

# SIEMENS

## SIMATIC

### Industrial PC Microsoft® Windows® 10

#### Operating Instructions

<u>Safety instructions</u>	<b>1</b>
<u>Initial startup: Commissioning the operating system</u>	<b>2</b>
<u>Restoring operating system and partitions</u>	<b>3</b>
<u>Configuring and updating the operating system</u>	<b>4</b>
<u>Extended scope of delivery of the provided USB stick</u>	<b>5</b>

## 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.

<b>⚠ DANGER</b>
indicates that death or severe personal injury <b>will</b> result if proper precautions are not taken.
<b>⚠ WARNING</b>
indicates that death or severe personal injury <b>may</b> result if proper precautions are not taken.
<b>⚠ CAUTION</b>
indicates that minor personal injury can result if proper precautions are not taken.
<b>NOTICE</b>
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:

<b>⚠ WARNING</b>
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>4</b>
1.1	Industrial Security .....	4
1.2	Disclaimer for third-party software updates .....	5
1.3	Notes on protecting administrator accounts .....	5
<b>2</b>	<b>Initial startup: Commissioning the operating system .....</b>	<b>6</b>
<b>3</b>	<b>Restoring operating system and partitions .....</b>	<b>7</b>
<b>4</b>	<b>Configuring and updating the operating system.....</b>	<b>9</b>
4.1	Changing the display language, region and formats of the operating system.....	9
4.2	Installing new display languages for the operating system from the provided USB stick .....	10
4.3	Updating the operating system .....	10
4.4	Display and manage data storage mediums .....	11
4.5	BitLocker with Trusted Platform Module (TPM).....	11
4.6	Unified Write Filter (UWF).....	12
4.6.1	Unified Write Filter (UWF).....	12
4.6.2	Enabling UWF .....	12
4.6.3	Configuring UWF in a command line window.....	13
<b>5</b>	<b>Extended scope of delivery of the provided USB stick.....</b>	<b>16</b>
5.1	Display languages supplied for the operating system .....	16
	<b>Index.....</b>	<b>17</b>

# 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>)

## 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.

## Initial startup: Commissioning the operating system

An operating system with installed device drivers and SIEMENS software products is already installed on your device in the delivery state.

After the initial startup, you can make the following personal settings using the menu:

- Set the display language and region
- Create a user account

### Requirements

- **No** USB data storage media are connected to the device.
- For devices with optical drives:  
There is **no** data storage medium in the optical drive.
- A keyboard, a mouse and a monitor are connected to the device.
- The default settings in the BIOS Setup are unchanged before the operating system is commissioned.

### Procedure

**NOTICE****Operational safety of the device and system in danger**

Faulty or interrupted commissioning of the operating system can put the operational safety of your device and the system at risk.

Therefore, note the following:

- Do not switch off the device during commissioning.

1. Switch on the device.
2. The operating system sets up automatically. During this process, the device can restart several times.
3. Wait until you are prompted to select the language.
4. Type in the product key as required. The product key is located on the "Certificate of Authenticity" label (COA label) or on an enclosed "Certificate of Authenticity Card".
5. Follow the instructions on the screen.

Once the user has logged on for the first time and the Windows® user interface has loaded, the operating system is fully operational.

# Restoring operating system and partitions

You can restore the factory settings of the target system (i.e. the volume partitions, the operating system with installed device drivers, and the SIEMENS software products).

This allows you to restore your device quickly if it has suffered damage.

## Setting Boot mode

---

### Note

We recommend that you restore the target system in the Boot mode that was set in the delivery state.

You can find information on this in the operating instructions of the device.

---

You can restore the target system in the following two boot modes:

### UEFI mode (GPT volume):

To support new features, such as TPM 2.0, Secure Boot and volumes larger than 2 TB, the operating system must be restored in the way that it boots in UEFI mode.

For this purpose, the provided USB stick must also be booted in UEFI mode.

The target system is then set up with a GPT volume and boots in UEFI mode.

### Legacy mode (MBR volume):

To support older extensions and functions, such as older PCI(e) cards and older software products, the operating system must be restored to boot in Legacy mode.

For this purpose, the provided USB stick must also be booted in Legacy mode.

The target system is then set up with an MBR volume and boots in Legacy mode.

## Requirements

If the data of partition D: (Data) should be retained during restore (see section "Selecting the partitions to be restored"), be aware of the following requirement:

- The complete target system is partitioned as in the delivery state.
- The target system is restored in the Boot mode that was set in the delivery state.

You can find information on the delivery state in the operating instructions of the device.

## Procedure

---

### Note

The firmware settings might have to be changed in order for the device to boot from the provided USB stick.

You can find additional information on this in the description of the firmware/BIOS for the device.

---

<b>NOTICE</b>
<b>Risk of data loss</b> Files, user settings as well as existing authorizations and license keys are lost when a restore is performed! <ul style="list-style-type: none"><li>• Back up your data before restoring.</li></ul>



1. Insert the provided USB stick into the device.
2. Restart the device.
3. Boot with the provided USB stick in the Boot mode you have set beforehand.  
The Restore program from Siemens starts after a few seconds.
4. Follow the instructions on the screen.

Note the following information.

## Selecting the partitions to be restored

### Option: "Restore complete system disk"

Use this option if you want to restore the entire target system, including the partitions C: (System) and D: (Data).

### Option: "Restore existing system partition only"

Use this option if you are want to restore only the C: (System) and the boot functionality. The partition D: (Data) and all data stored there is retained.

## Selecting the scope of restoration (operating system version)

### Option: "Factory settings"

Use this option if you want to restore the factory settings of the operating system with the installed device drivers and the SIEMENS software products.

### Option: "Administrator Basic"

Use this option if you only want to restore the operating system without additional device drivers and without SIEMENS software products.

# Configuring and updating the operating system

## 4.1 Changing the display language, region and formats of the operating system

### Changing the settings of the logged-in user account

1. Select: "Start > Settings > Time & language".
2. Make the desired changes in the following areas:
  - "Date & time"
  - "Region & language"

### Changing the system account and the standard user account settings

You can change the settings for the display language, region and formats of the system account (for example, the display language in the user login dialog) and the settings of the standard user account (default setting for new users).

The settings of the registered user are copied to the system account and the standard user account for this purpose.

1. Select: "Start > Settings > Time & language".
2. In the "Region & language" area, for the "Add a language" option define a desired "default" language.

## 4.2 Installing new display languages for the operating system from the provided USB stick

Install new display languages for the operating system if you want to select a language other than the languages available for selection in the settings for display language, region, and format settings.

You can find information on the languages that can be installed from the provided USB stick in the section "Display languages supplied for the operating system (Page 16)".

### Requirements

- You have administrator rights for the system.
- A keyboard is connected to the device.

### Procedure

1. Insert the provided USB stick into the device.
2. Press the key combination "Windows + r".
3. Enter "lpksetup" in the text box and confirm your entry.
4. In the "Install or uninstall display languages" window, click on the "Install display languages" button.
5. Select the language that you want to install from the "Languagepacks" folder on the provided USB stick.

## 4.3 Updating the operating system

As described in the section "Industrial Security (Page 4)", we recommend updating the operating system as soon as the appropriate updates are available.

### Requirement

- You have administrator rights for the system.
- The device is connected to the Internet.

### Procedure

1. Select "Start > Settings > Update & security > Windows Update > Check for update".  
Windows® determines the updates that are not installed.
2. Then start the download and installation process.

## 4.4 Display and manage data storage mediums

### Requirement

- You have administrator rights for the system.
- A keyboard is connected to the device.

### Procedure

1. Press the key combination "Windows + r".
2. Enter "diskmgmt.msc" in the text box and confirm your entry.  
The Windows disk management opens.

### Result

- The Windows disk management shows all data storage media available on your system.
- In the Windows disk management you can partition and format the data storage media.

## 4.5 BitLocker with Trusted Platform Module (TPM)

"BitLocker" drive encryption can be used together with the "Trusted Platform Module" (TPM).

To be able to use TPM, the TPM functionality must be activated in the BIOS setup and the operating system must be booted in UEFI mode.

<b>NOTICE</b>
<b>Risk of data loss if the password is lost</b>
If the password for data encryption is lost, it will no longer be possible to decrypt the data, for example, after a BIOS update.
Please store your passwords with care and protect them from unauthorized access.

## 4.6 Unified Write Filter (UWF)

### 4.6.1 Unified Write Filter (UWF)

The Unified Write Filter is a configurable write filter that makes it possible to assign write-protection to data storage media, such as hard disks, CFast cards, SSDs, internal USB drives, or external SATA drives.

External removable data storage media such as USB sticks and other flash drives, which are recognized by the operating system as a removable data storage medium, are not supported.

UWF combines the advantages of older write filters such as EWF and FBWF. It prevents all write access to protected media and transfers the data to buffer memory (overlay). This increases the reliability and stability of the system as well as the service life of write-sensitive media such as SSDs and CFast cards.

---

#### Note

UWF is disabled in the delivery state.

Note that memory is reduced when UWF is enabled.

---

<b>NOTICE</b>
<b>Risk of data loss with enabled UWF</b>
When UWF is enabled, all changes made to storage media with a UWF write protection after booting can be lost when the device is shut down. Proceed as follows to prevent this situation:
<ul style="list-style-type: none"><li>• Make changes to storage media only when UWF is disabled.</li></ul>



### 4.6.2 Enabling UWF

1. Press the key combination "Windows + x".
2. Select "Programs and Features".
3. Select "Turn Windows features on or off".
4. In the "Windows Features" window, click on the plus sign before the "Device Lockdown" item.
5. Enable the sub-item "Unified Write Filter" and confirm your selection with OK.
6. Restart your PC.

### 4.6.3 Configuring UWF in a command line window

1. Open a command line window with administrator rights.
2. To configure UWF, enter the following commands:

#### Calling help for individual commands

You can open the help for a single option with the "Help" command, for example: `uwfmgr volume help` opens the help for configuring volumes.

Function	Command	Note
<b>filter: set filter-specific and global settings</b>		
Enabling UWF	<code>uwfmgr filter enable</code>	Restart required
Disable UWF	<code>uwfmgr filter disable</code>	Restart required
Enable Hibernate Once Resume Many	<code>uwfmgr filter enable-horm</code>	
Disable Hibernate Once Resume Many	<code>uwfmgr filter disable-horm</code>	
Reset UWF settings	<code>uwfmgr filter reset-settings</code>	
<b>overlay: Configure overlay settings</b>		
Set the size of the overlay memory in MB	<code>uwfmgr overlay set-size</code>	Example: <ul style="list-style-type: none"> <li>• <code>uwfmgr overlay set-size 1024</code></li> </ul>
Set the type of overlay memory (RAM / disk)	<code>uwfmgr overlay set-type</code>	Example: <ul style="list-style-type: none"> <li>• <code>uwfmgr overlay set-type Disk</code></li> </ul>
Set the size of the overlay memory in MB as of which a memory warning occurs	<code>uwfmgr overlay set-warningthreshold</code>	Example: <ul style="list-style-type: none"> <li>• <code>uwfmgr overlay set-warningthreshold 256</code></li> </ul>
Set the size of the overlay memory in MB as of which a critical memory warning occurs	<code>uwfmgr overlay set-criticalthreshold</code>	Example: <ul style="list-style-type: none"> <li>• <code>uwfmgr overlay set-criticalthreshold 768</code></li> </ul>
Display overlay settings for this and the next session	<code>uwfmgr overlay get-config</code>	
Display free overlay memory for this session	<code>uwfmgr overlay get-availablespace</code>	
Display the current amount of overlay memory	<code>uwfmgr overlay get-consumption</code>	

4.6 Unified Write Filter (UWF)

Function	Command	Note
<b>volume: Make volume-specific settings</b>		
Enable protection for a volume	<code>uwmgr volume protect</code>	<p>Restart required</p> <p>Examples:</p> <ul style="list-style-type: none"> <li><code>uwmgr volume protect C:</code></li> <li><code>uwmgr volume protect \\?\GLOBALROOT\Device\HarddiskVolume1</code></li> <li><code>uwmgr volume protect \\?\Volume{4c1b02c1-d990-11dc-99ae-806e6f6e6963}</code></li> <li><code>uwmgr volume protect all</code></li> </ul>
Disable protection for a volume	<code>uwmgr volume unprotect</code>	<p>Example:</p> <ul style="list-style-type: none"> <li><code>uwmgr volume unprotect all</code></li> </ul>
Display configuration a volume for this and the next session	<code>uwmgr volume get-config</code>	<p>Example:</p> <ul style="list-style-type: none"> <li><code>uwmgr volume get-config all</code></li> </ul>
<b>registry: Configure and apply registry filters</b>		
Add a registry key to the exception list	<code>uwmgr registry add-exclusion</code>	<p>Restart required</p> <p>The registry key must exist at the time of configuration.</p> <p>Example:</p> <ul style="list-style-type: none"> <li><code>uwmgr registry add-exclusion HKLM\Software\Microsoft\Windows\run</code></li> </ul>
Remove a registry key from the exception list	<code>uwmgr registry remove-exclusion</code>	<p>Restart required</p> <p>Example:</p> <ul style="list-style-type: none"> <li><code>uwmgr registry remove-exclusion HKLM\Software\Microsoft\Windows\run</code></li> </ul>
Display exception list of this and the next session	<code>uwmgr registry get-exclusions</code>	
Apply a change to a registry value	<code>uwmgr registry commit</code>	<p>Example:</p> <ul style="list-style-type: none"> <li><code>uwmgr registry commit HKLM\Software\Test TestValue</code></li> </ul>
Delete a registry key or registry value	<code>uwmgr registry commit-delete</code>	<p>Example:</p> <ul style="list-style-type: none"> <li><code>uwmgr registry commit-delete HKLM\Software\Test TestValue</code></li> </ul>

Function	Command	Note
<b>servicing: Manage UWF Service Mode</b>		
Enable UWF Service Mode	<code>uwfmgr servicing enable</code>	Restart required
Disable UWF Service Mode	<code>uwfmgr servicing disable</code>	
Updating Windows	<code>uwfmgr servicing update-windows</code>	
Display the servicing status of UWF for this and the next session	<code>uwfmgr servicing get-config</code>	
<b>file: Configure exclusion settings for files and directories</b>		
Add a file or directory to the list of excluded files from a protected volume	<code>uwfmgr file add-exclusion</code>	Restart required Example: <ul style="list-style-type: none"> <li><code>uwfmgr file add-exclusion c:\dir1\dir2.txt</code></li> </ul>
Remove the file or directory from the list of excluded files from a protected volume	<code>uwfmgr file remove-exclusion</code>	Restart required Example: <ul style="list-style-type: none"> <li><code>uwfmgr file remove-exclusion \\?\Volume{4c1b02c1-d990-11dc-99ae-806e6f6e6963}\dir1\dir2.txt</code></li> </ul>
Display configuration information for exclusion of files for this and the next session	<code>uwfmgr file get-exclusions</code>	Example: <ul style="list-style-type: none"> <li><code>uwfmgr file get-exclusions all</code></li> </ul>
Apply change to the specified file	<code>uwfmgr file commit</code>	No commits can be performed for folders. Example: <ul style="list-style-type: none"> <li><code>uwfmgr file commit c:\dir1\dir2.txt</code></li> </ul>
Apply the deletion of a file	<code>uwfmgr file commit-delete</code>	A commit may be performed to delete a folder. However, the folder must be empty from the time of the last reboot. Example: <ul style="list-style-type: none"> <li><code>uwfmgr file commit-delete c:\dir1\dir2.txt</code></li> </ul>

A detailed guide to UWF can be found on the Internet (<https://docs.microsoft.com/en-us/windows-hardware/customize/enterprise/unified-write-filter>).

## Extended scope of delivery of the provided USB stick

### 5.1 Display languages supplied for the operating system

The following display languages for the operating system are stored in the "Languagepacks" folder on the provided USB stick:

Language (Country)	Country	Abbreviation
German	Germany	de-De
English	USA	en-us
Spanish	Spain	es-es
French	France	fr-fr
Italian	Italy	it-it
Japanese	Japan	ja-jp
Korean	Korea	ko-kr
Russian	Russian Federation	ru-ru
Chinese	China	zh-cn
Chinese	Taiwan	zh-tw
Arabic	Saudi Arabia	ar-sa
Bulgarian	Bulgaria	bg-bg
Czech	Czech Republic	cs-cz
Danish	Denmark	da-dk
Greek	Greece	el-gr
English	Great Britain	en-gb
Estonian	Estonia	et-ee
Finnish	Finland	fi-fi
French	Canada	fr-ca
Hebrew	Israel	he-il
Croatian	Croatia	hr-hr
Hungarian	Hungary	hu-hu
Lithuanian	Lithuania	lt-lt
Latvian	Latvia	lv-lv
Norwegian/Bokmål	Norway	nb-no
Dutch	The Netherlands	nl-nl
Polish	Poland	pl-pl
Portuguese	Brazil	pt-br
Portuguese	Portugal	pt-pt
Romanian	Romania	ro-ro
Slovakian	Slovakia	sk-sk
Slovenian	Slovenia	sl-si
Serbian/Latin	Serbia	sr-latn-rs
Swedish	Sweden	sv-se
Thai	Thailand	th-th
Turkish	Turkey	tr-tr
Ukrainian	Ukraine	uk-ua

# Index

## B

- Boot mode
  - Legacy mode, 7
  - UEFI mode, 7

## C

- Certificate of Authenticity, 6
- COA label, (Certificate of Authenticity)
- Configuring
  - Operating system, 11

## D

- Data storage medium
  - Displaying and managing, 11
- Disk management, 11
- Display languages for the operating system
  - Installing new display languages, 10
  - Provided, 16
  - Setting, 9

## G

- GPT volume, 7

## L

- Legacy mode
  - Restore, 7

## M

- MBR volume, 7

## O

- Operating system
  - Configuring, 11
  - Restoring, 8
  - Setting display languages, 9
  - Updating, 10

## P

- Product key, 6

## S

- Standard user account, 9
- Switching on, 6
- System account, 9

## T

- Trusted Platform Module, (TPM)

## U

- UEFI mode
  - Restore, 7
- Unified Write Filter, (UWF)
- Update
  - Operating system, 10
- UWF, 12
  - Configuring, 13

