Result

```
...
Locating boot information.....ok
0. UEFI    | USB    | HDD    | EFI USB Device (SIEMENS USB-FD 5)
1. UEFI    |        | HDD    | Windows Boot Manager
2. Legacy  | PCI    | NET    | IBA CL Slot 00FE v0104 (P1)
3. Legacy  | PCI    | NET    | IBA GE Slot 0200 v1570 (P2)
4. Legacy  | ATA    | HDD    | FUJITSU MHW2100BH
5. Legacy  | USB    | HDD    | SIEMENS USB-FD 5
Exitcode: 0
```

#### 3.6.2.2 Set boot device by index or name for next boot

##### Current boot order for following example

```
0. UEFI    | USB    | HDD    | EFI USB Device (SIEMENS USB-FD 5)
1. UEFI    |        | HDD    | Windows Boot Manager
2. Legacy  | PCI    | NET    | IBA CL Slot 00FE v0104 (P1)
3. Legacy  | PCI    | NET    | IBA GE Slot 0200 v1570 (P2)
4. Legacy  | ATA    | HDD    | FUJITSU MHW2100BH
5. Legacy  | USB    | HDD    | SIEMENS USB-FD 5
```

##### Example: Define Index 1 (Windows Boot Manager) exclusively as boot device for the next boot

- FwMgr -bn 1 -a

#### Result

```
Set next boot device.....Windows Boot Manager
```

### 3.6.2.3 Move boot entry by index or name in boot order

The index or a name can be specified.

#### Current boot sequence for following examples

0.	Legacy		PCI		NET		IBA CL Slot 00FE v0104	(P1)
1.	UEFI				HDD		Windows Boot Manager	
2.	Legacy		ATA		HDD		FUJITSU MHW2100BH	
3.	UEFI		USB		HDD		EFI USB Device (SIEMENS USB-FD 5)	
4.	Legacy		USB		HDD		SIEMENS USB-FD 5	
5.	Legacy		PCI		NET		IBA GE Slot 0200 v1570	(P2)

#### Example: Third entry to the very top

- FwMgr -bm 2 0 -a

#### Example: Entry with "P2" in the name to the very top

- FwMgr -bm "P2" 0 -a

#### Example: Entry with "P1" in the name to second place

- FwMgr -bm "P1" 1 -a

### 3.6.2.4 Sort boot order by type or name

#### Example: HDD up, leave remaining order

- FwMgr -bo HDD -a

##### Result

0. UEFI | | HDD | Windows Boot Manager
1. Legacy | ATA | HDD | FUJITSU MHW2100BH
2. UEFI | USB | HDD | EFI USB Device (SIEMENS USB-FD 5)
3. Legacy | PCI | NET | IBA CL Slot 00FE v0104 (P1)
4. Legacy | PCI | NET | IBA GE Slot 0200 v1570 (P2)
5. Legacy | USB | HDD | SIEMENS USB-FD 5

#### Example: First HDD, then Network/PXE-Boot, then USB drives (HDD/SSD)

- FwMgr -bo HDD NET USBHDD -a

##### Result

0. UEFI | | HDD | Windows Boot Manager
1. Legacy | ATA | HDD | FUJITSU MHW2100BH
2. Legacy | PCI | NET | IBA CL Slot 00FE v0104 (P1)
3. Legacy | PCI | NET | IBA GE Slot 0200 v1570 (P2)
4. UEFI | USB | HDD | EFI USB Device (SIEMENS USB-FD 5)
5. Legacy | USB | HDD | SIEMENS USB-FD 5

#### Example: First LAN 1 PXE ("IBA CL Slot 00FE v0104 (P1)"), then HDD, then USB drives (HDD/SSD/CD/DVD/BD)

- FwMgr -bo "P1" HDD USB -a

##### Result

0. Legacy | PCI | NET | IBA CL Slot 00FE v0104 (P1)
1. UEFI | | HDD | Windows Boot Manager
2. Legacy | ATA | HDD | FUJITSU MHW2100BH
3. UEFI | USB | HDD | EFI USB Device (SIEMENS USB-FD 5)
4. Legacy | USB | HDD | SIEMENS USB-FD 5
5. Legacy | PCI | NET | IBA GE Slot 0200 v1570 (P2)

## 3.7 SMBIOS

### Note

In order to apply the command line options and carry out the flash procedure, add the `-a` option to the respective command line.

### Procedure

1. Start the IPC FirmwareManager (Page 8) and enter one of the following command line options:

Command line option	Function
<code>-Lf</code>	If available list flash history.
<code>-Ls [Type] [save/load &lt;file&gt;]</code>	List SM-BIOS entries; the SM-BIOS DMI type can be specified (for example, 1 for system information) or the SM-BIOS tables can be saved/loaded.

## 3.8 Password parameter (supervisor or user)

### 3.8.1 Password parameter (supervisor or user): Command line options

### Note

In order to apply the command line options and carry out the flash procedure, add the `-a` option to the respective command line.

### Procedure

1. Start the IPC FirmwareManager (Page 8) and enter one of the following command line options:

Command line option	Function
<code>-password</code>	Set or change BIOS password (supervisor or user). The changes are only evaluated and applied by the BIOS during a reboot. The maximum password length is 10 characters or 32 characters for newer BIOS versions. The password can be specified as plain text or as hash. If <code>-password</code> is called without options, the current status is displayed.
<code>-password cert &lt;certificate&gt; &lt;private-Key&gt; [KeyPassword]</code>	Advanced protection against unauthorized modification of BIOS. Using this option, any modification will be only possible if the Private Key of the actual certificate is available. This option is always required if <code>-password set</code> or <code>-password</code> option is used.
<code>-password hash &lt;password&gt;</code>	Create a hash on base of a new-set password. The hash can be used instead of a password.

Command line option	Function
-password check supervisor <password or hash>	Check, if the set password is the same as the Supervisor Password. A hash can also be used instead of a password.
-password check user <password or hash>	Check, if the set password is the same as the User Password. A hash can also be used instead of a password.
-password set supervisor <current password or hash> <password or hash>	Replace Supervisor Password by new-set password. A hash can also be used instead of a password. Requires the -password cert option before the -password set option.
-password set user <current password or hash> <password or hash>	Replace actual User Password by new-set password. A hash can also be used instead of a password. Requires the -password cert option before the -password set option.
-password option <current password or hash> <option1> <option2> <option3>	<p>Set password options (see BIOS Setup under "Security"). Requires the -password cert option before the -password set option. The options have following meanings:</p> <ul style="list-style-type: none"> <li>• Option 1 PowerOn: Specifies whether the password should be prompted at system startup. <ul style="list-style-type: none"> <li>– 0=Keep actual settings</li> <li>– 1=Disable</li> <li>– 2=Enable</li> </ul> </li> <li>• Option 2 UserAccessLevel: Specifies the rights of the user password. <ul style="list-style-type: none"> <li>– 0=Keep actual settings</li> <li>– 1=View only</li> <li>– 2=Limited</li> <li>– 3=Full</li> </ul> </li> <li>• Option 3 DisableIF: <ul style="list-style-type: none"> <li>– 0=Keep actual settings</li> <li>– 1=Disable Password Interface (the command line option -password will not work any longer)</li> </ul> </li> </ul>

### 3.8.2 Password-password (supervisor or user): Examples

#### 3.8.2.1 Calling current status

- -password

##### Result

...

Interface Version: 3

Supervisor password: Not present

User password: Not present

Last error: Success (0)

Power On Password: Disabled

User Access Level: Full

Exitcode: 0

If an error is returned, the BIOS does not support this feature or it may have to be enabled in the BIOS setup under "Security" (Password Management Interface = "Enabled").

#### 3.8.2.2 Generating a hash

A hash is generated with:

- -password hash MyPassword

##### Result

Encode password.....ok:

h:24E84B69894206097B464DAD981C59A17EE7D71982459F0D05F458E91852C91F0AC825A13FD2

Exitcode: 0

The displayed hash (incl. h: with all values) can then be used instead of a plain text password.

#### 3.8.2.3 Setting a new password (none available yet)

- -password cert MyCert.crt MyKey.pem PemPw -password set supervisor ignored MyPassword

*ignored* is the current password, which is ignored in this case. After a reboot, the supervisor password is now set.

Requires the option -password cert, see "Saving password changes with certificate (Page 22)".

### 3.8.2.4 Setting the user password

- -password cert MyCert.crt MyKey.pem PemPw -password set user MyPassword UserPass

To set the user password, the old user password or the supervisor password must now be entered. After a reboot, the user password is now set.

Requires the option -password cert, see "Saving password changes with certificate (Page 22)".

### 3.8.2.5 Removing a password

- -password cert MyCert.crt MyKey.pem PemPw -password set supervisor MyPassword

Requires the option -password cert, see "Saving password changes with certificate (Page 22)".

### 3.8.2.6 Setting password options

#### Example: Set password options (PowerOn, UserAccessLevel, Password Interface)

- -password cert MyCert.crt MyKey.pem PemPw -password option MyPassword <PowerOn> <UserAccessLevel> <DisableIF>

##### PowerOn

- 0 - Keep actual setting (do not change anything)
- 1 - Disable
- 2 - Enable

##### UserAccessLevel

- 0 - Keep actual setting (do not change anything)
- 1 - View only
- 2 - Limited
- 3 - Full

##### DisableIF

- 0 - Keep actual setting (do not change anything)
- 1 - Disable Password Interface, -password will not work anymore. The interface can be reactivated in the setup.

Requires the option -password cert, see "Saving password changes with certificate (Page 22)".

## Additional functions

- Enable password query during boot and set "User Access Level" to "View Only".

```
-password cert MyCert.crt MyKey.pem PemPw -password option  
MyPassword 2 1 0
```

After a reboot, -password now displays:

...

```
Interface Version: 3  
Supervisor password: Present  
User password: Present  
Last error: Success (0)  
Power On Password: Enabled  
User Access Level: View only
```

Exitcode: 0

- Disable interface.

```
-password cert MyCert.crt MyKey.pem PemPw -password option  
MyPassword 0 0 1
```

The password management with -password is then no longer available after a reboot.

Password management.....failed: Unsupported

Exitcode: 4

It can be reactivated by the supervisor in the setup under "Security/Password Management Interface".

### 3.8.2.7 Saving password changes with certificate

To secure changes, they are protected with certificates. After this, it is only possible to make changes with the appropriate certificate/key pair. Only certificates in DER format are supported.

#### Generating a certificate/key for test

A certificate/key for the test can be generated, for example, with:

- `openssl req -x509 -nodes -days 3650 -newkey rsa:2048 -keyout  
MyKey.pem -outform DER -out MyCert.crt -sha256`

#### Setting the certificate and key

```
-password cert MyCert.crt MyKey.pem PemPw
```

This option must always be specified in advance when using -password set or -password option.

PemPw is the PEM password (if one has been assigned); otherwise, the value is ignored.

Without this certificate and the private key no changes can be made with -password , even if the current password is known.

#### Removing a certificate (for example, after removing the password)

```
-password cert MyCert.crt MyKey.pem PemPw delete
```

## 3.9 Setup settings

### 3.9.1 Setup settings: Command line options

---

#### Note

In order to apply the command line options and carry out the flash procedure, add the `-a` option to the respective command line.

---

#### Procedure

1. Start the IPC FirmwareManager (Page 8) and enter one of the following command line options:

Command line option	Function
<code>-setup [ ... ]</code>	Change Setup Settings. Possible flags: <ul style="list-style-type: none"> <li>• long: long format (Show detailed setup settings.)</li> <li>• diff: show items not set to default (Show setup settings that differ from the default values.)</li> <li>• help: show item help text (Show setup settings with help text.)</li> <li>• csv: output in CSV format (Show setup settings in CSV format.)</li> </ul>
<code>-setup list [Flag] [Flag2] ...</code>	Show Setup Settings.
<code>-setup save &lt;file&gt; [Flag] [Flag2] ...</code>	Save Setup Settings to file. Output can be used for <code>-setup load</code>
<code>-setup load &lt;file&gt;</code>	Load Setup Settings from file created by <code>-setup save</code> .
<code>-setup load &lt;file&gt; default</code>	Load Setup Settings from file as default. Default: When loading the setup defaults these settings are used, not the settings of the delivery state.
<code>-setup load &lt;file&gt; override</code>	Load Setup Settings as override. Override: These settings are ALWAYS used. Changes in the BIOS setup are neither stored nor used.
<code>-setup set &lt;name&gt; [index] &lt;value&gt;</code>	Modify single Setup Setting. Name of the setup setting like in BIOS setup.
<code>-setup get &lt;name&gt; [index]</code>	Shows the setup settings <code>&lt;name&gt;</code> (name as in BIOS setup).

---

### 3.9 Setup settings

Command line option	Function
-setup oem	Show OEM settings. Shows the -setup load <file> default/override settings (if they exist). Default: When loading the setup defaults these settings are used, not the settings of the delivery state. Override: These settings are ALWAYS used. Changes in the BIOS setup are neither stored nor used.
-setup sinfo	Displays SecureSetup information (if supported).
-setup cert <new certfile> <keyfile> [old certfile]	Installs new SecureSetup certificate.
-setup cert "" <keyfile> <password> <certfile>	Deletes the SecureSetup certificate.

## 3.9.2 Setup settings: Examples

### 3.9.2.1 Showing current setup settings (combine flags)

- -setup list

The flags long, diff, help, csv can be combined.

#### -setup list with "help" and "csv"

- -setup list help csv

##### Result:

...

Menu;Name;Help;Options;Default;Current

Advanced/Advanced;HPET - HPET Support;"The OS-Timer is driven by the HPET  
(case 'Enabled') or the System Timer (case  
'Disabled')";Disabled/Enabled;Enabled

Advanced/Boot Configuration;Numlock;"Selects Power-on state for  
Numlock";Off/On;Off;On

...

#### -setup list with "long"

- -setup list long

##### Result:

...

Form: Advanced

CPU Configuration

##### C-States

Disabled \* (Default)

Enabled

##### P-States(IST)

Disabled \* (Default)

Enabled

##### HT Support

Auto \* (Default)

Disabled

**VT Support**

Enabled \* (Default)

Disabled

**Peripheral Configuration**

**Onboard Ethernet 1**

Disabled

Enabled \* (Default)

**Video Configuration**

**Primary Video device**

IGD

PCIe \* (Default)

**Chipset Configuration**

**HPET - HPET Support**

Disabled

Enabled \* (Default)

...

### 3.9.2.2 Load setup settings from a file

With `-setup load <file>`, setup settings can be loaded from a file created with `-setup save`.

#### 1. Read out setup settings

```
-setup save setup.ini
```

or:

Save only differences to the defaults:

```
-setup save setup.ini diff
```

#### 2. If necessary: Adapt the setup.ini text file:

```
[Advanced/Advanced]
HPET - HPET Support=Enabled
[Advanced/Boot Configuration]
Numlock=On
[Advanced/Peripheral Configuration]
Internal COM 1=Auto
[Power/Advanced CPU Control]
P-States (IST)=Enabled
C-States=Enabled
[Boot/Boot]
Quick Boot=Enabled
```

#### 3. Load and save settings.

```
-a -setup load setup.ini
```

---

#### Note

For newer devices, the `-setup cert` option is required.

---

### Initializing values from a file

The values from the file can also be initialized with the additional parameters "default" or "override".

- "default":

Indicates that the values are to be accepted as a new default (F9).

- "override":

Indicates that the value is fixed.

#### Example:

Load Setup Settings from file as default:

```
-a setup load setup.ini default
```

Delete the saved default settings:

```
-a -d 1/12.1. -d 1/12.2.
```

### 3.9.2.3 Changing values of setup settings

- -setup set <name> [index] <value>

**Example:**

```
-setup set Numlock 0 off  
-setup set Numlock off  
-setup set "SNTP on LAN 2" 0 Enabled
```

---

#### Note

For newer devices, the -setup cert option is required first.

---

(Notice: If there are spaces in the name, it must be enclosed in quotation marks "")

### 3.9.2.4 Querying individual options

```
-setup get <name> [index]
```

**Example:**

```
-setup get Numlock
```

### 3.9.2.5 Showing SecureSetup information

If the firmware supports this, SecureSetup information can be displayed as follows:

In order for changes to the settings to be possible with -setup , a certificate must be installed by the user. All changes must then be signed with the user's key. The BIOS then verifies the signature on the basis of the certificate. Once the certificate has been installed, it can only be changed by the user with the appropriate private key.

**Example:**

```
-setup sinfo
```

**Result:**

```
...  
UEFI variable access.....ok: UEFI(SecureSetup)  
Secure Setup.....ok: Supported, certificate present  
Locating setup items.....ok  
SecureSetup.....ok: Version 1  
State: Enabled  
Error: 0  
Guid: 44332211-6655-8877-1122334455667788  
Certificate: Present  
Issuer: /C=DE/ST=BW/L=Karlsruhe/O=Siemens AG/OU=DF FA AS DH KHE 1  
Subject: /C=DE/ST=BW/L=Karlsruhe/O=Siemens AG/OU=DF FA AS DH KHE 1  
Serial: D2E7308402A709FB  
Valid: 190213102003Z to 290210102003Z  
Exitcode: 0
```

### 3.9.2.6 Installing or deleting a new SecureSetup certificate

#### Requirement

Only certificates in DER format are supported.

#### Example: No certificate available

- -setup cert TestCert.crt TestKey.pem

#### Result:

```
...
UEFI variable access.....ok: UEFI (SecureSetup)
Secure Setup.....ok: Supported, certificate not
present
Locating setup items.....ok
Set certificate.....ok: TestCert.crt/TestKey.pem
Exitcode: 0
```

#### Example: Replace a certificate

```
-setup cert NewTestCert.crt TestKey.pem TestCert.crt
```

#### Result:

```
...
UEFI variable access.....ok: UEFI (SecureSetup)
Secure Setup.....ok: Supported, certificate present
Locating setup items.....ok
Set certificate.....ok: NewTestCert.crt/TestKey.pem
Exitcode: 0
```

#### Example: Delete a certificate

```
-setup cert "" TestKey.pem TestCert.crt
```

#### Result:

```
...
UEFI variable access.....ok: UEFI (SecureSetup)
Secure Setup.....ok: Supported, certificate present
Locating setup items.....ok
Set certificate.....ok: Delete/TestKey.pem
Exitcode: 0
```

## 3.10 Boot Logo

Note the following for the Boot Logo:

- The maximum image size is 400 x 300 pixels.
- The maximum color depth is 8 bits per color.
- JPG images must not be saved as "progressive".

---

### Note

In order to apply the command line options and carry out the flash procedure, add the **-a** option to the respective command line.

---

### Procedure

1. Start the IPC FirmwareManager (Page 8) and enter one of the following command line options:

Command line option	Function
<code>-logo [file]</code>	Show information on Logo or set new Boot Logo.
<code>-logo delete</code>	Delete Boot Logo and show default logo.

### Example: Specify the image "NewLogo.jpg" as the new Boot Logo

- `FwMgr -logo NewLogo.jpg -a`

## 3.11 Secure Boot

### 3.11.1 Secure Boot: Command line options

---

#### Note

In order to apply the command line options and carry out the flash procedure, add the `-a` option to the respective command line.

---

#### Requirement

- Windows
  - Windows 8 or
  - Windows 10 in UEFI mode
  - No Windows 7 in UEFI mode, since this operating system lacks specific functions
- UEFI
  - None
- Linux
  - Mounted efivars at `/sys/firmware/efi/efivars`

#### Procedure

1. Start the IPC FirmwareManager (Page 8) and enter one of the following command line options:

Command line option	Function
<code>-sb [...]</code>	Show Secure Boot information.
<code>-sb param &lt;sign cert&gt; &lt;sign key&gt; [key pass]</code>	Set certificate and private key that are used for signing the Secure Boot variables.
<code>-sb default [Store] [Store] [...]</code>	Set Secure Boot to default settings.
<code>-sb add &lt;store&gt; x509 &lt;file&gt;</code>	Add X509 certificate to store (db, dbx, KEK, PK).
<code>-sb del &lt;store&gt; x509 &lt;subject&gt;</code>	Delete X509 certificate from store (db, dbx, KEK, PK).
<code>-sb add &lt;store&gt; sha256 &lt;file&gt;</code>	Add SHA256 hash for an .efi file to store (db, dbx, KEK, PK).
<code>-sb del &lt;store&gt; sha256 &lt;hash&gt;</code>	Delete SHA256 hash from store (db, dbx, KEK, PK).
<code>-sb get &lt;store&gt; &lt;index&gt; &lt;file&gt;</code>	Save entry from store (db, dbx, KEK, PK) to file.
<code>-sb load &lt;store&gt; &lt;file&gt;</code>	Load store to file.
<code>-sb save &lt;store&gt; &lt;file&gt;</code>	Save store to file.
<code>-sb x509 &lt;file&gt;</code>	Show X509 certificate from file (DER format).
<code>-sb sha256 &lt;file&gt;</code>	Show SHA256 hash for an .efi file.

### 3.11.2 Secure Boot: Examples

#### 3.11.2.1 Displaying Secure Boot settings

- -sb

**Result:**

```
...
UEFI variable access.....ok: UEFI
Supported: Yes
Secure boot: Enabled
Mode: User
Vendor keys: False
PK (Size 0x03ED):
    Type: (X509)
        Owner: 84A34C70-3900-441D-84626A659BD76647 (Siemens UCV7/03L/MEV5)
        Issuer: /C=DE/ST=BW/L=Karlsruhe/O=Siemens AG/OU=DF FA AS DH KHE
1/CN=PK UCV7 BOX
        Subject: /C=DE/ST=BW/L=Karlsruhe/O=Siemens AG/OU=DF FA AS DH KHE
1/CN=PK UCV7 BOX
        Serial: BD29DD373EB34988
        Valid: 170726111559Z to 270724111559Z
KEK (Size 0x0618):
    Type: (X509)
        Owner: 77FA9ABD-0359-4D32-BD6028F4E78F784B (Microsoft)
        Issuer: /C=US/ST=Washington/L=Redmond/O=Microsoft
Corporation/CN=Microsoft Corporation Third Party Marketplace Root
        Subject: /C=US/ST=Washington/L=Redmond/O=Microsoft
Corporation/CN=Microsoft Corporation KEK CA 2011
        Serial: 610AD1880000000000003
        Valid: 110624204129Z to 260624205129Z
db (Size 0x10AA):
    Type: (X509)
        Owner: 77FA9ABD-0359-4D32-BD6028F4E78F784B (Microsoft)
        Issuer: /C=US/ST=Washington/L=Redmond/O=Microsoft
Corporation/CN=Microsoft Root Certificate Authority 2010
        Subject: /C=US/ST=Washington/L=Redmond/O=Microsoft
Corporation/CN=Microsoft Windows Production PCA 2011
```

Serial: 61077656000000000008  
Valid: 111019184142Z to 261019185142Z  
Type: (X509)  
Owner: 77FA9ABD-0359-4D32-BD6028F4E78F784B (Microsoft)  
Issuer: /C=US/ST=Washington/L=Redmond/O=Microsoft Corporation/CN=Microsoft Corporation Third Party Marketplace Root  
Subject: /C=US/ST=Washington/L=Redmond/O=Microsoft Corporation/CN=Microsoft Corporation UEFI CA 2011  
Serial: 6108D3C4000000000004  
Valid: 110627212245Z to 260627213245Z  
Type: (X509)  
Owner: 84A34C70-3900-441D-84626A659BD76647 (Siemens UCV7/03L/MEV5)  
Issuer: /C=DE/ST=BW/L=Karlsruhe/O=Siemens AG/OU=DF FA AS DH KHE 1/CN=UCV7 BOX  
Subject: /C=DE/ST=BW/L=Karlsruhe/O=Siemens AG/OU=DF FA AS DH KHE 1/CN=UCV7 BOX  
Serial: F26AC8E46937854D  
Valid: 170726111111Z to 270724111111Z  
Type: (SHA-256)  
Owner: 0A47949A-1701-48AA-B71861A4453FD7B0 (Mine)  
Data:  
5D1F43B81993B6CFAA07179F2837115B9DF4B3519B8838C51F8986AC7CD9E6F1  
File: FlashMan.efs  
Owner: 00000000-0000-0000-000000000000  
Data:  
D07144FB52738D252427256C06CE4F9088DC912A672E5B3636F47481052EDB5F  
dbx (Size 0xE8C):  
Type: (SHA-256)  
Owner: 77FA9ABD-0359-4D32-BD6028F4E78F784B (Microsoft)  
Data:  
80B4D96931BF0D02FD91A61E19D14F1DA452E66DB2408CA8604D411F92659F0A  
Owner: 77FA9ABD-0359-4D32-BD6028F4E78F784B (Microsoft)  
Data:  
F52F83A3FA9CFBD6920F722824DBE4034534D25B8507246B3B957DAC6E1BCE7A  
Owner: 77FA9ABD-0359-4D32-BD6028F4E78F784B (Microsoft)  
Data:  
C5D9D8A186E2C82D09AFAA2A6F7F2E73870D3E64F72C4E08EF67796A840F0FBD  
Owner: 77FA9ABD-0359-4D32-BD6028F4E78F784B (Microsoft)

### 3.11 Secure Boot

```
Data:  
363384D14D1F2E0B7815626484C459AD57A318EF4396266048D058C5A19BBF76  
Owner: 77FA9ABD-0359-4D32-BD6028F4E78F784B (Microsoft)  
Data:  
1AEC84B84B6C65A51220A9BE7181965230210D62D6D33C48999C6B295A2B0A06  
...  
PKDefault (Size 0x03ED):  
Type: (X509)  
Owner: 84A34C70-3900-441D-84626A659BD76647 (Siemens UCV7/03L/MEV5)  
Issuer: /C=DE/ST=BW/L=Karlsruhe/O=Siemens AG/OU=DF FA AS DH KHE  
1/CN=PK UCV7 BOX  
Subject: /C=DE/ST=BW/L=Karlsruhe/O=Siemens AG/OU=DF FA AS DH KHE  
1/CN=PK UCV7 BOX  
Serial: BD29DD373EB34988  
Valid: 170726111559Z to 270724111559Z  
KEKDefault (Size 0x0618):  
Type: (X509)  
Owner: 77FA9ABD-0359-4D32-BD6028F4E78F784B (Microsoft)  
Issuer: /C=US/ST=Washington/L=Redmond/O=Microsoft  
Corporation/CN=Microsoft Corporation Third Party Marketplace Root  
Subject: /C=US/ST=Washington/L=Redmond/O=Microsoft  
Corporation/CN=Microsoft Corporation KEK CA 2011  
Serial: 610AD1880000000000003  
Valid: 110624204129Z to 260624205129Z  
dbDefault (Size 0x102E):  
Type: (X509)  
Owner: 77FA9ABD-0359-4D32-BD6028F4E78F784B (Microsoft)  
Issuer: /C=US/ST=Washington/L=Redmond/O=Microsoft  
Corporation/CN=Microsoft Root Certificate Authority 2010  
Subject: /C=US/ST=Washington/L=Redmond/O=Microsoft  
Corporation/CN=Microsoft Windows Production PCA 2011  
Serial: 61077656000000000008  
Valid: 111019184142Z to 261019185142Z  
Type: (X509)  
Owner: 77FA9ABD-0359-4D32-BD6028F4E78F784B (Microsoft)  
Issuer: /C=US/ST=Washington/L=Redmond/O=Microsoft  
Corporation/CN=Microsoft Corporation Third Party Marketplace Root
```

Subject: /C=US/ST=Washington/L=Redmond/O=Microsoft  
Corporation/CN=Microsoft Corporation UEFI CA 2011  
Serial: 6108D3C400000000000004  
Valid: 110627212245Z to 260627213245Z  
Type: (X509)  
Owner: 84A34C70-3900-441D-84626A659BD76647 (Siemens UCV7/03L/MEV5)  
Issuer: /C=DE/ST=BW/L=Karlsruhe/O=Siemens AG/OU=DF FA AS DH KHE  
1/CN=UCV7 BOX  
Subject: /C=DE/ST=BW/L=Karlsruhe/O=Siemens AG/OU=DF FA AS DH KHE  
1/CN=UCV7 BOX  
Serial: F26AC8E46937854D  
Valid: 170726111111Z to 270724111111Z  
dbxDefault (Size 0x0E8C):  
Type: (SHA-256)  
Owner: 77FA9ABD-0359-4D32-BD6028F4E78F784B (Microsoft)  
Data:  
80B4D96931BF0D02FD91A61E19D14F1DA452E66DB2408CA8604D411F92659F0A  
Owner: 77FA9ABD-0359-4D32-BD6028F4E78F784B (Microsoft)  
Data:  
F52F83A3FA9CFBD6920F722824DBE4034534D25B8507246B3B957DAC6E1BCE7A  
Owner: 77FA9ABD-0359-4D32-BD6028F4E78F784B (Microsoft)  
Data:  
C5D9D8A186E2C82D09AFAA2A6F7F2E73870D3E64F72C4E08EF67796A840F0FBD  
Owner: 77FA9ABD-0359-4D32-BD6028F4E78F784B (Microsoft)  
Data:  
363384D14D1F2E0B7815626484C459AD57A318EF4396266048D058C5A19BBF76  
Owner: 77FA9ABD-0359-4D32-BD6028F4E78F784B (Microsoft)  
Data:  
1AEC84B84B6C65A51220A9BE7181965230210D62D6D33C48999C6B295A2B0A06  
...

---

### 3.11 Secure Boot

#### 3.11.2.2 Loading Secure Boot defaults

If no PK is installed yet and the respective default variables (s. -sb) are available, the Secure Boot default settings for the respective database (db, dbx, KEK, PK) can be loaded.

Without options (-sb default), all four databases will be restored from the default settings. You have the option to set the database, which, for example, allows you to add an entry to the defaults.

```
-sb default db dbx KEK
-sb add db sha256 Shell.efi
-sb add db sha256 FwMgr.efi
-sb default PK
```

---

##### Note

Secure Boot is activated with setting the PK. It is then no longer possible to start programs that are not in the db. If FwMgr.efi is not in db, it cannot be called after setting the PK.

---

#### 3.11.2.3 Changing Secure Boot settings

If the PK is installed, all changes to the Secure Boot settings must be appropriately signed.

- db/dbx  
Certificate/key from the database KEK (Key Exchange Key) or the PK (Platform Key)
- KEK/PK  
Certificate/key of the PK

The certificate and the key for signing can be specified as follows:

```
-sb param <Zertifikat> <Key> [Optional: Passwort]
```

The file name of the certificate and the key are stored in the IPCFlash.ini file. This means that it is not necessary to specify -sb param every time the PK is called. There is an attempt to load these files with future calls of -sb. If these files are not found, the entry is deleted from the configuration file. You can specify other files at any time using -sb param .

##### Example: Add db entry

```
-sb param MyKEK.cer MyKEK.key -sb add db X509 MyDbCert.cer
```

#### 3.11.2.4 Initialization with own Secure Boot settings

When initializing with own Secure Boot settings, the order should be:

db, KEK, PK.

##### Example:

```
-sb add db sha256 MyBootFile.efi
-sb add db x509 MyBootCert.cer
-sb add KEK x509 MyKEK.cer
-sb add PK x509 MyPK.cer
```

Secure Boot is activated with the last instruction (setting the PK).