SIEMENS

SINUMERIK

SINUMERIK 828D
PCU-Basesoftware /IPC

Commissioning Manual

Introduction 1

Fundamental safety instructions 2

PCU-Basesoftware /IPC Microsoft Windows 10 3

First commissioning of SIMATIC IPCs 4

Configuration of the system 5

Installing and configuring updates and automation software 6

Backing up and restoring data 7

Service and diagnostics 8

Appendix A

Valid for:

CNC software V5.24
SINUMERIK PCU Base V15.0 SP3
Microsoft Windows 10

07/2024
A5E52001635B AE

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 Aktiengesellschaft. 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.

Siemens Aktiengesellschaft
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

A5E52001635B AE
Ⓟ 07/2024 Subject to change

Copyright © Siemens 2022 - 2024.
All rights reserved

Table of contents

1 Introduction 9

1.1 About SINUMERIK 9

1.2 About this documentation 10

1.3 Documentation on the internet 11
1.3.1 Documentation overview SINUMERIK 828D 11
1.3.2 Documentation overview SINUMERIK operator components 11

1.4 Feedback on the technical documentation 13

1.5 mySupport documentation 14

1.6 Service and Support 15

1.7 Using OpenSSL 17

1.8 Compliance with the General Data Protection Regulation 18

2 Fundamental safety instructions 19

2.1 General safety instructions 19

2.2 Equipment damage due to electric fields or electrostatic discharge 23

2.3 Warranty and liability for application examples 24

2.4 Cybersecurity information 25

2.5 Residual risks of power drive systems 26

3 PCU-Basesoftware /IPC Microsoft Windows 10 29

3.1 Hardware and software requirements 30
3.1.1 Supported SIMATIC IPC/IFP/ITC 30
3.1.2 Software and tools 32

3.2 Hardware configuration of SIMATIC IPC 34
3.2.1 Network settings 34
3.2.2 Partitioning of the SSD 34

3.3 Directory structure and file conventions 36

4 First commissioning of SIMATIC IPCs 37

4.1 Overview 37

4.2 Adapting the installation settings 38

4.3 Installing PCU-Basesoftware /IPC 39

5 Configuration of the system 41

5.1 Overview 41

5.2 Managing user accounts 42

5.3 Changing the name of the PC system 43

5.4 Setting the IP address and domain ... 44
5.5 Configuring USB interfaces ... 45
5.6 Configuring an SMB client ... 46
5.7 Configuring network access on the USB data storage medium ... 48
5.8 Displaying USB data memories with several partitions ... 49
5.9 Configuring the keyboard layout ... 50
5.10 Setting up an external screen ... 51
5.11 Setting the screen resolution ... 52
5.12 Set the resolution in the tcu.ini ... 53
5.13 Setting the color depth in the tcu.ini file ... 55
5.14 Setting the display for portrait or landscape in the tcu.ini file ... 56
5.15 Activating/deactivating the touchpad or other pointer devices ... 57
5.16 Configuring the SITOP UPS module for use with PCU-Basesoftware /IPC ... 58
5.16.1 Overview of SITOP UPS ... 58
5.16.2 SITOP modules for IPC ... 59
5.16.3 Configuring SITOP software for PCU Base ... 60
5.16.3.1 Configuring SITOP software V3.x (USB) ... 60
5.16.3.2 Configuring SITOP UPS Manager (Ethernet) ... 65
5.16.4 Hardware configuration of the SITOP UPS module ... 66
5.17 Configuration of the Service Center ... 69
5.17.1 Overview ... 69
5.17.2 Configuration of the network adapter ... 69
5.17.3 Configuration of the host ... 71
5.18 Adapting the firewall settings ... 72
5.18.1 Overview ... 72
5.18.2 Factory setting of the Microsoft Windows Firewall on the PC system ... 73
5.18.3 General information on the operating principle of the Microsoft Windows Firewall ... 74
5.18.4 General information on the settings recommended for Microsoft Windows ... 74
5.18.5 Configuration by means of a prompt or script/batch file ... 75
5.18.6 Enabling SNMP communication ... 76
5.18.7 Activate the remote access to the PC system ... 78
5.18.7.1 Overview ... 78
5.18.7.2 Via the Control Panel ... 78
5.18.7.3 By prompt, script or batch file ... 79
5.18.8 Activation/deactivation of the file and printer release ... 80
5.18.8.1 Overview ... 80
5.18.8.2 General information ... 82
5.18.8.3 General activation for all network profiles ... 82
5.18.8.4 Activation for a specific network profile ... 85
5.18.8.5 Activation for a specific connection ... 89
5.18.9 Activation of the ping execution (ICMP) ... 90
5.18.9.1 Via the Control Panel ... 90
5.18.9.2 By prompt, script or batch file ... 91
5.18.10 Saving and restoring firewall settings ... 92
5.18.10.1 Overview ... 92

5.18.10.2 Backup of firewall settings ... 93
5.18.10.3 Restoring of firewall settings ... 94

5.19 Using BitLocker drive encryption ... 97
5.19.1 Activating BitLocker setup ... 98
5.19.2 Configuring BitLocker via Microsoft Windows ... 100
5.19.3 Configuring BitLocker using a script ... 101

6 Installing and configuring updates and automation software ... 103

6.1 Overview ... 103

6.2 Patch management and security updates ... 104

6.3 Configuring Microsoft Windows log files storage ... 105

6.4 Installing and setting up SINUMERIK Operate ... 106
6.4.1 Installing SINUMERIK Operate /PCU Modular ... 106
6.4.2 Setting up SINUMERIK Operate for autologon mode ... 107
6.4.3 Modifying the user account for autologon mode. ... 108
6.4.4 Using interactive or silent installation versions ... 109
6.4.5 Configuring the PG/PC interface ... 111
6.4.6 Starting and setting up SINUMERIK Operate /PCU Modular ... 112
6.4.7 Configuring the SINUMERIK Operate display size ... 113
6.4.8 FindWindow program application ... 115
6.4.9 Further SINUMERIK Operate settings ... 117
6.4.9.1 Using user interfaces in parallel ... 117
6.4.9.2 Changing the skin design ... 118
6.4.9.3 Setting OEM functions for the softkeys "HMI restart" and "EXIT" ... 119
6.4.9.4 Defining the access right for the "EXIT" softkey ... 120
6.4.9.5 Inserting a user-specific run up screen ... 120
6.4.10 Integrating and parameterizing the OEMFrame application ... 121
6.4.10.1 Integrating an OEMFrame application into HMI sl ... 121
6.4.10.2 Creating configuration files ... 121
6.4.10.3 Parameterizing the OEMFrame application ... 129
6.4.10.4 Using parameters ... 131

6.5 Configuring a key filter for HMI software ... 138

6.6 Installing STEP 7 ... 142

6.7 Linking the HMI software with STEP 7 ... 143

6.8 PCU Installer ... 144
6.8.1 Overview ... 144
6.8.2 Activating the PCU Installer ... 144
6.8.2.1 Overview ... 144
6.8.2.2 Activating via a configuration template ... 145
6.8.3 Deactivating the PCU Installer ... 146
6.8.4 Copying and adapting the configuration file ... 147
6.8.5 Reference to the PCUInst.ini configuration file ... 148
6.8.6 Installing software with the PCU Installer ... 152
6.8.7 Procedure example of an installation with the PCU Installer ... 152
6.8.8 Log files (.log) ... 153
6.8.9 Program application Configure for CMC ... 154

6.9 Migration ... 156

7 Backing up and restoring data ... 157

7.1 Overview ... 157

7.2 Using Paragon Hard Disk Manager for data backup and restoration ... 158
7.2.1 Starting the Paragon Hard Disk Manager directly ... 158
7.2.2 Creating a disk image with Paragon Hard Disk Manager ... 159
7.2.3 Restoring a disk image with Paragon Hard Disk Manager ... 160
7.2.4 Securely deleting the SSD data storage medium ... 161

7.3 Starting the Service Center ... 163

7.4 Functions of the Service Center ... 164

7.5 Network settings in the Service Center ... 166

7.6 Create a disk image of the SSD ... 169

7.7 Restore a disk image of the SSD ... 171

7.8 Create a disk image of a partition ... 174

7.9 Restore a disk image of a partition ... 176

7.10 Network settings in the Service Center ... 179

7.11 Decrypting BitLocker-protected partitions ... 181

7.12 Creating an emergency boot system USB flash drive ... 183

7.13 Operating a service PC/PC in the network ... 184
7.13.1 Overview ... 184
7.13.2 Connection options in the system network ... 184
7.13.3 Configuring routing in the network ... 186
7.13.4 Configure the network settings of the PG/PC ... 187
7.13.5 Release directory of the PC/PC in the network ... 190
7.13.6 Creating a shortcut to the network drive ... 193

7.14 Starting up the replacement SSD ... 195

8 Service and diagnostics ... 197

8.1 Setting of the operating mode during run-up ... 197
8.1.1 Software-side setting (SIMATIC IPC) ... 197

8.2 Switching to the Service Desktop during autostart / autologon operation ... 198

8.3 Configuring the SINUMERIK power up screen ... 200

8.4 Remote access ... 202
8.4.1 Overview ... 202
8.4.2 Searching for devices in the system network ... 202
8.4.3 Display of accessible stations in SINUMERIK Operate ... 202
8.4.4 Remote access for operation and maintenance ... 203
8.4.5 Setting up and using SSH ... 205
8.4.6 Encryption via SSH protocol ... 206
8.4.7 Using individual SSH authorization for Operate ... 207

A Appendix ... 213

A.1 Script example for BitLocker activation ... 213

A.2 Overview of Microsoft Windows changes ... 215

A.3 Abbreviations 220
Index 223

Introduction

1

1.1 About SINUMERIK

From simple, standardized CNC machines to premium modular machine designs – the SINUMERIK CNCs offer the right solution for all machine concepts. Whether for individual parts or mass production, simple or complex workpieces – SINUMERIK is the highly dynamic automation solution, integrated for all areas of production. From prototype construction and tool design to mold making, all the way to large-scale series production.

Visit our website for more information SINUMERIK (https://www.siemens.com/sinumerik).

1.2 About this documentation

Target group

This document is intended for commissioning personnel.

The plant or system is installed, connected and ready to start. For the following steps, e.g. configuring the individual components, the Commissioning Manual contains all the necessary information or at least references.

Benefits

The Commissioning Manual allows the target group to test and commission the plant or the system in a professional and safe way.

Usage phase: Setup and commissioning phase

Standard scope

This documentation only describes the functionality of the standard version. This may differ from the scope of the functionality of the system that is actually supplied. Please refer to the ordering documentation only for the functionality of the supplied drive system.

It may be possible to execute other functions in the system which are not described in this documentation. This does not, however, represent an obligation to supply such functions with a new control or when servicing.

For reasons of clarity, this documentation cannot include all of the detailed information on all product types. Further, this documentation cannot take into consideration every conceivable type of installation, operation and service/maintenance.

The machine manufacturer must document any additions or modifications they make to the product themselves.

Websites of third-party companies

This document may contain hyperlinks to third-party websites. Siemens is not responsible for and shall not be liable for these websites and their content. Siemens has no control over the information which appears on these websites and is not responsible for the content and information provided there. The user bears the risk for their use.

1.3 Documentation on the internet

1.3.1 Documentation overview SINUMERIK 828D

Comprehensive documentation about the functions provided in SINUMERIK 828D Version 4.8 SP4 and higher is provided in the 828D documentation overview (https://support.industry.siemens.com/cs/ww/en/view/109766724).



You can display documents or download them in PDF and HTML5 format.

The documentation is divided into the following categories:

- User: Operating
- User: Programming
- Manufacturer/Service: Configuring
- Manufacturer/Service: Commissioning
- Manufacturer/Service: Functions
- Manufacturer/Service: Safety Integrated
- SINUMERIK Integrate/MindApp
- Info & Training

1.3.2 Documentation overview SINUMERIK operator components

Comprehensive documentation about the SINUMERIK operator components is provided in the Documentation overview SINUMERIK operator components (https://support.industry.siemens.com/cs/document/109783841/technische-dokumentation-zu-sinumerik-bedienkomponenten?dti=0&lc=en-WW).

You can display documents or download them in PDF and HTML5 format.

The documentation is divided into the following categories:

- Operator Panels
- Machine control panels

- Machine Pushbutton Panel
- Handheld Unit/Mini handheld devices
- Further operator components

An overview of the most important documents, entries and links to SINUMERIK is provided at SINUMERIK Overview - Topic Page (https://support.industry.siemens.com/cs/document/109766201/sinumerik-an-overview-of-the-most-important-documents-and-links?dti=0&lc=en-WW).

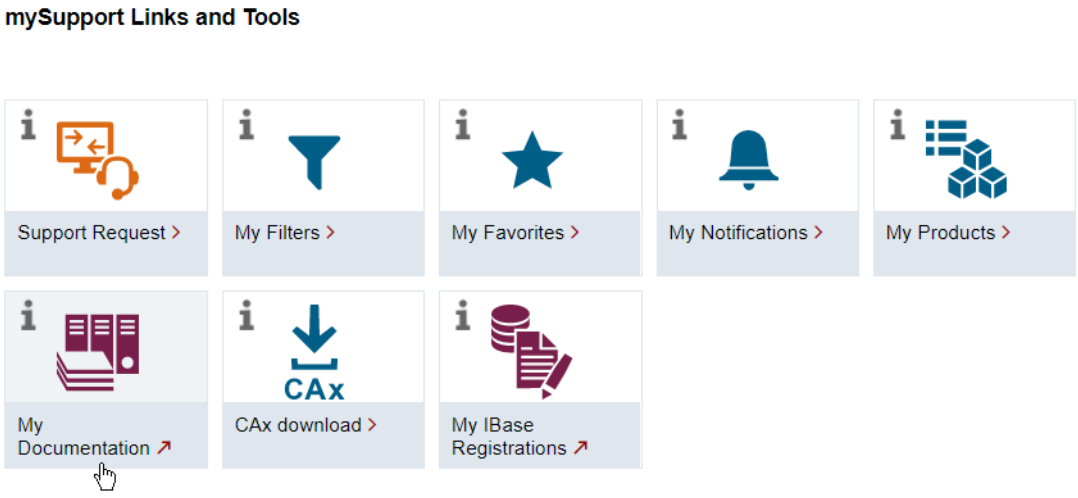
1.4 Feedback on the technical documentation

If you have any questions, suggestions, or corrections regarding the technical documentation published in the Siemens Industry Online Support, use the "Provide feedback" link which appears at the end of the entry.

1.5 mySupport documentation

With the "mySupport documentation" web-based system you can compile your own individual documentation based on Siemens content, and adapt it for your own machine documentation.

To start the application, click on the "My Documentation" tile on the "mySupport links and tools" (https://support.industry.siemens.com/cs/ww/en/my) portal page:



The configured manual can be exported in RTF, PDF or XML format.

Note

Siemens content that supports the mySupport documentation application can be identified by the presence of the "Configure" link.

1.6 Service and Support

Product support

You can find more information about products on the internet:

Product support (https://support.industry.siemens.com/cs/ww/en/)

The following is provided at this address:

- Up-to-date product information (product announcements)
- FAQs (frequently asked questions)
- Manuals
- Downloads
- Newsletters with the latest information about your products
- Global forum for information and best practice sharing between users and specialists
- Local contact persons via our Contacts at Siemens database (→ "Contact")
- Information about field services, repairs, spare parts, and much more (→ "Field Service")

Technical support

Country-specific telephone numbers for technical support are provided on the internet at address (https://support.industry.siemens.com/cs/ww/en/sc/4868) in the "Contact" area.

If you have any technical questions, please use the online form in the "Support Request" area.

Training

You can find information on SITRAIN at the following address (https://www.siemens.com/sitrain).
SITRAIN offers training courses for automation and drives products, systems and solutions from Siemens.

Siemens support on the go



With the award-winning "Industry Online Support" app, you can access more than 300,000 documents for Siemens Industry products – any time and from anywhere. The app can support you in areas including:

- Resolving problems when implementing a project
- Troubleshooting when faults develop
- Expanding a system or planning a new system

Furthermore, you have access to the Technical Forum and other articles from our experts:

- FAQs
- Application examples
- Manuals
- Certificates
- Product announcements and much more

The "Industry Online Support" app is available for Apple iOS and Android.

1.7 Using OpenSSL

This product can contain the following software:

- Software developed by the OpenSSL project for use in the OpenSSL toolkit
- Cryptographic software created by Eric Young.
- Software developed by Eric Young

You can find more information on the internet:

- OpenSSL (https://www.openssl.org)
- Cryptsoft (https://www.cryptsoft.com)

1.8 Compliance with the General Data Protection Regulation

Siemens observes standard data protection principles, in particular the data minimization rules (privacy by design).

For this product, this means:

The product does not process or store any personal data, only technical function data (e.g. time stamps). If the user links this data with other data (e.g. shift plans) or if he/she stores person-related data on the same data medium (e.g. hard disk), thus personalizing this data, he/she must ensure compliance with the applicable data protection stipulations.

SecureDigital Cards

- Do not remove the memory card while it is being accessed. This can lead to damage of the memory card and the SINUMERIK as well as the data on the memory card.
- Insert the memory card carefully and the right way round into the memory card slot (observe indicators such as arrow or similar). This way you avoid mechanical damage to the memory card or the device.
- Only use memory cards that have been approved by Siemens for use with SINUMERIK. Even though SINUMERIK follows general industry standards for memory cards, it is possible that memory cards from some manufacturers will not function perfectly in this device or are not completely compatible with it (you can obtain information on compatibility from the memory card manufacturer or supplier).
- For further information on handling SecureDigital Cards, please refer to the NCU manuals.

Fundamental safety instructions 2

2.1 General safety instructions



⚠ WARNING

Electric shock and danger to life due to other energy sources

Touching live components can result in death or severe injury.

- Only work on electrical devices when you are qualified for this job.
- Always observe the country-specific safety rules.

Generally, the following steps apply when establishing safety:

1. Prepare for disconnection. Notify all those who will be affected by the procedure.
2. Isolate the drive system from the power supply and take measures to prevent it being switched back on again.
3. Wait until the discharge time specified on the warning labels has elapsed.
4. Check that there is no voltage between any of the power connections, and between any of the power connections and the protective conductor connection.
5. Check whether the existing auxiliary supply circuits are de-energized.
6. Ensure that the motors cannot move.
7. Identify all other dangerous energy sources, e.g. compressed air, hydraulic systems, or water. Switch the energy sources to a safe state.
8. Check that the correct drive system is completely locked.

After you have completed the work, restore the operational readiness in the inverse sequence.



⚠ WARNING

Electric shock due to connection to an unsuitable power supply

When equipment is connected to an unsuitable power supply, exposed components may carry a hazardous voltage. Contact with hazardous voltage can result in severe injury or death.

- Only use power supplies that provide SELV (Safety Extra Low Voltage) or PELV- (Protective Extra Low Voltage) output voltages for all connections and terminals of the electronics modules.



⚠ WARNING

Electric shock due to equipment damage

Improper handling may cause damage to equipment. For damaged devices, hazardous voltages can be present at the enclosure or at exposed components; if touched, this can result in death or severe injury.

- Ensure compliance with the limit values specified in the technical data during transport, storage and operation.
- Do not use any damaged devices.



⚠ WARNING

Electric shock due to unconnected cable shields

Hazardous touch voltages can occur through capacitive cross-coupling due to unconnected cable shields.

- As a minimum, connect cable shields and the cores of cables that are not used at one end at the grounded housing potential.



⚠ WARNING

Electric shock if there is no ground connection

For missing or incorrectly implemented protective conductor connection for devices with protection class I, high voltages can be present at open, exposed parts, which when touched, can result in death or severe injury.

- Ground the device in compliance with the applicable regulations.

NOTICE

Damage to equipment due to unsuitable tightening tools.

Unsuitable tightening tools or fastening methods can damage the screws of the equipment.

- Only use screw inserts that exactly match the screw head.
- Tighten the screws with the torque specified in the technical documentation.
- Use a torque wrench or a mechanical precision nut runner with a dynamic torque sensor and speed limitation system.
- Adjust the tools used regularly.

⚠ CAUTION

Symptomatic respiratory and skin reaction to chemicals

A newly purchased product might contain traces of substances that are identified as sensitizers.

Sensitizers are substances which can cause sensitization in the lungs and skin after exposure to them.

Once sensitized, individuals can have severe reactions to further exposure, even in small amounts. In the most extreme cases, individuals might develop asthma or dermatitis respectively.

- If the product has a strong smell, keep it in a well-ventilated area for 14 days.

⚠ WARNING

Unexpected machine movement caused by radio devices or cellphones

Using radio devices, cellphones, or mobile WLAN devices in the immediate vicinity of the components can result in equipment malfunction or faults and damage to the devices. Malfunctions may impair the functional safety of machines and can therefore put people in danger or lead to property damage.

- Avoid operating radio devices, cellphones and mobile WLAN devices in the direct vicinity of converters and operating units.
- Scan the machine readable code, e.g. a QR code, from a greater distance or switch off the converter power supply before scanning.
- Only operate built-in devices with the control cabinet doors closed.
- When control cabinet doors are open, only qualified electrical personnel are allowed to carry out service and maintenance work.

⚠ WARNING

Fire due to inadequate ventilation clearances

Inadequate ventilation clearances can cause overheating of components with subsequent fire and smoke. This can cause severe injury or even death. This can also result in increased downtime and reduced service lives for devices/systems.

- Ensure compliance with the specified minimum clearance as ventilation clearance for the respective component.

NOTICE

Overheating due to inadmissible mounting position

The device may overheat and therefore be damaged if mounted in an inadmissible position.

- Only operate the device in admissible mounting positions.

⚠ WARNING

Unexpected movement of machines caused by inactive safety functions

Inactive or non-adapted safety functions can trigger unexpected machine movements that may result in serious injury or death.

- Observe the information in the appropriate product documentation before commissioning.
- Carry out a safety inspection for functions relevant to safety on the entire system, including all safety-related components.
- Ensure that the safety functions used in your drives and automation tasks are adjusted and activated through appropriate parameterizing.
- Perform a function test.
- Only put your plant into live operation once you have guaranteed that the functions relevant to safety are running correctly.

Note

Important Safety instructions for Safety Integrated

If you want to use Safety Integrated functions, you must observe the Safety instructions in the Safety Integrated documentation.

⚠ WARNING

Malfunctions of the machine as a result of incorrect or changed parameter settings

As a result of incorrect or changed parameterization, machines can malfunction, which in turn can lead to injuries or death.

- Protect the parameterization against unauthorized access.
- Handle possible malfunctions by taking suitable measures, e.g. emergency stop or emergency off.

2.2 Equipment damage due to electric fields or electrostatic discharge

Electrostatic sensitive devices (ESD) are individual components, integrated circuits, modules or devices that may be damaged by either electric fields or electrostatic discharge.



NOTICE

Equipment damage due to electric fields or electrostatic discharge

Electric fields or electrostatic discharge can cause malfunctions through damaged individual components, integrated circuits, modules or devices.

- Only pack, store, transport and send electronic components, modules or devices in their original packaging or in other suitable materials, e.g conductive foam rubber of aluminum foil.
- Only touch components, modules and devices when you are grounded by one of the following methods:
  - Wearing an ESD wrist strap
  - Wearing ESD shoes or ESD grounding straps in ESD areas with conductive flooring
- Only place electronic components, modules or devices on conductive surfaces (table with ESD surface, conductive ESD foam, ESD packaging, ESD transport container).

2.3 Warranty and liability for application examples

Application examples are not binding and do not claim to be complete regarding configuration, equipment, or any eventuality which may arise. Application examples do not represent customer-specific solutions, but merely serve to provide assistance with typical tasks.

As the user you yourself are responsible for ensuring that the products described are operated correctly. Application examples do not relieve you of your responsibility for safe handling when using, installing, operating and maintaining the equipment.

2.4 Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity 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 cybersecurity 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 cybersecurity measures that may be implemented, please visit
https://www.siemens.com/cybersecurity-industry.

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 customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under
https://new.siemens.com/cert.

Further information is provided on the Internet:

Industrial Security Configuration Manual (https://support.industry.siemens.com/cs/ww/en/view/108862708)

⚠ WARNING

Unsafe operating states resulting from software manipulation

Software manipulations, e.g. viruses, Trojans, or worms, can cause unsafe operating states in your system that may lead to death, serious injury, and property damage.

- Keep the software up to date.
- Incorporate the automation and drive components into a state-of-the-art, integrated industrial cybersecurity concept for the installation or machine.
- Make sure that you include all installed products in the integrated industrial cybersecurity concept.
- Protect files stored on exchangeable storage media from malicious software by with suitable protection measures, e.g. virus scanners.
- Carefully check all cybersecurity-related settings once commissioning has been completed.

2.5 Residual risks of power drive systems

When assessing the machine or system-related risk in accordance with the respective local regulations (e.g. EC Machinery Directive), the machine manufacturer or system integrator must take into account the following residual risks emanating from the control and drive components of a drive system:

1. Unintentional movements of driven machine or system components during commissioning, operation, maintenance, and repairs caused by, for example,
   - Hardware faults and/or software errors in the sensors, control system, actuators, and connections
   - Response times of the control system and of the drive
   - Operation and/or environmental conditions outside the specification
   - Condensation/conductive contamination
   - Parameterization, programming, cabling, and installation errors
   - Use of wireless devices/mobile phones in the immediate vicinity of electronic components
   - External influences/damage
   - X-ray, ionizing radiation and cosmic radiation
2. Unusually high temperatures inside and outside the components, including open flames, as well as emissions of light, noise, particles, gases, etc. due to fault conditions, e.g.:
   - Component failure
   - Software errors
   - Operation and/or environmental conditions outside the specification
   - External influences/damage
   - Short circuits or ground faults in the intermediate DC circuit of the converter
3. Hazardous shock voltages caused by, for example:
   - Component failure
   - Influence during electrostatic charging
   - Induction of voltages in moving motors
   - Operation and/or environmental conditions outside the specification
   - Condensation/conductive contamination
   - External influences/damage
4. Electrical, magnetic and electromagnetic fields generated in operation that can pose a risk to people with a pacemaker, implants or metal replacement joints, etc., if they are too close
5. Release of environmental pollutants or emissions as a result of improper operation of the system and/or failure to dispose of components safely and correctly

6. Influence of network-connected and wireless communications systems, e.g. ripple-control transmitters or data communication via the network or mobile radio, WLAN or Bluetooth.
7. Motors for use in potentially explosive areas:
   When moving components such as bearings become worn, this can cause enclosure components to exhibit unexpectedly high temperatures during operation, creating a hazard in areas with a potentially explosive atmosphere.

For more information about the residual risks of the drive system components, see the relevant sections in the technical user documentation.

PCU-Basesoftware /IPC Microsoft Windows 10

3

The software **PCU-Basesoftware /IPC** is the basis for operating SINUMERIK software (e.g. SINUMERIK Operate /PCU Modular) on your PC system.

This manual describes the installation of PCU-Basesoftware /IPC and the typical configuration for a preassembled and turnkey SINUMERIK 828D system.



Software option for SINUMERIK 828D

You require the following software option to use SINUMERIK PCU-Basesoftware /IPC:

- 6FC5800-0AP86-1YB0 (print license Col) or
- 6FC5800-0AP86-1YH0 (electronic license eCol)

PCU-Basesoftware /IPC is compatible from V15.0 in the SINUMERIK systems for the following CNC software versions:

- SINUMERIK 840D sl V4.95 SP3
- SINUMERIK ONE V6.15 SP3
- SINUMERIK 828D V5.21
- SINUMERIK MC V1.15 SP3

3.1 Hardware and software requirements

3.1.1 Supported SIMATIC IPC/IFP/ITC

NOTICE

For PC systems with Microsoft Windows, do not switch off the hardware!

Data may be lost for Microsoft Windows-based systems if the system is not shut down properly before it is disconnected from the power source. For technical reasons, data is still being written to the SSD/SD shortly after shutdown.

To avoid loss of data, use a SITOP UPS module.

More information information is provided under Configuring the SITOP UPS module for use with PCU-Basesoftware /IPC (Page 58).

Note

Microsoft Window support and compatibility

PCU Base Version 13 or higher is not supported by Microsoft Windows 7.

The PCU-Basesoftware /IPC software is tested and compatible with SIMATIC IPC systems with the following Microsoft Windows 10 configurations and IFP displays, ITC thin clients, and the HDBaseT Host Extended Sender:

SIMATIC IPC

Product	Article number	Configuration	Microsoft Windows 10		
			LTSB 2016	LTSC 2019	LTSC 2021
SIMATIC IPC 427E	6AG4141-1DA17-0FX0	Celeron, 4GB, 240GB SSD, 1x PCIe	●		
	6AG4141-1AA17-0FA0		●		
	6AG4141-1AA15-0FA0			●	
	6AG4141-1DA15-0FX0	6AG4141-1AA15-0FA0 incl. PCU-Basesoftware		●	
	6AG4141-5DB17-0FX0	Core i5, 8GB, 240GB SSD, 1x PCIe	●		
	6AG4141-5AB17-0FA0		●		
	6AG4141-5AB15-0FA0			●	
	6AG4141-5DB15-0FX0	6AG4141-5AB15-0FA0 incl. PCU-Basesoftware		●	
SIMATIC IPC 227G	6ES7647-8CD11-2AB*	Atom 2C, 4 GB, 256 GB SSD		●	
	6ES7647-8CD11-2AC*				●
	6ES7647-8CE21-2AB*	Atom 4C, 8 GB, 256 GB SSD		●	
	6ES7647-8CE21-2AC*				●
SIMATIC IPC 627E	6AG4131-3CC20-0AA2	Core i3, 16 GB, 480 GB SSD, 2x PCIe	●		
	6AG4131-3CC20-2AA2			●	
	6AG4131-3GC20-3AA1	Core i7, 16 GB 480 GB SSD, 1x PCIe, 1x PCI		●	

Product	Article number	Configuration	Microsoft Windows 10		
			LTSB 2016	LTSC 2019	LTSC 2021
SIMATIC BX-39A	6AG4142-3HB10-1AA0	Xeon W-11155MLE, 8 GB, 256 GB, 1x PCIe			●
	6AG4142-7HC10-2AA0	Xeon W-11865MLE, 16 GB, 256 GB, 1x PCIe			●

SIMATIC IPC - Panel-PC

Product	Article number	Configuration	Microsoft Windows 10		
			LTSB 2016	LTSC 2019	LTSC 2021
SIMATIC IPC 477E	6AV7241-1WA07-0FA0	15", Celeron, 240 GB SSD, 4 GB, without PCIe	●		
	6AV7241-1WA05-0FA0			●	
	6AV7241-3XB07-0FA0	19", Core i3, 240 GB SSD, 8 GB, without PCIe	●		
	6AV7241-3XB05-0FA0			●	
	6AV7241-3YA07-0FA0	22", Core i3, 240 GB SSD, 4 GB, without PCIe	●		
	6AV7241-3YA05-0FA0			●	
	6AV7241-5SB07-0FA0	24", Core i5, 240 GB SSD, 8 GB, without PCIe	●		
	6AV7241-5SB05-0FA0			●	
SIMATIC IPC 277G	6AV7886-0DD11-2AB0	15", Atom 2C, 4 GB, 256 GB SSD		●	
	6AV7886-0TD11-2AB0			●	
	6AV7886-0TD11-2AC0	15", Atom 4C, 8 GB, 256 GB SSD			●
	6AV7886-0EE21-2AB0	19", Atom 4C, 8 GB, 256 GB SSD		●	
	6AV7886-0UE21-2AB0			●	
	6AV7886-0UE21-2AC0				●
SIMATIC PX-39A	6AV7242-3NB10-1AA0	22", Xeon W-11155MLE, 8 GB, 256 GB, 1x PCIe			●
	6AV7242-3PC10-1AA0	24", Xeon W-11155MLE, 8 GB, 256 GB, 1x PCIe			●

SIMATIC IFP (local panels without integrated IPC)

Product	Article number
SIMATIC IFP 1500 MT Ext	6AV7863-5MA10-1AA0
SIMATIC IFP 1500 MT Ext Neutral	6AV7863-5MA10-1NA0
SIMATIC IFP 1900 MT	6AV7863-3MA00-0AAx
SIMATIC IFP 1900 MT Ext	6AV7863-6MA10-1AA0
SIMATIC IFP 1900 MT Ext Neutral	6AV7863-6MA10-1NA0
SIMATIC IFP 2200 MT	6AV7863-4MA00-0AAx
SIMATIC IFP 2200 MT	6AV7466-8MA00-0MT0
SIMATIC IFP 2200 MT EXT	6AV7466-8MA10-0AX0
SIMATIC IFP 2200 MT Ext Neutral	6AV7466-8MA10-0AA0
SIMATIC IFP 1500 V2 ext neutral	6AV7863-5MA10-2NA0
SIMATIC IFP 1900 V2 ext neutral	6AV7863-6MA10-2NA0
SIMATIC IFP 2200 V2 ext neutral	6AV7863-4MA10-2NA0

Product	Article number
SIMATIC IFP 2400 V2 ext neutral	6AV7863-7MA10-2NA0
SIMATIC IFP 2200 frameless	6AV7285-6LC00-0AA0
SIMATIC IFP 2400 frameless	6AV7285-6RC00-0AA0
SIMATIC IFP V2 Host Extended Transceiver	6AV7860-3EH00-0AA0

SIMATIC ITC

Product	Article number
SIMATIC ITC1200 V3	6AV6646-1BA12-0NA1
SIMATIC ITC1500 V3	6AV6646-1BA15-0NA0
	6AV6646-1BA16-0NA1
SIMATIC ITC1500 V3 PRO	6AV6646-1BC15-0AA0
SIMATIC ITC1900 V3	6AV6646-1BA18-0NA0
	6AV6646-1BA20-0NA1
SIMATIC ITC2200 V3	6AV6646-1BA22-1NA0
SIMATIC ITC2200 V3 frameless	6AV7295-6LC00-0AA0
SIMATIC ITC2400 V3	6AV6646-1BA24-0NA1
SIMATIC ITC2400 V3 frameless	6AV7295-6RC00-0AA0

Other respectively non-specified SIMATIC IPC configurations and screens can also work with PCU base software /IPC, but the use is exclusively under the responsibility of the machine manufacturer and without warranty and support from SIEMENS.

More information

You can find an example workflow for commissioning and configuration in this overview (Page 37).

You can find all of the information on the hardware in the Operating Instructions for the corresponding SIMATIC IPC.

3.1.2 Software and tools

Overview

PCU-Basesoftware /IPC includes the following software and tools:

Software	Function
Microsoft Windows 10	Service Desktop
Microsoft Windows PE	Service Center
Paragon Hard Disk Manager™ 17 Suite	Creating and restoring disk images
SIEMENS PCU Installer	Installing software and updates
VNC Viewer	Remote access to other devices from the PCU

Software	Function
PuTTY	Remote access to other devices from the PCU
PuTTY Key Generator	Generating an SSH key pair
Installing Microsoft VisualStudio Redistributables	Runtime components for Microsoft Windows 10
Microsoft .NET Framework	Microsoft platform for program execution and development
Driver package	Software components to support the hardware and I/O devices Microsoft Windows 10
Various configuration templates and scripts in the directory: `C:\ProgramData\Siemens\MotionControl\SIEMENS`	Templates for simplifying configuration

Note

Acknowledgements

- This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)
- This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)

Note

The software **Paragon Hard Disk Manager™ 17 Suite** requires a license and is implicitly included in the PCU-Basesoftware /IPC license. You do not require a separate license certificate.

Note

Disk images of the **Symantec Ghost** software in *.gho format are not supported by PCU-Basesoftware /IPC Version 15 or higher.

If you want to continue using data storage medium images of the Symantec Ghost application, use the emergency boot system on the USB flash drive for PCU Base V14.0 SP2.

The image for the creation of the USB flash drive is located on the installed PCU Base under: `D:\Eboot\`.

Additional software

PCU-Basesoftware /IPC additionally uses the following software:

SIMATIC IPC DiagBase is part of the SIEMENS Microsoft Windows installation, and is therefore installed when the PC system is shipped. SIMATIC IPC DiagBase is a diagnostic application, e.g. for temperature monitoring of hardware components.

Download:
SIMATIC IPC DiagBase (https://support.industry.siemens.com/cs/document/109792891/tool-downloads-for-simatic-ipcs-simatic-tablet-pcs-and-simatic-field-pgs?dti=0&lc=en-WW)

More information

An overview of the Microsoft Windows configurations changed by PCU-Basesoftware /IPC can be found in the Appendix (Page 215).

3.2 Hardware configuration of SIMATIC IPC

3.2.1 Network settings

The supported SIMATIC IPCs have two Ethernet interfaces, which are set by the PCU Base for connection to the SINUMERIK system.

Table 3-1 SIMATIC

Hardware designations	Designation in PCU Base[1]	Configuration
X1	Local Area Connection 2	Preset as a standard DHCP client for connection to a **company network**. The IP address is dynamically fetched from the DHCP server at X1.
X2	Local Area Connection	Preset as a SINUMERIK DHCP server for connection to a **system network**. A fixed IP address is preset at X2: If 192.168.214.241 is free in the system network, it is set. Otherwise you can view the allocated fixed IP address in the Control Panel.

[1] The network designation may deviate depending on the system.

Note

The industrial PCs SIMATIC IPC427E and IPC477E are equipped with 3 Ethernet interfaces. Interface X3 is optional, and is not supported by the PCU-Basesoftware /IPC software.

Further information

- Operating instructions of the SIMATIC IPC
- Setting the IP address and domain (Page 44)
- Adapting the firewall settings (Page 72)
- Remote access (Page 202)
- Network settings in the Service Center (Page 166)

3.2.2 Partitioning of the SSD

The partitioning of the SSD of your SIMATIC IPC is not changed when installing the PCU Base software. Partition C: must have a minimum of 30 GB in order to be able to install PCU Base.

Name of the partition	System (C:)	Data (D:)
File system	NTFS	NTFS
Memory used by the system	~ 20 GB	~ 0 GB

Already occupied by	• Microsoft Windows 10 • PCU Base, including various applications and configuration templates (see Chapter Software and tools (Page 32))	-
Application	Installing user programs	• Customer-specific data • Backup images • Setup packages

3.3 Directory structure and file conventions

Templates for configuration files

To assist you with the parameterization of the system, templates for various configuration files are provided on the PC system. The templates are organized into various directories, which you will find below the following directory:

- `C:\ProgramData\Siemens\MotionControl\siemens`

These templates are already fully functional when supplied and will be used automatically if you do not create your own configuration files based on these templates.

Note

Do not modify files in the template directory `siemens`!

The `siemens` directory contains only files with the factory settings that can be copied and used as templates.

Never overwrite these files. Instead copy them into another directory (see Section *Your settings*).

Directory hidden in delivery condition

For security reasons, the `C:\ProgramData` directory is hidden in the delivery condition.

To view the directory, proceed in one of the following ways:

- To switch quickly to a hidden directory, type the address in the Microsoft Windows Explorer.
- To show all hidden directories by default, change the setting in the Control Panel under "Appearance and Personalization > File Explorer Options > View > Advanced Settings".
- To show only one directory by default, first make the setting to show all hidden directories, then activate the attribute "Hidden" in the properties of the directory and finally again make the setting to not show all hidden directories.

Your settings

Several directories are available into which you can copy and adapt configuration files in order to make your own settings. In decreasing order of priority, these are:

- `C:\ProgramData\Siemens\MotionControl\`**user**
- `C:\ProgramData\Siemens\MotionControl\`**oem**

The settings in a configuration file in a directory with higher priority always replace those from one of lower priority. Template directory `siemens` has the lowest priority.

To define your own settings, therefore, copy a setting from the relevant template file into a directory with higher priority, e.g. below directory `user`.

First commissioning of SIMATIC IPCs

4

4.1 Overview

After you have completed the first commissioning of your supported SIMATIC IPC configuration (Page 30) with PCU-Basesoftware /IPC, you can configure the SIMATIC IPC like a SINUMERIK PCU.

You can find an example workflow of the first commissioning and configuration in this tabular overview.

Note

For PC systems with Microsoft Windows 10, do not switch off the hardware!

Data may be lost for Microsoft Windows-based systems if the system is not shut down properly before it is disconnected from the power source. For technical reasons, data is still being written to the SSD shortly after shutdown.

To avoid loss of data, use a SITOP UPS module.

See Configuring the SITOP UPS module for use with PCU-Basesoftware /IPC (Page 58).

Example workflow

No.	Step	Description
1	Set up and commissioning of the PC system (according to the operating instructions)	Information on setting up and installing your PC system can be found in the corresponding hardware documentation.
2	Install PCU-Basesoftware /IPC	If required, adapt the installation settings (Page 38) and install PCU-Basesoftware /IPC (Page 39).
3	Connect the PG/PC	To be able to access a directory of a PG/PC in the network, for example, connect the PG/PC in the network (Page 184).
4	Configure network settings on PG/PC	Once you have networked the PC system, a PG/PC and any other devices with one another, configure the network settings of your PG/PC (Page 184).
5	Set up further user accounts	Before you install software, at least one user account with limited rights must be set up (Page 42).
6	Install software and updates	Install the automation software and Microsoft Windows updates required (Page 103).
7	Configure the system	Configure the installed software (Page 103), Windows 10 and other system characteristics (Page 41) and, if necessary, the SITOP UPS module (Page 58).
8	Create a disk image (backup)	Create a disk image of the SSD as a backup (Page 157) to be able to return to this version in a maintenance situation.

4.2 Adapting the installation settings

The setup of PCU-Basesoftware /IPC also contains the setup.ini configuration file which can be parameterized before calling the setup. Note that some settings are only suitable for test purposes.

Before you adapt the settings in this file, you should copy the original file.

Section	Setting	Description
[IPC]	FirewallSettings=	• 1 (default setting) The Microsoft Windows Firewall settings are adapted appropriately for the company network by the PCU-Basesoftware /IPC, as described in this documentation. • 0 The current firewall settings are not changed by the setup.
	InstallWin10Updates=	• 1 (default setting) When setting up PCU-Basesoftware /IPC, important Microsoft Windows updates are installed that are required when using PCU Base. If these updates cannot be installed, then the setup of PCU Base is canceled. • 0 The setup does not check whether the Microsoft Windows updates required for PCU-Basesoftware /IPC have been installed or can be installed. This setting may be required when new updates have already been installed on the PC system, for example.
	TestSystemEnglish=	• 1 (default setting) The setup checks whether an English Microsoft Windows version has been installed. • 0 The setup does not check the Microsoft Windows language version. In this case, there is an additional prerequisite that the names of the network adapter do not, for example, contain a hyphen. Note that this setting is only suitable for test purposes. PCU-Basesoftware /IPC is only compatible with English Microsoft Windows versions.
[SetupControl]	FinalReboot=	• 1 (default setting) The PC system is restarted after installation. • 0 The setup does not restart the system or call a dialog after the installation as to whether a restart is to be performed (supervised installation).

4.3 Installing PCU-Basesoftware /IPC

You can install PCU-Basesoftware /IPC on the supported SIMATIC IPC configurations (Page 30) (using an installation medium that can be ordered and licensed individually).

In the Industry Mall you can find the PCU-Basesoftware /IPC under the following article number:

- 6FC5800-0AP86-1YB0 (print license CoI) or
- 6FC5800-0AP86-1YH0 (electronic license eCoI)

Requirement

- You can connect an operator panel front or screen and keyboard directly to the PC system.
- The commissioning of the PC system is completed and an administrator account is set up.
- There is an English Microsoft Windows installation on the PC system.
- The SINUMERIK CNC software version 5.21 or newer is installed on the control.
- The partition C: of the PC system has a minimum size of 30 GB.
- The installation medium is available on the PC system.

Procedure

To install PCU-Basesoftware /IPC on your PC system, proceed as follows:

1. Open Microsoft Windows Explorer and switch to the installation medium of PCU Base.
2. Right-click on "setup.exe" and select "Run as administrator".
3. Restart the PC system after you have installed PCU Base.

Result

PCU-Basesoftware /IPC has been installed. During the installation, the previously existing settings on the PC system, e.g. user accounts, keyboard layout, date and time settings, were imported. Set up additional user accounts (Page 42) if necessary and set the keyboard layout to English (Page 50).

The PCU Installer is initially inactive after the installation. It must be activated (Page 144) before software can be automatically installed.

Configuration of the system 5

5.1 Overview

Once you have completed the first commissioning, you can adapt the configuration of the system:

- For security reasons, set up user accounts (Page 42) with limited rights, e.g. for autologon mode.
- You can view or change (Page 43) the name of the PC system.
- The network settings (Page 44) in the state when delivered have been adapted for use with the SINUMERIK system, and usually do not have to be changed.
- You can deactivate the USB interfaces (Page 45) to prevent malicious software from entering the system network via this route.
- If necessary, connect the system to an external SMB server and check the configuration (Page 46).
- You can set up an external screen (Page 51) or set the screen resolution (Page 52) and color depth (Page 55).
- Use Activating/deactivating the touchpad or other pointer devices (Page 57) to avoid any inadvertent operating errors as a result of having two pointer devices.
- If you use a SITOP UPS module for the uninterruptible power supply or plan to use one, configure it for use with PCU-Basesoftware /IPC (Page 58).
- Use BitLocker drive encryption (Page 97). This protects your data storage media against data theft.

Other configuration options (e.g. desktop background) are available directly from the Service Desktop and can be implemented using Microsoft Windows 10 methods.

More information

- To call Microsoft Windows help, click "Get Help" in the Start menu.
- Help for Microsoft Windows 10 is available on the Internet on the Microsoft website: Microsoft Windows support (https://support.microsoft.com/en-us/hub/4338813/windows-help?os=windows-10)

5.2 Managing user accounts

Overview

When commissioning for the first time, you must create a local Microsoft Windows administrator account and define a password.

You can set up and manage additional Microsoft Windows user accounts in the Control Panel. To do that, log on with administrator rights.

Note

Administrator account cannot be recovered

If you have forgotten the password of the administrator account there is no way of recovering it!

5.3 Changing the name of the PC system

A unique computer name is set after installing PCU-Basesoftware /IPC. You can view and change it in the Control Panel of the Service Desktop.

You can find the computer name in the Control Panel under Category "System", Section "Computer name, domain and workgroup settings".

5.4 Setting the IP address and domain

The network settings in the state when delivered have been adapted for use with the SINUMERIK system, and usually do not have to be changed.

If you want to distinguish your network configuration from the factory settings, you can adapt them in the Microsoft Windows Control Panel.

You can find the settings in the following menu (icon view):

- "Control Panel > Network and Sharing Center > View network connections"

Further information

You can adapt the network settings for backing up and restoring disk images in the configuration of the Service Center (Page 69).

5.5 Configuring USB interfaces

To prevent malicious software from entering the control or the system network via the USB interfaces, you can deactivate the USB interfaces.

You can configure the USB interfaces on the Service Desktop via a command in the "Run" dialog box in the prompt.

Procedure

To activate or deactivate the USB interfaces, enter the relevant command on the Service Desktop in the "Run" dialog box or at the prompt:

Table 5-1 Disabling USB interfaces with the "sc_usb disable" command

Syntax:	sc_usb disable [-minutes] [all] [HOSTS...]
Description:	• Without a time indication [-minutes], a permanent disable is set. With time indication, the disable takes the time set in minutes. • The disable may refer to all network nodes of the system network, or a list of host names or IP addresses may be specified to which the disable should apply.

Table 5-2 Activating USB interfaces with the "sc_usb enable" command

Syntax:	sc_usb enable
Description:	With "sc_usb enable" USB storage units on permanently disabled USB interfaces or on certain host names or IP addresses are enabled again.

5.6 Configuring an SMB client

The server protocol SMB (Server Message Block) is used to connect the PU and the PC system in the network to an external Microsoft Windows server. Microsoft Windows 10 supports SMB servers with protocol versions SMBv1, SMBv2 and SMBv3. Depending on the configuration, different servers require a different protocol version to enable a connection with the PU and the PC system.

NOTICE
Network security Avoid unauthorized data access, e.g. via the Internet. Only connect systems within the company network if you want to set up the network via the configuration file `basesys.ini`, e.g. for a remote server connection for the system logbook (`Syslog_Remote_Host`).

Compatibility

The SMB protocol versions are compatible with the following software:

CNC software	SMB protocol version
V4.7 (828D, 840D sl) V4.8 (840D sl)	V1.0
V4.93 (828D, 840D sl)	V1.0, V2.0
V4.8 ab SP3 (828D) V4.95 (828D, 840D sl)	V1.0, V2.0, V3.0.2
V6.13 (ONE)	V1.0, V2.0, V2.1, V3.0.2
V6.15 (ONE)	V1.0, V2.0, V3.0, V3.0.2
V5.2x (828D) V6.2x (ONE)	V1.0, V2.0, V3.0.2, V3.1.1

Requirement

- Hidden directories are visible
- A copy of the `basesys.ini` configuration file is stored in the `user` directory: `C:\ProgramData\Siemens\MotionControl\`**`user`**`\System\etc\`
- The `basesys.ini` configuration file in the `user` directory is not write-protected.

Procedure

Proceed as follows to save an SMB server in the network of PU and the PC system in SINUMERIK Operate:

1. Open the `basesys.ini` configuration file in the directory `C:\ProgramData\Siemens\MotionControl\`**`user`**`\System\etc\`.
2. In the `[LinuxBase]` section, add the `DefaultCIFSVersion` line and set the desired value, e.g.:
   `DefaultCIFSVersion=3.11`
   The following values are possible depending on the SMB server:
   `none`, `1.0`, `2.0`, `2.1`, `3.0`, `3.02`, `3.11` or `auto` (default value)
3. Save and close the file.
4. Restart the PC system.

Configuring the SMB server connection in SINUMERIK Operate

The window "Configure drives" is available in the operating area "Setup > HMI > Log. drives" to configure the SMB server as softkey in the Program Manager.

Set up the SMB server as a Microsoft Windows network drive "NW Windows".

More information on the drive configuration is provided in the online help of SINUMERIK Operate.

Checking the SMB server configuration

1. Call PuTTY to check the SMB server configuration.
2. Log in as user "manufact".
3. Execute the command `mount | grep cifs`.
   You will receive the following output, which contains similar information, such as:
   `192.168.214.241/carlshare on /tmp/.logdrived_mnt. DEV_6 typ cifs (rw,nosuid,nodev,relatime,`**`vers=3.02`**`,sec=ntlmssp,cache=strict,...)`
   The example shows that the CIFS/Microsoft Windows release with SMB protocol v3.0.2 has been activated for the server.

Note

If the `DefaultCIFSVersion` line contains `auto` as the default value, activation is displayed as SMB protocol `vers=2.1` or `vers=1.0` when connecting to a Microsoft Windows XP/7 system.

5.7 Configuring network access on the USB data storage medium

If you connect a removable data storage medium (e.g. a USB flash drive) to a USB interface of the PC system, a network drive is set up automatically. This allows a removable data storage medium to be accessed from an NC in the network. The file and the printer release is activated automatically by Windows.

If you do not require network access to USB removable data storage medium, you should deactivate the automatic network release.

You can find this setting in the `basesys.ini` at `EnableUSBShares`.

Requirement

- Hidden directories are visible
- A copy of the basesys.ini configuration file is stored in the `user` directory:
  `C:\ProgramData\Siemens\MotionControl\`**`user`**`\System\etc\basesys.ini`
- The `basesys.ini` configuration file in the `user` directory is not write-protected

More information at Directory structure and file conventions (Page 36)

Procedure

To configure the automatic network release of USB data storage media of the PC system, proceed as follows:

1. Open the basesys.ini configuration file in the `C:\ProgramData\Siemens\MotionControl\`**`user`**`\System\etc\` directory.
2. Remove the semicolon in front of the EnableUSBShares line and set the required value.
   - `EnableUSBShares=0`
     The automatic network release of USB data storage media (and the associated file and printer release) is deactivated.
   - `EnableUSBShares=1` (default value)
     The automatic network release of USB data storage media is activated.
3. Save and close the file.

5.8 Displaying USB data memories with several partitions

If a USB data memory has several partitions, then the individual partitions are displayed as separate folders in SINUMERIK Operate. Previously used Microsoft Windows versions do not support the multiple partition display in conjunction with SINUMERIK Operate. However, to be able to use the function, parameterize the following:

Requirement

File `config.ini` must lie on the active boot server in the directory for the IPC.

Procedure

1. Open configuration file `config.ini` in the boot server directory.
   - NCU/PU: `.../`**user**`/common/tcu/<Name of the IPC>/common/tcu/config.ini`
   - IPC: `C:\ProgramData\siemens\MotionControl\`**user**`\common\tcu\<Name of the IPC>\common\tcu\config.ini`
2. In Section `[Station]`, insert the following value:
   `USBShareDisks=1`
   The multiple partition display is activated for the USB data storage medium.
3. Save and close the file.
   The function is active after a restart.

Result

If a USB data memory has several partitions and is connected with SINUMERIK Operate, then the individual partitions are displayed as separate folders.

5.9 Configuring the keyboard layout

It is assumed that the English keyboard layout is used in SINUMERIK Operate and for the SINUMERIK operator panel fronts.

If a different keyboard layout is set in Windows, this should therefore be changed before commissioning the PC system or before using SINUMERIK Operate.

The setting of the keyboard layout as well as the display of the active keyboard layout is shown in the Windows task bar.

5.10 Setting up an external screen

You can connect an external screen to the PC system. The procedure follows the usual procedure under Windows 10.

Requirements

- The PC system is switched off.
- The external screen is connected to the DisplayPort interface of the PC system (with an adapter, if necessary).

Procedure

To use an external screen for the Service Desktop or service system, proceed as follows:

1. Let the PC system run up in the Service desktop.
2. Right-click on the Desktop and then select the "Display settings" command from the shortcut menu.
3. In the "Display" dialog box, select the screen and set the resolution:
   - If you are using an LCD or LED screen, you should ideally set the native resolution of your screen.
   - If you are using an older CRT screen, you can select any resolution.
4. Click "OK" to confirm the settings.

Result

The external screen has been connected and can be used.

5.11 Setting the screen resolution

You can set the screen resolution directly in Windows 10 or use the PCU Base-specific file tcu.ini. The settings in tcu.ini overwrite the Windows system settings. Compared with Windows, they offer additional functions for switching over the resolution of the PC system depending on, for example, the screen connected during run-up.

Further information regarding configuration file tcu.ini is available in the following Chapter.

5.12 Set the resolution in the tcu.ini

Overview

The system behavior during run-up for the screen resolution is set in the `tcu.ini` file in Section [VNCServer].

You will find a template of the `tcu.ini` under `C:\ProgramData\Siemens\Motion Control\siemens\System\etc\`
Do not overwrite this template, but rather create your own `tcu.ini` inside one of the user directories.

More information: Directory structure and file conventions (Page 36)

Setting the resolution during run-up of the PC system

The following options are available for selection in the tcu.ini file in the [VNCServer] section (below the `# RESOLUTION` comment):

`0 = SYSTEM`

`1 = AUTO_OP_1`

`2 = AUTO_OP_2`

`3 = AUTO_MON_1` (default)

`4 = AUTO_MON_2`

`5 = 640x480`

`6 = 800x600`

`7 = 1024x768`

`8 = 1280x1024`

`9 = 800x480`

`10 = 1280x800`

`11 = 1366x768`

`12 = 1920x1080`

`13=3840x2160`

The meaning of the settings are as follows:

Table 5-3 Settings in the configuration file `tcu.ini`

Setting	Meaning
SYSTEM	The resolution is not specially set during run-up. i.e. the resolution last used in the system is active, e.g. the resolution which had been set manually in the Control Panel.
AUTO_OP_1	When running up, the resolution is automatically set in accordance with the following scenarios:

Setting	Meaning
Example 1:	There is a panel (irrespective of whether a monitor possibly exists): The resolution is set to the max. resolution of the panel (max. 1920x1080).
Example 2:	There is no panel, but there is a monitor: The resolution is not specially set, i.e. the resolution last used in the system is active, e.g. the resolution which had been set manually in the Control Panel. (Difference with respect to AUTO_OP_2 !)
AUTO_OP_2	Like AUTO_OP_1, except: Example 2: There is no panel, but there is a monitor: The resolution is set to the max. resolution of the monitor, reduced to the next lowest SINUMERIK resolution. SINUMERIK resolutions are 640x480, 800x600, 1024x768, 1280x1024, 800x480, 1280x800, 1366x768 and 1920x1080. **Example:** In the case of a monitor with a max. resolution of 2048x1152, the SINUMERIK resolution setting is 1920x1080.
AUTO_MON_1	Default: While running up, the resolution is automatically set ("monitor" has priority) in accordance with the following scenarios:
Example 1:	There is a monitor (irrespective of whether a panel possibly exists): The resolution is set to the max. resolution of the monitor, reduced to the next lowest SINUMERIK resolution. SINUMERIK resolutions are 640x480, 800x600, 1024x768, 1280x1024, 800x480, 1280x800, 1366x768 and 1920x1080. **Example:** In the case of a monitor with a max. resolution of 2048x1152, the SINUMERIK resolution setting is 1920x1080. If there is a panel, the display there is panned if the max. resolution of the panel is lower than the max. resolution of the monitor.
Example 2:	There is no monitor, but there is a panel: The resolution is not specially set; i.e. the resolution last used in the system is active, e.g. the resolution which had been set manually in the Control Panel. (Difference with respect to AUTO_MON_2 !)
Example 3:	There is neither a monitor nor a panel (headless operation): The resolution is not specially set, i.e. the resolution used during the previous session in the system is active, e.g. the resolution set manually in the Control Panel.
AUTO_MON_2	Like AUTO_MON_1, except: Example 2: There is no monitor, but there is a panel: The resolution is set to the max. resolution of the panel (max. 1920x1080).
640x480	During run-up, the SINUMERIK resolution is set to 640x480.
800x600	During run-up, the SINUMERIK resolution is set to 800x600.
1024x768	During run-up, the SINUMERIK resolution is set to 1024x768.
1280x1024	During run-up, the SINUMERIK resolution is set to 1280x1024.
800x480	During run-up, the SINUMERIK resolution is set to 800x480.
1280x800	During run-up, the SINUMERIK resolution is set to 1280x800.
1366x768	During run-up, the SINUMERIK resolution is set to 1366x768.
1920x1080	During run-up, the SINUMERIK resolution is set to 1920x1080.
3840x2160	During run-up, the SINUMERIK resolution is set to 3840x2160.

5.13 Setting the color depth in the tcu.ini file

The color depth of the PC system is set to 16 bit as default setting via the `tcu.ini` configuration file, and is reset to this value each time the system runs up.

To use a different color depth, you must adapt the setting in the `tcu.ini` file in the [VNCServer] section.

Requirement

- Hidden directories are visible
- A copy of the tcu.ini configuration file is stored in the `user` directory:
  `C:\ProgramData\Siemens\MotionControl\`**`user`**`\System\etc\tcu.ini`
- The `tcu.ini` configuration file in the `user` directory is not write-protected

Procedure

To adapt the color depth of the PC system, proceed as follows:

1. Open the tcu.ini configuration file in the `C:\ProgramData\Siemens\MotionControl\`**`user`**`\System\etc\` directory.
2. Enter the required value in the [VNCServer] section (below the `#COLOR DEPTH` comment):
   - `ColorDepth=0`
     The color depth is not changed during run-up, but rather the color depth used last is retained. In this way, you can adapt the color depth in the Windows settings.
   - `ColorDepth=1` (default value)
     The color depth is set to 16 bit while running up.
   - `ColorDepth=2`
     The color depth is set to 32 bit while running up.
3. Save and close the file.

5.14 Setting the display for portrait or landscape in the tcu.ini file

If you want to change the Microsoft Windows default orientation for portrait or landscape format for locally connected Panels or external monitors, parameterize the configuration file `tcu.ini` in the section `[VNCServer]` using the parameter `DisplayOrientation`.

Requirement

- Hidden directories are visible
- A copy of the tcu.ini configuration file is stored in the `user` directory:
  `C:\ProgramData\Siemens\MotionControl\`**`user`**`\System\etc\tcu.ini`
- The `tcu.ini` configuration file in the `user` directory is not write-protected

Procedure

Proceed as follows to adapt the orientation of the format:

1. Open configuration file `tcu.ini` in directory
   `C:\ProgramData\Siemens\MotionControl\`**`user`**`\System\etc\`.
2. Enter the required value:
   - `DisplayOrientation=1` (default value)
     The display alignment is set to 0 degrees.
   - `DisplayOrientation=2`
     The display alignment is set to 90 degrees in the clockwise direction.
   - `DisplayOrientation=3`
     The display alignment is set to 180 degrees in the clockwise direction.
   - `DisplayOrientation=4`
     The display alignment is set to 270 degrees in the clockwise direction.
3. Save and close the file.
   The orientation is active after restarting the PC system.

When starting a remote connection, if an external monitor is detected, then the display orientates itself to the display at the VNC server configuration. The setting defined by Microsoft Windows is overwritten. If no orientation has been selected, then a compatible 0 or 90 degree setting is automatically specified.

5.15 Activating/deactivating the touchpad or other pointer devices

If you are using an control panel with touchpad or mouse, incorrect operator actions may inadvertently occur. Therefore, if required, you can deactivate the touchpad in the Microsoft Windows Device Manager.

Note

The procedure described will be made easier using a USB-connected mouse. Alternatively, you can carry out changes using the keyboard.

Requirement

You must be logged in as the administrator to be able to execute these steps.

Procedure

1. Search for the Device Manager by typing "Device Manager" into the entry field of the Start menu.
   You are given a list of options.
2. Open the "Device Manager" in the "Control Panel" selection.
3. Search the list for "Mice and other pointing devices" and then double-click on the device name.
4. Right-click on "HID-compliant mouse" and select "Enable" or "Disable".
   The touchpad is activated/deactivated.

5.16 Configuring the SITOP UPS module for use with PCU-Basesoftware /IPC

5.16.1 Overview of SITOP UPS

SITOP UPS modules can continue operation of the PC system temporarily if a power failure occurs and/or shut down the system correctly.

For example, a SITOP UPS module also protects against data loss when the PC system hardware is shut down, because with Microsoft Windows-based systems, data is still briefly written to the SSD after the system has been run down for technical reasons.

- You will find general information about SITOP UPS modules used in combination with PCU-Basesoftware /IPC in Chapter SITOP modules for IPC (Page 59).
- If you want to use a SITOP UPS module in combination with PCU-Basesoftware /IPC, you must first adapt the settings of the SITOP software (Page 60).
- Optionally, you can adapt the delay time after which the HMI software will be forced to shut down (Page 63).
- You must configure the hardware (Page 66) of the SITOP UPS module before using it with PCU-Basesoftware /IPC.

NOTICE
Ensure the readiness for operation of the SITOP power supply In order to prevent data loss, the SITOP power supply must be ready for operation. Note the following: • The SITOP power supply may not be ready for operation immediately after being switched on (a capacitor-buffered UPS500 requires 1-2 minutes make time, for example). • The operating system and the SITOP software must have run up so that the SITOP software can shut down the system correctly when a power failure occurs. • The readiness for operation and the functional capability of the SITOP power supply must be ensured (e.g. battery of capacitor charged) • Please also note all the information on the readiness for operation in the documentation of your SITOP device.

More information

Information on using SITOP UPS modules in combination with PCU-Basesoftware /IPC can also be found on the Internet:

- Service & Support Portal: Example of using an uninterruptible power supply (http://support.automation.siemens.com/WW/view/en/90142681)
- Service & Support Portal: Typical values for an operator station with Windows (http://support.automation.siemens.com/WW/view/en/76773241)

- Catalog KT 10.1 SITOP Power Supply
- SiePortal: 24 V DC uninterruptible power supplies (https://eb.automation.siemens.com/mall/en/US/Catalog/Products/7010117)

5.16.2 SITOP modules for IPC

Suitable SITOP UPS modules

SITOP UPS modules can continue operation of a PC system temporarily if a power failure occurs and/or shut down the system correctly.

In conjunction with PCU-Basesoftware /IPC, all specific applications are taken into account (e.g. HMI software) with the `USVShutdown.bat` component.

Safe shutdown after a power failure of an IPC in the state that it was delivered takes approximately 20 seconds. For a typical power consumption of approx. 60 W, a capacitor-buffered UPS with an energy storage device of 2.5 kW is recommended. If longer buffer times are required, then several expansion modules can be connected in a cascade connection.

Example of a SITOP UPS module that can be used (USB):

SITOP 500S (15 A / 2.5 kWs capacitor)

Article No.: 6EP1933-2EC41

Example of a SITOP UPS with Ethernet/PROFINET interface that can be used:

SITOP UPS1600 starter kit

- DC-UPS SITOP UPS1600 24V DC/10A
- SITOP UPS1100 3.2 AH battery module

Article No.: 6EP4134-3AB00-2AP0

Note

Information about the test environment for machine OEMs

The functionality has been tested in the standard configuration with PCU-Basesoftware /IPC.

When installing add-on or OEM software components, you must check the shutdown procedure of the entire system and adapt the factory setting (180 seconds).

Further information at Parameterizing a delay time for quitting the HMI software (Page 63)

5.16.3 Configuring SITOP software for PCU Base

5.16.3.1 Configuring SITOP software V3.x (USB)

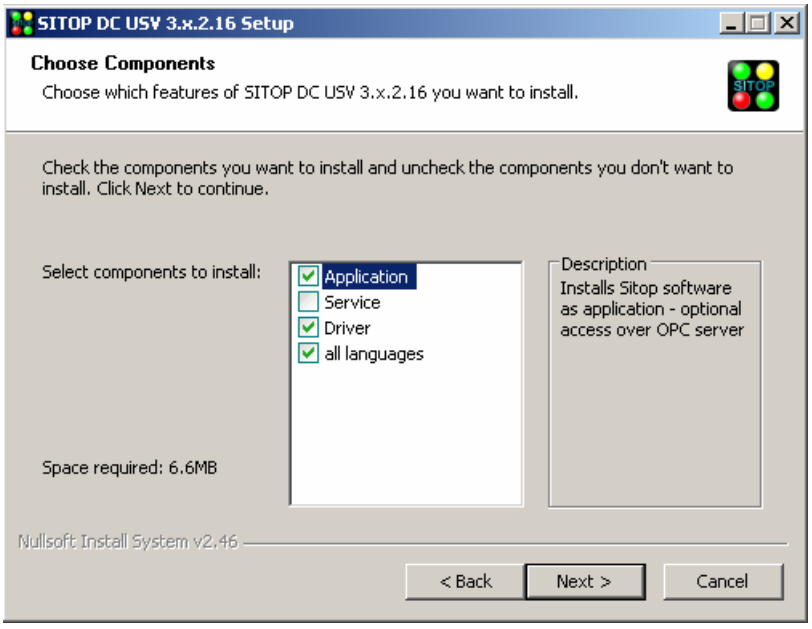
Configuring SITOP software V3.x (USB)

If you want to use a SITOP UPS module in combination with PCU-Basesoftware /IPC, you must first adapt the settings of the SITOP software.

Precondition

- The SITOP UPS hardware is connected via the USB interface.
- The SITOP software of version 3.x.2.16 or later is installed in directory `C:\Program Files (x86)\SITOP\`

- If you want to use SITOP software of version 3.2.1.16 or older, this must be installed as a normal application, not as a service.



Note

Microsoft Windows service of the SITOP software version 3.2.1.16 or older is not compatible with PCU-Basesoftware /IPC

If you use SITOP software, version 3.2.1.16 or older as a Microsoft Windows service with PCU Base, the correct shutdown procedure cannot be performed!

If you have installed the SITOP software of version 3.2.1.16 as a Microsoft Windows service, you must uninstall this and install it again as an application in order to be able to use it in conjunction with PCU Base.

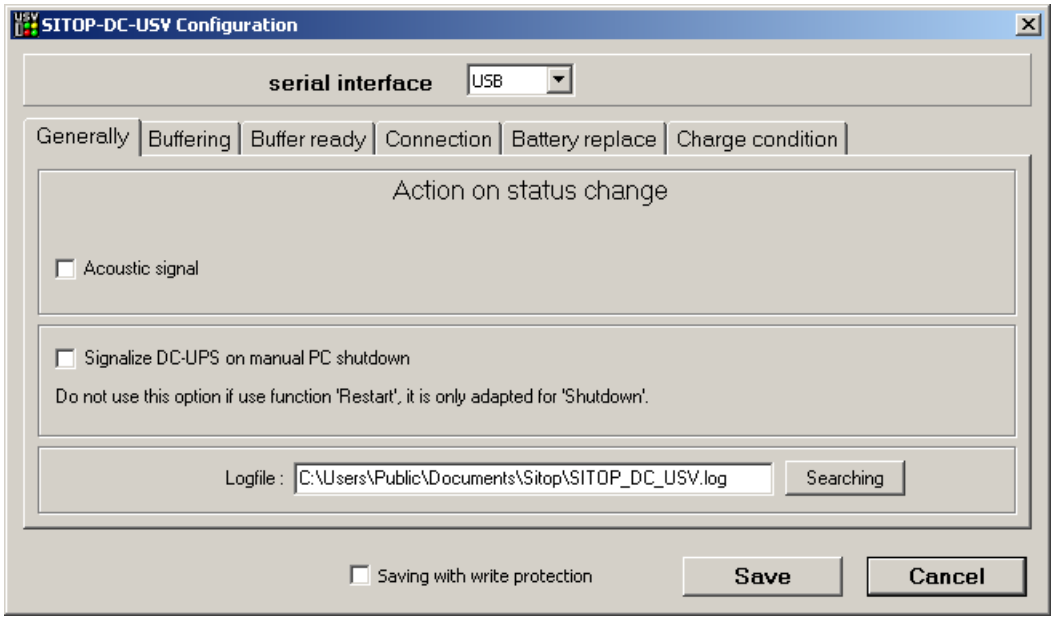
From version 3.2.1.17, the SITOP software can be used as service with PCU-Basesoftware /IPC and is recommended.

- The SITOP software was configured during the installation so that it starts automatically when Microsoft Windows is run up (factory setting).
- The Service Desktop is active.

Procedure

Proceed as follows to configure the SITOP software for use with PCU-Basesoftware /IPC:

1. Call the settings of the SITOP software, for example, by right-clicking the SITOP UPS icon in the Microsoft Windows information area and then selecting "Configuration".
   The "SITOP DC UPS Configuration" dialog box opens.



2. In the "General" tab, select "UPS" in the drop-down list at "Serial interface".

3. Switch to the "Floating operation" tab and make the following settings:
   - Deactivate the "Display monitoring window after" checkbox

     Note

     Deactivating the monitoring window

     Display of the monitoring window can cause malfunctioning of the operating software.

   - Click directly in the text field at "Start application after" and specify the path of the `USVShutdown.bat`:
     `C:\Program Files (x86)\Siemens\MotionControl\siemens\sinumerik\hmi\base\USVShutdown.bat`

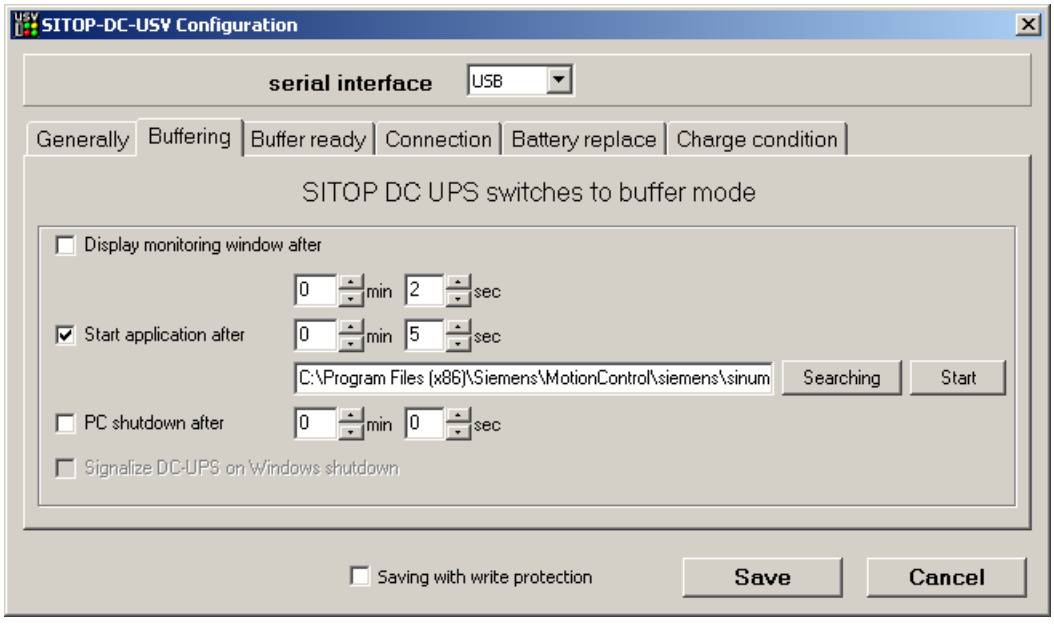
     Note

     Do not use the "Browse" button

     The dialog can crash if you use the "Browse" button to specify the path of the `USVShutdown.bat`.

     Instead, enter the path directly in the text field.

   - After you have specified the path of the `USVShutdown.bat`, activate the "Start application after" checkbox. Optionally, you can specify the wait time after which the `USVShutdown.bat` is to be executed (e.g. 5 seconds).



4. Confirm the settings with "Save".

Parameterizing a delay time for quitting the HMI software

Before the SITOP Monitor runs down Microsoft Windows, `USVShutdown.bat` shuts down operation of the HMI software.

If the HMI software cannot be shut down within 180 seconds (factory setting) due to an error, HMI software shutdown is forced and Microsoft Windows is shut down.

If the HMI software of your OEM installation is not shut down within 180 seconds, you can parameterize this wait time manually.

Note

Information about the test environment for machine OEMs

The function "SITOP UPS" has been tested in the standard configuration with PCU-Basesoftware /IPC. When installing add-on or OEM software components, you must check the shutdown procedure of the entire system and adapt the factory setting.

Precondition

- The SITOP UPS module is configured for use with PCU-Basesoftware /IPC.
  For further information see under Configuring SITOP software V3.x (USB) (Page 60).
- The Service Desktop is active.

Procedure

Proceed as follows to change the delay time:

1. Call the settings of the SITOP software, for example, by right-clicking the SITOP UPS icon in the information area and then selecting "Configuration".
2. In the "SITOP DC UPS Configuration" dialog box, enter the wait time in seconds as a command line parameter in the "Buffering" tab:
   - Syntax: `<Path>\USVShutdown.bat -<time in seconds>`
   - Example: `C:\Program Files (x86)\Siemens\MotionControl\siemens\sinumerik\hmi\base\USVShutdown.bat -180`

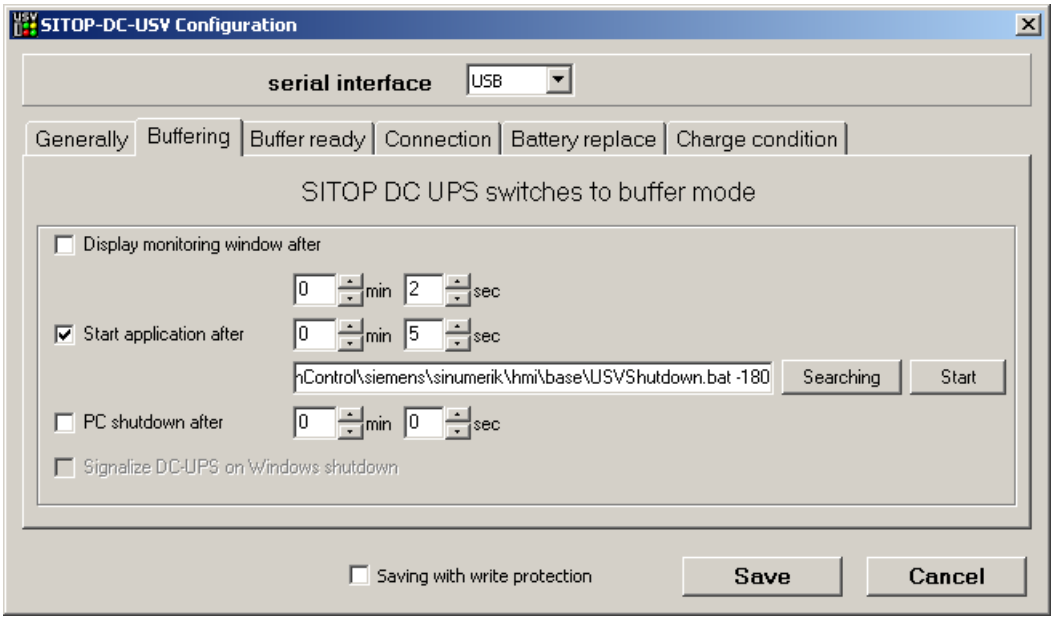


Figure 5-1 SITOP Monitor Floating operation

3. Confirm the setting with "Save".

5.16.3.2 Configuring SITOP UPS Manager (Ethernet)

Precondition

- The SITOP UPS hardware is connected via the Ethernet interface.
- The SITOP-UPS Manager has been installed and configured for Ethernet.

Note

Validity of the information on the SITOP components in this manual

This information only involves the configuration of the settings relevant for PCU Base. In addition, all the information and notes in the corresponding manuals of your SITOP UPS hardware and SITOP UPS Manager apply.

Procedure

1. Call the SITOP UPS Manager.
2. Change to "Software configuration > Buffer mode".
3. Make the following settings:
   - Activate the checkbox "Start application on power failure" - and there, enter the path of USVShutdown.bat:
     C:\Program Files (x86)\Siemens\MotionControl\siemens\sinumerik\hmi\base\USVShutdown.bat
   - When required, configure the wait time until the HMI software is terminated by USVShutdown.bat (factory setting = 180 seconds).

     Note

     Information about the test environment for machine OEMs

     The function "SITOP UPS" has been tested in the standard configuration with PCU-Basesoftware /IPC. When installing add-on or OEM software components, you must check the shutdown procedure of the entire system and adapt the factory setting.

     To do this, enter the wait time in seconds as command line parameter:
     Syntax: <Path>\USVShutdown.bat -<time in seconds>
     Example: C:\Program Files (x86)\Siemens\MotionControl\siemens\sinumerik\hmi\base\USVShutdown.bat -180
4. Confirm the settings with "Configuration changed, restart application now".

5.16.4 Hardware configuration of the SITOP UPS module

Buffering parameterization

The UPS module can be used to select whether buffering should be completed after a predetermined period of time or not until the accumulator's lowest discharge threshold (= maximum buffer time) has been reached. Both buffering parameterizations result from this.

"Maximum buffer time" mode

This mode enables the system to be shut down in a time-optimized manner. The UPS module is synchronized with the shutdown of the operating system. Buffering is maintained until the operating system has been shut down. The operating system must shut down within a maximum of 5 minutes (including all applications). Otherwise, the UPS module buffers for the maximum buffer time (dependent on the accumulator state).

Required settings on the UPS module (USB interface)

	On - Off			
1		○	+2V	Cut-in threshold +22V fixed
2		○	+1V	
3	○		+0.5V	

	On - Off			
4		○	+1V	End-of-charge voltage + 26.3V fixed
5		○	+1V	
6	○		+0.5V	
7	○		+0.2V	
8		○	+0.2V	
9		○	+0.1V	
10		○	0.35A / 0.7A	Charging current

	On - Off			
1		●		Set time/max. time
2		○	+320 s	Buffer time +5 s fixed
3		○	+160s	
4		○	+80s	
5		○	+40s	
6		○	+20s	
7		○	+10s	
8	●			Disconnection
9		○		Battery operating state on/off

Legend:

○ Delivery condition setting

● Setting for operation on the PCU

"Fixed buffer time" mode

In this mode, the UPS module always buffers for the pre-selected, fixed period of time. It is not possible to synchronize the UPS module with the operating system shutdown.

Required settings on the UPS module

	On - Off			
1		○	+2V	Cut-in threshold +22V fixed
2		○	+1V	
3	○		+0.5V	

	On - Off			
4		○	+1V	∘ ∘ End-of-charge voltage + 26.3V fixed
5		○	+1V	
6	○		+0.5V	
7	○		+0.2V	
8		○	+0.2V	
9		○	+0.1V	
10		○	0.35A / 0.7A	Charging current

	On - Off			
1	●			Set time/max. time
2		○	+320 s	∘ ∘ Buffer time +5 s fixed
3	●		+160s	
4		○	+80s	
5		○	+40s	
6		○	+20s	
7		○	+10s	
8	●			Disconnection
9		○		Battery operating state on/off

Legend:

○ Delivery condition setting

● Setting for operation on the PCU

5.17 Configuration of the Service Center

5.17.1 Overview

You can permanently adapt the settings for the backup and restoration of disk images (Service Center (Page 157) component) in the "Service Center Backup/Restore" dialog box:

- Configuration of the network adapter (Page 69)
- Configuration of the host (Page 71)

Adaptations that you make here are stored in the `servicesystem.ini` configuration file.

You can also adapt the settings directly in the configuration file `servicesystem.ini`.

You can also view the log files of the Service Center or restart the PC system in the Service Center in the "Service Center Backup/Restore" dialog box.

To open the dialog box, click the ServiceCenter Backup-Restore icon on the Desktop.

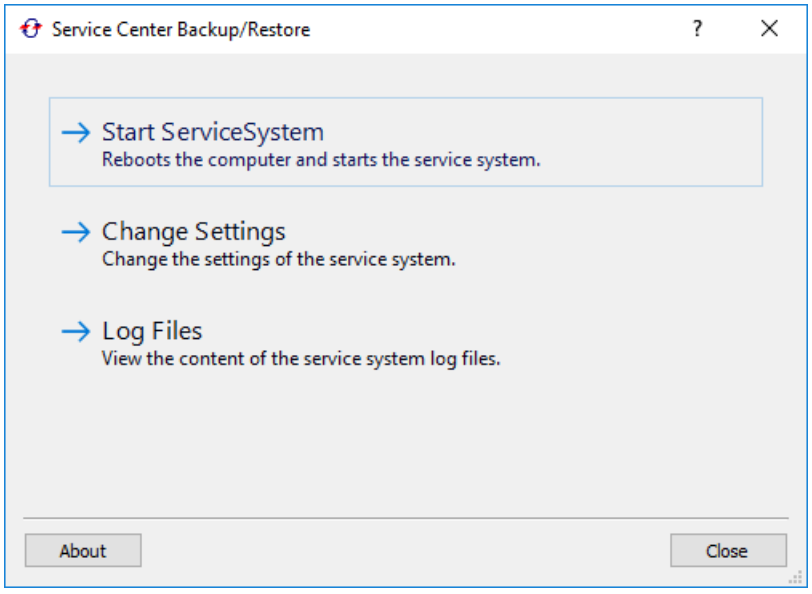


Figure 5-2 ServiceCenter Backup/Restore

Note

Deactivate BitLocker encryption to be able to make settings in the "Service Center Backup/Restore" dialog via headless mode.

5.17.2 Configuration of the network adapter

You can make the network settings in the "Adapter Settings" tab and permanently save this configuration, in contrast to the settings in the "Network Settings" dialog box of the Service Center (Page 166).

Settings that you make in this dialog box are stored in the `servicesystem.ini` configuration file.

Overview

You can make the following IP settings in the "Adapter Settings" dialog box:

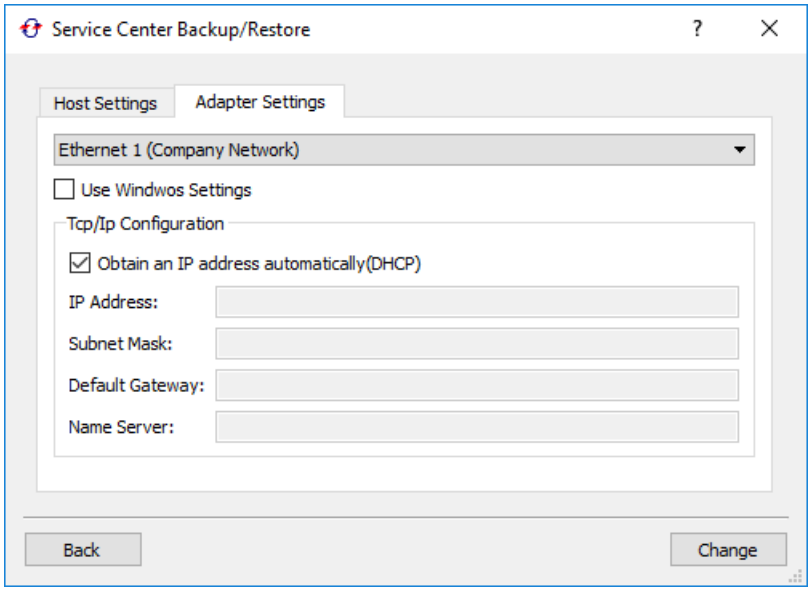


Figure 5-3 Adapter settings - Ethernet 1 (company network)

Table 5-4 Settings in the "Adapter Settings" dialog box

Settings	Purpose
Adapter	Select the Ethernet interface that you want to configure. All settings in this dialog box refer to the selected Ethernet interface.
Use Windows Settings	Select whether the values set in the Control Panel are to be used.
Obtain an IP address automatically (DHCP)	Select whether the addresses are to be fetched dynamically from the DHCP server. If the checkbox is deactivated, you must make the settings manually.
IP Address	Set the IP address of the NCU. You can specify an IP address from the following range: 192.168.214.250 - 254
Subnet Mask	Specify a subnet mask, e.g. 255.255.255.0
Default Gateway	Set the IP address of the standard gateway. A standard gateway creates a standard route in the IP routing table for all destinations that are not in the subnet.
Name Server	Set the IP address of the name server. A name server answers questions asked about a domain name zone using a DNS database.

5.17.3 Configuration of the host

You can make the network settings in the "Host Settings" tab and permanently save this configuration, in contrast to the settings in the "Network Settings" dialog box of the Service Center (Page 166).

Settings that you make in this dialog box are stored in the `servicesystem.ini` configuration file.

Overview

You can make the following settings in the "Host Settings" dialog box:

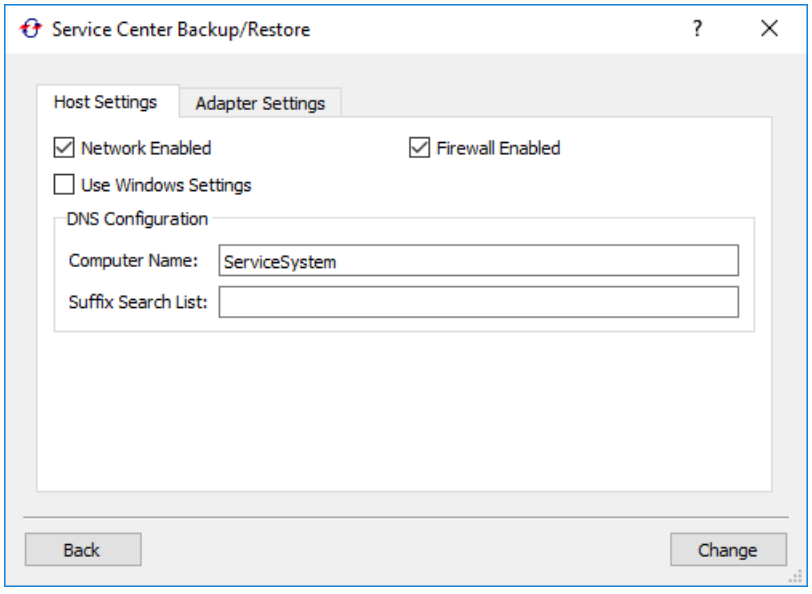


Figure 5-4 Host settings

Table 5-5 IP settings in the "Host Settings" dialog box

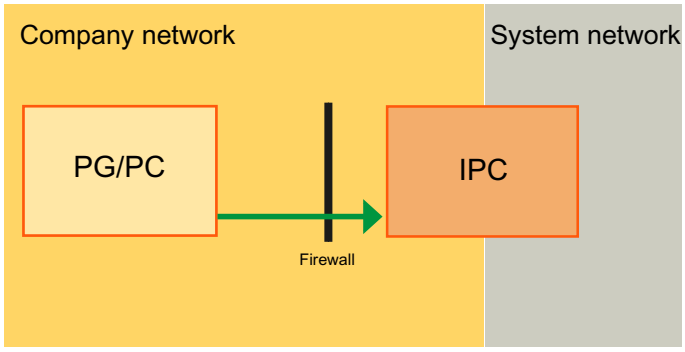
Settings	Purpose
Network enabled	Activate or deactivate the network interfaces of the PC system.
Firewall enabled	Activate or deactivate the firewall of the PC system.
Use Windows Settings	Select whether the values set in the Control Panel are to be used.
DNS Configuration > Computer Name	Specify the DNS computer name.
DNS Configuration > Suffix Search List	Parameterize a search list for DNS suffix, e.g. "network.com". The factory setting of the Ethernet interface "Local Area Connection" is ".local".

5.18 Adapting the firewall settings

5.18.1 Overview

From a PG/PC in the plant network, you can directly access resources on the PC system. The same applies when accessing a PG/PC from the PC system in the plant network or in the company network.

If you want to access the PC system via the company network instead or in addition, you must adapt the firewall settings.



You can adapt the following settings:

- Activate the remote access to the PC system (Page 78)
- Enabling SNMP communication (Page 76)
- Activation/deactivation of the file and printer release (Page 80)
- Activation of the ping execution (ICMP) (Page 90)

As a rule, you can make these settings in the Control Panel or via the prompt or a script/batch file (relevant for series commissioning) (Page 75).

You can save and restore (Page 92) the firewall settings. (Even on different PC systems, e.g. due to series commissioning)

Also note the general information in this chapter:

- Factory setting of the Microsoft Windows Firewall on the PC system (Page 73)
- General information on the operating principle of the Microsoft Windows Firewall (Page 74)
- General information on the settings recommended for Microsoft Windows (Page 74)

5.18.2 Factory setting of the Microsoft Windows Firewall on the PC system

The Microsoft Windows Firewall settings on your PC system are appropriately configured by PCU-Basesoftware /IPC for the use of SINUMERIK software and systems. For security reasons, the Microsoft Windows Firewall is activated in the company network and expanded by additional rules. The Microsoft Windows Firewall is deactivated in the system network. The descriptions in this chapter therefore largely relate to the adaptation of the firewall settings for the company network.

Table 5-6 Factory settings for network adapter and Microsoft Windows Firewall

	System network	**Company network**
Interface	X2	X1
Network name IPC	Local Area Connection	Local Area Connection 2
Network profile	Public	Public
Microsoft Windows Firewall status Further information: General information on the settings recommended for Microsoft Windows (Page 74)	Deactivated	Activated
File and printer release Further information: Activation/deactivation of the file and printer release (Page 80)	Activated and permitted	Deactivated and blocked by firewall
SNMP communication Further information: Enabling SNMP communication (Page 76)	Permitted	Blocked
Remote access (via port 5900) Further information: Activate the remote access to the PC system (Page 78)	Permitted	Blocked
Outgoing ICMP Ping requests from the PC system Further information: Activation of the ping execution (ICMP) (Page 90)	Permitted	Permitted
Incoming ICMP Ping requests on the PC system Further information: Activation of the ping execution (ICMP) (Page 90)	Permitted	Blocked

Note

Automatic network release of USB data storage media results in activation of the file and printer release

The automatic network share of USB data storage media is activated in the default setting of PCU-Basesoftware /IPC. The file and printer sharing is then activated by Microsoft Windows when a USB data storage medium is connected.

Further information: Configuring network access on the USB data storage medium (Page 48)

5.18.3 General information on the operating principle of the Microsoft Windows Firewall

Microsoft Windows Firewall rules are structured as follows:

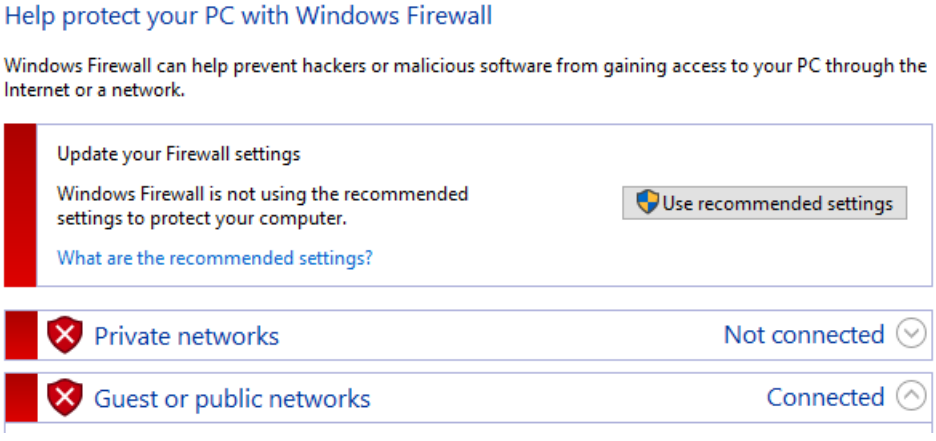
- The firewall rules are divided into Inbound Rules and Outbound Rules.
- Each firewall rule is valid for one or several network profiles (Profiles).
  Each network connection in Microsoft Windows is assigned to a specific network profile. In the factory settings state of the PC system, both the plant network ("Local Area Connection") and the company network ("Local Area Connection 2") have the network profile "Public".
- Some firewall rules are already assigned to so-called "Groups". As a result, you can more easily activate or deactivate specific related network functionalities (e.g. file and printer release).

You can make the Microsoft Windows Firewall settings using the Control Panel and using the prompt or script/batch files. The use of script/batch files is particularly recommended for series commissioning. Alternatively, for series commissioning, you can make all of the Microsoft Windows Firewall settings on an individual PC system, save these settings, and apply them on other devices (Page 92).

5.18.4 General information on the settings recommended for Microsoft Windows

Firewall settings recommended by Microsoft Windows are unsuitable for use in the system network

In the Control Panel, under "Windows Defender Firewall", there is a display indicating that the firewall settings do not correspond to the settings recommended and automatically checked by Microsoft Windows. The corresponding sections are highlighted in red:



However, the settings automatically recommended by Microsoft Windows are not suitable for use in the system network, and would restrict the functioning of the plant. The network

security in the plant network must therefore be ensured by other security precautions. In this regard, observe the information on industrial cybersecurity (Page 104).

Note

Do not use firewall settings that are automatically recommended by Microsoft Windows!

The command "Use recommended settings" overwrites the existing firewall settings, which are required for operating PCU-Basesoftware /IPC, and therefore this command must not be used.

Otherwise, the Microsoft Windows Firewall will be activated in the system network and communication of internal services of the PCU Base will be inhibited.

5.18.5 Configuration by means of a prompt or script/batch file

You can make most of the settings described in this chapter both using the Control Panel and using the prompt or script/batch files. The use of script/batch files is particularly recommended for series commissioning.

Basic procedure

You can enter these commands either directly into the prompt or save the command in a script or batch file:

- **Direct input of the command:**
  - Call the prompt as the administrator.
  - You can enter the commands either directly or in succession.
- **Calling the command via a script file (or batch file):**
  - Save the command in a text file.
  - Call the prompt as the administrator.
  - Specify the script file as follows:
    `netsh -f <File name of the script file>`

Further information

Descriptions of the commands and of all of the associated parameters of Netsh within the Advfirewall firewall context can be found on the Microsoft website:

- Microsoft Windows Server documentation (https://docs.microsoft.com/en-us/windows-server/index)
- Microsoft TechNet: Netsh (command line program) (https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc785383(v=ws.10)?redirectedfrom=MSDN)

- Microsoft TechNet: Netsh AdvFirewall Firewall Commands (https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd734783(v=ws.10)?redirectedfrom=MSDN#BKMK_3_set)
- Microsoft TechNet: Netsh Commands for Windows Firewall with Advanced Security (https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc771920(v=ws.10)?redirectedfrom=MSDN)

5.18.6 Enabling SNMP communication

Some network diagnostics functions use SNMP communication (e.g. in SINUMERIK Operate). This is not blocked in the plant network. If, however, you have productively linked your plant in the company network, SNMP communication is partially blocked:

- In the factory settings version of the PCU-Basesoftware /IPC, incoming SNMP communication is blocked in the company network.
- Outgoing SNMP communication in the company network is not blocked.

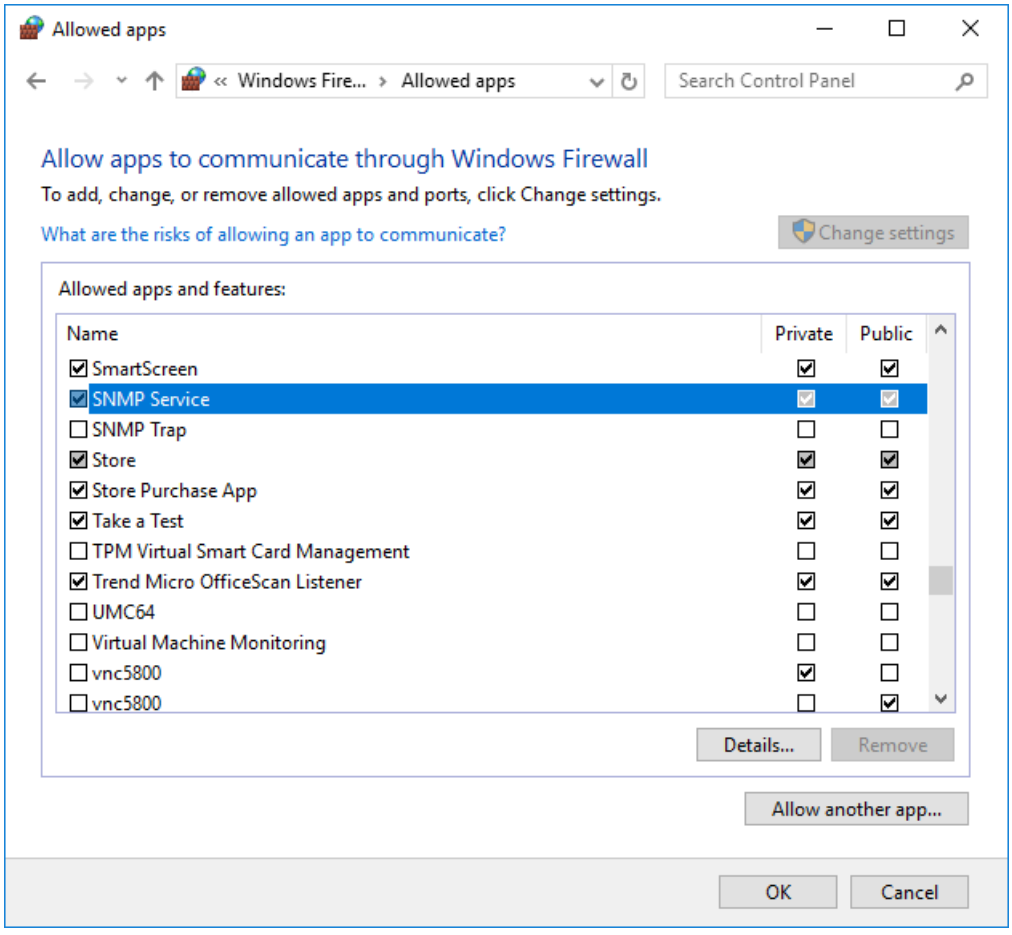
In the settings for the Microsoft Windows Firewall, you can activate SNMP communication via check box "SNMP Service" for specific network profiles.

Procedure

To permit incoming SNMP communication on the PC system, proceed as follows:

1. Enter "Control Panel" in the search field and then click on "Control Panel" in the search results.
   The desktop App "Control Panel" opens.
2. Click on the display selection and switch from the "Category" view to "Icons".
   The "All Control Panel Items" dialog box opens.

3. Click on "Windows Defender Firewall" > "Allow a app or feature through Windows Defender Firewall".
   The "Allowed apps" dialog box opens. The various check boxes for "SNMP Service" are checked and displayed with a green or gray background, because the SNMP service is partially activated. Incoming queries are blocked on the PC system and outgoing queries from the PC system are permitted.



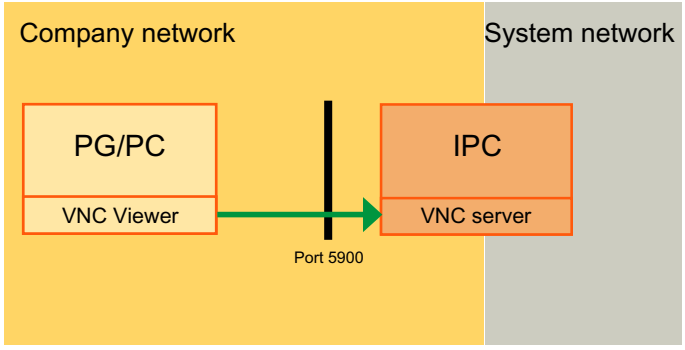
4. Click on "Change Settings" and confirm with "Yes", if applicable.
5. Activate the checkbox of the corresponding network profile completely, e.g. "Public" for the company network (factory setting).
6. Click "OK" to confirm the change.

5.18.7 Activate the remote access to the PC system

5.18.7.1 Overview

Basically, it is possible to access the PC system both via the plant network and via the company network via VNC:

- Remote access to the PC system from a PG/PC in the system network is activated via the factory setting (Page 184).
- If you want to access the PC system via the company network instead or in addition, you must adapt the firewall settings.



The inbound rule "vnc5900", which is deactivated in the factory settings state, is available for this purpose in the expanded settings for the Windows Firewall. To activate the remote access to the PC system in the company network, you can activate this rule either directly in the Control Panel (Page 78), or in the prompt or by means of a script/batch file (Page 79).

More information

In addition to the firewall settings, you may have to adapt other settings to establish a remote connection in the company network.

You can find more information on this in Chapter Remote access (Page 202), especially under AUTOHOTSPOT.

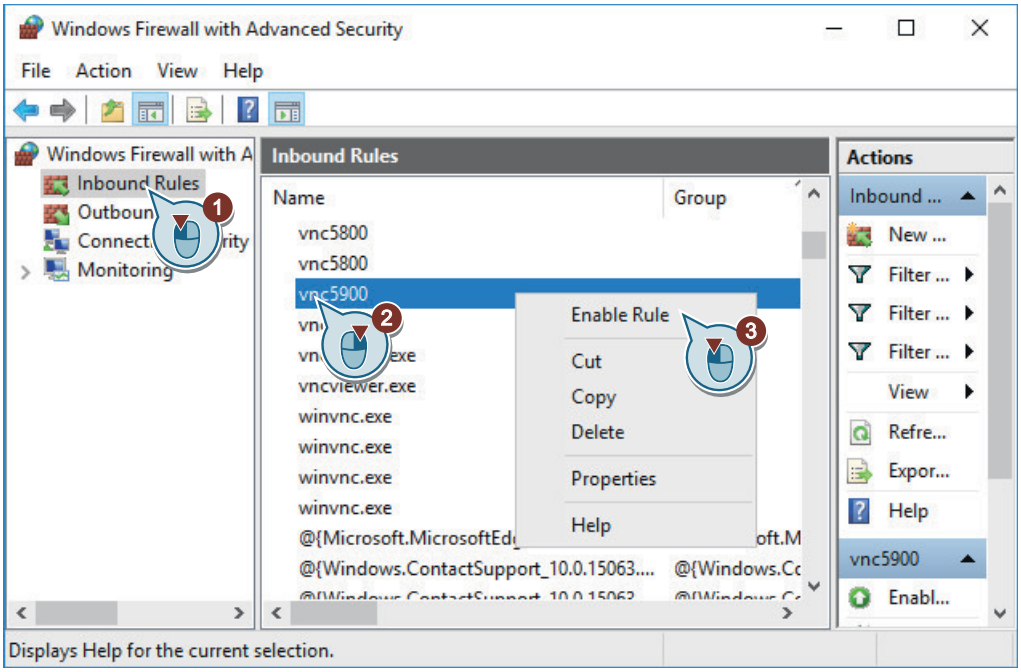
5.18.7.2 Via the Control Panel

Procedure

To activate remote access from the PG/PC in the company network to the PC system, proceed as follows:

1. Enter "Control Panel" in the search field and then click on "Control Panel" in the search results. The desktop App "Control Panel" opens.
2. Click on the display selection and switch from the "Category" view to "Icons". The "All Control Panel Items" dialog box opens.
3. Click on "Windows Defender Firewall".

4. Click on "Advanced settings" and confirm the call of the expanded settings with "Yes" if necessary.
5. In the "Windows Firewall with Advanced Security" dialog, right-click under "Inbound Rules" on the rule "vnc5900", then click on "Enable Rule".



The "vnc5900" rule is activated and a symbol with a green background is displayed.

Result

With the activation of the inbound rule "vnc5900", Port 5900 was activated in the company network, which allows remote access from a PG/PC to the PC system in the company network.

If you want to deactivate remote access in the company network, right-click on the rule "vnc5900" and select "Disable Rule" in the shortcut menu.

More information

You can find general information on remote access to the PC system (via VNC Viewer or SSH client) in Chapter Remote access (Page 202).

5.18.7.3 By prompt, script or batch file

Basic procedure

With a command according to the following scheme, you can activate remote access from the PG/PC in the company network to the PC system.

To do this, call the prompt as the administrator and enter the command either completely or successively.

Alternatively, you can save the command and the associated parameters in a script file (Page 75).

Syntax for activating a firewall rule via the prompt

```
netsh advfirewall firewall set rule name="<Name of the firewall rule>" new
enable=yes profile=<Name of the network profile>
```

Table 5-7 Description of the Netsh commands in the context of the advfirewall firewall

Command	Parameter	Description	Value
netsh		Specification of the command line program, which executes the following commands.	-
advfirewall		Defines the context in which the following commands are to be carried out.	-
firewall		Subcontext of "advfirewall".	-
set rule		Adaptation of an existing firewall rule.	-
	name	Name of the firewall rule in quotation marks	"vnc5900" | ... | all
	new	Specifies that the following parameters are to be changed or added.	-
	enable	Activates or deactivates the specified firewall rule.	yes | no
	profile	Name of the network profile for which the corresponding firewall rule is to be activated or deactivated.	public | private | domain | any | ...

Example

Activation of the firewall rule "vnc5900" for the "Public" profile.

```
netsh advfirewall firewall set rule name="vnc5900" new enable=yes profile=public
```

5.18.8 Activation/deactivation of the file and printer release

5.18.8.1 Overview

From a PG/PC in the system network, you can easily and directly access a directory on the PC system.

If you want to access the PC system via the company network instead or in addition, you must adapt the firewall settings.

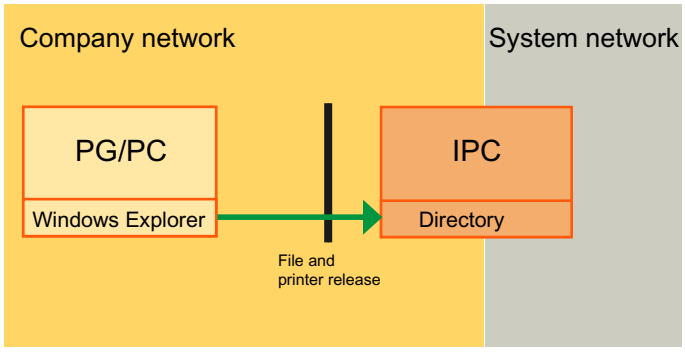


Figure 5-5 Access to a shared directory in the IPC from a PG/PC in the company network

Overview

You can activate the file and printer release either for all of the network profiles, for a specific network profile, or for a specific network connection:

- General activation for all network profiles (Page 82)
  - Via the Control Panel (Page 82)
  - By prompt or script file (Page 84)
- Activation for a specific network profile (Page 85)
  - Via the Control Panel (Page 85)
  - By prompt or script file (Page 87)
- Activation for a specific connection (Page 89)
  - Via the Control Panel (Page 89)
  - By prompt or script file (Page 90)

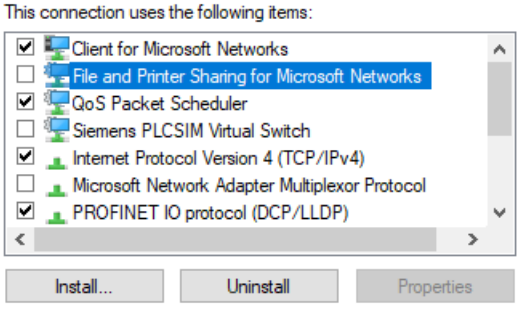
5.18.8.2 General information

General information on the file and printer release in Windows

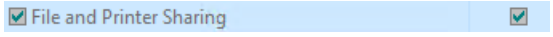
In Windows, there are basically settings for the file and printer release at two different locations: In the settings of the corresponding network adapter and in the Windows Firewall settings.

- In the Windows Firewall settings, the file and printer release is at least partially blocked:
  - The Windows Firewall is deactivated in the plant network, however, which allows access to USB flash drives and external hard disks.
  - In the company network, the Windows Firewall is activated and the file and printer release is blocked by the Windows Firewall.

  These settings can be changed in various dialog boxes, e.g. in the "Network and Sharing Center" or in the "Allowed apps" dialog box.
- In the settings of the network adapter for the plant network, the file and printer release is activated. However, in the settings of the network adapter for the company network, the file and printer release is deactivated. This setting primarily takes effect prior to the general setting of the Windows Firewall.



This can be seen in the corresponding Windows Firewall settings dialogs by means of a partially activated checkbox (green or gray background).



Further information

Further information on file and printer sharing is provided in Microsoft Windows support (https://support.microsoft.com/en-us/hub/4338813/windows-help?os=windows-10).

5.18.8.3 General activation for all network profiles

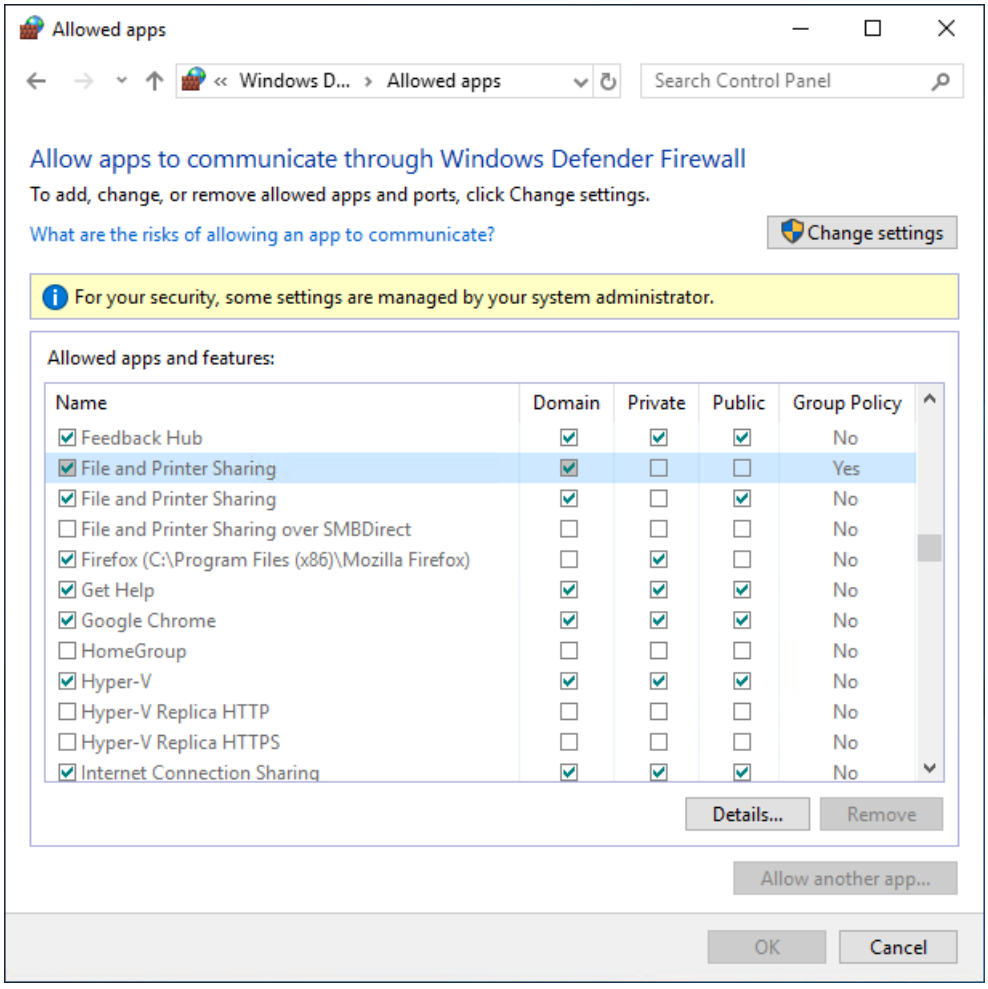
Via the Control Panel

There are several procedures for activating the file and printer release for all of the network profiles in the Windows Firewall. (For example, there is the alternative procedure via the "Network and Sharing Center" under "Change advanced sharing settings").

Procedure

To activate the file and printer release on the PC system, proceed as follows:

1. Enter "Control Panel" in the search field and then click on "Control Panel" in the search results.
   The desktop App "Control Panel" opens.
2. Click on the display selection and switch from the "Category" view to "Icons".
   The "All Control Panel Items" dialog box opens.
3. Click on "Windows Defender Firewall" > "Allow a app or feature through Windows Defender Firewall".
4. Click on "Change Settings" and confirm with "Yes", if applicable.
   The "Allowed apps" dialog box opens.
   Also observe the entry in the column "Group Policy" and the color of the checkboxes (a checkbox with a green or gray background indicates partial activation).



5. Activate the corresponding checkbox for the corresponding entry "File and Printer Sharing" for the desired network profiles.
6. Click "OK" to confirm the change.

By prompt, script or batch file

Basic procedure

With a command according to the following scheme, you can allow the file and printer release in the company network for all of the network profiles together. All of the firewall rules of the group "File and Printer Sharing" are changed for all network profiles.

To do this, call the prompt as the administrator and enter the command either completely or successively.

Alternatively, you can save the command and the associated parameters in a script file (Page 75).

Syntax for activating a group of firewall rules via the prompt

```
netsh advfirewall firewall set rule group="<group name>" new enable=yes
```

Table 5-8 Description of the Netsh commands in the context of the advfirewall firewall

Command	Parameter	Description	Value
netsh		Specification of the command line program, which executes the following commands.	-
advfirewall		Defines the context in which the following commands are to be carried out.	-
firewall		Subcontext of "advfirewall".	-
set rule		Adaptation of existing firewall rules.	-
	group	Name of the group with firewall rules	"File and Printer Sharing" | ...
	new	Specifies that the following parameters are to be changed or added.	-
	enable	Activates or deactivates the specified group of firewall rules.	yes | no

Example

Activation of the firewall rule "File and printer release" for the "Public" profile.

```
netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=yes
```

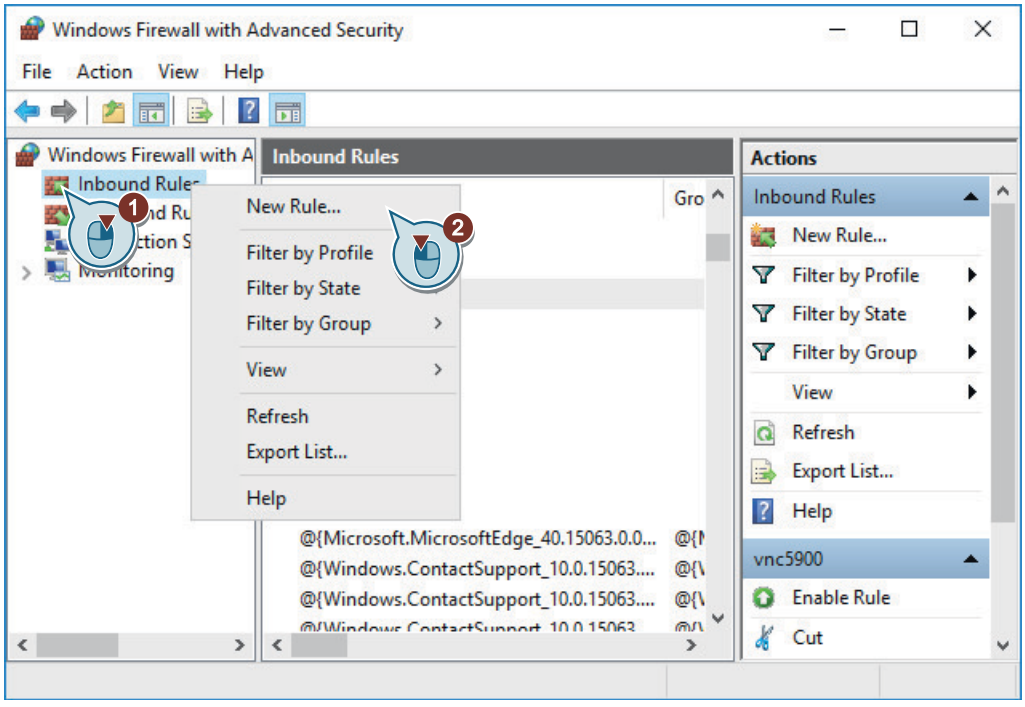
5.18.8.4 Activation for a specific network profile

Via the Control Panel

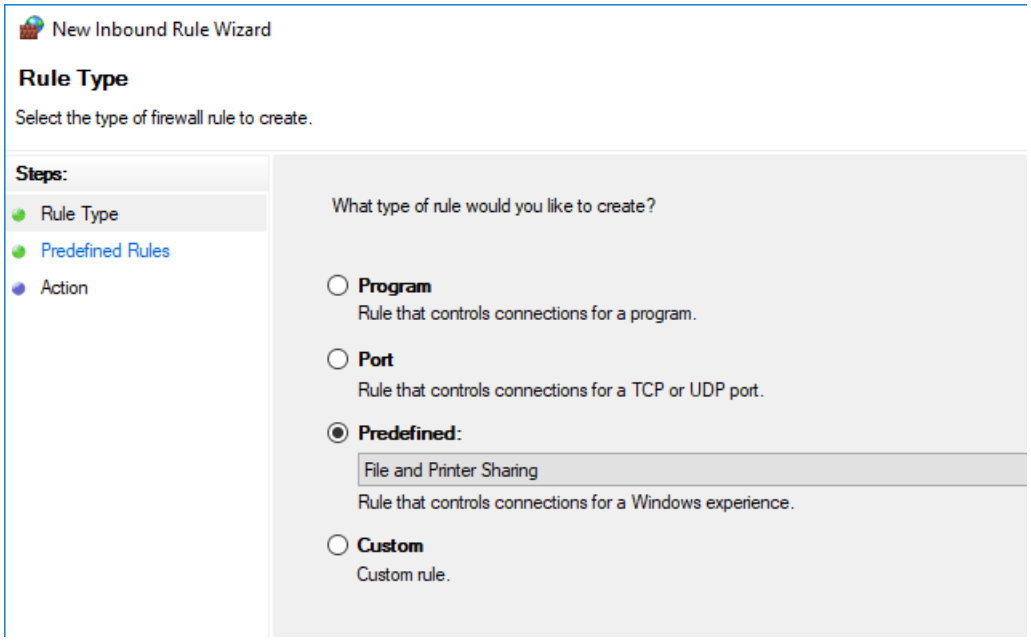
Procedure

Proceed as follows to share a PG/PC file and printer in the company network with the IPC for a specific network profile:

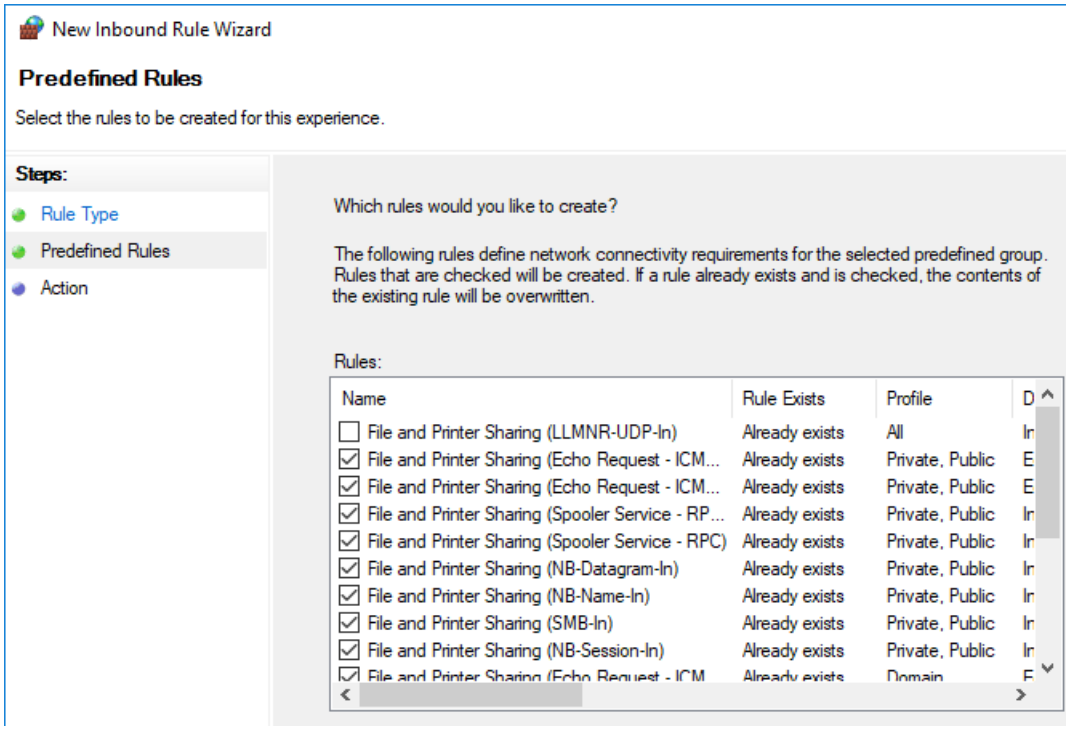
1. Enter "Control Panel" in the search field and then click on "Control Panel" in the search results. The desktop App "Control Panel" opens.
2. Click on the display selection and switch from the "Category" view to "Icons". The "All Control Panel Items" dialog box opens.
3. Click on "Windows Defender Firewall".
4. Click on "Advanced settings" and confirm the call of the expanded settings with "Yes" if necessary.
5. In the "Windows Defender Firewall with Advanced Security" dialog, right-click on the rule "Inbound Rules", then click on "New Rule..."



6. In the "New Inbound Rule Wizard" dialog, select the option button "Predefined", select in the "File and Printer Sharing" drop-down list, and click on "Next".



7. Depending on the network profile (e.g. Public or Domain) for which the file and printer release is to be activated, check the corresponding checkbox.



8. Click on "Next".
9. Select the option button "Allow the connection" and click on "Finish".

By prompt, script or batch file

Basic procedure

With a command according to the following scheme, you can switch off the blocking of the file and printer release by the Windows Firewall for a special network profile.

To do this, call the prompt as the administrator and enter the command either completely or successively.

Alternatively, you can save the command and the associated parameters in a script file (Page 75).

Syntax for the activation of all firewall rules regarding file and printer release

```
netsh
advfirewall firewall
set rule name="File and Printer Sharing (NB-Session-In)" new enable=yes
profile=<profile>
set rule name="File and Printer Sharing (NB-Session-Out)" new enable=yes
profile=<profile>
set rule name="File and Printer Sharing (SMB-In)" new enable=yes
profile=<profile>
set rule name="File and Printer Sharing (SMB-Out)" new enable=yes
profile=<profile>
set rule name="File and Printer Sharing (NB-Name-In)" new enable=yes
profile=<profile>
set rule name="File and Printer Sharing (NB-Name-Out)" new enable=yes
profile=<profile>
set rule name="File and Printer Sharing (NB-Datagram-In)" new enable=yes
profile=<profile>
set rule name="File and Printer Sharing (NB-Datagram-Out)" new enable=yes
profile=<profile>
set rule name="File and Printer Sharing (Spooler Service - RPC)" new
enable=yes profile=<profile>
set rule name="File and Printer Sharing (Spooler Service - RPC-EPMAP)" new
enable=yes profile=<profile>
set rule name="File and Printer Sharing (Echo Request - ICMPv4-In)" new
enable=yes profile=<profile>
set rule name="File and Printer Sharing (Echo Request - ICMPv4-Out)" new
enable=yes profile=<profile>
set rule name="File and Printer Sharing (Echo Request - ICMPv6-In)" new
enable=yes profile=<profile>
set rule name="File and Printer Sharing (Echo Request - ICMPv6-Out)" new
enable=yes profile=<profile>
set rule name="File and Printer Sharing (LLMNR-UDP-In)" new enable=yes
profile=<profile>
set rule name="File and Printer Sharing (LLMNR-UDP-Out)" new enable=yes
profile=<profile>
```

Table 5-9 Description of the Netsh commands in the context of the advfirewall firewall

Command	**Parameter**	**Description**	**Value**
netsh		Specification of the command line program, which executes the following commands.	-
advfirewall		Defines the context in which the following commands are to be carried out.	-
firewall		Subcontext of "advfirewall".	-
set rule		Adaptation of existing firewall rules.	-
	name	Name of the firewall rule in quotation marks.	"File and Printer Sharing (NB-Session-In)" | ...
	new	Specifies that the following parameters are to be changed or added.	-
	enable	Activates or deactivates the specified firewall rule.	yes | no

Example

Example for the activation of all firewall rules regarding file and printer release

```
netsh
advfirewall firewall
set rule name="File and Printer Sharing (NB-Session-In)" new enable=yes
profile=public
set rule name="File and Printer Sharing (NB-Session-Out)" new enable=yes
profile=public
set rule name="File and Printer Sharing (SMB-In)" new enable=yes
profile=public
set rule name="File and Printer Sharing (SMB-Out)" new enable=yes
profile=public
set rule name="File and Printer Sharing (NB-Name-In)" new enable=yes
profile=public
set rule name="File and Printer Sharing (NB-Name-Out)" new enable=yes
profile=public
set rule name="File and Printer Sharing (NB-Datagram-In)" new enable=yes
profile=public
set rule name="File and Printer Sharing (NB-Datagram-Out)" new enable=yes
profile=public
set rule name="File and Printer Sharing (Spooler Service - RPC)" new
enable=yes profile=public
set rule name="File and Printer Sharing (Spooler Service - RPC-EPMAP)" new
enable=yes profile=public
set rule name="File and Printer Sharing (Echo Request - ICMPv4-In)" new
enable=yes profile=public
set rule name="File and Printer Sharing (Echo Request - ICMPv4-Out)" new
enable=yes profile=public
set rule name="File and Printer Sharing (Echo Request - ICMPv6-In)" new
enable=yes profile=public
set rule name="File and Printer Sharing (Echo Request - ICMPv6-Out)" new
enable=yes profile=public
set rule name="File and Printer Sharing (LLMNR-UDP-In)" new enable=yes
profile=public
set rule name="File and Printer Sharing (LLMNR-UDP-Out)" new enable=yes
profile=public
```

5.18.8.5 Activation for a specific connection

Via the Control Panel

Procedure

To activate the file and printer release for a specific connection (e.g. company network), proceed as follows:

1. Enter "Control Panel" in the search field and then click on "Control Panel" in the search results.
   The desktop App "Control Panel" opens.
2. Click on the display selection and switch from the "Category" view to "Icons".
   The "All Control Panel Items" dialog box opens.
3. Click on "Network and Sharing Center".

4. Click on the desired connection, e.g. "Local Area Connection 2" (company network).
5. Click on "Properties" and confirm the call of the properties with "Yes" if applicable.
6. In the "Networking" tab, check the checkbox "File and Printer Sharing for Microsoft Networks" and confirm the change with "OK".

By prompt, script or batch file

In Windows, the activation of the file and printer release for a specific connection via the prompt or script/batch file is not supported. However, this is possible using the special command line program "Hyper-V Network VSP Bind (nvspbind)", which is free of charge:

Example: Activation of the file and printer release for "Local Area Connection 2" (company network)

```
nvspbind -e "Local Area Connection 2" ms_server
```

Further information

You can find further information in the documentation for nvspbind under Microsoft TechNet - Hyper-V Network VSP Bind (nvspbind) (https://gallery.technet.microsoft.com/Hyper-V-Network-VSP-Bind-cf937850).

(Command line program for configuring network adapters and connections via the prompt)

5.18.9 Activation of the ping execution (ICMP)

5.18.9.1 Via the Control Panel

In the factory setting state, incoming ping requests are blocked on the company network interface (X1) of the PC system. Outgoing ping requests are permitted.

Note

Dependency for the file and printer release

If you activated the file and printer release in the company network, incoming ping requests are already permitted because they are required for the file and printer release.

Procedure

To permit ICMP pings, which arrive at the company network interface (X1) of the PC system, proceed as follows:

1. Enter "Control Panel" in the search field and then click on "Control Panel" in the search results. The desktop App "Control Panel" opens.
2. Click on the display selection and switch from the "Category" view to "Icons". The "All Control Panel Items" dialog box opens.
3. Click on "Windows Defender Firewall".

4. Click on "Advanced settings" and confirm the call of the expanded settings with "Yes" if necessary.
5. In the "Windows Defender Firewall with Advanced Security" dialog, click on "Inbound Rules".
6. Select the corresponding rule for the relevant network profile:
   – File and Printer Sharing (Echo Request - ICMPv4-In) - Profile "Domain"
   – File and Printer Sharing (Echo Request - ICMPv4-In) - Profile "Public"
   – File and Printer Sharing (Echo Request - ICMPv4-In) - Profile "Private"

   In the factory setting state, the network profile "Public" is assigned to the company network.

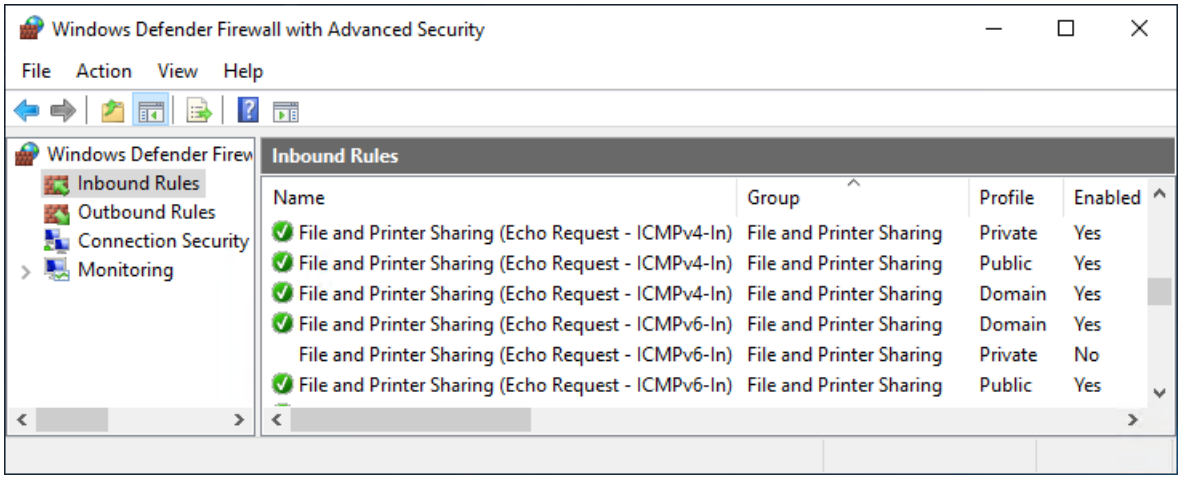


Figure 5-6 Rules for incoming ICMP pings, separate for each network profile

7. Right-click on the selected rule, then click "Enable Rule".

5.18.9.2 By prompt, script or batch file

Basic procedure

With a command according to the following scheme, you can permit ICMP pings which arrive at the company network interface (X1) of the PC system. Outgoing pings from the PC system are already activated.

Note

Dependency for the file and printer release

If you activated the file and printer release in the company network, incoming ping requests are already permitted because they are required for the file and printer release.

The name of the relevant firewall rule is "File and Printer Sharing (Echo Request - ICMPv4-In)". To do this, call the prompt as the administrator and enter the command either completely or successively.

Alternatively, you can save the command and the associated parameters in a script or batch file (Page 75).

Syntax for activating a firewall rule via the prompt

```
netsh advfirewall firewall set rule name="<Name of the firewall rule>" new enable=yes
profile=<Name of the network profile>
```

Table 5-10 Description of the Netsh commands in the context of the advfirewall firewall

Command	Parameter	Description	Value
netsh		Specification of the command line program, which executes the following commands.	-
advfirewall		Defines the context in which the following commands are to be carried out.	-
firewall		Subcontext of "advfirewall".	-
set rule		Adaptation of existing firewall rules.	-
	name	Name firewall rule	"File and Printer Sharing (Echo Request - ICMPv4-In)" | ...
	new	Specifies that the following parameters are to be changed or added.	-
	enable	Activates or deactivates the specified firewall rule.	yes | no
	profile	Name of the network profile for which the firewall rule is to be changed.	

Example

Activation of incoming ping requests

```
netsh advfirewall firewall set rule name="File and Printer Sharing (Echo Request - ICMPv4-
In)" new enable=yes profile=public
```

5.18.10 Saving and restoring firewall settings

5.18.10.1 Overview

Overview

You can save all of the Windows Firewall settings of the PC system as a policy file with the file extension ".wfw". Policy files are saved in binary format and are Windows version-dependent.

You have the following options for backing up or restoring the firewall settings:

- Backup of firewall settings (Page 93)
  - Via the Control Panel (Page 93)
  - By prompt, script or batch file (Page 93)
- Restoring of firewall settings (Page 94)
  You can restore the firewall settings on the same PC system or import the same policy file to different PC systems for the purpose of series commissioning.
  - Via the Control Panel (Page 94)
  - By prompt, script or batch file (Page 95)

5.18.10.2 Backup of firewall settings

Via the Control Panel

Procedure

To back up the Windows Firewall settings of the PC, proceed as follows:

1. Enter "Control Panel" in the search field and then click on "Control Panel" in the search results. The desktop App "Control Panel" opens.
2. Click on the display selection and switch from the "Category" view to "Icons". The "All Control Panel Items" dialog box opens.
3. Click on "Windows Defender Firewall".
4. Click on "Advanced settings" and confirm the call of the expanded settings with "Yes" if necessary.
5. Right-click on the master object "Windows Defender Firewall with Advanced Security on Local Computer" and then click on "Export Policy...".
6. In the "Save As" dialog, select a save location and file name and confirm with "Save".

By prompt, script or batch file

Basic procedure

With a command according to the following scheme, you can back up the Windows Firewall settings in a policy file (.wfw).

To do this, call the prompt as the administrator and first define the save location of the policy memory, then enter a file path for backing up the policy file.

Alternatively, you can save the commands and the associated parameters in a script or batch file (Page 75).

Syntax of the Netsh commands for defining the policy memory and for exporting the policy file

```
netsh advfirewall set store local
export <File path and file name>.wfw
```

Table 5-11 Description of the Netsh commands for defining the policy memory and for exporting the policy file

Command	Parameter	Description	Value
netsh		Specification of the command line program, which executes the following commands.	-
advfirewall		Defines the context in which the following commands are to be carried out.	-
set store		Definition of the save location of the policy memory for the following commands.	-
	local	Defines that the work is to be done with the local policy memory.	-
export		Backup of all firewall settings in a policy file (.wfw).	<File path and file name>.wfw

Example

Example of the Netsh commands for defining the policy memory and for exporting the policy file

```
netsh advfirewall set store local
export D:\Backup\DefaultSettings.wfw
```

5.18.10.3 Restoring of firewall settings

Via the Control Panel

Procedure

Note

Importing a policy file overwrites all existing firewall rules

When the firewall settings are restored, all of the existing firewall rules are overwritten. You cannot undo the import of firewall rules via a policy file.

Therefore, back up (export) the existing firewall settings before you import a policy file.

To restore the Windows Firewall settings of the PC system, proceed as follows:

1. Enter "Control Panel" in the search field and then click on "Control Panel" in the search results. The desktop App "Control Panel" opens.
2. Click on the display selection and switch from the "Category" view to "Icons". The "All Control Panel Items" dialog box opens.
3. Click on "Windows Defender Firewall".
4. Click on "Advanced settings" and confirm the call of the expanded settings with "Yes" if necessary.
5. Right-click on the master object, then click "Windows Defender Firewall with Advanced Security on Local Computer", then click on "Import Policy..." and confirm the command with "Yes".
6. In the "Open" dialog, select the policy file and confirm with "Open".

By prompt, script or batch file

Basic procedure

Note

Importing a policy file overwrites all existing firewall rules

When the firewall settings are restored, all of the existing firewall rules are overwritten. You cannot undo the import of firewall rules via a policy file.

Therefore, back up (export) the existing firewall settings before you import a policy file.

With a command according to the following scheme, you can restore the Windows Firewall settings from a policy file (.wfw).

To do this, call the prompt as the administrator and first define the save location of the policy memory, then enter a file path for backing up the policy file.

Alternatively, you can save the commands and the associated parameters in a script or batch file (Page 75).

Syntax of the Netsh commands for defining the policy memory and for importing the policy file

```
netsh advfirewall set store local
import <File path and file name>.wfw
```

Table 5-12 Description of the Netsh commands for defining the policy memory and for importing the policy file

Command	Parameter	Description	Value
netsh		Specification of the command line program, which executes the following commands.	-
advfirewall		Defines the context in which the following commands are to be carried out.	-
set store		Definition of the save location of the policy memory for the following commands.	-
	local	Defines that the work is to be done with the local policy memory.	-
import		Restoration of firewall settings from a policy file (.wfw).	<File path and file name>.wfw

Example of the Netsh commands for defining the policy memory and for importing the policy file

```
netsh advfirewall set store local
import D:\Backup\DefaultSettings.wfw
```

5.19 Using BitLocker drive encryption

Introduction

The BitLocker is a security feature of Microsoft Windows that provides encryption for all data storage media of the PC system and eliminates the dangers of data theft or disclosure through lost, stolen or inappropriately decommissioned devices. The data storage media can only be used with the assigned PC system. If the data storage media is used in another PC system, all data remains encrypted and cannot be used.

You can set up the BitLocker function via the Control Panel under "BitLocker Drive Encryption". Alternatively, you can configure BitLocker encryption using a script.

Note

The setup for BitLocker drive encryption is deactivated by default on the PC system with the PCU base software /IPC installed. To use BitLocker encryption, activate the setup in Microsoft Windows (Page 98).

NOTICE
Data loss An active BitLocker always requires a restore password for data storage media decryption in the case of servicing or emergency. Always save the password **outside the system** to prevent data loss or data misuse.

NOTICE
Unencrypted backup data You can create a backup using a BitLocker-protected data storage medium with the **Paragon Hard Disk Manager**™ application. The backup data are archived unencrypted with the application by default. In the event of data theft, the backup is unprotected and can be manipulated. Protect the backup through manual password encryption.

Note

Remote access to the PC system is not possible when BitLocker is active.

Requirement

The following is a prerequisite for using the Bitlocker functions:

- PCU base software /IPC version 15 SP3 or higher, including Paragon Hard Disk Manager software™ 17 Suite
- Administration rights for the PC system

Displaying the BitLocker status

Open the Microsoft Windows Explorer and click on "This PC". All drives connected to the PC system are displayed.

The status of the Bitlocker encryption is indicated by a lock symbol:



BitLocker active



BitLocker inactive

Note

Other data storage media icons without an integrated lock symbol indicate that Microsoft Windows BitLocker drive encryption is deactivated.

5.19.1 Activating BitLocker setup

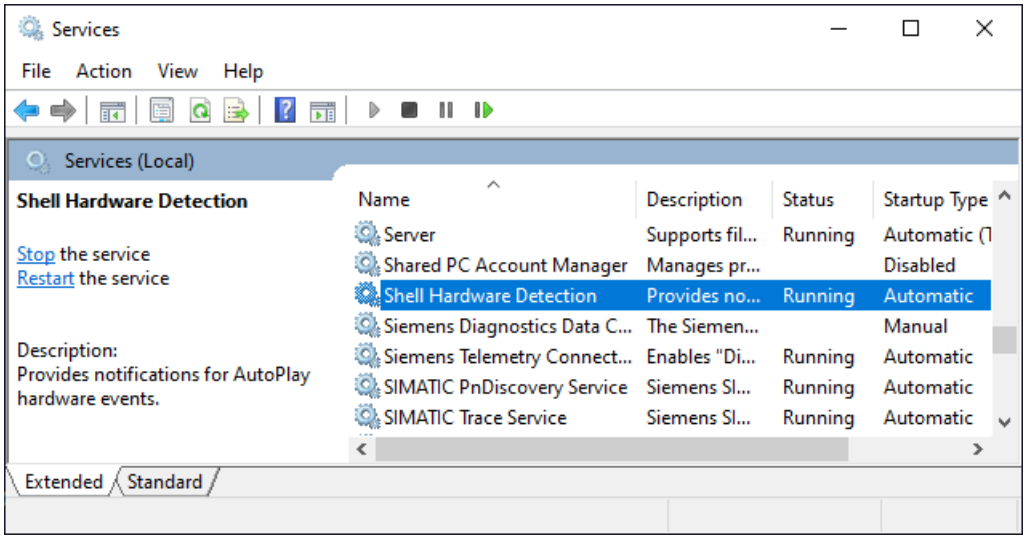
The setup for Microsoft Windows BitLocker drive encryption is disabled by default on the PC system with PCU Base installed. To use the BitLocker setup, activate the corresponding service as follows:

Procedure

1. Enter "services" in the Microsoft Windows search bar and open the Services application with "Run as Administrator".
2. Confirm the confirmation prompt with "Yes".
   The Microsoft Windows Services application opens.
3. In the Extended tab, search for the "Shell Hardware Detection" service and double-click on the entry.
   The "ShellHWDetection" service function opens.
4. In the General tab under "Startup type", switch to "Automatic" and click "Start".
   The service is activated.
5. Confirm the setting with "Ok".

Result

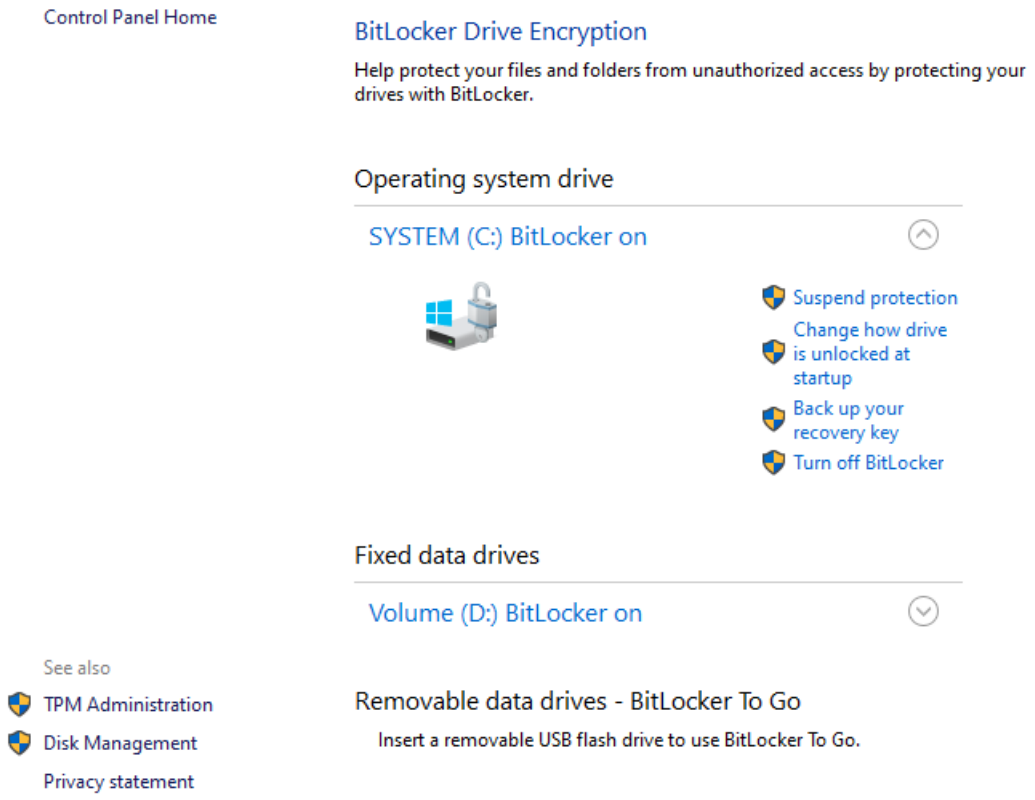
The "Shell Hardware Detection" is active. "Running" appears in the Status column.



The setup is active, BitLocker drive encryption can now be used under Microsoft Windows.

5.19.2 Configuring BitLocker via Microsoft Windows

With the Microsoft Windows user interface **BitLocker Drive Encryption**, you can set up BitLocker encryption for each drive individually. Each drive receives its own encryption and recovery password. The BitLocker Drive Encryption user interface is an application from the Control Panel.



Procedure

1. The PC system has started up, you are logged in.
2. Open the Microsoft Windows Explorer and click on "This PC".
   All drives connected to the PC system are displayed.
3. In the drive overview, right-click on the drive, then on "Manage BitLocker".
   - or -
   If no BitLocker is active, select "Turn on BitLocker" and follow the instructions.
   The BitLocker Drive Encryption user interface opens.
4. Configure the drive:
   - Activate BitLocker, e.g. after an SSD backup has been restored on the IPC with Paragon.
   - Save the recovery key on **an external data storage medium**, e.g. on a USB flash drive.
   - Deactivate BitLocker if you do not need protection.

More information on BitLocker encryption can be found under Microsoft Learn (https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/).

Result

BitLocker encryption is active/inactive separately for each drive in the PC system.

5.19.3 Configuring BitLocker using a script

You have the option of using a script with which you can automatically protect the drives of the PC system with the same Bitlocker encryption, e.g. for series commissioning. A uniform recovery password applies to the drives.

You will find the BitLocker script example for your configuration in the annex (Page 213).

NOTICE
Data loss Always save the script and the recovery password **outside the system** to prevent data loss or misuse.

Creating a script file

1. Open a text editor.
2. Copy the **BitLocker script example** (Page 213) in the annex into the text editor.
3. Save the script example as a ps1 file (character encoding ASCII or ANSI) on a USB flash drive, for example:
   `E:/enableIPCBitlocker.ps1`
4. Close the script.

Applying the script file

1. Open the **Microsoft Windows PowerShell** application. Enter the term "powershell" in the search field and open the application as administrator.
   The Microsoft Windows PowerShell application opens.
2. Enter the following command in PowerShell:
   `Set-ExecutionPolicy -Scope Process -ExecutionPolicy Unrestricted`
   A confirmation prompt is displayed.
3. Respond to the confirmation prompt with "Y" for yes.
   The provisions for script usage are changed.

4. Navigate to the storage directory of the script file, e.g. on the USB flash drive with the following command:
   `e:`
   PowerShell displays drive E: `E:\>`
5. Enter the following command for BitLocker activation in PowerShell:
   `.\enableIPCBitlocker -RecoveryPasswordFile "E:\BitlockerRecoveryPassword.txt"`
   BitLocker encryption is activated and a random recovery password is saved as TXT file:
   `E:/BitlockerRecoveryPassword.txt`

Result

BitLocker encryption is active for the drives in the PC system.

The uniform recovery password applies to the drives.

Note

Use the **Service Center** (Page 181) if you wish to deactivate BitLocker encryption.

Installing and configuring updates and automation software

6

6.1 Overview

After you have completed the installation of PCU-Basesoftware /IPC and configured the network settings as required, you can set up the handling of security updates, patches and software installations or install them directly.

- Information about Microsoft Windows updates and network security of an automation system is provided in Chapter Patch management and security updates (Page 104).
- The PCU Installer (Page 144) will assist you with automatic installation of setup packages.
- You can install SINUMERIK Operate (Page 106) or other HMI software and at the same time (Page 107) or subsequently (Page 108) set it up for autologon mode.
- To prevent operation of the HMI software from being interrupted by key combinations such as CTRL+ALT+DEL, you can activate and configure the key filter (Page 138).
- You can install STEP 7 and the SINUMERIK add-on (Page 142) and add a softkey to the HMI software to start STEP 7 (Page 143).
- If you want to transfer existing data to the newly installed automation software, read Chapter Migration (Page 156).

6.2 Patch management and security updates

Microsoft regularly eliminates security vulnerabilities in Microsoft Windows 10, and makes these corrections available on its "Windows Update" website:

"Start > Settings > Update & Security"

As a solution for managing and making Microsoft Windows updates available in a network, Microsoft offers the components in the Microsoft Update Catalog (http://www.catalog.update.microsoft.com).

Industrial cybersecurity

You will find information about network security for an automation system and a comprehensive protection concept under Industrial Cybersecurity on the SIEMENS website:

Industrial cybersecurity (https://www.siemens.com/industrialsecurity)

SINUMERIK-specific information can also be found in the following documents:

SINUMERIK/SIMOTION/SINAMICS Configuration Manual Industrial Security (https://support.industry.siemens.com/cs/document/108862708?lc=en-WW)

Compatibility with automation software

Information about the compatibility of a Microsoft Windows update with specific application software of SIEMENS may possibly be available on the product pages of the application software involved in the Service&Support portal:

SiePortal (https://support.industry.siemens.com/)

Generally, it is recommended that you check the compatibility of updates in a dedicated project test environment before installing it in a productive environment.

6.3 Configuring Microsoft Windows log files storage

As a result of Microsoft Windows updates and other operations, larger quantities of data can accumulate that are no longer required, e.g. temporary update and system files or Microsoft Windows log files (`CBS.log`).

PCU-Basesoftware /IPC contains 2 batch files, which you can use to configure how files such as these are saved:

- Deactivate saving
  - Saving new log files `CBS.log` is deactivated, and existing files are deleted: `C:\Windows\Logs\CBS`
  - The temporary directory is cleared once: C:\Windows\Temp
  - The data storage medium cleanup is carried out.
- Activate saving
  - Reactivates that new log files `CBS.log` are saved for diagnostics.

You can refer to the information file in the following directory to identify whether the log files are being saved or not: `C:\Windows\Logs\CBS`

Precondition

- You require administrator rights to run batch files.

Procedure

1. Change to directory `D:\etc` and double-click on the appropriate batch file.

6.4 Installing and setting up SINUMERIK Operate

6.4.1 Installing SINUMERIK Operate /PCU Modular

The **SINUMERIK Operate /PCU Modular** installation package is on the installation medium provided.

Note

The term "installation medium" is synonymous with USB, download, or other supplied media.

Requirement

- The hardware and software of the PC meet the system requirements.
- You have administrator rights on your PC system.
- All running programs are closed.

How to install SINUMERIK Operate

Navigate to the setup files on the installation medium of SINUMERIK Operate.

Perform one of the following installation options:

- For a standard guided installation, double-click on setup file *.exe, and follow the wizard's instructions. In the wizard, select "SINUMERIK Operate /PCU Modular" and set up the autologon mode (Page 107).

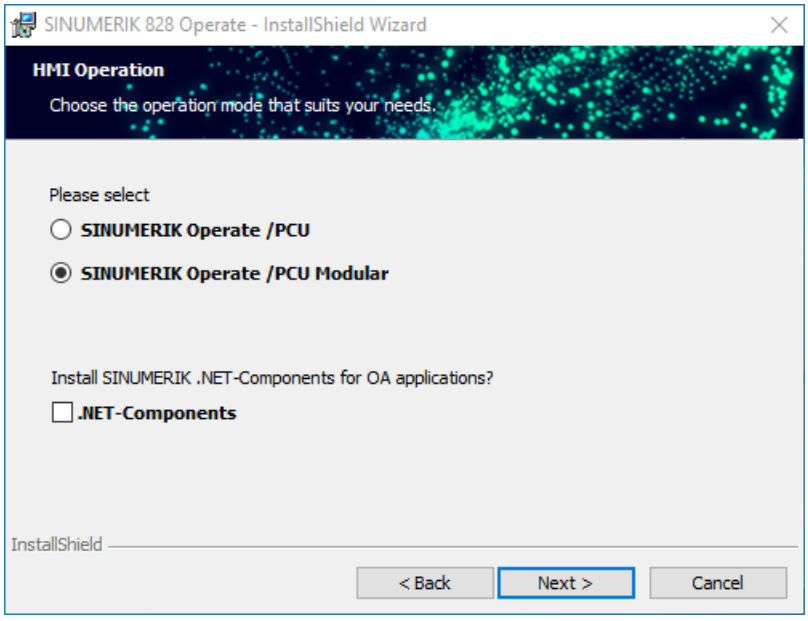


Figure 6-1 SINUMERIK Operate Installer - default setting

- Use the interactive or silent installation variants (Page 109) via command line arguments.

After successful installation, you must restart the PC system.
SINUMERIK Operate is now installed.

Note

Parallel SINUMERIK Operate installations on a PC system

It is possible to install further versions of the operating software on the PC system, e.g. for test purposes.

- During the installation of another version, change the main directory via the wizard:
  `C:\Program Files(x86)\Siemens\MotionControl\...`
  e.g. to
  `C:\Program Files(x86)\Siemens\MotionControl_V520\...`
- Avoid malfunctions between the versions. Only operate one SINUMERIK Operate version at a time.

Further procedure

- Configure the communication settings (Page 111) (PG/PC interface) on the PC system to enable communication between the PLC and SINUMERIK Operate.
- Set up the PU connection (Page 112) so that communication between SINUMERIK Operate and the PU is possible.
- Adjust the display size of (Page 113) SINUMERIK Operate, e.g. to improve operation on an external monitor.
- Make any required other settings (Page 117). For example, connect the OEMFrame application (Page 121) with SINUMERIK Operate.

6.4.2 Setting up SINUMERIK Operate for autologon mode

If you want the PC system to start automatically in SINUMERIK Operate after switching on without having to make any further entries, set up the autologon mode.

When installing SINUMERIK Operate, you can define an existing user account as an autologon account. The PC system then starts without the password for this user account being entered. SINUMERIK Operate is then started automatically because a link is created in the "Startup" Autostart folder.

For security reasons, you should use a special user account without administrator rights.

You can also configure the key filter and deactivate certain keyboard entries (Page 138), e.g. to prevent a switchover from SINUMERIK Operate to the Microsoft Windows desktop. (Desktop access is then only possible via the splash screen (Page 198).)

Requirement

- A Microsoft Windows user account without administrator rights is set up.
- SINUMERIK Operate is not installed.

- You are logged on as an administrator or you know the password of the administrator account.
- The keyboard layout of the system is set to English.
  See: Configuring the keyboard layout (Page 50)

Procedure

To set up autologon mode, proceed as follows:

1. Start installation of SINUMERIK Operate and, in the installation wizard, proceed to step "Autologon".

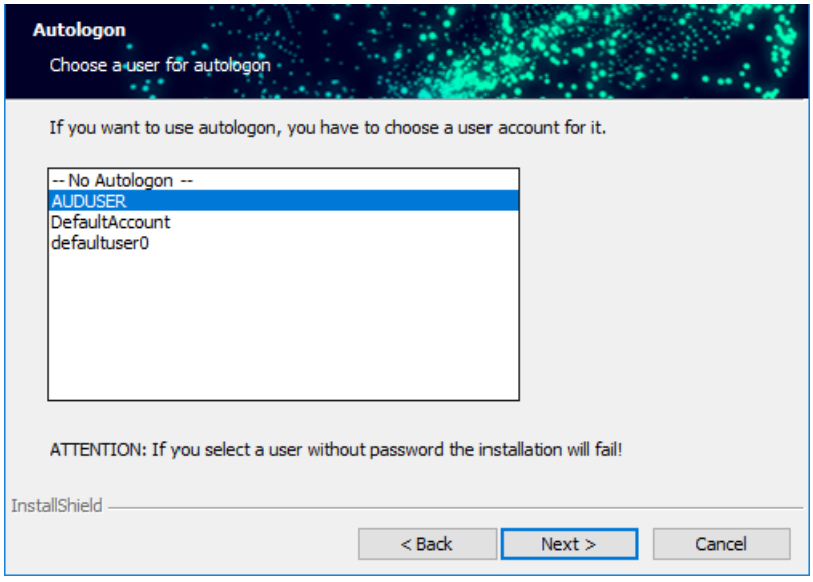


Figure 6-2 SINUMERIK Operate Installer - Autologon

2. In the list, select the user account to be logged on automatically.
3. Confirm with "Next", then in the next steps of the installation wizard make all the necessary settings and confirm the installation with "Finish".

Result

SINUMERIK Operate is installed and autologon mode of the PC system is set up. During this process the password of the autologon user account is stored encrypted in Microsoft Windows, and SINUMERIK Operate is linked with the autostart folder "Startup".

Autologon mode is active at the next startup. The autologon user account is automatically logged on and SINUMERIK Operate is started.

6.4.3 Modifying the user account for autologon mode.

Because of the way autologon works, only one user account can ever be set up for autologon mode.

If you set up autologon mode during installation of SINUMERIK Operate for one particular user account, but now want to use another user account for autologon mode, you can change this manually in the Service Desktop.

Precondition

- SINUMERIK Operate is installed and autologon mode is set up.
- The Service Desktop is active.

Procedure

To change the user account that is used for automatic run-up in autologon mode, proceed as follows:

1. To open the "User Accounts" dialog box, proceed in one of the following ways:
   - On the Desktop, double-click the "Netplwiz" icon.
   - In the search field of the Start menu, enter `netplwiz` and confirm the entry.
   - At the prompt, enter `control userpasswords2`.

   The "User Accounts" dialog box opens.
2. Activate the "Users must enter a user name and password to use this computer" checkbox.
3. In the "Users for this computer" list, select the user account to be used for autologon mode.
4. Deactivate the "Users must enter a user name and password to use this computer" checkbox. You may be prompted to enter a password.
5. Confirm these settings in the "User Accounts" dialog box with "OK".
6. In the Autostart folder of the autologon mode user account, create a link to SINUMERIK Operate.

6.4.4 Using interactive or silent installation versions

If you install SINUMERIK Operate, then the following installation variants are available, which you can use via the Microsoft Windows command line in the interactive or silent mode:

- SINUMERIK Operate complete installation
- SINUMERIK Operate base installation with auxiliary files
- SINUMERIK Operate base installation without auxiliary files

Execution

You control setup execution using command line arguments. The interactive mode `/v` allows you to transfer parameter strings to setup.exe. If you wish to run setup without user interaction, then you can extend the parameter string with the silent mode `/qn`.

Place the parameter string in inverted commas. If you use several parameters in the string, separate these using spaces.

If you do not specify any arguments when calling setup.exe, then the complete installation is run in the interactive mode.

Note

Do not put any spaces between `/v` and the parameter string.

Note

If you want a progress display in the silent mode, then instead of specifying `/qn` you can also specify `/qb!`.

Interactive installation versions

`setup.exe`	Complete installation in the interactive mode
`setup.exe /v"BASEONLY=1"`	Base installation in the interactive mode with help files
`setup.exe /v"BASEONLY=1 HELPFILES=0"`	Base installation in the interactive mode without help files

Silent installation versions

`setup.exe /v"/qn"` `setup.exe /s /v"/qn"`	Complete installation in the silent mode (`/s` suppresses all setup messages)
`setup.exe /v"/qn BASEONLY=1"` `setup.exe /s /v"/qn BASEONLY=1"`	Base installation in the silent mode with help files (`/s` suppresses all setup messages)

`setup.exe /v"/`
`qn BASEONLY=1 HELPFILES=0"`
`setup.exe /s /v"/`
`qn BASEONLY=1 HELPFILES=0"`
	Base installation in the silent mode without help files
	(`/s` suppresses all setup messages)

Note

Procedure if the installation was terminated with feedback errors about the progress or result

If the installation process of SINUMERIK Operate is terminated with feedback errors before successful completion, use the following installation command:

```
start /wait setup.exe /clone_wait /s /v"...
```

Command processing thus waits until setup.exe has been completely installed.

Additional parameter assignments

Installation path

If you install SINUMERIK Operate, then you can also specify the installation path:

```
setup.exe /s /v"/qn INSTALLDIR=C:\Programme\testdir"
```

For spaces in the path:
```
setup.exe /s /v"/qn INSTALLDIR=\"C:\Program Files\testdir\""
```

Exit code

You can identify a successful installation or errors based on the exit code of the setup.exe call:

`Exit code == 0`	No error
`Exit code <> 0`	Error

Log file

During the installation you can generate a log file with `/L`:
```
setup.exe /s /v"/qb! /L*vx log.txt"
```

6.4.5 Configuring the PG/PC interface

For communication between SINUMERIK Operate and the PLC, you must set the PG/PC interface on the PC system. Use Siemens Communication Settings application for configuring.

If you select an interface parameter assignment, then assign this to the access point. This means that you establish the connection between the access point, the interface parameter assignment and the interface itself.

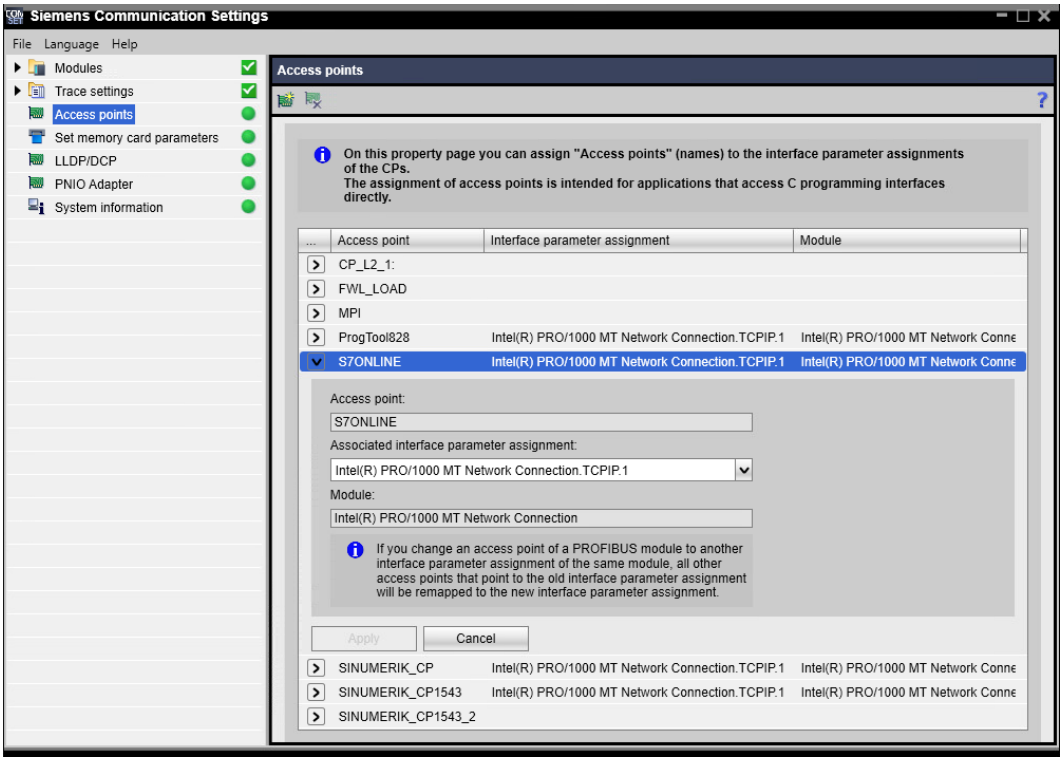


Figure 6-3 Setting the access point

Requirement

The Siemens Communication Settings application is installed on the PC system.

Note

The application is a system tool and part of TIA Portal.

This is how you configure the PG/PC interface using the Siemens Communication Settings application

1. Enter "Control Panel" in the Microsoft Windows search field and in the search results, click on "Control Panel".
   The desktop app "Control Panel" opens.
2. If necessary, click on the display selection and switch from the view "Category" to "Icons".
   The "All Control Panel Items" dialog opens.
3. Click on "Communication Settings".
   The "Siemens Communication Settings" window is displayed.
4. Click on "Access points" in the navigation.
   The available access points are displayed in the right-hand area.
5. Click the arrow in front of "S7ONLINE" to display the settings.
6. In the "Associated interface parameter assignment" field, select the entry "<network adapter>.TCPIP.1". <network adapter> is a placeholder for the interface name of your deployed hardware.
7. Click on "Apply".
8. Click the arrow in front of "SINUMERIK_CP1543" to display the settings.
9. In the "Associated interface parameter assignment" field, select the entry "<network adapter>.TCPIP.1". <network adapter> is a placeholder for the interface name as used previously.
10. Click on "Apply".
11. Select "File > Exit" in the menu to close the window.
12. Restart the PC system to apply the changes.

Result

You have now configured the access points for the application. SINUMERIK Operate can be used.

6.4.6 Starting and setting up SINUMERIK Operate /PCU Modular

When starting SINUMERIK Operate /PCU Modular, the application is opened with the preselected PU connection.

Starting SINUMERIK Operate

1. On the desktop, double-click the "SINUMERIK 828 Operate" icon or select "Start > Siemens Automation > SINUMERIK 828 Operate"
   The user interface of SINUMERIK Operate is displayed.
2. Select the "Commissioning" operating area and press the "Change language" softkey.
   The language selection opens.
3. Select your language and click "OK".
4. In the "Commissioning" operating area, press the "Password" softkey.
5. Press the "Set password" softkey, enter the manufacturer password and confirm with "OK".
   A valid password is acknowledged as set and the manufacturer access level is set.

More information on the access levels can be found in the online help of SINUMERIK Operate.

Manually changing the SINUMERIK Operate connection with PU

1. In the "Commissioning" operating area, select the softkeys "HMI > cursor key > NCU Connection".
   The "NCU Connection" dialog box opens.
2. Select address type "IP Address", enter the value for PU connection X120 (system network) and confirm with "OK"
   SINUMERIK Operate connects to the PU when it restarts.

Note

Alternatively, you can also configure the connection between SINUMERIK Operate and the PU via the `mmc.ini` file.

Copy of the file from directory `.../siemens/sinumerik/hmi/cfg` and insert the copy below `user` or `oem` with the same path. Change the IP addresses and start SINUMERIK Operate.

6.4.7 Configuring the SINUMERIK Operate display size

Adjust the SINUMERIK Operate display size, e.g. to improve the user interface operation on an external monitor with higher image resolution.

Procedure

Proceed as follows to configure the display size of SINUMERIK Operate:

1. Open the configuration file slrs.ini in the directory
   `...\MotionControl\user\sinumerik\hmi\cfg\`.
2. In the `[Global]` section, change the display size in the following lines:
   - `Resolution=`
     Sets the display size of the user interface
   - `DisplayResolution=`
     Sets the display size of the window area when the window mode is activated

   The following values are permissible: `640x480`, `800x600`, `1024x768` or `1280x1024`
3. Save and close the slrs.ini file.

Result

The display size is configured when you restart SINUMERIK Operate.

Note

Avoid display errors in the window mode of SINUMERIK Operate. Set at least the same value for `DisplayResolution` as for `Resolution`.

6.4.8 FindWindow program application

You can use the FindWindow program to determine all relevant parameters of the configuration file systemconfiguration.ini which are important for an integration of an OEMFrame application in SINUMERIK Operate.

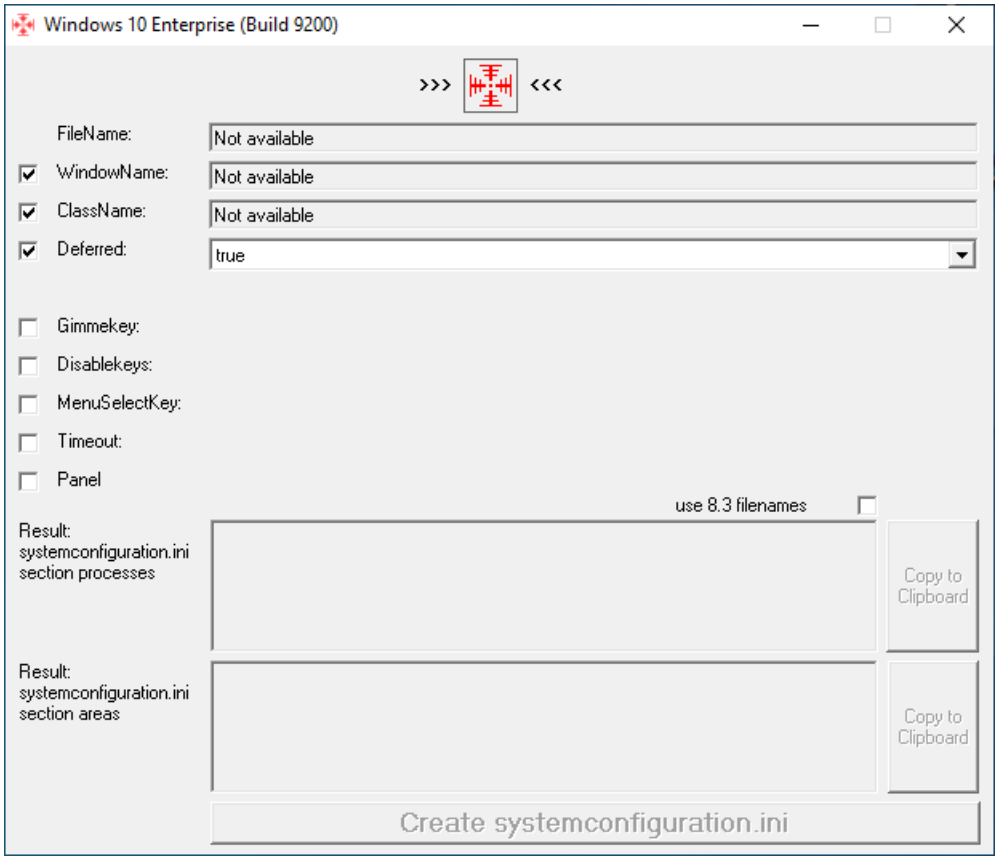


Figure 6-4 SINUMERIK Operate - FindWindow program application

More information

For more information about the systemconfiguration.ini configuration file and OEMFrame application, see Chapter "Integrating and parameterizing the OEMFrame application (Page 121)".

Requirement

For changes to become effective in SINUMERIK Operate through the FindWindow program, you need access level 2 (Service).

Installation

FindWindow can be used on any PC system without installation and is automatically installed with SINUMERIK Operate.

FindWindow (findwindow.exe) is located in the following directory:

`C:\Program Files (x86)\Siemens\MotionControl\Common\FindWindow\`

Application

1. Start the PC system.
2. Install the application to be integrated using OEMFrame.
3. Open the application.
4. Open the FindWindow program.
5. Left-click to drag the red cross to the title bar of the application in the FindWindow program.
6. Check the application parameters "FileName", "ClassName", etc.
7. Select the parameters "Gimmekey", "Disablekeys", etc. via the checkboxes as needed.
   If the configuration file systemconfiguration.ini exists and you want to expand it:
8. Copy the entries to the clipboard by clicking on "Copy to Clipboard".
9. Open the existing configuration file and insert the parameters from the clipboard. To do this, right-click on the position at which the parameters are to be inserted and then click on "Insert".
10. Save the modified configuration file.
    - or -
    If the configuration file systemconfiguration.ini does not exist and you want to create it:
11. Click on the "Create systemconfiguration.ini" button.
    A new configuration file is simultaneously created in the directory for FindWindow. Any existing configuration file will be overwritten.
12. Insert a copy of the new configuration file into the provided directory:
    /**oem**/sinumerik/hmi/cfg or /**user**/sinumerik/hmi/cfg

Note

If you include a 64-bit application, no parameter data is displayed under "FileName". In this case, an information dialog opens, which allows you to manually select the application.

Note

Only use the 8.3 Notation for file names if problems occur without this parameterization.

6.4.9 Further SINUMERIK Operate settings

6.4.9.1 Using user interfaces in parallel

SINUMERIK Operate can be used in parallel on several user interfaces connected with one control system. When doing so, only one user interface may be used as the main interface, while all other user interfaces behave passively and can only be used to a limited extent.

NOTICE
System error System errors may occur if you operate SINUMERIK Operate in parallel on other user interfaces with an NCU. An extended setting via the `HMIFunctionMode` parameter is only permitted for commissioning and service tasks. For productive operation, only loading and unloading as well as repositioning of tools via more than two user interfaces is permitted. The machine must always be operated via the main user interface.

To avoid function conflicts between the individual user interfaces and the controlled system, adapt the following configuration file:

File systemconfiguration.ini

Create the systemconfiguration.ini configuration file in one of the two directories:

`.../`**`user`**`/sinumerik/hmi/cfg`

`.../`**`oem`**`/sinumerik/hmi/cfg`

In the configuration file, enter the section `[miscellaneous]` with the parameter `HMIFunctionMode` and the appropriate value. The following value specifications are possible:

Value	Description
`PanelMode` or `<empty>`	The operating software and the system behave by default. **Note** Errors may occur in the system if SINUMERIK Operate is operated in parallel on another user interface with this value. Configure only one user interface per T:M:N group ⇒ T:1:N
`InterfaceMode`	SINUMERIK Operate is switched to passive in the system and does not log on as a regular user interface. The operating software: • does not write to the PLC interface • does not monitor PLC hardkeys • does not monitor MMC commands • does not monitor language selection via PLC • does not monitor PLC commands • does not monitor Ctrl-Energy • does not monitor dark-ON via PLC • does not set HMI-Ready in the PLC
`TerminalMode`	SINUMERIK Operate is used in the system as a tool loading station. The user interface behaves passively.

Example

For a CNC machine, two user interfaces should be used in the same system with one control.

Setting of the main user interface:
```
[miscellaneous]
HMIFunctionMode=PanelMode
```

Setting of the secondary user interface:
```
[miscellaneous]
HMIFunctionMode=TerminalMode
```

6.4.9.2 Changing the skin design

Display machine data

You can change the skin design via the following item of machine data.

MD9112 $MM_HMI_SKIN	Skin design The number of the skin is indicated
= 0	Skin 0
= 1	Skin 1
= 2	Skin 2 (default)

After changing the machine data, the operating software must be restarted.

6.4.9.3 Setting OEM functions for the softkeys "HMI restart" and "EXIT"

You can influence the default functional behavior of the "HMI restart" or "EXIT" softkey. You can set the configuration in the slamconfig.ini file.

Creating the slamconfig.ini configuration file

Insert a copy of the slamconfig.ini file into one of the following directories:

`.../`**user**`/sinumerik/hmi/cfg`

`.../`**oem**`/sinumerik/hmi/cfg`

Configuring the slamconfig.ini file

Configure the values via the following sections in the slamconfig.ini file:

Section	Description
`[ExitSoftkey]`	Section for Exit softkey
`[RebootSoftkey]`	Section for HMI restart softkey

Value	Description
`Visible`	`true` or `false` Switches the softkey to visible or invisible in the operating area
`SoftkeyPosition`	Fixed softkey position of the area softkey In this case, softkey positions `1` to `8` are located on the 1st horizontal bar and softkey positions `9` to `16` on the 2nd horizontal bar, etc.
`AccessLevel`	`0` to `7` Access level as of which the softkey will be displayed This value is a compatibility value for operating software without MD9110 support.
`QueryUser`	`true` or `false` Activates or deactivates a confirmation dialog

Note

Compatibility value for access level

Please note that the configuration for the access right with the value `AccessLevel` has no effect in this version of SINUMERIK Operate. You set the access right via MD9110 (Page 120).

Example

The following example describes the default configuration for slamconfig.ini:

```
[ExitSoftkey]
Visible=true
SoftkeyPosition=16
AccessLevel=1
QueryUser=false

[RebootSoftkey]
Visible=false
SoftkeyPosition=15
AccessLevel=1
QueryUser=false
```

More information

More information on the slamconfig.ini configuration file can be found in Chapter "Integrating and parameterizing the OEMFrame application (Page 121)".

6.4.9.4 Defining the access right for the "EXIT" softkey

Display machine data

Using the following display machine data, set the access rights from which access level the "EXIT" softkey is displayed.

MD9110_$MM_ACCESS_HMI_EXIT	Access level of the "EXIT" softkey
= 1	Access level 1 (manufacturer), default value

6.4.9.5 Inserting a user-specific run up screen

You can replace the Siemens run-up screen for SINUMERIK OPERATE by your own run-up screen.

Procedure

1. Call your own run-up screen `splash.png`.

   Note

   The file name must not contain any lower case letters.

2. Save your own run up screen in one of the following directories:
   `.../`**user**`/sinumerik/hmi/ico/ico640`
   `.../`**oem**`/sinumerik/hmi/ico/ico640`

   Note

   The size of the screen is of no significance. A resolution of 640x480 pixels is always set.

Result

Your run-up screen will be displayed when you restart SINUMERIK Operate.

6.4.10 Integrating and parameterizing the OEMFrame application

6.4.10.1 Integrating an OEMFrame application into HMI sl

Configure the following files to integrate an OEMFrame application into SINUMERIK Operate:

- Configuration file systemconfiguration.ini
  The operating software is started and controlled from the system manager; the system manager also controls the OEMFrame applications. The system manager is configured using the configuration file systemconfiguration.ini.
- Configuring the start softkey
  In order to start an OEMFrame application from the operating software, configure a softkey on the expansion bar of the operating area.
- Configuration file slamconfig.ini
  In order to configure the softkey position with text and/or symbol for the OEMFrame application, generate the slamconfig.ini file.
- Save the language-dependent text for a softkey in the file mytext_<lng>.ts.

6.4.10.2 Creating configuration files

File systemconfiguration.ini

In order to integrate an OEMFrame application into SINUMERIK Operate, copy the systemconfiguration.ini configuration file and place it in one of the two directories:

`.../`**`user`**`/sinumerik/hmi/cfg`

`.../`**`oem`**`/sinumerik/hmi/cfg`

All of the processes to be managed by the system manager, as well as the applications that are to be integrated as OEMFrame applications are in the `[processes]` section.

Value	Meaning
`process`	Symbolic name of the OEMFrame application. This is required to configure the operating areas.
`cmdline`	Command line, passed to the oemframe.exe process on starting.
`oemframe`	For OEMFrame applications, always set to `true`.
`windowname`	Window name of the OEMFrame application - to be determined with the program FindWindow (Page 115).
`classname`	Class name of the OEMFrame application - to be determined with the program FindWindow (Page 115).
`deferred`	`true`: OEMFrame application is not started when SINUMERIK Operate powers up, but only when selected for the first time.

Value	Meaning
`startupTime`	The linked process starts as follows: `immediately`: immediately (default) `afterServices`: after all services have started `afterGuis`: after all GUI components have started If SINUMERIK Operate is shut down, the process goes in reverse: `immediately`: immediately (default) `afterServices`: after all services have shut down `afterGuis`: after all GUI components have shut down
`gimmekeys`	Release mask for system configuration keys that are to be handled by the OEMFrame application. The parameterization is performed in the form of a bit mask.
`disablekeys`	Parameterization for the keyboard filter behavior. The parameterization is performed in the form of a bit mask.
`menuselectkey`	The value is used for changing the key that calls the operating area menu (default F10). The value is a logical OR combination of the modifications (Microsoft definition) `Key_Shift`, `Key_Alt`, `Key_Ctrl`, and the virtual key code.

`timeout`	Maximum duration for the search for the OEMFrame application in milliseconds. If the OEMFrame application was not found within this time, it is not managed by the System Manager.
	Default setting in the systemconfiguration.ini file:
	`[miscellaneous]`
	`startTimeoutDefault`

`shutdowntime`	Maximum duration for downloading the OEMFrame application in milliseconds. If the OEMFrame application was not found after this period of time, the process is canceled.
	Default setting in the systemconfiguration.ini file:
	`[miscellaneous]`
	`shutdownTimeoutDefault`

Bit mask "gimmekeys"

The bit mask for an OEMFrame application is set to the binary value 0xF by default. All of the key combinations from F1 to F8 are fed to the OEMFrame application. The OEMFrame application itself can handle a specific key/key combination by setting additional bits. Otherwise, the system configuration will evaluate the key/key combination and it will not even reach the OEMFrame application.

You can parameterize the bit mask "gimmekeys" as follows:

Bit	Keys	Meaning
0	F1 - F8	Horizontal softkeys (upper bar, HU)
1	Shift+F1 - Shift+F8	Vertical softkeys (right bar, VR)
2	Ctrl+F1 - Ctrl+F8	Horizontal softkeys (lower bar, HL)
3	Shift+Ctrl+F1 - Shift+Ctrl+F8	Vertical softkeys (left bar, VL)
4	F9	Recall
5	Shift+F9	ETC switchover
6	F10	Operating area menu
7	Shift+F10	M key

Bit	Keys	Meaning
8	F11	Channel switchover key
9	Shift+F11	M key (hard key)
10	F12	Info/help
11	Shift+F12	Custom key (hard key)
12	ESC	Alarm cancel
13	HOME	Window switchover key
14	END	PROGRAM (hard key)
15	PAGE UP	ALARM (hard key)
16	PAGE DOWN	TOOL OFFSET (hard key)
17	HOME (NUMPAD)	PROGRAM MANAGER (hard key)
18	F13 - F20	Extended, horizontal softkeys (upper bar, HU)
19	Shift+F13 - Shift+F20	Extended, vertical softkeys (right bar, VR) and right direct keys HT8
20	Ctrl+F13 - Ctrl+F20	Extended, horizontal softkeys (lower bar, HL)
21	Shift+Ctrl+F13 - Shift+Ctrl+F20	Extended, vertical softkeys (left bar, VL) and left direct keys HT8

Bit mask "disablekeys"

The bit mask for an OEMFrame application is set to the binary value 0x3FFFF by default. Thus, all of the keyboard sequences are filtered out and not forwarded to the OEMFrame application. If a bit is set to 0, the keyboard filter for the corresponding sequence is deactivated and the OEMFrame application is able to receive the keyboard sequence.

If, for example, an OEMFrame application is to receive all of the softkeys of left and bottom softkey bar, set the "disablekeys" bit mask to the binary value 0x300FF.

You can parameterize the bit mask "disablekeys" as follows:

Bit	Keys	Meaning
0 - 7	Reserved	
8	(Shift)+Ctrl+F1	Lower and left-hand softkey bar (HL, VL)
9	(Shift)+Ctrl+F2	Lower and left-hand softkey bar (HL, VL)
10	(Shift)+Ctrl+F3	Lower and left-hand softkey bar (HL, VL)
11	(Shift)+Ctrl+F4	Lower and left-hand softkey bar (HL, VL)
12	(Shift)+Ctrl+F5	Lower and left-hand softkey bar (HL, VL)
13	(Shift)+Ctrl+F6	Lower and left-hand softkey bar (HL, VL)
14	(Shift)+Ctrl+F7	Lower and left-hand softkey bar (HL, VL)
15	(Shift)+Ctrl+F8	Lower and left-hand softkey bar (HL, VL)
16	Reserved	
17	Reserved	

Bit mask "disablekeyshigh"

It may be necessary to map key sequences because the operating system already responds to Ctrl-F4 and Ctrl-F6 in certain situations.

You can parameterize the bit mask "disablekeyshigh" as follows:

Bit	Meaning
0 - 28	Reserved
29	Key sequences Ctrl-F1 to Ctrl-F8 can be mapped onto key sequences Ctrl-F13 to Ctrl-F20.
30 - 31	Reserved

Note

The "gimmekeys", "disablekeys" and "disablekeyshigh" bit masks can be specified both with a decimal code (e.g. 31) and a hexadecimal code (e.g. 0x1F).

Examples

Note

Write error

Avoid write errors. Determine entries for the sections `[processes]` and `[areas]` only with the program FindWindow (Page 115).

notepad.exe and calc.exe

In the following example, the two Microsoft Windows applications notepad.exe and calc.exe are configured as OEMFrame applications:

```
[processes]

PROC500=process:=notepadOEM, cmdline:="C:\\WINDOWS\\system32\
\notepad.exe", oemframe:=true, deferred:=true,
windowname:="Untitled - Notepad", classname:="Notepad"


PROC501=process:=calcOEM, cmdline:="C:\\WINDOWS\\system32\
\calc.exe", oemframe:=true, deferred:=true,
windowname:="Calculator", classname:="SciCalc"


[areas]

AREA500=name:=AreaNote, process:=notepadOEM

AREA501=name:=AreaCalc, process:=calcOEM
```

keycatcher.exe

The Microsoft Windows application keycatcher.exe is integrated in the following example. In this case, all four softkey bars and the Recall key are sent to the Microsoft Windows application. The keyboard filter for the lower and the left-hand softkey bar is deactivated:

```
[processes]
```

```
PROC500= process:=keycatcherOEM, cmdline:="keycatcher.exe",
oemframe:=true, deferred:=true, windowname:="keycatcher",
classname:="QWidget", gimmekeys:=0x1F, disablekeys:=0x300FF


[areas]

AREA500=name:=AreaKeyCatcher, process:= keycatcherOEM
```

The Microsoft Windows application keycatcher.exe is integrated in the following example. In this case, all four softkey bars and the F10 key are sent to the Microsoft Windows application. To show the operating area menu when a Microsoft Windows application is displaying (the system configuration no longer evaluates F10), press Ctrl+F12:

```
[processes]

PROC500= process:=keycatcherOEM, cmdline:="keycatcher.exe",
oemframe:=true, deferred:=true, windowname:="keycatcher",
classname:="QWidget", gimmekeys:=0x4F, disablekeys:=0x300FF,
menuselectkey:=Key_Control|0x7B


[areas]

AREA500=name:=AreaKeyCatcher, process:= keycatcherOEM
```

The Microsoft Windows application keycatcher.exe is integrated in the following example. In this case, all four softkey bars are sent to the Microsoft Windows application. Key sequences Ctrl-F1 to Ctrl-F8 can be mapped onto key sequences Ctrl-F13 to Ctrl-F20:

```
[processes]

PROC500= process:=keycatcherOEM, cmdline:="keycatcher.exe",
oemframe:=true, deferred:=true, windowname:="keycatcher",
classname:="QWidget", gimmekeys:=0xF, disablekeys:=0x300FF


[areas]

AREA500=name:=AreaKeyCatcher, process:= keycatcherOEM
```

The [areas] section

The SINUMERIK Operate operating areas are configured in this section.

Value	Meaning
`name`	Symbolic name for the operating area
`process`	Name of the OEMFrame application according to section `[processes]`
`panel`	Name of the panel (header) to be used Only `SlHdStdHeaderPanel` is currently available for OEMFrame applications.
`plcid`	ID to identify the operating area using the SINUMERIK Operate monitor Only values in the range of 150 to 199 are permitted.

NOTICE
Basic components are overwritten If you use numbers less than 500, then it is possible that Siemens basis components will be overwritten. In the `[processes]` and `[areas]` sections, only the number range 500 - 999 is permissible.

Example

```
[areas]
AREA600= name:=AreaOEM, process:=notepadOEM
AREA601= name:=AreaCalc, process:=calcOEM, panel:=SlHdStdHeaderPanel
```

Note

Only OEMFrame applications are supported that use programming interfaces of SINUMERIK Operate.

The [miscellaneous] section

You can make various settings in this section. Generally, only the start operating area is changed.

Key	Value
`startuparea`	Name of the start operating area

Example

```
[miscellaneous]
startuparea = AreaOEM
```

Configuring the operating area menu

The operating area menu is intended for switching over the operating areas configured in the systemconfiguration.ini configuration file. A softkey for selecting the appropriate operating area is provided on the horizontal softkey bar for each operating area configured.

The operating area displays the names of the operating areas from the systemconfiguration.ini configuration file as the text on the operating area softkeys. The system automatically searches for a free softkey on the horizontal softkey bar for each operating area.

Configuring additional settings

In order to configure the following settings, you require the slamconfig.ini configuration file:

- Assigning a softkey position to a specific operating area.
- Creating a language-dependent text for the softkey.
- Displaying a symbol for the operating area on the softkey.

Creating the slamconfig.ini configuration file

Copy the slamconfig.ini configuration file and place the file in the same directory in which the systemconfiguration.ini file is located:

`.../`**`user`**`/sinumerik/hmi/cfg`

`.../`**`oem`**`/sinumerik/hmi/cfg`

slamconfig.ini file

In the slamconfig.ini configuration file, for every operating area, you can create a section that was configured in the systemconfiguration.ini file. The section must bear the configured name of the operating area, e.g. `[AreaOEM]`.

Value	Meaning
`TextId`	Text ID for a foreign-language text which will be displayed as the softkey label.
`TextContext`	Context of the foreign-language text.
`TextFile`	Name of the text file which includes the context and the foreign-language text.
`Graphic`	Name of an image file which will be used as an icon for the softkey.
`SoftkeyPosition`	Fixed softkey position of the area softkey. In this case, softkey positions 1 to 8 are located on the 1st horizontal bar and softkey positions 9 to 16 on the 2nd horizontal bar, etc.
`AccessLevel`	Access level from which the softkey will be displayed. If this value is not specified, the access level 7 (keyswitch position 0) is set.

Example

The softkey for the "AreaOEM" operating area with the following properties is configured in the following example:

- The softkey displays the text which has been stored in the mytext_<lng>.ts text file in the context under `mycontext` with the text ID `MY_AREA`.
- The `mypicture.png` icon is displayed on the softkey.
- The softkey is located at position 7 in the operating area menu.
- The softkey with access level 5 (keyswitch position 2) is displayed.

```
[AreaOEM]
; Text-ID of a language dependent text
TextId = MY_AREA
; File name of the text file which contains the Text-ID
```

```
TextFile = mytext
; Context in the text file to which the Text-ID is assigned to
TextContext = mycontext
; File name of an icon shown on the area softkey
Picture = mypicture.png
; Position of the area softkey on area menu,
; If no position is specified, an empty position is searched
SoftkeyPosition = 7
; Access level of the area softkey
AccessLevel = 5
```

Note

Operating area position 7 is reserved for OEM users.

Labeling text for the softkey

Storage path:

`.../`**`user`**`/sinumerik/hmi/lng`

`.../`**`oem`**`/sinumerik/hmi/lng`

The XML identifiers have the following meanings:

Attribute	Description
`context`	Context within the text file. Each file must have at least one context.
`name`	Name of the context.
`message`	Text translation. There must be at least one message per context.
`source`	Text identifier.
`translation`	Translated text.
`remark`	Text comment (optional).
`chars`	Maximum possible length of the text in characters. If nothing is specified, the text can have any length (optional).
`lines`	Maximum number of lines available for display. If nothing is specified, the number of lines is unlimited (optional).

Structure of the language-dependent TS file that contains the labeling text for the softkey:

`mytext_<lng>.ts`

```
<?xml version="1.0" encoding="utf-8" standalone="yes"?>
<!DOCTYPE TS>
```

mytext_<lng>.ts

```
<TS>
  <context>
  <name>mycontext</name>
    <message>
      <source>MY_AREA</source>
        <translation>Text, which is displayed on the softkey</translation>
        <remark>comment (optional)</remark>
        <chars>20</chars>
        <lines>2</lines>
    </message>
  </context>
</TS>
```

<lng> stands for the language code.

6.4.10.3 Parameterizing the OEMFrame application

oemframe.ini file

Using the oemframe.ini file, it is possible to further parameterize OEMFrame applications. Create the file in the following directory:

`.../compat/oem`

Create a separate section with the required parameters for each OEMFrame application. Name the section according to the corresponding program file without a filename extension. Place the name in square brackets.

Example

`[notepad]`

NOTICE

Configurations with oemframe.ini are not taken into account for DSF archiving!

If you create a DSF archive, the directory `.../compat/oem` is not taken into account, e.g. with the configuration file oemframe.ini. You have the following options for archiving the data from this directory:

- Manually copy your own settings from the directory `.../compat/oem` to another storage medium.
- Create a Paragon data storage medium image (Page 157) of all settings.

Parameter overview

The following parameters can be used for OEM applications:

Parameter	Meaning	Default value
`WindowStyle_On`	Defines properties to be assigned to the window	0
`WindowStyte_Off`	Defines properties that the window must not have	0
`x`	Horizontal starting coordinate of the OEMFrame application (unit: pixels)	0
`y`	Vertical starting coordinate of the OEMFrame application (unit: pixels)	0
`Width`	Width of the OEMFrame application (unit: pixels)	Desktop width
`Height`	Height of the OEMFrame application (unit: pixels)	Desktop height
`nDelayInitComplete`	Delays the feedback to the System Manager	0
`fSearchOnlyForTaskWindow`	States whether the window specified in the systemconfiguration.ini file belongs to the task specified there	1
`fRestoreTaskWindow`	Defines the behavior when exiting an application that was started from the OEMFrame application	0
`fKeepPlacement`	Deactivates the size adaptation	0
`fForceTaskFocus` `fSearchForPopUps`	Define which window of the OEMFrame application will be displayed when starting.	0 1
`nInitShowMode`	State in which the window of the OEMFrame application is displayed when the application is started.	`SW_SHOWMINNOACTIVE`
`nShowMode`	State in which the window of the OEMFrame application is displayed when it is shown.	`SW_SHOWNORMAL`
`nUnShowMode`	State into which the window of the OEMFrame application is put when it is hidden.	`SW_SHOWMINNOACTIVE`
`fWinForms`	Must be set if the application is a "Windows Forms Application"	0
`nSwitchToTaskAfterTermination`	Controls the behavior when the OEMFrame application is exited	-1
`fFindWindowWithWildcards`	Used for wildcards (`?`, `*`) for the attribute `Windowname`	0

6.4.10.4 Using parameters

WindowStyle_On/WindowStyle_Off

The appearance of a Microsoft Windows application is defined using the Microsoft Windows API function `SetWindowLong`. When the `SetWindowLong` function is called, the appearance of the application is controlled using an 8-byte word. 2 bytes of this word can be changed using the `WindowStyle_On` and `WindowStyle_Off` parameters.

The `WindowStyle_On` parameter defines properties to be assigned to the window. The `WindowStyle_Off` defines properties that the window must not have.

The following control options are possible with WindowsStyle parameters (binary characteristic values):

0000	**0000**	**xxxx**	**xxxx**	**0000**	**0000**	**0000**	**0000**
		1010		Header			
		1000		Border			
		0100		Type of window frame on a dialog box			
		0010		Vertical scroll bar			
		0001		Horizontal scroll bar			
			1000	System menu			
			0100	Frame (Thickframe)			
			0010	Minimize box			
			0001	Maximize box			

Assign binary characteristic values to the WindowStyle parameters as decimal numbers. The conversion can be performed using the calculator in Microsoft Windows, for example.

Example conversion

The properties of the system menu as well as the horizontal and vertical scroll bar should be defined. According to the table, these are:

```
0000 0000 0011 1000 0000 0000 0000 0000 binary or

0038 0000 hexadecimal
```

1. Select Hex on the calculator.
2. Enter the digit string 00380000 (leading zeroes can be omitted).
3. Select Dec.
   Result: 3670016
4. Assign the result to the parameter as a characteristic value.

Application examples

For the Microsoft Windows application Notepad, the system menu as well as the horizontal and vertical scroll bar should be activated:

```
[notepad]

WindowStyle_On = 3670016
```

No minimize box and no maximize box should be displayed for the Microsoft Windows application Notepad:

```
[notepad]
WindowStyle_Off = 196608
```

x/y

Parameters `x` and `y` define the starting coordinates of the window of the Microsoft Windows application to be linked, measured from an origin located in the upper left corner of the screen. `x` is the horizontal coordinate, `y` is the vertical coordinate pointing downward. The unit of measurement is pixels.

The available working area depends on the screen layout being used.

Width

This parameter defines the width of the window for the Microsoft Windows application, measured in pixels from the window origin according to parameter `x`.

Height

This parameter defines the height of the window for the Microsoft Windows application, measured in pixels from the window origin according to parameter `y`.

nDelayInitComplete

As soon as the window of a Microsoft Windows application has been initiated, the information is sent to the System Manager. The Microsoft Windows application can then be selected via the system manager. This information can be delayed using the `nDelayInitComplete` parameter. The unit is specified in milliseconds.

A delay is necessary, for example, if the Microsoft Windows application must carry out other actions while generating its window. If the window is activated too soon by the system manager, display errors will occur in the Window.

Example

After creating its window, the Microsoft Windows application app.exe reads additional state data from a database. The window of the Microsoft Windows application may only be displayed after all status data have been read. This read operation should take approximately one second. The following parameter assignment is possible:

```
[app]
nDelayInitComplete = 2000
```

fSearchOnlyForTaskWindow

This parameter specifies whether the window specified in the file systemconfiguration.ini using `ClassName`/`WindowName` belongs to the task that is also specified there.

The following values can be used:

fSearchOnlyForTaskWindow	
= 0	The window does not belong to the specified task.
= 1	The window belongs to the specified task.

When searching, not only are the windows of the task configured in systemconfiguration.ini taken into account, but all of the windows that exist in the system at the time of the search.

Example

The Microsoft Windows application comprises several processes, e.g. a startup.exe and a user.exe. In the systemconfiguration.ini file, only startup.exe is entered, from which user.exe is started. The application window belongs to user.exe and is therefore not found when searching is restricted to the windows of startup.exe.

The following parameter assignment is possible:

```
[startup]
fSearchOnlyForTaskWindow = 0
```

fRestoreTaskWindow

This parameter defines the behavior when exiting a Microsoft Windows application that was started from the OEMFrame application as second task level.

When the OEMFrame application is deselected, the last window that was active (`ForegroundWindow`) is saved by default. When reselecting the OEMFrame application, this window is reactivated.

If another application was started from the OEMFrame application, then the active window refers to the new Microsoft Windows application.

Note

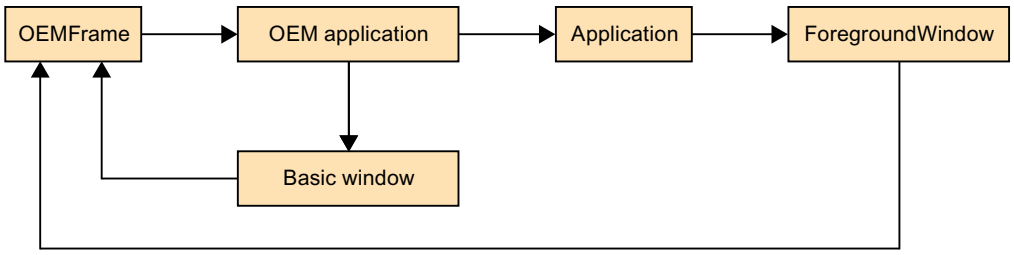
Incorrect displays

In many cases, the proxy application oemframe.exe cannot detect when the new Microsoft Windows application is exited. Display errors can occur in the second task level. Activate a basic window for the OEMFrame application.

The behavior can be influenced via the following values:

fRestoreTaskWindow	
= 0	When selecting the OEMFrame application or starting a Microsoft Windows application from the OEMFrame application, window `ForegroundWindow` is activated. When exiting the second task level, the OEMFrame application is displayed.
= 1	When selecting the OEMFrame application or starting a Microsoft Windows application from the OEMFrame application, a basic window is placed in front of the `ForegroundWindow`. When exiting the second task level, the basic window of the OEMFrame application is always displayed.

Schematic



fForceTaskFocus/fSearchForPopUps

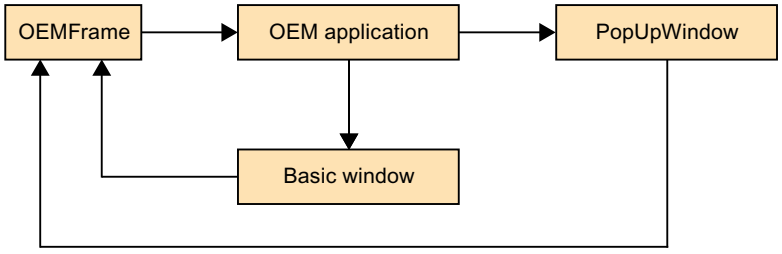
These two parameters define which window the OEMFrame application will activate after it has been deselected and reselected again.

On switching from one operating area to another, the last active window `ForegroundWindow` of the OEMFrame application is saved. When reselecting the application, the `ForegroundWindow` window is then reactivated.

The behavior can be changed via the following values:

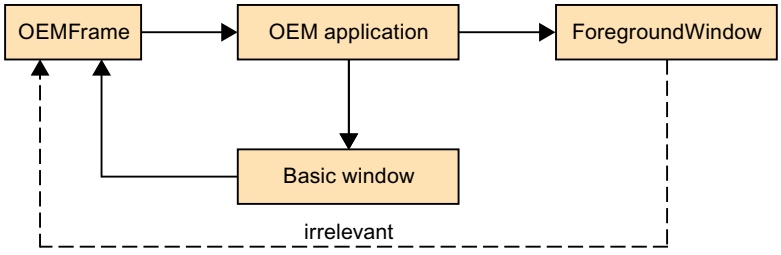
`fForceTaskFocus` and `fSearchForPopUps`	
`= 1`	When the OEMFrame application is deselected, an active popup window is searched for rather than the `ForegroundWindow` window. Behavior of the search: • If a popup window was found, it is displayed when the OEMFrame application is reselected. • If no popup window exists or was found, the basic window of the application is displayed when the application is reselected.

Schema fForceTaskFocus/fSearchForPopUps with value 1



With the following value change, only the basic window of the OEMFrame application is taken into consideration when an application is selected or deselected. The basic window is specified via `ClassName`/`WindowName` in the systemconfiguration.ini file:

Schema fForceTaskFocus with value 1 and fSearchForPopUps with value 0



fKeepPlacement

This parameter deactivates the resizing (zooming) for the basic window of the OEMFrame application. By default, the application is zoomed to the screen size before it is displayed. In the case of applications that do not allow their windows to be zoomed, the resizing can result in display problems. In such cases, the zoom function must be deactivated.

Example

An application fixres.exe should be displayed in its programmed window size. The following parameter assignment is required:

```
[fixres]
fKeepPlacement = 1
```

fSearchForPopUps	
= 0	No active pop-up window is searched for.

nInitShowMode/nShowMode/nUnShowMode

The three parameters define how the application window will be displayed when the application is started, hidden, and shown.

The parameter `nInitShowMode` starts the application. The `nShowMode` parameter refers to showing the application (area is activated). The parameter `nUnShowMode` hides the application.

The following value range exists for the parameters `nShowMode` and `nUnShowMode`:

`nShowMode` and `nUnShowMode`	
= 0	The application window is hidden (`SW_HIDE`).
= 1	The application window is displayed in its original form (position, size) and has the input focus (`SW_SHOWNORMAL`, `SW_NORMAL`).
= 2	The application window is minimized and has the input focus (`SW_SHOWMINIMIZED`).
= 3	The application window is maximized (`SW_SHOWMAXIMIZED`).
= 4	The application window is displayed without having the input focus (`SW_SHOWNOACTIVATE`).
= 5	The application window is displayed and has the input focus (`SW_SHOW`).
= 6	The application window is minimized and loses the input focus (`SW_MINIMIZE`).

= 7	The application window is minimized without having the input focus (SW_SHOWMINNOACTIVE).
= 8	The application window is displayed without having the input focus (SW_SHOWNA).
= 9	The application window is displayed in its original form (position, size) (SW_RESTORE).
= 10	The application window is displayed in the same way as when the application was started (SW_SHOWDEFAULT).

Note

Display problems

The default settings function for most of the applications.

In exceptional cases, display problems can occur in applications with Borland-Delphi development, i.e. shifted windows, etc.

Use the following parameters in this case:

```
nUnShowMode = 0
```

```
fKeepPlacement = 1
```

or

```
nInitShowMode = 1
```

fWinForms

Microsoft Windows Forms parameters provide control elements to applications which also use Microsoft Windows default applications, e.g. dialog boxes, menus and buttons.

If the OEMFrame application is a Microsoft Windows Forms application, then the following parameterization is required:

```
[<app-name>]
```

```
fWinForms = 1
```

Note

Deactivated size adjustment

If the parameter `fWinForms` is not set, the OEMFrame application does not open to the maximum size. The specified size adjustments (`x`, `y`, `Width` and `Height`) are deactivated.

nSwitchToTaskAfterTermination

This parameter controls the behavior when the OEMFrame application is exited. Normally in this situation, the system manager displays the operating area switchover, which can be used to switch over to another area.

The parameter `nSwitchToTaskAfterTermination` can be used to initiate an automatic switch to the previously active area:

`nSwitchToTaskAfterTermination`	
`= -1`	Display of the operating area switchover (default)
`= -2`	Switchover to the previously active area

Example

When exiting Microsoft Windows application closeapp.exe, a switch should be made to the previous area. The following parameter assignment is required:

```
[closeapp]
nSwitchToTaskAfterTermination = -2
```

fFindWindowWithWildcards

With this parameter, a wildcard search can be activated for the attribute `Windowname`. In this way it is possible to identify applications that do not have the same attribute `window name` at every start, e.g. access level, time-of-day under `window name`, etc.:

`fFindWindowWithWildcards`		
`= 0`	Wildcard search is switched off	
`= 1`	Wildcard search is switched on Wildcard:	
	`?`	One arbitrary character
	`*`	Any number of characters

Example

An application is to be integrated that contains the start time in the attribute `window name`:

oemframe.ini

```
[MyQtTest]
fFindWindowWithWildcards = 1
```

systemconfiguration.ini

```
[processes]
PROC500=process:=ProcessOEM, cmdline:="C:\\Program Files(x86)\\Siemens\\
MotionControl\\oem\\sinumerik\\hmi\\appl\\MyQtTest.exe",oemframe:=true,
windowname:="MyQtTest - ??:??:??", classname:="QWidget",deferred:=true

[areas]
AREA500=name:=Test, process:=ProcessOEM
```

6.5 Configuring a key filter for HMI software

To prevent unwanted interruption of the HMI software while it is running, you can specify that certain keyboard entries will be filtered out and thus ignored.

You can configure the key filter in the pcuhwsvc.ini configuration file:

- This key filter is not activated as delivered.
- You can activate the key filter and individually select which of the 20 filterable keyboard entries will be ignored. During this, you can deactivate known shortcut keys, for example, or even deactivate individual add-on keys, such as the left (SeqActive_16) or right (SeqActive_17) Microsoft Windows key.
  You cannot configure any additional keyboard entries to be filtered.
- You can also completely deactivate the repeat function of the F1-F12 keys and all hard keys with the key filter. When the repeat function is deactivated, a key held pressed is considered as pressed once and not as pressed repeatedly.
  Per default, the repeat function is activated during Service or Desktop operation. The repeat function is always deactivated during operation of SINUMERIK Operate.

Requirement

- The Microsoft Windows Service Desktop is active
- Hidden directories are visible
  Further information: Directory structure and file conventions (Page 36)

Procedure

To configure the key filter, proceed as follows:

1. Switch to the template directory: `C:\ProgramData\Siemens\MotionControl\siemens\System\etc\`
   The settings can be viewed in the template `pcuhwsvc.ini`.
2. Save a copy of the template `pcuhwsvc.ini` to one of the user directories:
   - `C:\ProgramData\Siemens\MotionControl\user\System\etc\`
   - `C:\ProgramData\Siemens\MotionControl\oem\System\etc\`
3. In the new file (e.g. `...\oem\System\etc\pcuhwsvc.ini`), delete all data except for the section name `[KEYB_FILTER]` and the keys that are to differ from the template.
   All data and keys that do not occur in your file are automatically taken over from the template in the `siemens` directory.
4. Save your file.

Example: Activating the key filter, but allowing use of the NUM-lock key.

This example activates the key filter (`KeySequencesEnable = 1`) and filters all possible keyboard entries except the NUM-lock key.

`KEYB_FILTER`	Section name (mandatory):
`KeySequencesEnable = 1`	Activate key filter
`SeqActive_19= 0`	Do not filter NUM-lock key

In the adapted file in the user directory (e.g. `...\oem\System\etc\`) therefore only the section name `[KEYB_FILTER]` is mandatory as well as the settings that you want to adapt. All other settings and values are taken over from the template.

Template of the key filter in the delivery condition

The template is located in
directory `C:\ProgramData\Siemens\MotionControl\siemens\System\etc\`

Do not overwrite this template, but save a copy of this template `pcuhwsvc.ini` in one of the user directories.

- `C:\ProgramData\Siemens\MotionControl\`**user**`\System\etc\`
- `C:\ProgramData\Siemens\MotionControl\`**oem**`\System\etc\`

How the configuration file works

You can configure the key filter in section `[KEYB_FILTER]`. The lines identified by a number sign (#) are comments as to which line further down deactivates a particular keyboard entry.

- To activate a particular keyboard entry, find the key in the comment and then set the value to 0.
- To allow all keyboard entries and thus deactivate the key filter (factory setting), set the value to 0 in the `KeySequencesEnable` key.
  If the value 0 is set for this key, all other keys will be ignored and the key filter is deactivated.
- To completely deactivate the repeat function of the F1-F12 keys and all hard keys, set the value 1 at the `AutorepeatSuppression` key.

Table 6-1 Overview: Key filter in the configuration file pcuhwsvc.ini

Section	[KEYB_FILTER]
Key	SeqActive_x
Value	0 = specific keyboard entry activated 1 = specific keyboard entry will be filtered and is deactivated
Factory setting	1

pcuhwsvc.ini (Vorlage im Verzeichnis ...\siemens\System\etc)

```
[GLOBAL]
# ------------------------
# SIEMENS GLOBAL SECTION
# ------------------------
```

pcuhwsvc.ini (Vorlage im Verzeichnis ...\siemens\System\etc)

```
# enable logfile PCUHardwareservice.log
EnableLogFile=0
#  Emulating of "Mode-Switch" from Sinumerik PCU50 Box.
# "Mode-Switch" is a rotary switch, which is attached to the rear side of the PCU50 V5 Box.
#  About this, different methods of booting the computer are controlled.
# 0  Normal mode
# 3  Desktop mode (welcome screen)
ModeSwitch=0
[SERVER]
FTP=hmisvr_PCU_betaftpd
DHCP=hmisvr_PCU_udhcpd
TFTP=hmisvr_PCU_netkit-tftpd
TCUHWS=hmisvr_TCU_hardware_services
VNC=uvnc_service

[APPLICATION]
# ---------------------------------------
# STARTUP APPLICATION DIAGNOSTIC SECTION
# ---------------------------------------

[KEYB_FILTER]
# -----------------------------------------
# SIEMENS KEYBOARD-FILTER DRIVER SECTION
# -----------------------------------------

# Filtering Key Sequences
# =======================
# Activation of Key-Sequences to be ignored
# SeqAct_x
# The following 20 sequences are implemented
# 0  CTRL-ALT-DEL
# 1  ALT-F4
# 2  ALT-TAB
# 3  LEFTSHIFT-ALT-TAB
# 4  RIGHTSHIFT-ALT-TAB
# 5  CTRL-ESC
# 6  ALT-ESC
# 7  ALT-SPACE
# 8  (SHIFT)-CTRL-F1
# 9  (SHIFT)-CTRL-F2
# 10 (SHIFT)-CTRL-F3
# 11 (SHIFT)-CTRL-F4
# 12 (SHIFT)-CTRL-F5
# 13 (SHIFT)-CTRL-F6
```

pcuhwsvc.ini (Vorlage im Verzeichnis ...\siemens\System\etc)

```
# 14 (SHIFT)-CTRL-F7
# 15 (SHIFT)-CTRL-F8
# 16 M$_1
# 17 M$_2
# 18 CAPSLOCK
# 19 NUMLOCK
# 20 (reserved)

KeySequencesEnable = 0

SeqActive_0= 1
SeqActive_1= 1
SeqActive_2= 1
SeqActive_3= 1
SeqActive_4= 1
SeqActive_5= 1
SeqActive_6= 1
SeqActive_7= 1
SeqActive_8= 1
SeqActive_9= 1
SeqActive_11= 1
SeqActive_12= 1
SeqActive_13= 1
SeqActive_14= 1
SeqActive_15= 1
SeqActive_16= 1
SeqActive_17= 1
SeqActive_18= 1
SeqActive_19= 1
SeqActive_20= 1

# Autorepeat-Suppression of Function Keys F1-F12 and Hardkeys
#================================================
AutorepeatSuppression = 0
```

6.6 Installing STEP 7

Precondition

- The Service Desktop is active
- The STEP 7 product DVD is available on the PC system, e.g. via an external DVD drive or network.

Procedure

1. To start the installation assistant of STEP 7, on the product DVD in directory "`CD_1`", double-click `setup.exe`
2. Confirm the preselected directory under `C:\Program Files (x86)\Siemens\Step7\` as the installation directory.
3. In step "Transfer license keys", select "No, transfer license keys later".

   Note

   Licensing of STEP 7 with SINUMERIK Add-on

   The licensing for STEP 7 is performed during installation of the SINUMERIK Add-on.

4. After you have installed STEP 7, restart the PC system and switch to the Service Desktop.
5. To start the installation wizard of the SINUMERIK Add-on, double-click `setup.exe` on the product DVD in directory "`Sinumerik_Add_On`".
   The installation wizard guides you through the following steps.
6. After you have installed the SINUMERIK Add-on, restart the PC system.

Result

STEP 7 has been installed with SINUMERIK Add-on.

The software has been registered in the Control Panel under the following designations:

- STEP 7
- SINUMERIK add-on for STEP7

6.7 Linking the HMI software with STEP 7

If you want to make it possible to start STEP 7 directly from the user interface of the installed HMI software, add a softkey to it.

Precondition

- STEP 7 V5.5 SP3 or higher is installed
- The SINUMERIK Add-on for STEP 7 V5.5 or higher is installed
- An HMI software version is installed (SINUMERIK Operate or HMI Pro sl)
- The Service Desktop is active

Procedure

To add a softkey to the menu of the HMI software for starting STEP 7, proceed as follows:

1. Double-click the "`STEP7-Authorizing`" desktop icon.

Result

A softkey for starting STEP 7 has been added to the HMI software. This softkey requires access level 3.

In `C:\Program Files (x86)\Siemens\MotionControl\compat\add_on\oemframe.ini`, the following settings have been made for this purpose:

```
[s7tgtopx]
; with HMI-Advanced: eliminate minimize- / maximize-buttons of the
STEP7-window
WindowStyle_Off=196608
; with HMI-Advanced: switch to previous task when STEP7 is
terminated
nSwitchToTaskAfterTermination= -2
```

Note

Adjustments for OEM configurations

The entries in `oemframe.ini` can be modified for OEM configurations.

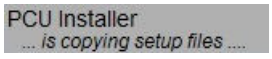
For more information about templates for parameterizing the system, see Chapter Directory structure and file conventions (Page 36).

6.8 PCU Installer

6.8.1 Overview

The PCU Installer assists you with the installation of setup packages on PC systems:

- The PCU Installer checks definable setup directories on the PC system, on removable data storage media, or in the network.
  These setup directories must not be write-protected.
- If setup packages exist, they are automatically installed one after the other. The order in which these packages are installed can be parameterized (Page 148).
- On the top right of the screen, a status display is displayed while the PCU Installer carries out such activities.



For further information on the activities of the PCU Installer, see Chapter Procedure example of an installation with the PCU Installer (Page 152).

Overview of the configuration and operation

- In the delivery state of PCU-Basesoftware /IPC, the PCU Installer is disabled. You can activate the PCU Installer during the unsupervised installation of PCU Base for IPC via the response file or activate it manually after the supervised installation (Page 144).
- After you have made all of the settings for the PCU Installer, using program application Configure for CMC you can also activate or deactivate the PCU Installer (Page 154).
- You can make all settings in the PCU Installer in the associated configuration file (Page 148).
- Copy the setup packages to the defined directories to start the installation (Page 152).
- The PCU Installer consists of a client and a service, whereby setup packages can also be installed for a user account without administrator rights.

6.8.2 Activating the PCU Installer

6.8.2.1 Overview

In the delivery condition of the PCU-Basesoftware /IPC, the PCU Installer is deactivated.

If you are supervising the installation of PCU-Basesoftware /IPC with Microsoft Windows 10, then you must manually activate PCU Installer. To do this, use one of the following procedures:

- Copy a preconfigured template of the PCUInst.ini to the "user" directory (Page 145)
- Create your own version of the PCUInst.ini in one of the user directories and set the appropriate values
  See: Reference to the PCUInst.ini configuration file (Page 148)

6.8.2.2 Activating via a configuration template

Requirement

- The PCU Installer is deactivated
- The Service Desktop is active
- The PCU Installer has not been configured yet and there is no adapted PCUInst.ini configuration file

Procedure

To activate the PCU Installer by copying a preconfigured template, proceed as follows:

1. Copy the following file to the clipboard: `D:\etc\Template_PCUInst.ini`
2. Paste the file into the following directory: `C:\ProgramData\Siemens\MotionControl\user\system\etc`
3. Rename the copied file to PCUInst.ini

Result

The PCU Installer has been activated and checks the setup directories during startup of the PC system, but not during system operation.

The copied configuration file only differs from the default configuration file by the following value:

```
[processing_loginphase]
StartState=activated
```

The settings of the copied configuration file are used because they are in a directory with higher priority than the default configuration file.

See: Directory structure and file conventions (Page 36)

To also use the PCU Installer during system operation, you must make an additional setting in the copied configuration file (Page 148):

```
[processing_systemphase]
StartState=activated
```

6.8.3 Deactivating the PCU Installer

In the delivery state of PCU-Basesoftware /IPC, the PCU Installer is disabled.

Note

Troubleshooting for incorrect installation routines

If completion of an installation requires a restart, but the installation cannot be completed after the restart, the Service Desktop is not started.

In this case, restart the PC system in protected mode to prevent the PCU Installer from starting.

Then reconfigure the PCU Installer or remove the setup packages.

Precondition

- The Service Desktop is active
- Hidden directories are not shown (at least `C:\ProgramData\`)
  Further information: Directories hidden in delivery condition (Page 36).
- A copy of the `PCUInst.ini` configuration file is stored in the `user` directory:
  `C:\ProgramData\Siemens\MotionControl\`**user**`\System\etc\PCUInst.ini`
- The `PCUInst.ini` configuration file in the `user` directory is not write-protected

Procedure

To partly or completely deactivate the installation of the setup files by means of the PCU Installer, proceed as follows:

1. Open the `PCUInst.ini` configuration file in the `C:\ProgramData\Siemens\MotionControl\`**user**`\System\etc\PCUInst.ini` directory.
2. Deactivate the start of the PCU Installer in the desired phase:
   - To deactivate the PCU Installer during system operation, change the relevant key value in the `[processing_systemphase]` section: `StartState=stopped`.
   - To only deactivate the PCU Installer while a specific application is being executed (e.g. SINUMERIK Operate), enter the file name of the relevant application in the `[noactivation]` section, e.g. `APP001=run_hmi.exe`
     (You can specify any number of applications, e.g. `APP002=Siemens.Automation.Portal.exe`)
   - To deactivate the PCU Installer during run-up, change the relevant key value in the `[processing_loginphase]` section: `StartState=stopped`.
3. Save and close the file.

Further information

- For information on all configuration options, see Reference to the PCUInst.ini configuration file (Page 148).
- Microsoft Windows support: Start Microsoft Windows 10 in the safe mode (https://support.microsoft.com/en-us/help/12376/windows-10-start-your-pc-in-safe-mode)

6.8.4 Copying and adapting the configuration file

You can define PCU Installer operation in the associated configuration file. To do this, you must first copy the configuration file to a user directory.

Alternatively, you can copy a template in which the PCU Installer has already been activated (Page 145).

For example, you can configure the following in the configuration file:

- Which directories have been checked how many times for new setup packages.
- That installations are not started automatically while certain software is active.

A list of all setting options can be found under Reference to the PCUInst.ini configuration file (Page 148).

Requirement

- The Service Desktop is active
- The PCU Installer has not been configured yet and there is no adapted PCUInst.ini configuration file

Procedure

To copy and adapt the configuration file of the PCU Installer, proceed as follows:

1. Switch to the template directory: `C:\ProgramData\Siemens\MotionControl\siemens\System\etc\`
   The settings can be viewed in the template `PCUInst.ini`.
2. Save a copy of the template `PCUInst.ini` to one of the user directories:
   - `C:\ProgramData\Siemens\MotionControl\user\System\etc\`
   - `C:\ProgramData\Siemens\MotionControl\oem\System\etc\`

Note

Storage of the configuration file in the setup directory

Alternatively, a configuration file can also be located directly with an installation setup.

In other words, if, for example, `E:\Setup` is a setup directory, this (or one of the direct subdirectories) can be the location of a configuration file. Settings made in this configuration file have a higher weighting than the settings in configuration files in the above-mentioned directories.

3. Adapt the values of the keys. You will find information about the syntax and setting options at Reference to the PCUInst.ini configuration file (Page 148) or in the comments of the configuration file.

   Note

   The factory setting is taken if key pairs are missing

   All key pairs that are not available in your file are taken automatically from the template in the `siemens` directory.

   Therefore, in the new file (e.g. `...\oem\System\etc\PCUInst.ini`), delete all the data except the section names and the keys that are to differ from the template.

   More information: Directory structure and file conventions (Page 36), Reference to the PCUInst.ini configuration file (Page 148)

4. Save and close the file.

Result

The configuration file has been copied to a user directory and can be adapted.

More information on the various setting options is provided in the following chapters.

6.8.5 Reference to the PCUInst.ini configuration file

You can define PCU Installer operation in the associated `PCUInst.ini` configuration file.

For example, you can configure the following:

- Which directories have been checked how many times for new setup packages.
- That installations are not started automatically while certain software is active.

The priority concept of this configuration file is the same as that of the other configuration files. **Further information:** Directory structure and file conventions (Page 36)

You can also deactivate settings in `PCUInst.ini` by deleting the value of the key in the higher priority configuration file. For example, to deactivate `DIR002=C:\Setup` in a file of lower priority, enter `DIR002=` in the file with higher priority.

Note

Maximum length of the file path

The file path to a setup must not exceed 255 characters (including the file name).

Table 6-2 Setting options in the configuration file of the PCU Installer

Section	Setting	Description
[local_setupdirs]	DIR001= DIR002= ...	Specifies the local setup directories on the PC system to be checked. The directories must not be write-protected. You can specify several directories, which are then checked in the specified order. You define the order with a number after "DIR". Subdirectories at the first level are also scanned.
[removable_ setupdirs]	DIR001= DIR002= ...	Specifies the setup directories on removable data storage media to be checked. The directories must not be write-protected. You can specify several directories, which are then checked in the specified order. You define the order with a number after "DIR". Subdirectories at the first level are also scanned. If you do not know the drive letters to be checked, use the <REMOVABLE_MEDIA> drive variable, e.g.: DIR001=<REMOVABLE_MEDIA>:\Install The drive variable then represents all the removable data storage media that are known at the time in Windows. You can also specify fixed drive letters without the directories being checked twice. The drive variable is only valid in the [removable_setupdirs] section.
[net_setupdirs]	DIR001= DIR002= ...	Specifies the setup directories on network drives to be checked. The directories must not be write-protected. **Further information:** Creating a shortcut to the network drive (Page 193) You can specify several directories, which are then checked in the specified order. You define the order with a number after "DIR". Subdirectories at the first level are also scanned.
[setupdirs_ settings]	deleteTmpLocal SetupDirs=	Temporary directories are created during installation of a setup from a removable data storage medium, network drive or the default setup directory D:\Install **Further information:** Procedure example of an installation with the PCU Installer (Page 152) Here you can specify whether these temporary directories are to be deleted again after installation. Possible values: yes; no
	keepDInstall SubdirsWithPrefix=	You can specify that subdirectories of D:\Install with a particular prefix in the directory name are not to be deleted after setup is completed.
[setupnames]	NAME001= NAME002= ...	Specifies which files are setup packages and are to be included in the check of setup directories. You can specify entire file names with their file extensions or represent individual parts of them with wildcard character *.
[setupexecution]	checkSetupLogFile=	Specifies whether a check is to be performed as to whether the file has already been installed before the installation of a setup file. The check is performed based on the computer name and the setup name of the setup-specific log file. Possible values: yes; no
	copyToTmp LocalSetupDir=	You can specify whether setup files on removable data storage media are to be copied to a temporary, local directory before installation. Setup files on network drives are always copied before installation. Possible values: yes; no
[noactivation]	APP001= APP002=	Specifies which applications of the PCU Installer are inactive during operation. This setting is required to prevent operation of the HMI software or another application from being interrupted during execution of a setup.

Section	Setting	Description
[processing_ loginphase]	StartState=	Specifies whether the PCU Installer is active before the Desktop runs up. The setting StartState=activated is required, in particular, if an installation requires a cold start. Possible values: • activated PCU Installer starts setups • stopped PCU Installer is stopped completely
	continueSetups=	Some setups can only be completed after the system has been restarted. In this case, the PCU Installer waits until you restart the PC system. You can specify here whether setups such as these are to be continued after a restart. **Further information:** Note: Troubleshooting for incorrect installation routines (Page 152) Possible values: yes; no
	scanSetupDirs=	Specifies whether setup directories are to be checked and, if required, setup files executed before the Desktop run-up. The following directories are checked if this setting has been activated: • Local setup directories from the [local_setupdirs] setting are always checked. • You can define separately whether additional directories on removable data storage media or in the network are to be checked. (See settings "scanRemovableDriveSetupDirs" and "scanNetworkDriveSetupDirs") If you deactivate this setting, neither local directories, nor directories on removable data storage media or in the network are checked, i.e. the setting scanSetupDirs=no overwrites, for example, scanNetworkDriveSetupDirs=yes. Possible values: yes; no
	scanRemovableDrive SetupDirs=	Specifies whether directories on removable data storage media are to be checked from the setting [removable_setupdirs] and, if required, setup files executed before the Desktop run-up. The setting "scanSetupDirs" must also be activated so that these directories are checked. Possible values: yes; no
	scanNetworkDrive SetupDirs=	Specifies whether network directories are to be checked from the setting [net_setupdirs] and, if required, setup files executed before the Desktop run-up. The setting "scanSetupDirs" must also be activated so that these directories are checked. Possible values: yes; no
	waitTimeDevicesDetection=	Specifies the maximum wait time for device detection (removable data storage media) in the system run-up. This setting is only relevant if the PCU Installer searches for setups on removable data storage media prior to the desktop run-up. (See settings "scanSetupDirs", "scanRemovableDriveSetupDirs" in the section [processing_loginphase] and section [removable_setupdirs]) Possible values: • Positive integer (milliseconds) • infinite
	waitTimeDriveLettersAssignment=	Specifies how long the PCU Installer will wait during the system run-up until the system has assigned a drive letter to all of the logical drives. This setting is only relevant if the PCU Installer searches for setups on removable data storage media prior to the desktop run-up. (See settings "scanSetupDirs", "scanRemovableDriveSetupDirs" in the section [processing_loginphase] and section [removable_setupdirs]) Possible values: • Positive integer (milliseconds) • infinite

Section	Setting	Description
[processing_ systemphase]	StartState=	Specifies whether the PCU Installer is active during operation of the Desktop. Possible values: • activated PCU Installer starts setups • stopped PCU Installer is stopped completely You can define exceptions in Section [noactivation].
	scanSetupDirs=	Specifies whether setup directories are to be checked and, if required, setup files executed during Desktop operation. The following directories are checked if this setting has been activated: • Local setup directories from the [local_setupdirs] setting are always checked. • You can define separately whether additional directories on removable data storage media or in the network are to be checked. (See settings "scanRemovableDriveSetupDirs" and "scanNetworkDriveSetupDirs") If you deactivate this setting, neither local directories, nor directories on removable data storage media or in the network are checked, i.e. the setting scanSetupDirs=no overwrites, for example, scanNetworkDriveSetupDirs=yes. Possible values: yes; no
	scanRemovableDrive SetupDirs=	Specifies whether directories on removable data storage media are to be checked from the setting [removable_setupdirs] and, if required, setup files executed during Desktop operation. The setting "scanSetupDirs" must also be activated so that these directories are checked. Possible values: yes; no
	scanNetworkDrive SetupDirs=	Specifies whether network directories are to be checked from the setting [net_setupdirs] and, if required, setup files executed during Desktop operation. The setting "scanSetupDirs" must also be activated so that these directories are checked. Possible values: yes; no
	numberOfScanCycles	Specifies whether and how often the setup directories check for new setup packages. Possible values: • infinite Infinite • Integer You can define the waiting time between checks in key waitTimeBetweenScanCycles
	waitTimeBetween ScanCycles	Specifies how long the PCU Installer waits after the setup directories have been checked before checking them again. Enter the waiting time in milliseconds. In key numberOfScanCycles, you can specify how often the setup directories will be checked.
report	InfoLevel	Specifies how detailed the information is to be which is stored in the log files. Possible values: • 1: Only basic information on the actions of the PCU Installer is logged • 2: All PCU Installer-specific information is logged • 3: All PCU Installer-specific information and some trace information is logged • 4: All PCU Installer-specific information and additional trace information is logged • 5: All PCU Installer-specific information and all trace information is logged

6.8.6 Installing software with the PCU Installer

Precondition

- The PCU Installer is activated
- If you want to install multiple setup packages one after the other, you must have defined multiple setup directories in the configuration file
- The setup directories to be used are empty and not write-protected

Procedure

To make the PCU Installer accessible to setup packages, proceed as follows:

1. Copy the setup packages to be installed into the setup directories. Copy each setup package into a separate directory.

Note

Maximum length of the file path

The file path to a setup must not exceed 255 characters (including the file name).

Result

The installation of the setup packages is started.
After a setup has been completed or cancelled, a specific log file is stored in the associated setup directory. The general log files of the PCU Installer are also supplemented in the log directory.

Further information

- Log files (.log) (Page 153)
- Procedure example of an installation with the PCU Installer (Page 152)

Note

Troubleshooting for incorrect installation routines

If completion of an installation requires a restart, but the installation cannot be completed after the restart, the Service Desktop is not started.

In this case, restart the PC system in protected mode to prevent the PCU Installer from starting.

Then reconfigure the PCU Installer or remove the setup packages.

6.8.7 Procedure example of an installation with the PCU Installer

The following example describes the activities of the PCU Installer if you have stored a setup file on a removable data storage media or network drive after the activation and configuration of the PCU Installer.

In this procedure example, it is assumed that you have already performed the following steps:

- You have activated the PCU Installer
- You have activated the checking of the network directories in the settings of the PCU Installer and defined an additional setup directory on a network drive.
  In the example: F:\Setup with F: as network drive.
- You have stored a setup file in this additional setup directory (e.g. F:\Setup\Update.exe).
- The setup directory is not write-protected.

Example: Activities of the PCU Installer during installation of a network drive

- The defined setup directories are checked.
- The Update.exe file is found in the F:\Setup directory.
  As the Update.exe file has not been installed yet, there is no setup-specific log file in the directory.
- The Update.exe file is copied to a local temporary directory, e.g. D:\Install39\Update.exe
- The copied setup file is executed from the local temporary directory, e.g. D:\Install39\Update.exe.
- Log files are created after completion of the installation:
  - The general log files are extended
  - The setup-specific log file is created in the original setup directory F:\Setup and in the local temporary directory D:\Install39

  Further information: Log files (.log) (Page 153)

6.8.8 Log files (.log)

In order to be able to track which setup packages and updates have been installed at any time, the activities of the PCU Installer are recorded in various log files.

Setup-specific log files

A separate setup-specific log file is created for each setup package that is executed by the PCU Installer. The name of the setup and the name of the computer are entered in the file name of the log.

Archiving	The setup directory in which the associated setup file was originally located, and (if copied by the setup) the local temporary directory.
File name	The log file is designated according to the following scheme: <Name of the setup file>@<Computer name>.log, e.g. Update@MyIPC.log

If you activate the checkSetupLogFile= setting in the "PCUInst.ini" configuration file (Page 148), then the setup-specific log file prevents the same setup being installed several times on the same computer. The check is performed based on the computer name and the setup name.

In the delivery condition of the base software, this setting is deactivated. The setting should remain deactivated for the series start-up of devices with the same name or for the repair of an installation.

General log files

The general PCU Installer log files record the operation and the communication of the PCU Installer client and PCU Installer service. There are therefore separate files for the client and service.

Archiving	`C:\ProgramData\Siemens\MotionControl\User\System\Log\`
File name	PCU Installer client: `PCUInstaller_C.log`
	PCU Installer service: `PCUInstaller_S.log`

6.8.9 Program application Configure for CMC

Overview

Using Configure for CMC you can activate or deactivate the PCU Installer, and therefore execute setup packages on the PC system, removable data storage medium or network without having to make any manual changes to `PCUInst.ini`.

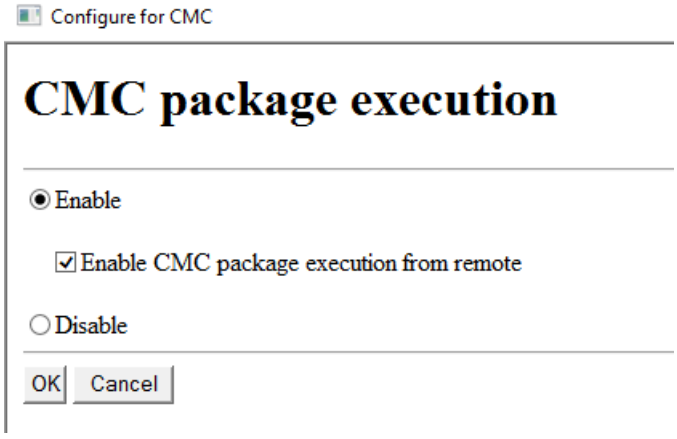


Figure 6-5 Program application Configure for CMC

Precondition

- The PCU Installer was configured.
- An adapted configuration file `PCUInst.ini` exists.

Procedure

1. Open the program application using icon "Configure for CMC" on the desktop.
2. Using the option box, activate or deactivate the check for setup packages.
3. Confirm with OK to accept the setting.
   The setting becomes active after restarting Windows.

6.9 Migration

Basic procedure

To transfer data from a PCU with Windows 7 to a PC system with Windows 10, store the data on a USB flash drive, for example, and then copy it to the PC system:

- For SINUMERIK Operate, use the functions for generating and reading in commissioning archives.
- For STEP 7, copy the generated STEP 7 project data to the PC system.

More information

More information on how commissioning archives work is provided in the SINUMERIK Operate online help.

- Information on STEP 7 can be found in the associated online help.
- Information about other SINUMERIK applications is provided in the relevant documentation. You will find documentation on a large number of products in the SIEMENS Service&Support portal:
  Service&Support portal > CNC automation system SINUMERIK (http://support.automation.siemens.com/WW/view/en/10805517/133300)

Backing up and restoring data 7

7.1 Overview

Note

As of PCU base software /IPC V15.0, the Service Center uses the **Paragon Hard Disk Manager™ 17 Suite** software. It is recommended to use the software for disk image backup and restoration. You can call the **Paragon Hard Disk Manager™** separately (Page 158):

You can perform installation and commissioning work on the PC system in the Service Center, which is based on Microsoft Windows PE.

When the Desktop is active, configuration of the Service Center is possible via the "ServiceCenter Backup-Restore" (Page 69) icon.

Most of the functions of the Service Center are available in the main menu (Page 164).

In particular, you can create or restore disk images in the Service Center. The following options are available:

- If necessary, decrypt BitLocker-protected partitions (Page 181)
- Create a disk image of the SSD (Page 169)
- Restore a disk image of the SSD (Page 171)
- Create a disk image of a partition (Page 174)
- Restore a disk image of a partition (Page 176)

7.2 Using Paragon Hard Disk Manager for data backup and restoration

7.2.1 Starting the Paragon Hard Disk Manager directly

Using the **Paragon Hard Disk Manager™ 17 Suite** software, you can store the entire contents of an SSD as a disk image. Disk images can be kept on various storage media for subsequent restoration of the data on the SSD.

Paragon Hard Disk Manager™ is included in the PCU-Basesoftware /IPC scope of delivery and on the replacement SSD for the IPC. Paragon Hard Disk Manager™ is used by the components of PCU base software /IPC to back up or restore data.

You can also launch Paragon Hard Disk Manager™ directly from the Microsoft Windows desktop to perform backup tasks in the application's user interface. This is necessary, for example, when using SD cards.

Procedure

To start Paragon Hard Disk Manager™ directly on the PC system, proceed as follows:

1. In the Microsoft Windows 10 desktop, double-click the "Paragon Hard Disk Manager™ 17 Suite" icon.
2. Acknowledge the confirmation prompt by clicking "Yes".

To start Paragon Hard Disk Manager™ directly on the USB flash drive with Service Center, proceed as follows:

1. The PC system is switched off. Shut down the PC system if necessary.
2. Connect the USB flash drive to the PC system.
3. Switch on the PC system.
4. Immediately after switching on the device, press and hold the <Esc> key.
   The firmware selection menu is opened.
5. Select "Boot Manager".
   The "Boot Manager" with the "Boot Options Menu" overview is opened.
6. Under "EFI USB Boot Device", select the USB flash drive and confirm the entry.
7. Confirm the following message "Microsoft Windows Preinstallation Environment".
   The "SIMATIC IPC Image & Partition Creator" application interface is displayed under Microsoft Windows PE (Service Center).
8. Select the option "Hard Disk Manager 17 Suite" and click "Run".

Result

The application Paragon Hard Disk Manager™ 17 Suite is opened.

Example: Restoring individual files from the disk image

The Paragon Hard Disk Manager™ 17 Suite software allows you to select and restore individual data from a disk image:

1. Start the Paragon Hard Disk Manager directly.
   The application is opened.
2. Click the "Restore from file" tab in the "Backup & Recovery" view.
3. Select an existing disk image under the sidebar option "Explore and export files".
   The "View backup contents" dialog box opens.
4. Select the required settings. Locate and mark the required individual data and directories.
5. Select your target details.
6. Transfer the data from the disk image.

More information

On the Internet, you can find more information about the application on the website www.paragon-software.com (https://kb.paragon-software.com/home-home-office-manuals).

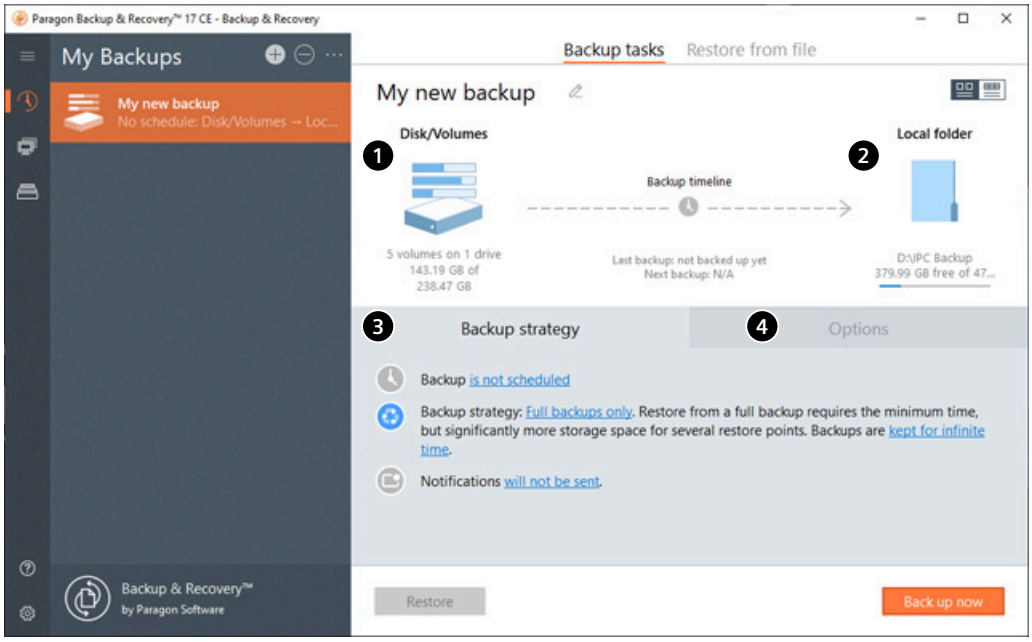
For more information on how to operate the application with SIMATIC IPC, refer to the SIMATIC IPC Image & Partition Creator Operating Manual (https://support.industry.siemens.com/cs/document/109780775/simatic-ipc-image-partition-creator-v3-6?dti=0&lc=en-WW).

7.2.2 Creating a disk image with Paragon Hard Disk Manager

The Paragon Hard Disk Manager™ software allows you to create a disk image of the SSD:

- The application Paragon Hard Disk Manager™ application is opened.
- Click the "Backup tasks" tab in the "Backup & Recovery" view.

Creating and encrypting an SSD disk image



① Select the SSD disk as the backup source under "Disk/Volumes".

② Select the backup destination to specify the storage location of the disk image.

③ If necessary, create a backup schedule in the "Backup strategy" tab and select a schedule routine: daily, weekly, monthly, or after an event, e.g. following a system start.

Note: This process is performance-intensive and should not be carried out during the productive phase.

④ If necessary, use password protection to encrypt the disk image in the "Options" tab.

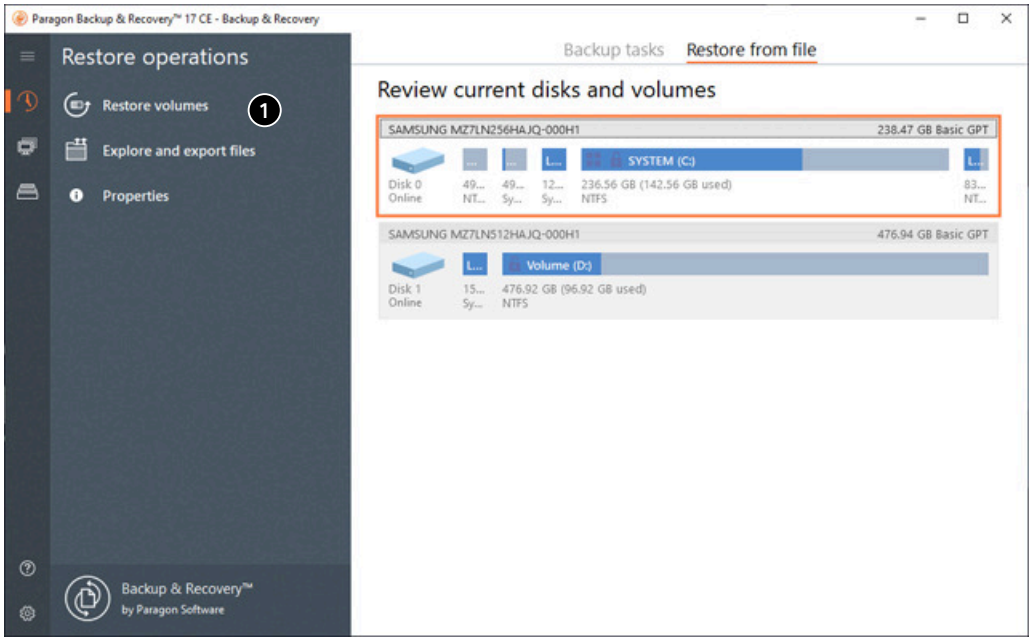
7.2.3 Restoring a disk image with Paragon Hard Disk Manager

The Paragon Hard Disk Manager™ software allows you to select a disk image and restore it to the SSD disk:

- The application Paragon Hard Disk Manager™ application on the USB flash drive is opened.
- Click the "Restore from file" tab in the "Backup & Recovery" view.

Restoring the SSD disk image

NOTICE
Inactive BitLocker key
After a disk image restoration, the BitLocker key on the PC system is inactive.
Activate the BitLocker after an SSD backup has been restored with Paragon.



① Click "Restore volumes" and select the folder that contains the restoration archive. Transfer the data to the SSD.

Note: If necessary, decrypt the password-protected archive.

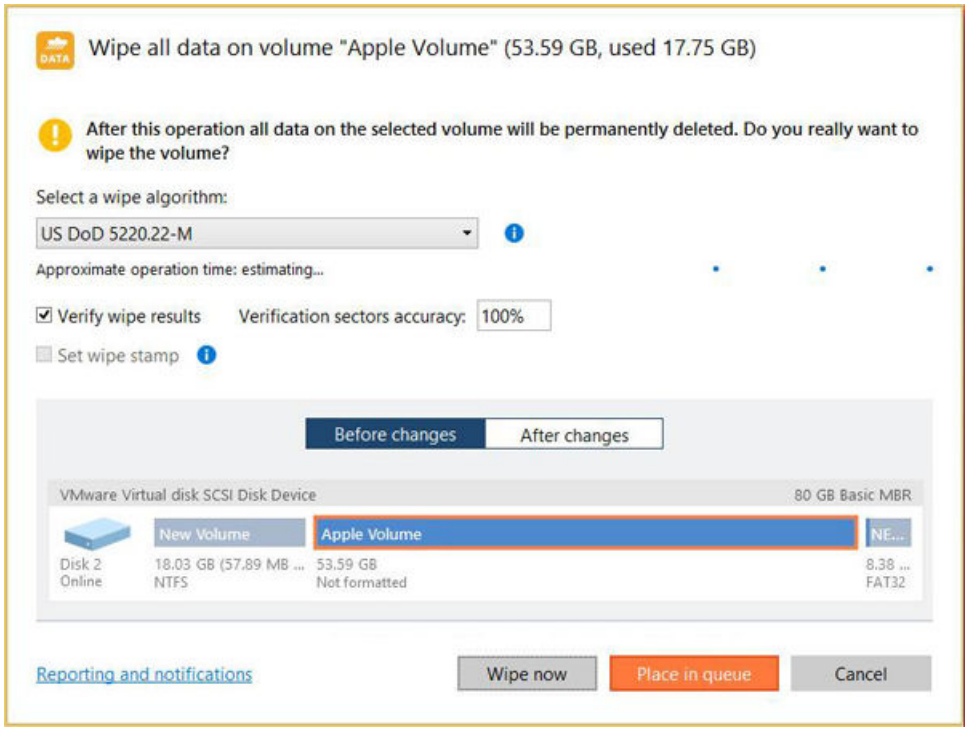
7.2.4 Securely deleting the SSD data storage medium

With Paragon Hard Disk Manager™ you can securely erase all SSD data from your PC system.

NOTICE
Data loss Always store data additionally outside the PC system to prevent data loss.

Procedure

1. The application Paragon Hard Disk Manager™ application on the USB flash drive is opened.
2. In the "Disks & Volumes" view, click on "Wipe all".
   The function dialog opens:



3. If necessary, change the default settings and select the deletion algorithm.
4. Click on "Wipe now".

Result

All data on the SSD is irrevocably deleted.

7.3 Starting the Service Center

To start the Service Center, proceed in one of the following ways:

- To call the emergency boot system on a USB flash drive during PC system startup, press F12 or Esc during the boot process to display the boot selection.
- To switch to the Service Center while the Service Desktop (Microsoft Windows 10) is active, click the "ServiceCenter Backup-Restore" icon on the Desktop, and then click "Start ServiceSystem".

7.4 Functions of the Service Center

Overview

In the upper section of the Service Center main menu, you can select one of five tasks. Buttons for additional functions are available in the lower section.

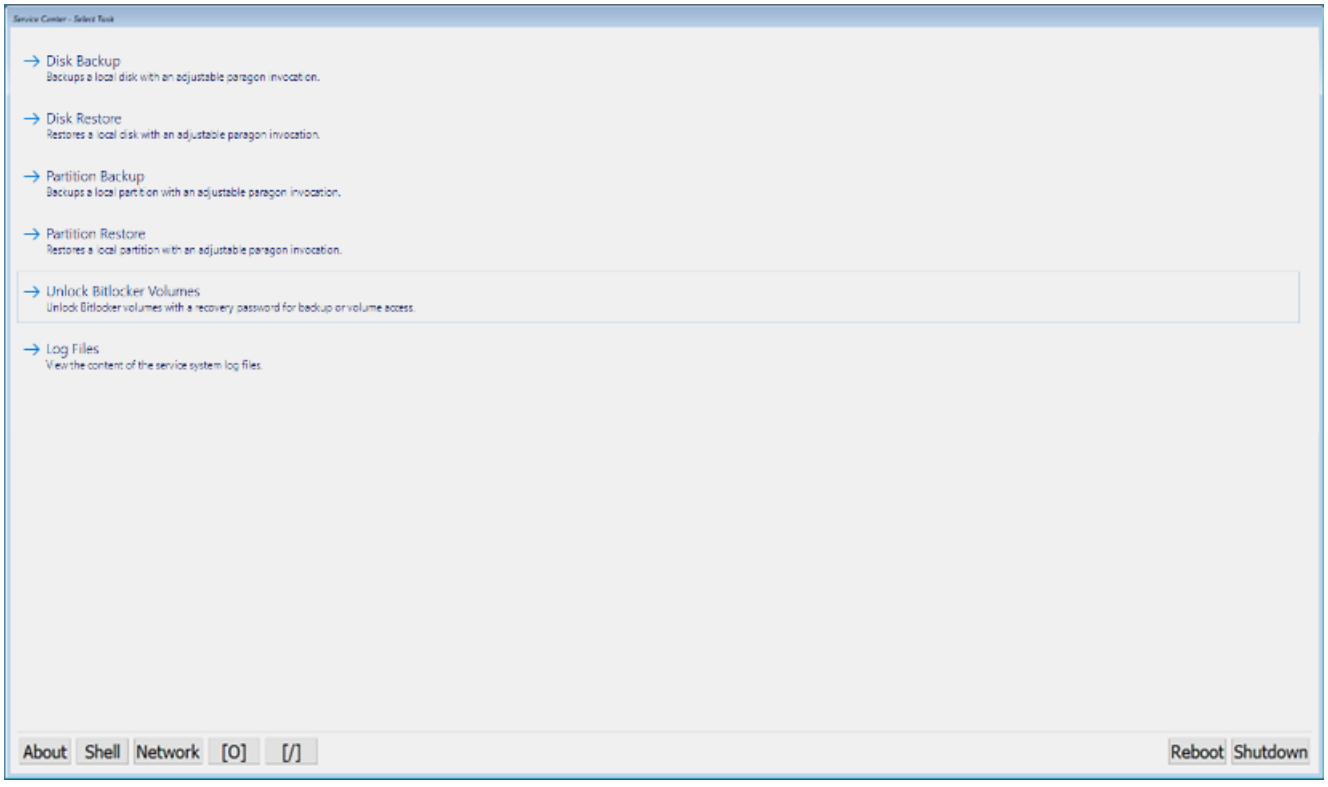


Figure 7-1 Service Center - Main menu

Table 7-1 Functions in the main menu of the Service Center

Element of the window	Purpose
Disk Backup	Create a disk image of the local SSD. With this command, you can create a disk image of the entire SSD (with all partitions).
Disk Restore	Restore the local SSD with an existing disk image. With this command, you can restore the complete SSD (with all partitions) with a previously created disk image.
Partition Backup	Create a disk image of a partition on the local SSD. With this command, you can create a disk image of an individual partition of the SSD.
Partition Restore	Restore a partition on the local SSD with a disk image. With this command, you can restore an individual partition of the SSD with a previously created disk image.
Unlock Bitlocker Volumes	Decrypts BitLocker-protected partitions. Decrypt BitLocker-protected partitions with the separately stored recovery password to be able to create disk images.
Log Files	View and save log files.
About	Viewing information about the Service Center.

Element of the window	Purpose
Shell	Open the Prompt. Here you can enter commands for executing tasks on the PC system without using a graphic user interface.
Network	Making network settings (Page 166). Any network settings you make in this dialog box are temporary. To change network settings permanently, switch to the Service Desktop.
Rotate	Rotates the screen through 90° in the clockwise direction.
Reboot	Restart the PC system.
Shutdown	Shut down the PC system.

7.5 Network settings in the Service Center

You can make network settings in the main menu of the Service Center by clicking "Network":

- IP settings at the enterprise network interface X1 (Local Area Connection 2)
- IP settings at the plant network interface X2 (Local Area Connection)
- Configuration of the host
- Configuration of IP routing

Note

Temporarily storing network settings in the Service Center

Any network settings you make in this dialog box are immediately effective, but temporary.

To change network settings permanently, switch to the Service Desktop.

Further information can be found in Chapter Configuration of the Service Center (Page 69).

Overview

IP settings

You can make the following IP settings in the "Network Settings" dialog box:

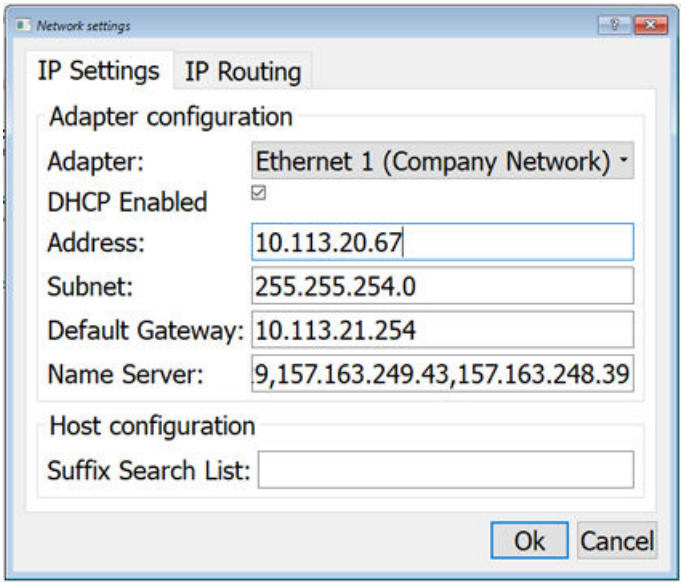


Figure 7-2 Service Center - IP settings

Note

The IP settings can only be parameterized with a connected network interface.

Table 7-2 IP settings in the "Network Settings" dialog box

Section	Setting	Purpose
Adapter configuration	Adapter	Select the Ethernet interface that you want to configure. All settings in Section "Adapter configuration" refer to the selected Ethernet interface.
	DHCP Enabled	Select whether the addresses are to be fetched dynamically from the DHCP server. If the checkbox is deactivated, you must make the settings manually.
	Address	Set the IP address of the NCU. You can specify an IP address from the following range: 192.168.214.250 - 254
	Subnet	Specify a subnet mask, e.g. 255.255.255.0
	Default Gateway	Set the IP address of the standard gateway. A standard gateway creates a standard route in the IP routing table for all destinations that are not in the subnet.
	Name Server	Set the IP address of the name server. A name server answers questions asked about a domain name zone using a DNS database.
Host configuration	Suffix Search List	Parameterize a search list for DNS suffix, e.g. "network.com". The factory setting of the Ethernet interface "Local Area Connection" is ".local".

Routing settings

You can make the following routing settings in the "Network Settings" dialog box:

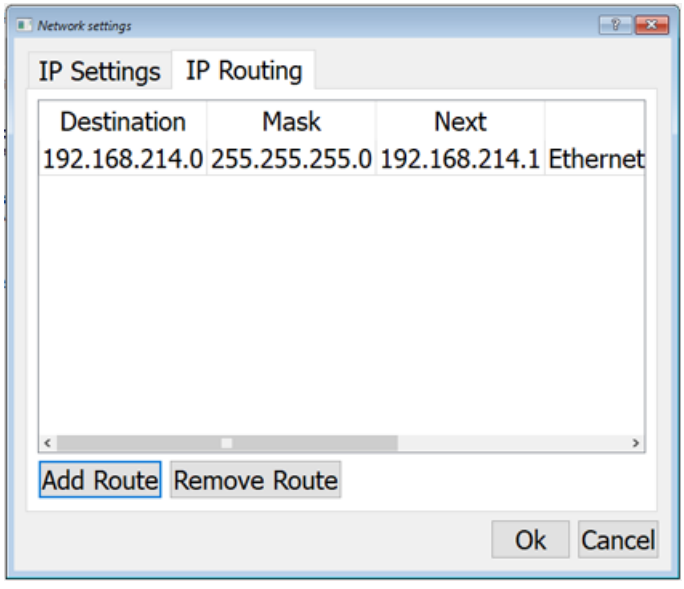


Figure 7-3 Service Center - IP routing

Table 7-3 Routing settings in the "Network Settings" dialog box

Setting	Purpose
Add Route	Add a new route.
Remove Route	Delete a selected route.
Destination	Specify the network destination of the route as an IP address.
Mask	Subnet mask of the specified IP addresses.
Next	Next hop or forwarding IP address via which the network destination can be accessed.
Interface	Select an interface to which the configured IP routing applies: • Enterprise network interface X1 (Local Area Connection 2) • Plant network interface X2 (Local Area Connection)
Metric	Integer cost metric (1 to 9999). Required if several routes for sending a packet to a network destination are possible in the routing table.

7.6 Create a disk image of the SSD

You can create a disk image of the entire SSD in the Service Center with the "Disk Backup" function.

Procedure

To save the SSD as a disk image, proceed as follows:

1. Start the Service Center, e.g. from the Microsoft Windows boot menu.
   More information: Starting the Service Center (Page 163)
2. If necessary, decrypt the BitLocker-protected partitions.
   More information: Decrypting BitLocker-protected partitions (Page 181)
3. In the main menu of the Service Center, click "Disk Backup".
   The "Service Center - Disk Backup" dialog box opens.

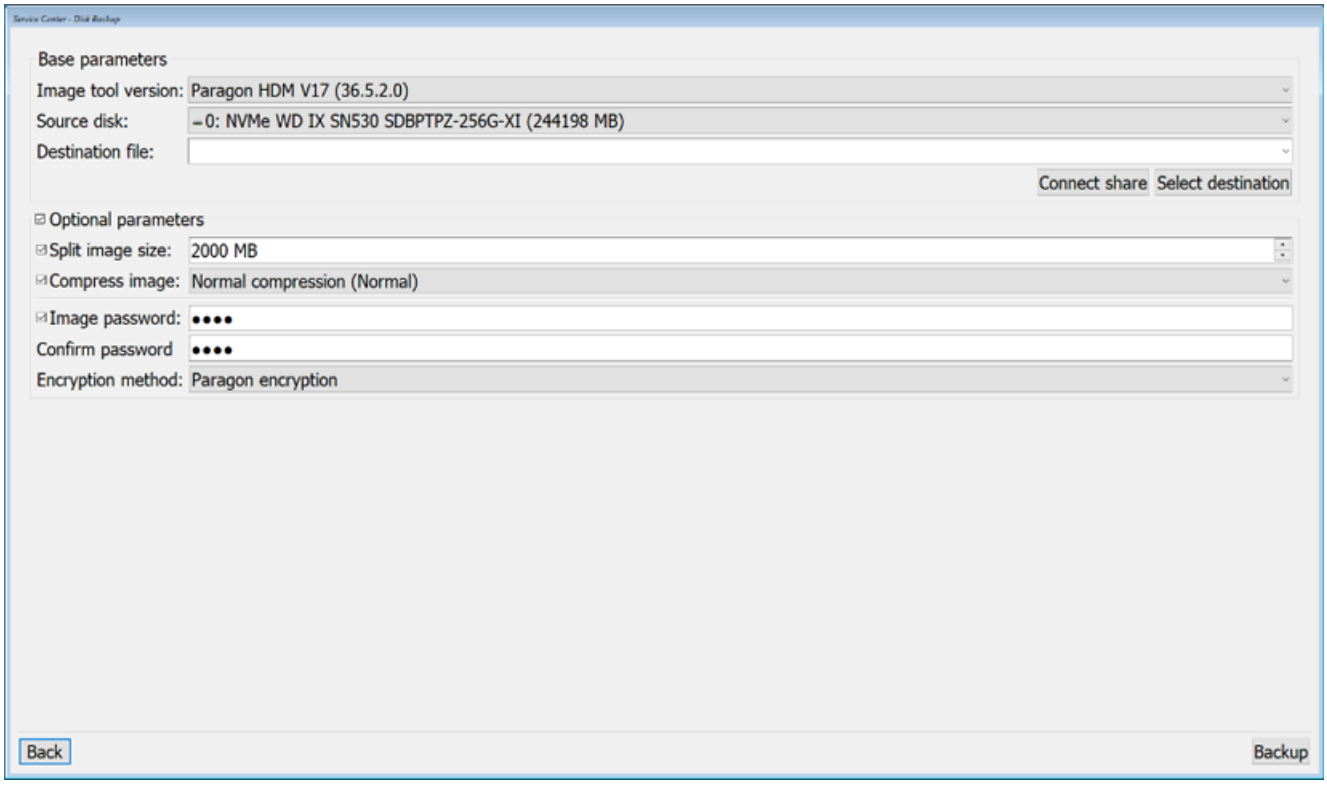


Figure 7-4 Service Center - Disk Backup

4. Make the required settings here:

Section	Setting	Purpose
Base parameters	Image tool version	Select the Paragon Hard Disk Manager™ version that is to be used when creating the disk image. Version for Microsoft Windows 10: "Paragon HDM V17 (36.5.2.0)"
	Source disk	Select a data storage medium of which you want to create a disk image.
	Destination file	Specify the target directory and file name. Disk images can be stored either locally or in the network.
Base parameters > Destination file	Connect share	Open the "Connect a Share" dialog box (Page 179). You can set up a shared resource (e.g. a directory in the network), to which you can store the disk image.
	Select destination	Open the "Select Destination File" dialog box. You can navigate through a local directory of the PC system and enter a file name.
Optional parameters	Split image size	Split the disk image and select a split image size. You can split the disk image into several files of a defined size. Split the disk image size in the following cases: • If the file system (e.g. FAT32) can only manage files of a certain size. • If the disk image is to be archived onto multiple data storage media, for example, when using CDs.
	Compress image	Activate Compression or select a compression level. Higher compression results in a smaller file size, but increases the time needed to compress or decompress the data.
	Image password	Use password protection to encrypt the disk image. Enter the password again to rule out typing errors.
	Encryption method	Select an encryption method. Standard encryption: "Paragon encryption".

5. Confirm your settings with "Backup" to start generation of the disk image.

NOTICE
Inactive BitLocker key The BitLocker key on the PC system is inactive for the disk image creation. Activate BitLocker again after the backup has been created.

7.7 Restore a disk image of the SSD

If your system is no longer functioning stably, you can restore it with a disk image.

NOTICE
Inactive BitLocker key
After a disk image restoration, the BitLocker key on the PC system is inactive.
Activate the BitLocker after an SSD backup has been restored.

Note

Restoring replaces all current files

When you restore the PC system from a disk image, all programs, settings and files are completely replaced by the disk image. Use the Paragon Hard Disk Manager™ software directly if you want to recover only individual files or exclude them from recovery (Page 158).

Requirement

A disk image in *.pvhd (Paragon HDM virtual image) format exists

More information: Create a disk image of the SSD (Page 169)

Procedure

To restore a disk image, proceed as follows:

1. Start the Service Center, e.g. from the Microsoft Windows boot menu.
   More information: Starting the Service Center (Page 163)
2. In the main menu of the Service Center, click "Disk Restore".
   The "Disk Restore" dialog box opens.

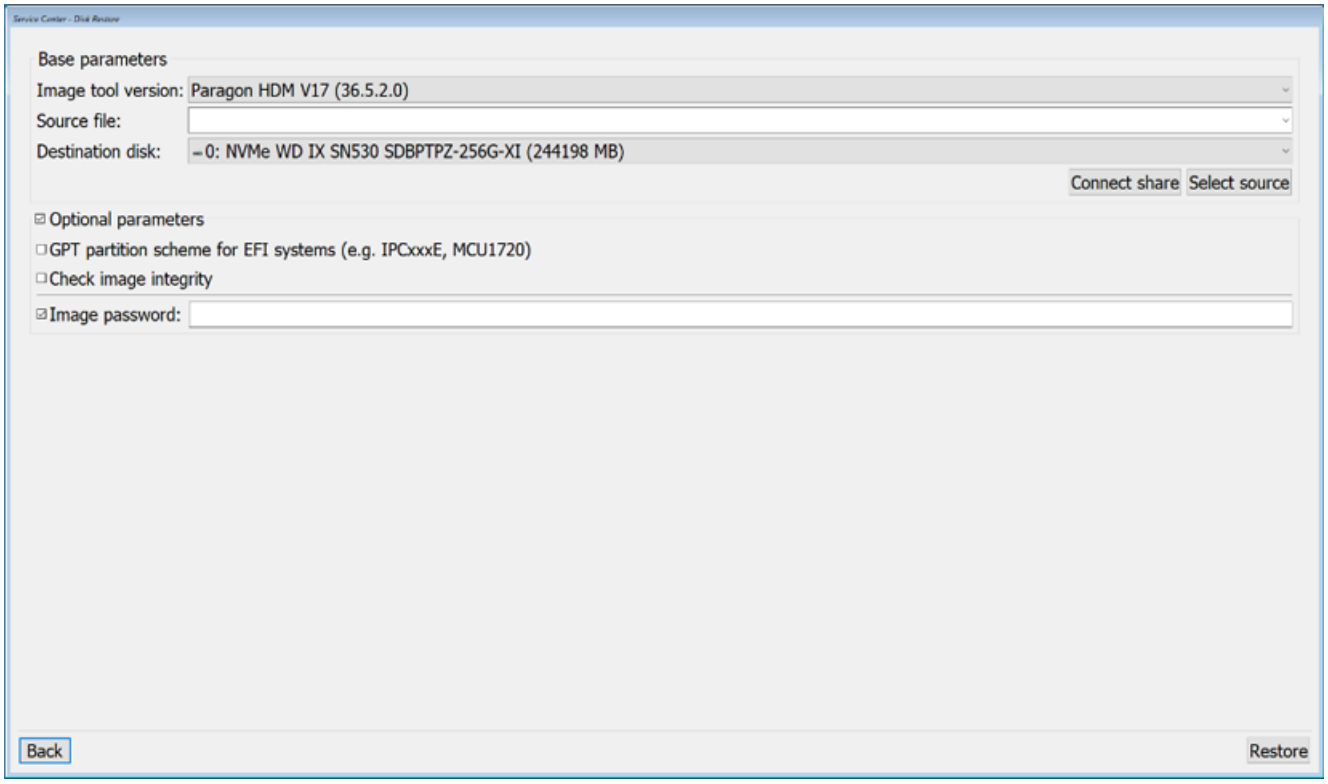


Figure 7-5 Service Center - Disk Restore

3. Make the required settings here:

Section	Setting	Purpose
Base parameters	Image tool version	Select the Paragon Hard Disk Manager™ version to be used when restoring the data storage medium. Version for Microsoft Windows 10: "Paragon HDM V17 (36.5.2.0)"
	Source file	Select the disk image from which the SSD is to be restored. You can use local disk images or disk images stored in the network.
	Destination disk	Select the SSD to be restored from the disk image.
Base parameters > Destination disk	Connect share	Open the "Connect a Share" dialog box (Page 179). You can manage a shared resource (e.g. a directory in the network), to use a disk image stored on the network to restore the SSD.
	Select source	Open the "Select Source File" dialog box. You can navigate through a local directory of the PC system and select a disk image for restoration.
Optional parameters	GPT partition scheme for EFI systems	If necessary, use the GUID partitioning scheme (GPT) for EFI systems when restoring the disk image on MCU 1760 or IPCxxE systems.
	Check image integrity	Check the integrity of the data storage medium before restoration.
	Image password	Use the password to decrypt the protected disk image.

4. To start the restore process and entirely replace the existing data on the SSD with the disk image, confirm the settings with "Restore".

Result

The restore process is started.

Note

Troubleshooting if reading in of the disk image fails

If data transfer is interrupted during the restore process, the PC system will have no executable system.

In this case, use a USB flash drive with Service Center to read the disk image in again.

7.8 Create a disk image of a partition

You can create a disk image of an individual partition of the SSD in the Service Center with the "Partition Backup" function.

Procedure

To save a partition of the SSD as a disk image, proceed as follows:

1. Start the Service Center, e.g. from the Microsoft Windows boot menu.
   More information: Starting the Service Center (Page 163)
2. If necessary, decrypt the BitLocker-protected partition.
   More information: Decrypting BitLocker-protected partitions (Page 181)
3. In the main menu of the Service Center, click "Partition Backup".
   The "Service Center - Partition Backup" dialog box opens.

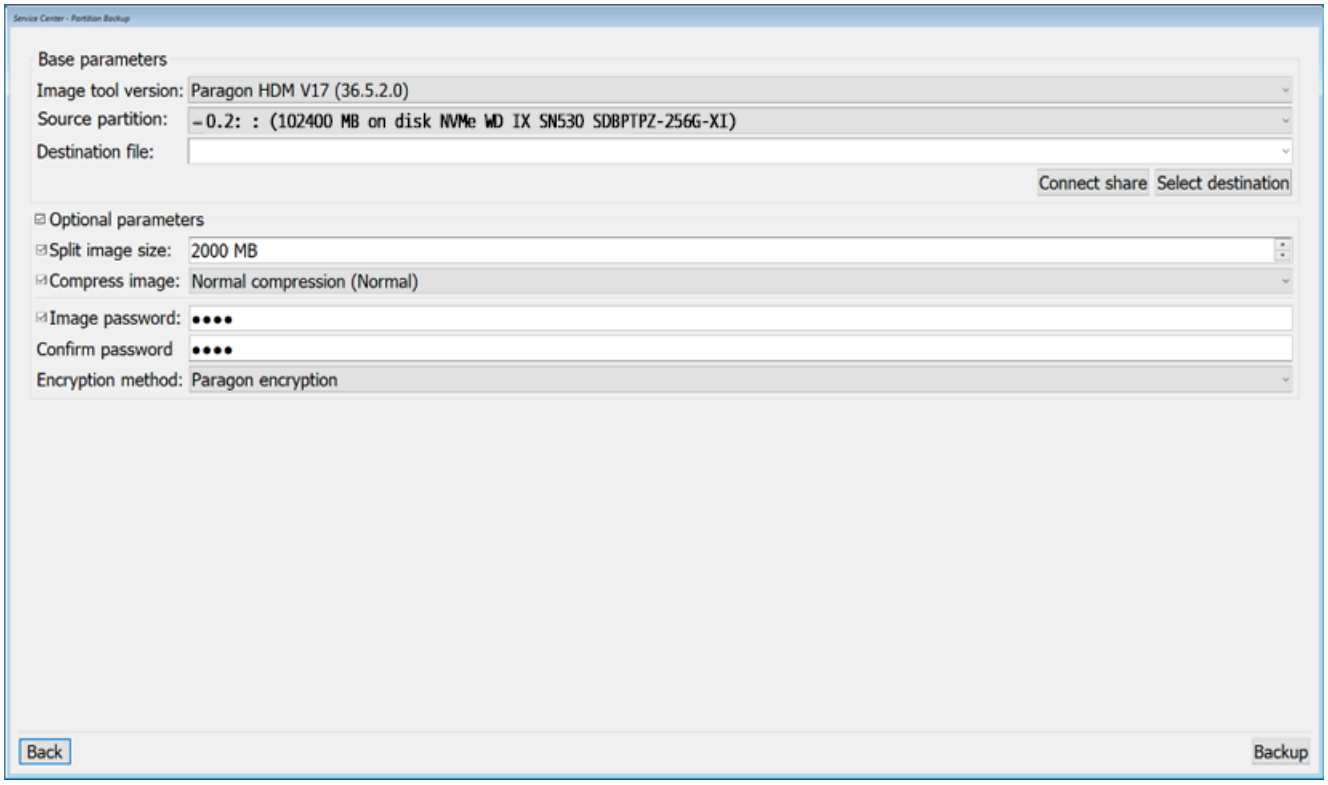


Figure 7-6 Service Center - Partition Backup

4. Make the required settings here:

Section	Setting	Purpose
Base parameters	Image tool version	Select the Paragon Hard Disk Manager™ version that is to be used when creating the disk image. Version for Microsoft Windows 10: "Paragon HDM V17 (36.5.2.0)"
	Source partition	Select a data storage medium of which you want to create a disk image.
	Destination file	Enter a destination directory and file name. Disk images can be stored either locally or in the network.
Base parameters > Destination file	Connect share	Open the "Connect a Share" dialog box (Page 179). You can set up a shared resource (e.g. a directory in the network), to which you can store the disk image.
	Select destination	Open the "Select destination file" dialog box. You can navigate through a local directory of the PC system and enter a file name.
Optional parameters	Split image size	**No PC system setting**, only PCU 50.x: Split the disk image and select a split image size. If you are using a PCU 50.5, you can split the disk image into several files of a defined size. Split the disk image size in the following cases: • If the file system (e.g. FAT32) can only manage files of a certain size. • If the disk image is to be archived onto multiple data storage media, for example, when using CDs. If you are using a different PC system than the PCU 50.5, you must deactivate the "Split image size" setting.
	Compress image	Activate Compression or select a compression level. Higher compression results in a smaller file size, but increases the time needed to compress or decompress the data.
	Image password	Use password protection to encrypt the disk image. Enter the password again to rule out typing errors.
	Encryption method	Select an encryption method. Standard encryption: "Paragon encryption".

5. Confirm your settings with "Backup" to start generation of the disk image.

NOTICE
Inactive BitLocker key The BitLocker key on the PC system is inactive for the disk image creation. Activate BitLocker again after the backup has been created.

7.9 Restore a disk image of a partition

If your system is no longer functioning stably, you can restore it with a disk image.

NOTICE
Inactive BitLocker key
After a disk image restoration, the BitLocker key of the partition is inactive.
Activate the BitLocker after a backup has been restored.

Note

Restoring replaces all current files

When you restore a partition from a disk image, all programs, settings, and files are completely replaced on this partition by the disk image. Use the Paragon Hard Disk Manager™ software directly if you want to recover only individual files or exclude them from recovery (Page 158).

Requirement

A disk image of a partition in *.pvhd (Paragon HDM virtual image) format exists

More information: Starting the Service Center (Page 163)

Procedure

To restore a partition from a disk image, proceed as follows:

1. Start the Service Center, e.g. from the Windows boot menu.
   More information: Create a disk image of a partition (Page 174)
2. In the main menu of the Service Center, click "Partition Restore".
   The "Partition Restore" dialog box opens.

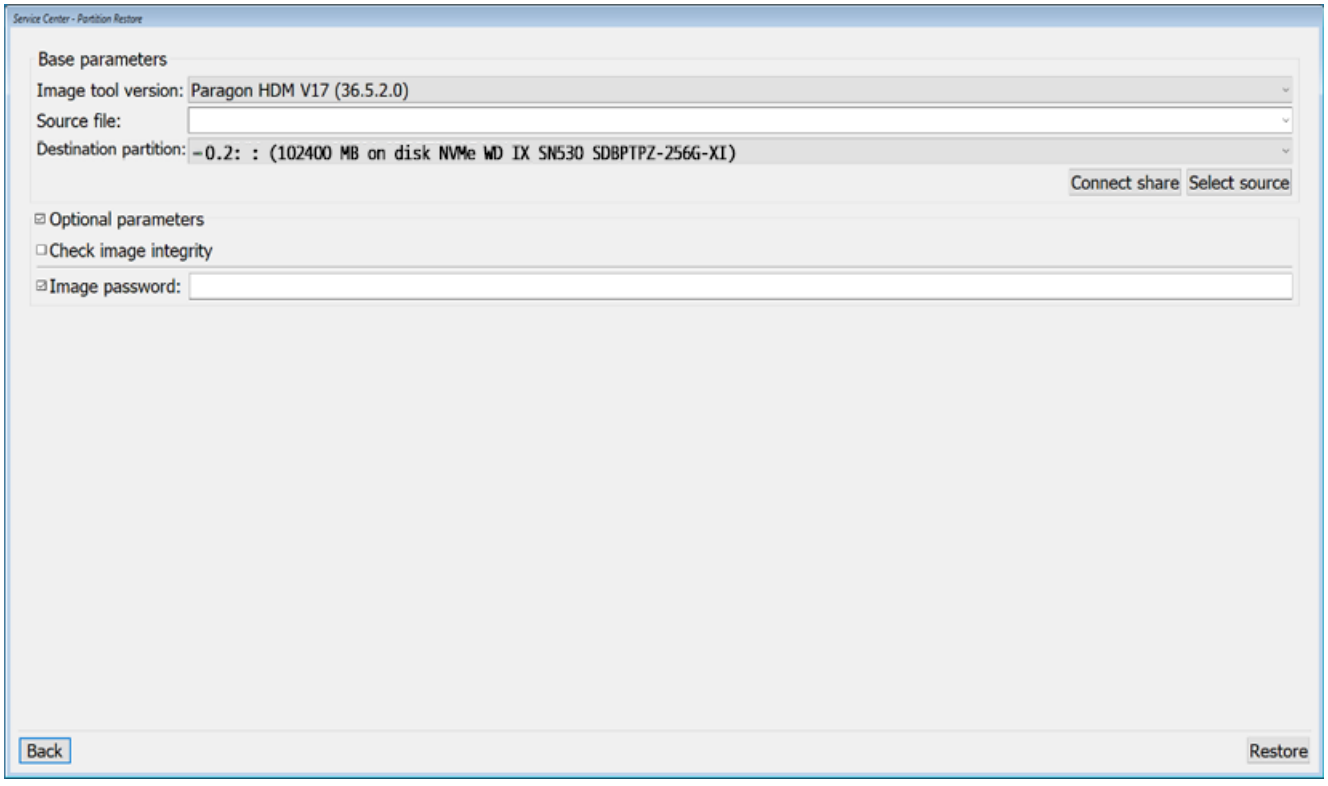


Figure 7-7 Service Center - Partition Restore

3. Make the required settings here:

Section	Setting	Purpose
Base parameters	Image tool version	Select the Paragon Hard Disk Manager™ version to be used when restoring the disk partition. Version for Microsoft Windows 10: "Paragon HDM V17 (36.5.2.0)"
	Source file	Select the disk image from which the partition is to be restored. You can use local disk images or disk images stored in the network.
	Destination partition	Select the partition to be restored from the disk image.
Base parameters > Destination partition	Connect share	Open the "Connect a Share" dialog box (Page 179). You can manage a shared resource (e.g. a directory in the network), to use a disk image stored on the network to restore the SSD.
	Select source	Open the "Select source file" dialog box. You can navigate through a local directory on the PC system and select a disk image for restoration.
Optional parameters	Check image integrity	Check the integrity of the data storage medium before restoration.
	Image password	Use the password to decrypt the protected disk image.

4. To start the restore process and entirely replace the existing data on the partition with the disk image, confirm the settings with "Restore".

Result

The restore process is started.

Note

Troubleshooting if reading in of the disk image fails

If data transfer is interrupted during the restore process, the PC system will have no executable system.

In this case, use a USB flash drive with Service Center to read the disk image in again.

7.10 Network settings in the Service Center

To manage a disk image in the network, you can display a shared network directory on the PC system as a drive.

In the Service Center, you configure network drives in the "Connect a share" dialog box. You can call this dialog box directly from the relevant dialog boxes to both create (Page 169) and restore (Page 171) disk images.

Precondition

The network directory is shared with the relevant user accounts in the domain and on the PC system.

Further information: Release directory of the PC/PC in the network (Page 190)

Overview

The setting options in the "Connect a share" dialog box have the following meaning:

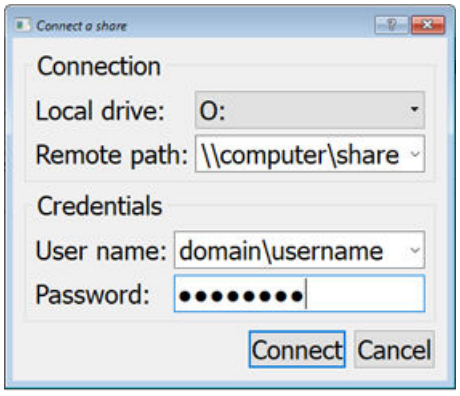


Figure 7-8 "Connect a Share" dialog box

Table 7-4 Settings in the "Connect a Share" dialog box in the Service Center

Section	Setting	Purpose
Connection	Local drive	Select drive letters under which the network directories are to be accessible on the PC system. The drive letters Z, Y and X are assigned to USB interfaces on SINUMERIK TCUs and operator panels. Do not use these drive letters for other purposes in order to avoid problems when using these USB interfaces.
	Remote path	Specify the device in the network and share name of the resource. Syntax: `\\Name of the server\share name of the network directory` Example: `\\Backup_Server\PCU_Backup`
Credentials	User name	Enter the user account under which the resource in the network can be accessed. If you have shared the resource on the server for certain users only, you must enter one of these user accounts here.
	Password	Enter the password of the user account.

Further information

You will find information about sharing directories in the network and network drives in the following chapters:

- Release directory of the PC/PC in the network (Page 190)
- Creating a shortcut to the network drive (Page 193)

7.11 Decrypting BitLocker-protected partitions

Decrypt BitLocker-protected partitions with the separately stored recovery password to be able to create disk images.

Requirement

You need the encrypted recovery password in a text file (*.txt).

More information: Using BitLocker drive encryption (Page 97)

Key statement

To decrypt BitLocker-protected partitions, proceed as follows:

1. Start the Service Center, e.g. from the Windows boot menu.
   More information: Starting the Service Center (Page 163)
2. In the main menu of the Service Center, click "Unlock Bitlocker Volumes".
   The "Unlock Volumes" dialog box opens.

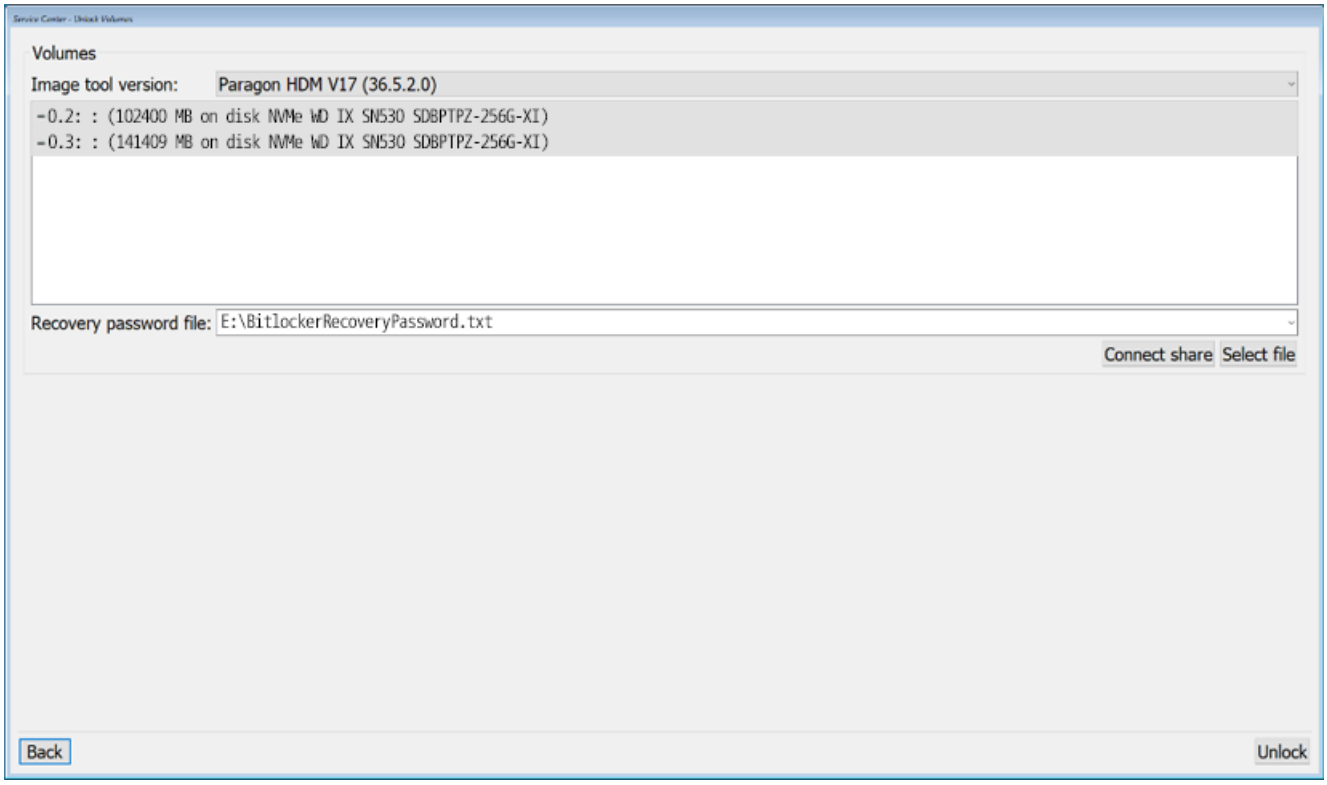


Figure 7-9 Service Center - Unlock Volumes

3. Make the required settings here:

Section	Setting	Purpose
Volumes	Image tool version	Select the Paragon Hard Disk Manager™ version that is to be used when creating the disk image. Version for Microsoft Windows 10: "Paragon HDM V17 (36.5.2.0)"
	Select BitLocker-protected partitions to be decrypted. **Note:** Unencrypted partitions are not displayed in the selection box.	
	Recovery password file	Specifies the storage location of the password file.
	Connect share	Open the "Connect a Share" dialog box (Page 179). You can use a shared resource (e.g. a directory in the network).
	Select file	Open the "Select file" dialog box. You can navigate to a local directory on the PC system and select a password file for decryption.

4. To decrypt the partitions, confirm the settings with "Unlock".
   The BitLocker-protected partitions are decrypted.
   The operation may take several minutes.

7.12 Creating an emergency boot system USB flash drive

Usage

You can generate a Service Center (emergency boot system) based on Microsoft Windows PE on a USB flash drive as preventive measure in the case of a defect.

The image for the creation of the USB flash drive is on the installed PCU Base under: `D:\Eboot\eboot.zip`.

Precondition

- The Microsoft Windows Service Desktop is active
- A 32 GB USB flash drive in FAT32 format is available (e.g. SIMATIC PC USB flash drive)

Preparation

If necessary, format the data storage medium:

1. Connect the USB flash drive to a USB interface of the PC system.
2. Open the application in Microsoft Windows Explorer.
3. In the drive overview, right-click on the USB flash drive, then on "Format...".
4. If required, acknowledge the system event message with "Yes".
   The formatting dialog is opened.
5. Select the FAT32 format and insert the EBOOT volume designation.
6. Start the formatting process.

Procedure

To create a USB flash drive, proceed as follows:

1. Connect the USB flash drive to a USB interface of the PC system.
2. Open the application in Microsoft Windows Explorer.
3. Copy the `eboot.zip` image from the `D:\Eboot\` directory to the USB flash drive.
4. Extract the contents of the ZIP file directly to the root directory of the USB flash drive, e.g. under `E:\`.
   Use Microsoft Windows, for example, right-click on the ZIP file, then "Extract all...".
   Follow the instructions on how to extract the data.

Result

The emergency boot system has been installed on the USB flash drive and the data storage medium has been renamed to EBOOT. The Service Center on the USB flash drive can be used.

7.13 Operating a service PC/PC in the network

7.13.1 Overview

System network

In the following applications, you will need, for example, a connection between the PC system and a PG/PC in the system network:

- Save the disk image of the SSD to a PG/PC
- Restore the SSD of a PC system via the DVD drive of a PG/PC
- Start up the replacement SSD
- Install the software on the PC system via the DVD drive of a PG/PC

Company network

If you want to connect the service PG/PC via a company network (Local Area Connection 2; interface X1), contact your network service center.

Further information on the Windows Firewall settings in the company network can be found in the Chapter Adapting the firewall settings (Page 72).

7.13.2 Connection options in the system network

Overview

The following figures show the typical connection options in the system network:

- Service PG/PC with (twisted) Ethernet cable directly to the interface "X2" of the PC system.
- Service PG/PC with (non-twisted) Ethernet cable via switch to the interface "X2" of the PC system.

Configuration with PG/PC directly to the PC system

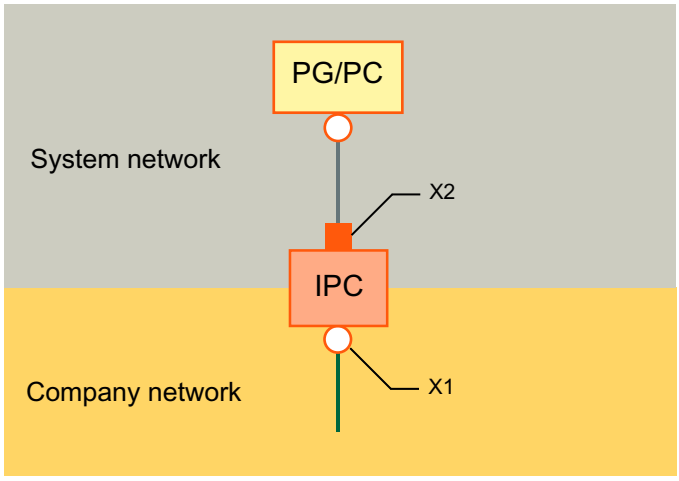


Figure 7-10 Connecting a PG/PC directly at the IPC

Configuration with PG/PC and switch to the PC system

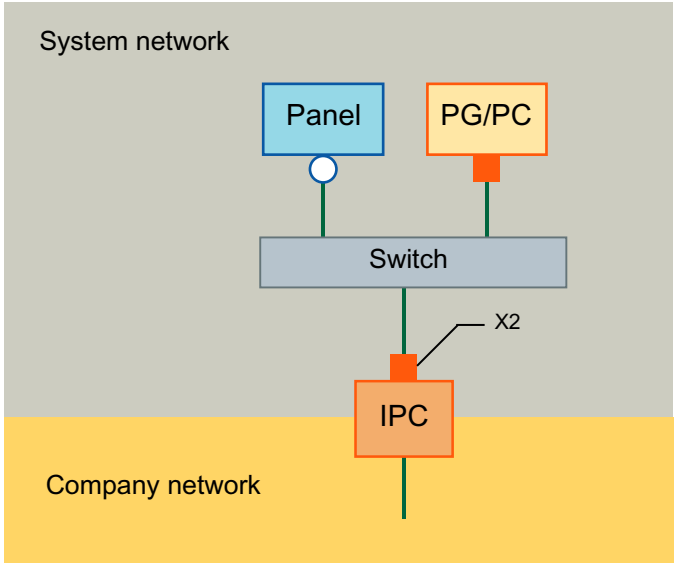


Figure 7-11 Connecting a PG/PC at the IPC via a switch

Basic procedure

On the PG/PC with Microsoft Windows 10:

- Connecting a PG/PC to a PC system according to one of the configurations shown above.
- The network protocol used is: TCP/IP.
  TCP/IP is already pre-configured on the PC system.
- Setting up IP addresses on the same subnetwork.
- Sharing a directory on the PG/PC for network access.

On the PC system in the Service Center:

- Start the Service Center on the IPC.
- Establish a network connection to the shared directory of the PG/PC.
  More information: Functions of the Service Center (Page 164)

7.13.3 Configuring routing in the network

Overview

If you have connected a PG/PC at NC interface X127 of the PU, configure the network routing to establish the connection between the PG/PC and the IPC.

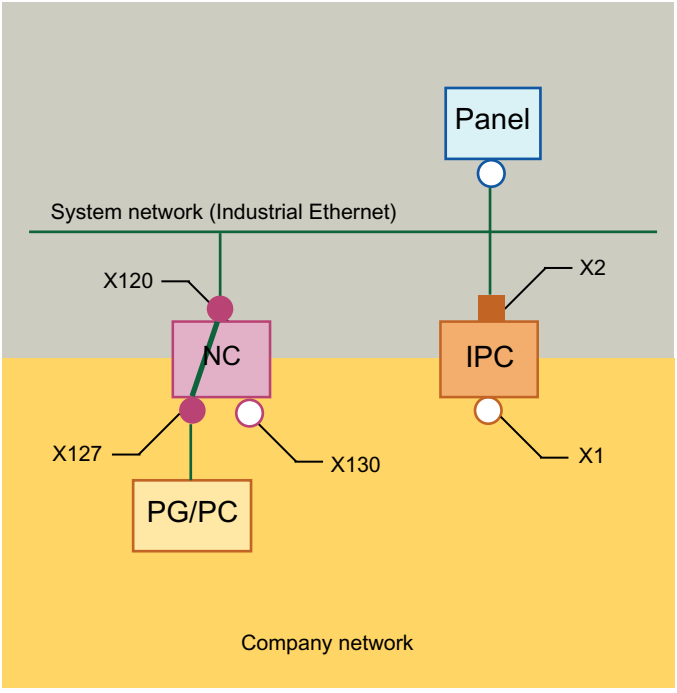


Figure 7-12 A networking example using IP routing

Preconditions

The following conditions must be met in order to use this function:

- The PG is connected to NC interface X127 in the system network.
- NC and IPC are connected via the system network.
- On the NC the routing is activated in one of the following ways:
  - In SINUMERIK Operate /PCU Modular, the routing is configured in the user interface "System network settings".
  - In the configuration file basesys.ini, key EnableSysNetToIBNForwarding=1 is set.

- If you wish to access a network directory, it must be shared.
- The user account in question is known to the PG/PC.
- The Service Center is active.

Procedure

To configure the IP routing in the Service Center, proceed as follows:

1. In the main menu of the Service Center, click "Network".
2. In the "Network Settings" dialog box, click the "IP Routing" tab.

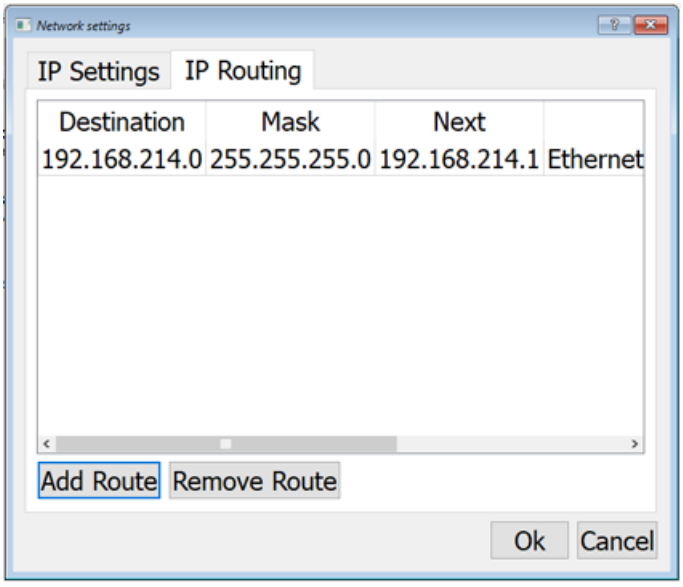


Figure 7-13 Service Center - IP routing

3. Configure the necessary routes.
   More information: Network settings in the Service Center (Page 166)

Result

The routing has been configured and the PG/PC and PC system are connected via the NC.

Now, perform the desired steps, for example, a Restore a disk image of the SSD (Page 171).

7.13.4 Configure the network settings of the PG/PC

Once you have connected a PG/PC in the network, make the network settings on the PG/PC.

The basic procedure for setup under Microsoft Windows 10 or Microsoft Windows 7 is described below. More information from Microsoft is in the Internet: Microsoft Windows support (https://support.microsoft.com/en-us/hub/4338813/windows-help?os=windows-10)

Requirement

- The PG/PC is linked with the PC system in one of the following ways:
  - The PG/PC is connected to the PC system (Page 184) using an Ethernet cable (either directly or via a switch)
  - The PG/PC is networked with the PC system via an interface of the NC (Page 186) and the routing is configured.
- A current Microsoft Windows operating system is installed on the PG/PC
- The PG/PC is switched on

Procedure

To configure the network settings of the PG/PC for connecting a PC system in the system network, proceed as follows:

1. Open the "network connections" window:
   - To do this under Microsoft Windows 7, click in the Control Panel in category "Network and Internet > View network status and tasks," select "Change adapter settings".
   - To do this under Microsoft Windows 10: enter "Control Panel" in the search field, then click on "Control Panel > Network and Sharing Center > Change Adapter Settings".
2. Right-click on the network adapter you want to configure, then in the shortcut menu click on "Properties".
   Dialog "Properties of <connection>" opens.

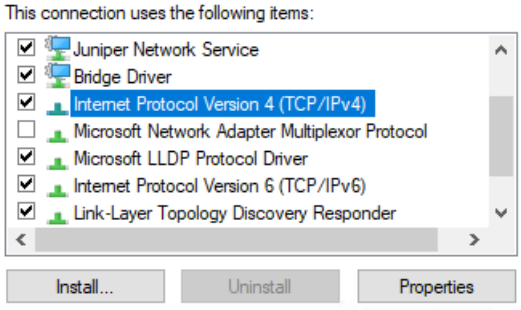


Figure 7-14 Properties of <connection>

3. Make the following settings:
   - Click "File and Printer Sharing for Microsoft Networks."
   - To change the IP address of the PG/PC, double-click "Internet Protocol Version 4 (TCP/IPv4)", then configure the settings as follows:

Section	Element	Setting
Use the following IP address	IP address	The following IP addresses in the system network can be used for the PG/PC: • 192.168.214.250 • 192.168.214.251 • 192.168.214.252 • 192.168.214.253 • 192.168.214.254
	Subnet mask	• 255.255.255.0

Result

The network settings of the PG/PC are now configured for use with the PC system.

7.13.5 Release directory of the PC/PC in the network

If you want to, for example, store disk images on a PG/PC that you have linked to the PC system via the network, set up a network drive.

As soon as it has been set up, a new drive will appear on the PC system, which is really a directory on the PG/PC.

The basic procedure for setup under Microsoft Windows 10 or Microsoft Windows 7 is described below. Further information from Microsoft is in the Internet: Microsoft Windows support (https://support.microsoft.com/en-us/hub/4338813/windows-help?os=windows-10)

Requirement

- The PG/PC is switched on.
- There is sufficient free space on the PG/PC, to save disk images of the PC system, for example.
- The user accounts to which you want to grant share rights are known in the domain or on the PC system.

Procedure

Proceed as follows to share a directory for use in the network:

1. On the PG/PC, in the Control Panel call up Computer Management.
2. Under "System > Shared Folders" select the file "Shares."
3. In the "Action" menu, click the "New File Share..." command.
   The "Create A Shared Folder Wizard" opens.

4. Under step "Name, Description, and Settings," make a note of the Share path, which is a combination of the computer name and the share name. You will have to specify this name when you create a link to the network drive on the PC system.

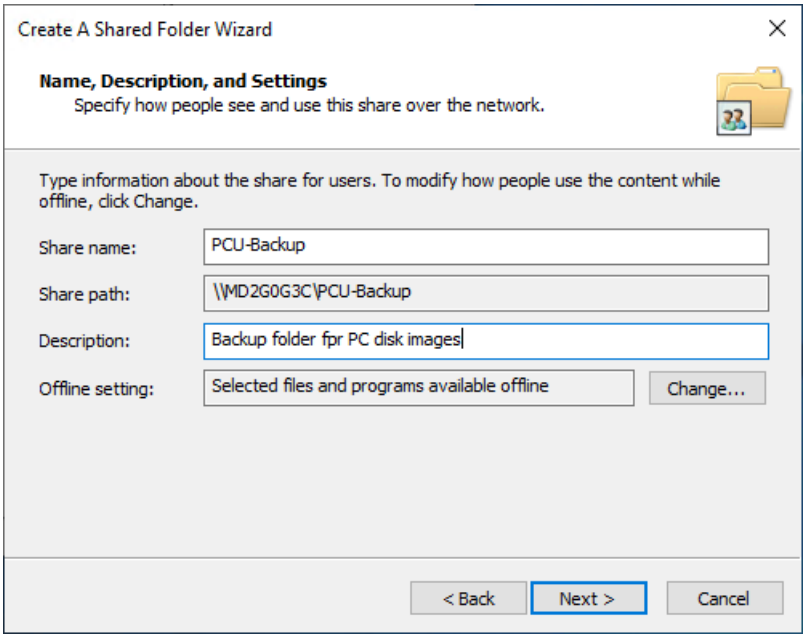


Figure 7-15 Create A Shared Folder Wizard - Name, Description, and Settings

5. Under step "Shared Folder Permissions," select the "Customize permissions" option button, then click "Custom..."

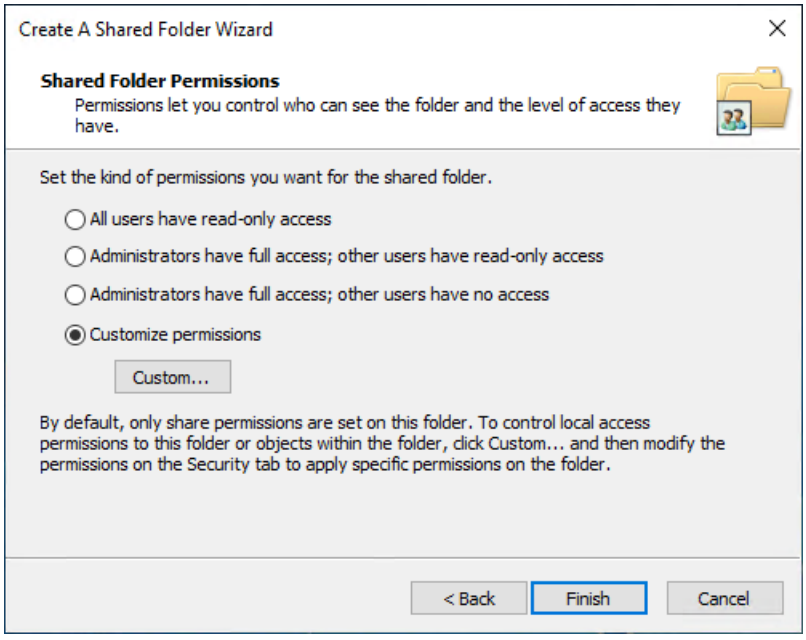


Figure 7-16 Create a Shared Folder Wizard - Shared Folder Permissions

The "Customize Permissions" dialog box opens.

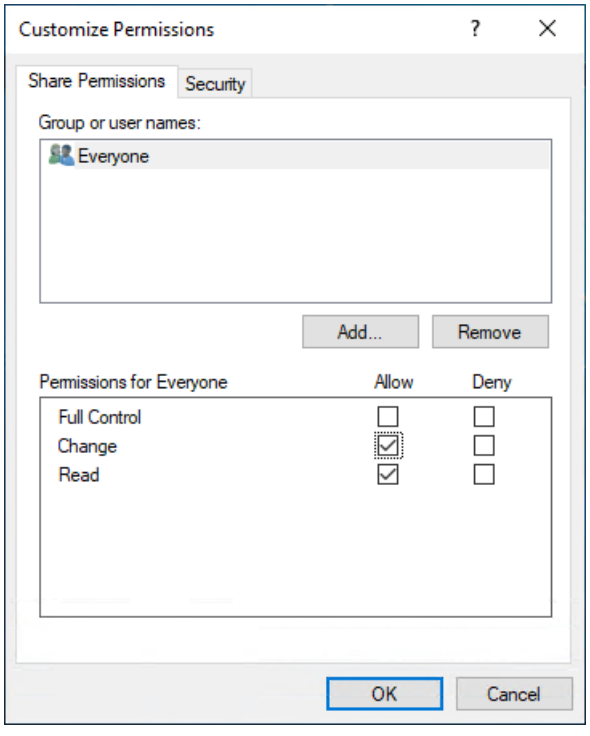


Figure 7-17 "Customize Permissions" dialog box

6. In section "Group or user names," click "Add..."
   The "Select Users, Computers, Service Accounts, or Groups" opens.

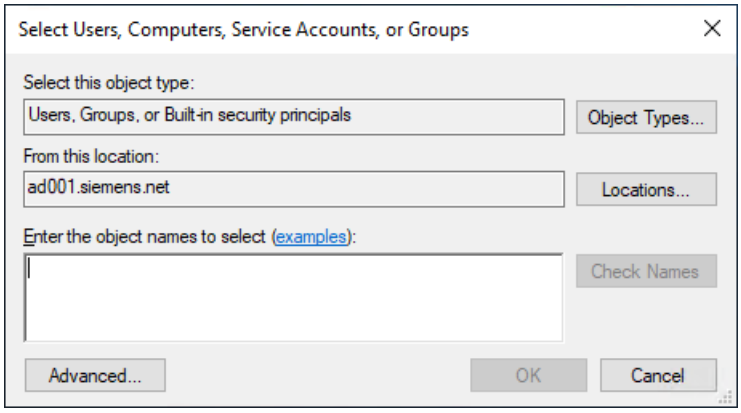


Figure 7-18 "Select Users, Computers, Service Accounts, or Groups" dialog box

7. In section "Permissions for <user name>," under column "Allow," click the "Change" checkbox.
8. Confirm these settings in the "Customize Permissions" dialog box with "OK."
9. In the next steps of the wizard, make all the settings you require and confirm the share with "Finish".

7.13.6 Creating a shortcut to the network drive

To be able to access the shared directory on the PG/PC from the PC system, after you have connected and configured the PG/PC in the network, you must set up the shared folder on the PC system as a network drive.

As soon as it has been set up, a new drive will appear on the PC system, which is really a directory on the PG/PC.

The basic procedure for setup under Microsoft Windows 10 or Microsoft Windows 7 is described below. Further information from Microsoft is in the Internet: Microsoft Windows support (https://support.microsoft.com/en-us/hub/4338813/windows-help?os=windows-10)

Requirement

- The PG/PC is switched on.
- The Service Desktop is active.
- The folder on the PG/PC is shared for the relevant user accounts on the domain and on the PC system.

Procedure

Proceed as follows to connect a shared directory as a network drive:

1. Start the Microsoft Windows Explorer and click the "Map network drive" button.
2. Make the following settings in the "Map network drive" dialog box:

Setting	Purpose
Drive	Select drive letters under which the network directories are to be accessible on the PC system. The drive letters Z, Y and X are assigned to USB interfaces on SINUMERIK TCUs and operator panels. Do not use these drive letters for other purposes in order to avoid problems when using these USB interfaces.
Folder	Specify the device in the network and share name of the resource. Syntax: `\\Name of the server\share name of the network directory` Example: `\\Backup_Server\PCU_Backup`
Reconnect at logon	Activate this checkbox to automatically connect the network drive while running up.
Connect using different credentials	Activate this checkbox if you have not shared the directory in the network with the user for whom you would like to set up the network drive. In the next dialog box "Enter Network Password," enter the log-on information of a user with whom the network directory is shared.

3. Confirm your settings with "Finish".

7.14 Starting up the replacement SSD

More information

Further information on the replacement or installation of an SSD can be found in the hardware documentation for your PC system in the SIMATIC IPC Operating Instructions:

Note

Troubleshooting if reading in of the disk image fails

If data transfer is interrupted during the reading process, there will be no executable operating system available on the PC system.

In this case, use a USB flash drive with Service Center to read the disk image in again.

Further information to restore a disk image is provided under Restore a disk image of the SSD (Page 171).

Service and diagnostics

8

8.1 Setting of the operating mode during run-up

8.1.1 Software-side setting (SIMATIC IPC)

In contrast to SINUMERIK PCUs, SIMATIC IPCs have no service switch on the hardware side for selecting the mode. Therefore, on the SIMATIC devices, you can define the mode on the software side in the configuration file `pcuhwsvc.ini`.

Archiving of the configuration file pcuhwsvc.ini

The template is located in directory
`C:\ProgramData\Siemens\MotionControl\siemens\System\etc\`

Do not overwrite this template, but save a copy of the template `pcuhwsvc.ini` in one of the user directories:

- `C:\ProgramData\Siemens\MotionControl\`**user**`\System\etc\`
- `C:\ProgramData\Siemens\MotionControl\`**oem**`\System\etc\`

You can find further information on how configuration files function in the Chapter Directory structure and file conventions (Page 36).

Table 8-1 Mode setting in configuration file pcuhwsvc.ini

Section	[GLOBAL]
Key	`ModeSwitch=`
Value	0 = Normal mode 3 = Desktop mode (run-up in the welcome screen) Other modes are not permitted in the software-side setting for SIMATIC IPC.
Factory setting	0

8.2 Switching to the Service Desktop during autostart / autologon operation

If you have set up the autologon operation and the autostart of SINUMERIK Operate with the activated keyboard filter, the PC system runs up with SINUMERIK Operate after being switched on.

To be able to switch to the Windows desktop in this case, interrupt the run-up of SINUMERIK Operate with an entry, as described here.

Alternatively, you can switch over the operating mode for the next run-up in the software (SIMATIC IPC) (Page 197).

Precondition

- SINUMERIK Operate is installed and autologon mode is set up.
  Further information: Setting up SINUMERIK Operate for autologon mode (Page 107)
- The PC system is switched off.

Procedure

To switch to the desktop when the autostart/autologon mode is activated, proceed as follows:

1. Switch on the PC system and wait until the "SINUMERIK" welcome screen is displayed.
2. While the "SINUMERIK" welcome screen is being displayed, make one of the following entries:
   - Press the key 3 on your keyboard.
   - Click or tip the copyright information.

   The counter for starting SINUMERIK Operate is suspended and you can select one of three options:



Figure 8-1 Welcome screen "SINUMERIK" after key input

3. Select the "Display Desktop" option.

Result

The Service Desktop opens.

8.3 Configuring the SINUMERIK power up screen

You can parameterize various settings to change to the service desktop or to the SINUMERIK welcome screen. These settings can be especially helpful if you wish to carry out diagnostics and maintenance to a system in the headless mode.

Requirement

- In the corresponding user directory, file `slstartup.ini` is either not available, or there is no `slstartup.ini` with different settings in a user directory with a higher priority.
- If the file already exists in the corresponding user directory, then do not create a new `slstartup.ini`, but instead, adapt the existing file or insert section `[StartScreen]` using the appropriate keys.

Procedure

Proceed as follows to create the configuration file for the direct key layout:

1. Open a text editor, and as character coding, set ASCII or ANSI.
2. Insert the section designation:
   `[StartScreen]`
3. Enter those keys, whose values you wish to parameterize, and make the required settings:

Setting/key	Possible values	Description
ShowButtons=	[true|false]	Specifies as to whether the buttons are displayed with run-up options directly in the "SINUMERIK" welcome screen. For "ShowButtons=false", the buttons are only displayed after making a selection (key 3 or click on the Copyright note).
Timeout=	s	Time in seconds, after which the system runs up with SINUMERIK Operate. The counter starts to run after an operator panel, screen or a VNC connection has been identified.
MaxTimeout=	s	Maximum time in seconds, after which the system runs up with SINUMERIK Operate. The counter starts to run immediately, irrespective of whether an operator panel, screen or a VNC connection exists.
ShutdownTimeout=	s	Time in seconds, within which the system power down can be interrupted (key 3 or click on the Copyright note).
ShowCountdown=	[true|false]	Displays a countdown until the system runs up with SINUMERIK Operate.

4. Save the file as `slstartup.ini` in one of the user directories.
   - `C:\ProgramData\Siemens\MotionControl\user\sinumerik\hmi\cfg\slstartup.ini`
   - `C:\ProgramData\Siemens\MotionControl\oem\sinumerik\hmi\cfg\slstartup.ini`

   More information: Directory structure and file conventions (Page 36)

Example

Default setting of the section [StartScreen] in startup.ini

```
[StartScreen]
ShowButtons=false
Specifies as to whether the buttons are displayed with run-up options
directly in the "SINUMERIK" welcome screen (without key 3 or clicking on the
copyright note).
Timeout=5
# Time in seconds, after which the system runs up with SINUMERIK Operate
(assuming that a screen was identified).
MaxTimeout=300
# Maximum time in seconds, after which the system runs up with SINUMERIK
Operate (without a screen having been identified).
ShutdownTimeout=3
# Time in seconds, within which the system power down can be interrupted
(key 3 or click on the Copyright note).
ShowCountdown=true
# Displays a countdown until the system runs up with SINUMERIK Operate.
```

8.4 Remote access

8.4.1 Overview

You can use a remote connection to access other devices via the network:

- Access to maintenance with prompt (SSH) via PuTTY.
- Access via VNC Viewer with all of the operating and servicing options, which are also provided directly on the PC system.

Further information: Setting up and using SSH (Page 205)

8.4.2 Searching for devices in the system network

The "sc_show_net" command shows devices available in the system network in the prompt and offers additional information about these devices.

As both these functions rely on SNMP (Simple Network Management Protocol), only SNMP-capable devices will be found. In the case of Windows-based devices, this depends on the software version. If a simple call is made without any additional options, a list of the devices found will appear showing the relevant IP address, DNS name (if known), and a short description (module name).

sc_show_net command

This command is executed in the prompt:

Syntax:	sc_show_net [-xml] [[-hw] [-tco] [-sw | -swfull] [-loc] [-panel] [-dhcp] [-switch] | -all] [HOSTS...]
Authorization level:	None

8.4.3 Display of accessible stations in SINUMERIK Operate

You can use the network diagnostics function in SINUMERIK Operate to show accessible nodes in the system network.

Procedure

Proceed as follows to show accessible nodes:

1. Select "MENU SELECT" to open the menu.
2. In the horizontal softkey menu, choose "Diagnostics > Bus TCP/IP".
3. In the vertical softkey menu, select "TCP/IP > Diagnostics Network > Accessible nodes". The "Accessible nodes" user interface opens showing all nodes that use the SNMP or DCP protocol.

More information for the display of accessible nodes is provided in the online help of SINUMERIK Operate.

8.4.4 Remote access for operation and maintenance

You can connect via remote access to SINUMERIK components that have an active VNC server.

- Remote access to the PC system from a PG/PC in the system network (Page 184) is activated via the factory setting. You can optionally define a password for this:
  If you want to access the PC system via the company network instead or in addition, you must adapt the firewall settings (Page 78) and define a password.

  Note

  Access to the PC system in the company network requires a secure password

  A password is required to access the PC system via remote access in the company network. The password is not yet defined in the factory settings. If the PC is to be accessed in the company network, you must specify a password.

- The factory settings only enable you to monitor a PC system via an external VNC Viewer. To operate the system from another station, the system in question must grant permission. You make the necessary settings in the **tcu.ini** in section `[VNCViewer]`.

Defining the password

To define passwords for remote access to the PC system, call the prompt and enter the "sc_vncpwd" command.

Command	Parameter	Value	Meaning
sc_vncpwd	set	companynetwork|systemnetwork [password]	Sets the specified password and activates the password prompt for remote access
	reset	companynetwork|systemnetwork	Deactivates the password prompt (remote access without password)

- Example for company network (X1):
  `sc_vncpwd set companynetwork mypasswd`
- Command for system network (X2):
  `sc_vncpwd set systemnetwork mypasswd`

The password may contain a maximum of 8 characters. Passwords are saved in encrypted form in the following file:

`C:\ProgramData\Siemens\MotionControl\user\System\etc\sinumerikvnc.ini`

Defining the password using SINUMERIK Operate

To define passwords for remote access using SINUMERIK Operate, switch to operating area "Diagnostics" via
"MENU SELECT > Diagnostics > Remote diag. > Password".

More information on the settings in window "Remote diagnostics (RCS)" for remote access is provided in the online help under
Commissioning functions and service.

Options for the VNC Viewer

Note

Do not change the factory settings!

To ensure that the VNC Viewer works properly, the following options must not be changed.

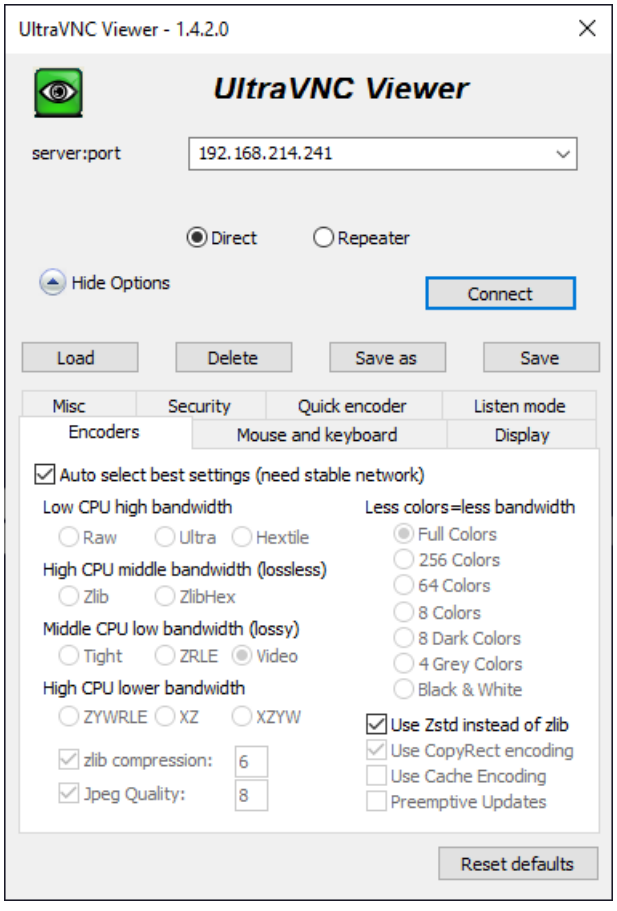


Table 8-2 Connection settings in the VNC viewer ("Show Options" button)

Register	Factory setting
Quick encoder	AUTO (Auto select best settings)
Encoders	Auto select best settings (need stable network)
Security	Share the Server, allow other to connect.
Mouse and keyboard	Emulate 3 Buttons (with 2-button click)
	Let remote server deal with mouse cursor
Display	Show Toolbar.

Display of the status

If remote access is active, using these icons information is provided in the status bar of SINUMERIK Operate as to whether a remote access is presently active or whether only monitoring is permitted.



Remote monitoring active



Remote control active

8.4.5 Setting up and using SSH

You can use remote access to access devices from the PC system.

An SSH environment is initially set up when installing PCU-Basesoftware /IPC for Microsoft Windows 10. You can log on with PuTTY.

You can use an SSH key to log on. A script for setting up the infrastructure on devices is provided. However, for security reasons no previously generated keys have been stored.

More information

- Chapter Remote access (Page 202)
- Chapter Encryption via SSH protocol (Page 206)
- Chapter Using individual SSH authorization for Operate (Page 207)

Setting up remote access with SSH and key pair

The procedure for setting up users and using remote access is the same as the usual procedure for remote access with SSH.

Table 8-3 Support with setting up remote access

Task	Recommended application	Storage path	Help
Generate key pair	PuTTY Key Generator	C:\Program Files\PuTTY\puttygen.exe	Online help in PuTTY (Chapter *Public key for pasting into authorized_keys file*)

Set up infrastructure on devices	Supplied script ssh_key_login.bat	C:\ProgramData\Siemens\Motion Control\siemens\System\etc.\ssh_key_login.bat	Call up the script via the prompt. To do this, enter user name and file name of the public key as the parameters.
			Syntax:
			`ssh_key_login.bat <user name> <public key>`
			Example:
			`ssh_key_login.bat username publicKey.pub`

Access devices via remote connection	PuTTY	C:\Program Files\PuTTY\putty.exe	Online help in PuTTY IP address of the PCU (factory setting): • System network: 192.168.214.241 • Company network: The IP address is taken from the DHCP server

8.4.6 Encryption via SSH protocol

Security

The security of SSH is ensured by a series of cryptographic algorithms for encryption and authentication.

Authentication

The server identifies itself to the client with an RSA, DSA or ECDSA certificate, which enables detection of manipulation in the network (no other server can identify itself as a known server).

The client can authenticate itself either by public key authentication with a private key whose public key is stored on the server, or with a normal password. While in the latter case, user interaction is always necessary (unless the password is stored unencrypted on the client computer), public key authentication allows client computers to log on to SSH servers without user interaction, without a password having to be stored in plain text on the client. However, for added security the private SSH keys can also be protected with a password.

Subsystems

In the case of Secure Subsystem Execution, subsystems that were defined in an SSH server installation can be executed remotely without knowing the precise path of the program executed on the server. SFTP is the most common subsystem.

More information

- Chapter Setting up and using SSH (Page 205)
- Description of PuTTY

8.4.7 Using individual SSH authorization for Operate

SINUMERIK Operate on the IPC uses SSH to access the NCU/PU. For easy commissioning/ maintenance, the NCU/PU allows SINUMERIK Operate to be accessed based on a fixed standard key. In addition to this global SSH standard encryption, SINUMERIK offers the possibility to set up an individual SSH authorization for non-paired system devices. The protection of these system devices against data misuse can thus be improved.

Note

The SSH key is automatically individualized by pairing an NCU/PU with the PC/IPC. Manual SSH authorization is not necessary for NCU/PU-based systems.

However, the SSH standard key can still be used. **It is therefore recommended to manually deactivate the standard key** to prevent access based on the standard key.



More information is provided in the SINUMERIK Operate online help Commissioning functions and service.

Requirement

- Applications:
  - PuTTY Key Generator
  - SINUMERIK Access MyMachine P2P or WinSCP
- With active user management: You have the "Security Admin" or "Service" role.
  - or -
- Without active user management: You have at least access level 3 (user).

Application

Note

By deactivating the SSH standard key, you exclude all non-paired devices from an SSH connection!

- In SINUMERIK Operate, deactivate the "Allow legacy access for Operate" option under the "Commissioning > Security > HMI security" user interface.
  The SSH standard key is therefore inactive for all external system devices.

You have the following options if you still wish to establish an SSH connection to non-paired external devices:

SSH connection with non-paired PC system

- With the aid of the applications SINUMERIK Access MyMachine P2P, PuTTY or WinSCP
- With user management activated: Login via user name and password
- Without activated user management: Login via access level and password

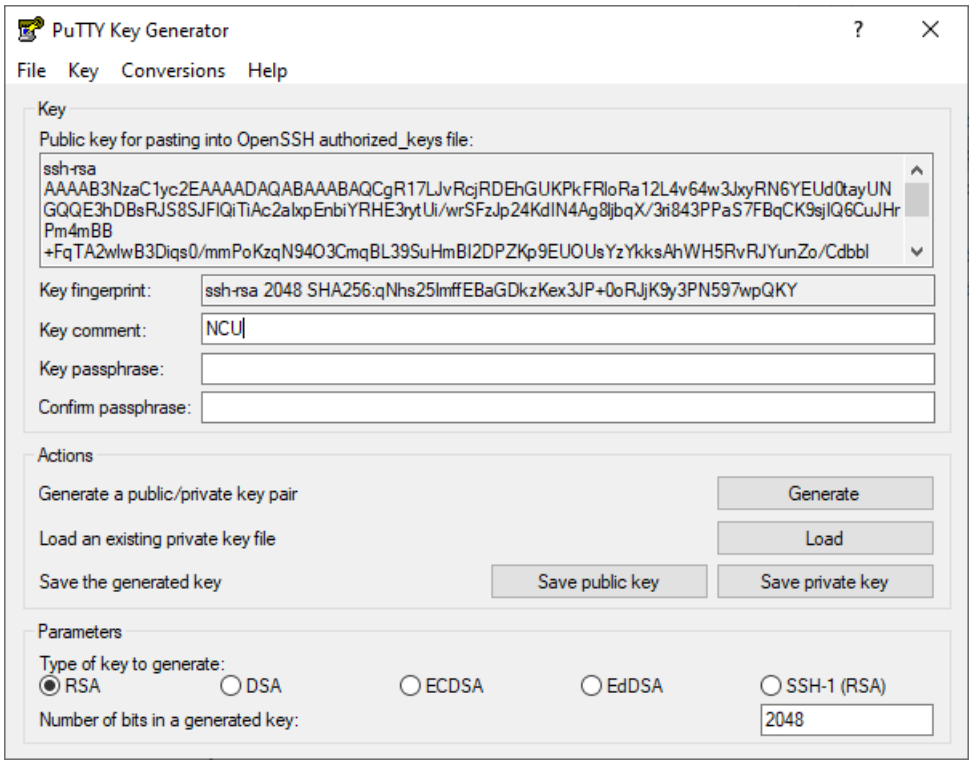
SSH connection with SINUMERIK Edge, SINUMERIK Commissioning Tool or HMI Base application on an external device

- Import the individual SSH key (PKK file)
  - or -
- Activate the legacy access in SINUMERIK Operate

Creating an individual SSH key

To create an individual SSH key, proceed as follows:

1. Under Microsoft Windows, call the PuTTY Key Generator application:
   `C:\Program Files\PuTTY\puttygen.exe`



2. Select the RSA type and a sufficient bit key size (2048 bits are recommended). You can add an optional comment in the "Key comment" field.

Note

Do not enter a password for additional encryption of the PPK file in the "Key passphrase" field.

3. Click on "Generate".
   An SSH key pair is generated and displayed in the "Public key for pasting into OpenSSH authorized_keys file" field.
4. Click on "Save private key" and save the individual key as a PKK file in a local directory, e.g. under:
   `C:/Program Files(x86)/Siemens/MotionControl/oem/sinumerik/hmi/config/private_ssh.pkk`
   The individual SSH key is unencrypted and must be readable for the account user on the PC system.

Installing an individual SSH key

Install the individual SSH key manually on the NCU/PU:

1. Call up the Access MyMachine P2P or WinSCP application under Microsoft Windows. Log in, for example, as "manufact" user.
2. Open the SSH file `authorized_keys` under the following NCU/PU directory: `.../home/manufact/.ssh/authorized_keys`
3. Copy the individual SSH key in the "Public key for pasting into OpenSSH authorized_keys file" field from the PuTTY Key Generator application to the clipboard, e.g. with CTRL + C.
4. Paste the SSH key from the clipboard into the SSH file `authorized_keys`. Optionally, you can remove the existing global SSH standard key from the SSH file `authorized_keys`.
5. Save the changes to the SSH file `authorized_keys` and close it.
6. Disconnect the user connection and close the Access MyMachine P2P or WinSCP application.
7. Open a text editor.
8. Use the text editor to create the files `slfsssh.xml` and `slsc.xml` (character encoding ASCII or ANSI) in the following directory: `C:/Program Files(x86)/Siemens/MotionControl/`**oem**`/sinumerik/hmi/cfg`
9. Copy the **XML configuration** described below into both XML files.
10. Replace the PKK file names in all `<SSHKeyPath>` markups with the file name of the individual SSH key. If necessary, add the real path specification, e.g.: `C:\Program Files(x86)\Siemens\MotionControl \oem\sinumerik\hmi\config\private_ssh.pkk`
11. Save the changes to the configuration files and close them.
12. Restart the system.

Result

The SINUMERIK system starts up. The PC system connects to the controller via the individual SSH authorization.

Example of XML configuration

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<CONFIGURATION>
  <SSHShell>
     <Path type="QString" value="plink.exe"/>
     <UserName type="QString" value="manufact"/>
     <SSHKeyPath type="QString"
value="C:\Program Files(x86)\Siemens\MotionControl
\oem\sinumerik\hmi\config\private_ssh.pkk"/>
  </SSHShell>
```

```
  <SSHCopy>
     <Path type="QString" value="pscp.exe"/>
     <UserName type="QString" value="manufact"/>
     <SSHKeyPath type="QString"
value="C:\Program Files(x86)\Siemens\MotionControl
\oem\sinumerik\hmi\config\private_ssh.pkk"/>
  </SSHCopy>
</CONFIGURATION>
```

Appendix

A

A.1 Script example for BitLocker activation

Script for ps1 format

Use the script example for BitLocker encryption in the Microsoft Windows PowerShell (Page 101) application.

```
#!pwsh

#Requires -Version 5.1
#Requires -RunAsAdministrator

# Script params and variables
[CmdletBinding()]
param(
    [Parameter(Mandatory=$false)][string]$RecoveryPassword=$null,
    [Parameter(Mandatory=$false)][string]$RecoveryPasswordFile=$null,

    [Parameter(Mandatory=$false)][string[]]$Partitions=@()
)

# enable BitLocker for volumes
function enableBitlockerForVolumes
{
    trap { continue }
    # enable bitlocker for volume system drive
    $bitlockerSystemVolume = Enable-BitLocker -MountPoint "${env:SystemDrive}"
-EncryptionMethod XtsAes256 -TpmProtector -SkipHardwareTest -ErrorAction SilentlyContinue
    if (-not $bitlockerSystemVolume) {
        # error activating bitlocker on system drive
        return $false
    }
    # add recovery password to volume system drive
    if ($RecoveryPassword) {
       $bitlockerSystemVolume = Add-BitLockerKeyProtector -MountPoint "${env:SystemDrive}"
-RecoveryPasswordProtector -RecoveryPassword "$RecoveryPassword" -ErrorAction
SilentlyContinue
    }
    else {
       $bitlockerSystemVolume = Add-BitLockerKeyProtector -MountPoint "${env:SystemDrive}"
-RecoveryPasswordProtector -ErrorAction SilentlyContinue
    }
```

```
    if (-not $bitlockerSystemVolume) {
        # couldn't add recovery password to system drive
        return $false
    }
    # get recovery password from volume info
    $foundRcvPwd = $false
    foreach ($protector in $bitlockerSystemVolume.KeyProtector) {
        if ($protector.KeyProtectorType -eq "RecoveryPassword") {
            $script:RecoveryPassword = $protector.RecoveryPassword
            $foundRcvPwd = $true
            break
        }
    }
    if (-not $foundRcvPwd) {
        # no recovery password for system volume
        return $false
    }
    # enable bitlocker for additional volumes
    $bitlockerVolumes = Enable-BitLocker -MountPoint $Partitions -EncryptionMethod
XtsAes256 -RecoveryPasswordProtector -RecoveryPassword "$RecoveryPassword"
-SkipHardwareTest -ErrorAction SilentlyContinue
    if (-not $bitlockerVolumes) {
        # error activating bitlocker on additional volumes
        return $false
    }
    # enable auto unlock for additional volumes
    $bitlockerVolumes = Enable-BitLockerAutoUnlock -MountPoint $Partitions -ErrorAction
SilentlyContinue
    if (-not $bitlockerVolumes) {
        # error enabling auto unlock bitlocker for additional volumes
        return $false
    }
    # save recovery password in file if specified
    if ($RecoveryPasswordFile) {
        $RecoveryPassword | Out-File -FilePath $RecoveryPasswordFile -Encoding ASCII
-ErrorAction SilentlyContinue -ErrorVariable saveRcvPwdError
        if ($saveRcvPwdError) {
            # couldn't save recovery password in file
        }
        else {
            # saved recovery password in file
        }
    }

    return $true
}

$ret = enableBitlockerForVolumes
```

A.2 Overview of Microsoft Windows changes

Installing PCU-Basesoftware /IPC changes the default Microsoft Windows 10 configuration in the following categories:

Microsoft Windows 10 system changes

Category	Change	Detail
Control Panel settings	Windows Defender (Page 74) deactivated	
	Energy settings	Hibernate state deactivated
	File and printer release (Page 80) deactivated	
	Changes to the firewall settings (Page 72)	• Firewall system network deactivated • Firewall company network blocked for incoming connections (exception: mcp_server.exe TCP and UDP private and public)
	Network settings (Page 34)	IP settings of the system network set to 192.168.214.241 and 255.255.255.0
	Firewall release for VNC (Page 78)	Firewall inputs: Port 5800 and 5900 with write permission, but remain deactivated

Category	Change	Detail
Changing the registry settings	Automatic start DiagBase Management Explorer removed	Delete "DMRunStartup" from "HKLM\Software\Microsoft\Windows\CurrentVersion\Run"
	Automatic start removed from FilterCheck (IPC Wizard)	Delete "FilterCheck" from "HKLM\Software\Microsoft\Windows\CurrentVersion\Run"
	Automatic start HidLock removed	Delete "HidLock" and "HidLockCounter" from "HKLM\Software\Microsoft\Windows\CurrentVersion\Run"
	Registry entry for background image activated at logon screen	Registry key: "HKLM\Software\Microsoft\Windows\CurrentVersion\Authentication\LogonUI\Background", "OEMBackground"=1
	File names are not case sensitive	Registry key: "HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\kernel", "obcaseinsensitive"=1
	Startup delay set to 0	Registry key: "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Serialize", "Startupdelayinmsec"=0
	Mouse pointer control with numpad	Registry key: "HKCU\Control Panel\Accessibility\MouseKeys", "Flags"="63"
	Edge Swipe deactivated	Registry key: "HKLM\SOFTWARE\Policies\Microsoft\Windows\EdgeUI", "AllowEdgeSwipe"=0
	Do NOT show window contents when moving	Registry key: "HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\VisualEffects", "VisualFXSetting"=3; Key: "HKLM\Control Panel\Desktop", "DragFullWindows"=0
	Duration Welcome Screen, timeout duration of approx. 3 seconds	Registry key: "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System", "DelayedDesktopSwitchTimeout"=3
	Balloon tips deactivated	Registry key: ""HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced"", ""EnableBalloonTips""=0"
	SoftwareSASGeneration Policy set to 1 (32 and 64 bit)	Registry key: "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System", "SoftwareSASGeneration"=1
	FastUserSwitching deactivated	Registry key: ""HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System"", ""HideFastUserSwitching""=1"
	Autorun deactivated	Registry key: ""HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer"", ""NoDriveTypeAutoRun""=255"
Deactivated services	Windows feature "Games"	
	SSDP Discovery Service (SSDPSRV)	Startup type: Disabled
	UPnP Device Host (upnphost)	
	Remote Desktop Services (TermService)	
	Shell Hardware Detection (ShellHWDetection)	
	Telephony Service (TapiSrv)	
	MiniWeb Service (MiniWeb)	
	DMAlarmManager (DMAlarmManager)	
	DMMsgService (DMMsgService)	
	Windows queries during run-up after power off (BCDEdit)	bcdedit.exe /set [current] bootstatuspolicy ignoreallfailures
	WebClient Service (WebClient)	Startup type: Manual

Category	Change	Detail
Configured services	TCU Hardware Service (PCU TCU-HWS / hmisvr_TCU_hard-ware_services)	Startup type: Automatic
	DHCP Server (Page 34) (PCU DHCPD / hmisvr_PCU_udhcpd)	
	TFTP Server (PCU TFTPD / hmisvr_PCU_netkit-tftpd)	
	FTP Server (PCU FTPD / hmisvr_PCU_betaftpd)	
	Localhws Service (PCU LO-CALHWS / hmisvr_PCU_localhws)	
	Syslogd Service (PCU SYSLOGD / hmisvr_TCU_syslogd)	
	PCU Hardware Service (PCUHard-wareService)	
	UltraVNC uvnc_service (uvnc_service)	
	Windows Time Service (W32Time)	
	Windows Feature "SNMP" (Page 76)	
	SNMP ExtensionAgent	Installation SNMP extension, registration as standard SNMP service
	SmartD Service/ smartmontools (smartd) (Opensource)	Startup type: Manual
	Windows feature "Services for NFS" (incl. NFS Client and Admin Tools)	

Category	Change	Detail
Additional applications (Page 32)	Installation of VisualStudio 2008 Redistributables (x86)	
	Installation of VisualStudio 2008 Redistributables (x64)	
	Installation of VisualStudio 2010 Redistributables (x86)	
	Installation of VisualStudio 2010 Redistributables (x64)	
	Installation of VisualStudio 2012 Redistributables (x86)	
	Installation of VisualStudio 2012 Redistributables (x64)	
	Installation of VisualStudio 2017 Redistributables (x86)	
	Installation of VisualStudio 2017 Redistributables (x64)	
	Keyboard filter driver	
	Mouse filter driver	
	HID filter driver	
	Npcap Version 1.78	
	VNC Server Version 2.0.0.3	
	PuTTY Version 0.79	
	SIEMENS PCU Installer (Policies, Autostart, Service)	
	Paragon Hard Disk Manager™ 17 Suite (36.5.2.0)	
	DualBoot of the service system	
	Windows feature ".NET Framework 3.5"	
	SIMATIC IPC DiagBase	IPC standard (preinstalled)
	Power configuration	SIEMENS Power Configuration (powercfg.exe -import sinumerikpowercfg 74c897bc-2b4e-4dd9-a29d-5b9e04241364)

Category	Change	Detail
Directory structure (Page 36) for SINUMERIK Operate	Change of access rights	Full write permissions to `D:\Install`
		Full write permission for `Users Group` on `C:\ProgramData\Siemens\MotionControl`
	Directory deleted	`C:\Windows\Web\SIMATIC`
	Registered Siemens applications	Path variable `C:\Program Files\Siemens\MotionControl\Siemens\System\etc`
		Path variable `C:\Program Files (x86)\Siemens\MotionControl\Siemens\System\etc`
	Symbolic links set	Symbolic link for `ProgramData\Siemens\MotionControl\addon` to `Program Files` and `Program Files (x86)`
		Symbolic link for `ProgramData\Siemens\MotionControl\oem` to `Program Files` and `Program Files (x86)`
		Symbolic link for `ProgramData\Siemens\MotionControl\user` to `Program Files` and `Program Files (x86)`
		Symbolic link for `Program Files\Siemens\MotionControl\Siemens\system\etc\libsvic.dll` to `...siemens\services\snmp\libsvic.dll`
		Symbolic link for `Program Files\Siemens\MotionControl\Siemens\system\etc\slhw.dll` to `...siemens\services\snmp\slhw.dll`
Other settings	Login script for PCU Installer is written to the group policies of the user group	PCU Installer is executed before desktop is available
	CBS Logs deactivated	Logging from the Microsoft Windows Update Service is disabled.
	MountTCUS.exe in automatic start	
	Full write permission for Users Group set on RunOnce registry key	All entries under this registry key are executed once when logging in. Execution always only at the next login.

A.3 Abbreviations

ASCII	American Standard Code for Information Interchange: American coding standard for the exchange of information
AUTO	AUTO mode: Continuous and automatic execution of programs
CFS	Compressed File System
CIFS	Common Internet File System
DCK	Direct Control Keys: direct keys
DCP	Discovery and Basic Configuration Protocol
DHCP	Dynamic Host Configuration Protocol: dynamic assignment of an IP address and other configuration parameters to a computer in a network
DNS	Domain Name System: conversion of domain names to IP addresses
EES	Execution from External Storage
EUNA	End User Notification Administration
GDIR	Global Directory: Global part program memory
IFP	Industrial Flat Panel
IPC	Industrial PC
IRT	Isochronous Real Time (Ethernet)
ITC	Industrial Thin Client
INI	Initializing Data: Initializing data
JOG	Jogging: Setup mode
LLDP	Link Layer Discovery Protocol: manufacturer-independent Layer 2 protocol, defined according to the IEEE-802.1AB standard and offering the possibility to exchange information between devices
MAC	Media Access Control: In Ethernet networks, the MAC address is comprised of 48 bits in hexadecimal format.
MCP	Machine Control Panel:
MD	Machine data
MPI	Multi Point Interface: multiple-point interface
MUI	Multilingual User Interface
NAT	Network Address Translation
NC	Numerical Control: Numerical control
NCK	Numerical Control Kernel: Numeric kernel with block preparation, traversing range, etc.
NCU	Numerical Control Unit: SINUMERIK control
NFS	Network File System is a network protocol. Synonym: Network File Service
NRT	Non-Realtime (Ethernet)
NTFS	New Technology File System
NTLMSSP	NT LAN Manager (NTLM) Security Support Provider
NTP	Network Time Protocol: standard for synchronizing clocks in the entire network
NTPD	NTP Daemon: Utility program that works in the background and does not have to be started by the user.
PC	Personal Computer
PG	Programming device
PLC	Programmable Logic Control: programmable logic controller
PridaNet	Product Information and Data Net

RAM	Random Access Memory: program memory that can be read and written to
RDY	Ready: The system is ready for operation.
RPC	Remote Procedure Call Synonym: Remote Function Call (RFC)
SD	Setting Data
SD Card	SecureDigital Card
SMB	Server Message Block
SNMP	Simple Network Management Protocol (network protocol for monitoring and controlling network elements such as routers, servers, switches, printers, etc. from a central station).
SSD	Solid State Drive
SSH	Secure Shell: protocol for an encrypted network connection to a remote device
TCU	Thin Client Unit
TFTP	Trivial File Transfer Protocol: very simple data transmission protocol
UDP	User Datagram Protocol: NTP is mostly processed via UDP.
USB	Universal Serial Bus
UPS	Uninterruptible power supply
UTC	Universal Time, Coordinated: (formerly: Greenwich Mean Time)
VNC	Virtual Network Computing
WCS	Workpiece coordinate system
XML	Extensible Markup Language

Index

A

Autologon
  Switch to Service Desktop, 198
Autologon mode, 108
AutoRepeat, 138

B

Backup time, 66
Batch file
  USVShutdown.bat, 59, 60, 63
Batch processing file, (Batch file)
Benefits, 29
BitLocker, 97
  Activate setup, 98
  Activate via script, 101
  Activating via Microsoft Windows, 100
Boot stick, 183

C

Color depth, 55
Command
  control userpasswords2, 109
  sc_show_net, 202
  sc_usb disable, 45
  sc_usb enable, 45
  sc_vncpwd reset, 203
  sc_vncpwd set, 203
Company network
  Defining the password, 203
Configuration file
  Archiving, 36
  basesys.ini, 46, 48, 186
  config.ini, 49
  mmc.ini, 113
  oemframe.ini, 129, 137, 143
  pcuhwsvc.ini, 138, 197
  PCUInst.ini, 144, 146, 147, 148
  servicesystem.ini, 69, 71
  setup.ini, 38
  sinumerikvnc.ini, 203
  slamconfig.ini, 119, 121, 127
  slrs.ini, 114
  slstartup.ini, 200
  systemconfiguration.ini, 115, 117, 121, 132, 134, 137
  tcu.ini, 52, 53, 55, 56, 203
  Templates, 36
Configure for CMC, 154

D

DHCP, 34
Dialog box
  netplwiz, 108
  ServiceCenter Backup/Restore, 69, 71
Directory
  C:\ProgramData, 36
Disk image
  Restoring, 171, 176
  Troubleshooting, 173, 178

E

Emergency Boot System, 183

F

File and printer release, 48

H

Hard disk
  Replacing, 195
HMI software, 143

I

Initialization files, (Configuration file)
Input area scheme, (Keyboard layout)
Installation
  Interactive, 110
  silent, 110
Interface
  Ethernet, 34
  X1, 34
  X2, 34

K

Key, (Repeat function)
  Key filter, 138
Key filter, 138
Keyboard layout, 50, 107
Kiosk mode, (Autologon mode; key filter)

L

Language
  Configuring the keyboard layout, (Keyboard layout)
Language bar, (Keyboard layout)
Log file
  CBS.log, 105
  PCUHardwareservice.log, 139, 140, 141
  PCUInstaller_C.log, 151, 152, 153, 154
  PCUInstaller_S.log, 151, 152, 153, 154
  Setup-specific, 153
Log File, (Log file)

N

Network
  Adapting settings, 44, 69, 71
  Company network, 34
  Domain, 44
  IP address, 44
  System network, 34
Network protocol
  SNMP, (SNMP)
Network release
  Driven on PG/PC, 190
Network security
  Define password for VNC server, 203

O

OEM
  Configuration, 143
OEMFrame application
  configuring, 121
  extended parameterization, 129
  FindWindow program application, 116
  integrating, 121
Operating mode, 197
  Autologon mode, (Autologon mode)

P

Paragon Hard Disk Manager, 158
Password
  Administrator account, 42
  Authentication for SSH encryption, 206
  Configure for VNC server, 203
  For network drive, 179
PCU Installer
  Activating, 144, 146
  Configure for CMC, 154
  Configuring, 147, 148
  Log file, 153, (Log file)
  PCUInst.ini, 148
  Troubleshooting, 146, 152
  Using, 152
Pointer devices
  Activate/deactivate, 57
Portrait and landscape, 56

R

Remote access, 203
  Via VNC server, 203
  With SSH encryption, 205
Run-up
  Operating mode during run-up, 197

S

Screen resolution, 52, 53
Service Center
  Decrypting BitLocker, 181
Service Desktop, 198, 200
Service switch, 197
Service system for PCU Base, 183
Set PG/PC interface, 111
Shutdown, 58
SINUMERIK Operate
  Access level "EXIT" softkey, 120
  Autologon mode, 107
  Changing the design, 118
  Communication settings, 112
  Configuring the display size, 114
  Functional behavior of softkeys "HMI restart" or "EXIT", 119
  Inserting a run-up screen, 120
  installing, 106
  OEMFrame application, 121
  parallel user interfaces, 117

Program FindWindow, 116
starting, 113
Using interactive or silent mode, 109
SITOP UPS, 58
SMB client, 46
Softkey, 143
SSD
Replacing, 195
SSH encryption, 205, 206
Individual, 209
STEP 7, 143

T

Troubleshooting
PCU Installer, 146, 152
Restore failure, 173, 178

U

Uninterruptible power supply, 58
USB flash drive
Deactivate network access, 48
Displaying several partitions, 49
with emergency boot system, 183
USB interface
Activating, 45
Disabling, 45
User account, (Setting up for autologon mode)
Setting up, 41, 42
Setting up for autologon mode, 107
User administration, 42

V

VNC Viewer, 203