SIEMENS

Edition 08/2023

CONFIGURATION MANUAL

SINAMICS

Industrial cybersecurity

SINAMICS converter from firmware V6.2

www.siemens.com/drives

SIEMENS

SINAMICS

Converters
Industrial cybersecurity

Configuration Manual

Introduction 1

Fundamental safety instructions 2

Basic information 3

Security measures in automation and drive technology 4

Security management 5

Operating environment and general security measures 6

System overview 7

Security functions 8

Recommendations for secure operation and secure disposal 9

Security programs 10

Security settings in Startdrive 11

Security settings in the web server 12

Appendix A

Valid for
Firmware from V6.2
Startdrive V18 SP1 or higher

08/2023, FW V6.2
A5E52484547B AB

Legal information

Warning notice system

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

⚠ **DANGER**
indicates that death or severe personal injury **will** result if proper precautions are not taken.

⚠ **WARNING**
indicates that death or severe personal injury **may** result if proper precautions are not taken.

⚠ **CAUTION**
indicates that minor personal injury can result if proper precautions are not taken.

NOTICE
indicates that property damage can result if proper precautions are not taken.

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

Qualified Personnel

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

Proper use of Siemens products

Note the following:

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

Trademarks

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

Disclaimer of Liability

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

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

A5E52484547B AB
Ⓟ 09/2023 Subject to change

Copyright © Siemens AG 2023.
All rights reserved

Table of contents

1 Introduction 9

1.1 About SINAMICS 9

1.2 About this manual 10
1.2.1 Content 10
1.2.2 Sales law 10
1.2.3 Target group 10
1.2.4 Standard scope 10
1.2.5 Websites of third-party companies 11

1.3 SINAMICS documentation 12

1.4 Service and Support 13
1.4.1 Siemens Industry Online Support on the Web 13
1.4.2 Siemens Industry Online Support on the road 13
1.4.3 Getting information about the product 14
1.4.4 Feedback on the technical documentation 15
1.4.5 mySupport documentation 15
1.4.6 Technical support 16
1.4.7 Training 17
1.4.8 Spare parts services 17

1.5 Important product information 18
1.5.1 Open-source software (OSS) 18
1.5.2 Compliance with the General Data Protection Regulation 18

2 Fundamental safety instructions 19

2.1 General safety instructions 19

2.2 Warranty and liability for application examples 20

2.3 Security information 21

3 Basic information 23

3.1 Data security in the industrial environment 23

3.2 Industrial cybersecurity 24

3.3 Functional safety and industrial cybersecurity 25

4 Security measures in automation and drive technology 27

4.1 Security measures 27

5 Security management 29

6 Operating environment and general security measures 31

6.1 Defense in depth concept 31

6.2 Security requirements for the intended operating environment 33

6.3 Plant security 34

6.3.1 Physical protection of critical production areas ... 34

6.4 Network security ... 36
6.4.1 Network segmentation ... 36
6.4.1.1 Separation between production and office networks ... 36
6.4.1.2 Network segmentation with SCALANCE S ... 37
6.4.2 Cloud Security ... 40

6.5 System integrity ... 41
6.5.1 IT infrastructure hardening measures ... 41
6.5.1.1 Services and ports ... 41
6.5.1.2 User accounts ... 41
6.5.1.3 Operating units used in the industrial context ... 42
6.5.1.4 Store sensitive data securely ... 42
6.5.1.5 Transport sensitive data securely ... 43
6.5.1.6 Secure passwords ... 43
6.5.1.7 Virus scanner ... 44
6.5.1.8 Allow lists ... 44
6.5.1.9 Product security notifications ... 45
6.5.2 Patch management ... 45
6.5.2.1 Windows patch management ... 45
6.5.2.2 Program updates in the TIA Portal ... 46
6.5.3 Data integrity ... 47

7 System overview ... 49

7.1 Communications interfaces ... 49
7.1.1 Service interface X127 ... 49
7.1.2 PROFINET interface X150 ... 50

7.2 Communication links ... 51

8 Security functions ... 53

8.1 Security settings ... 53

8.2 Secure network ... 55

8.3 User Management & Access Control (UMAC) ... 56
8.3.1 User management ... 56
8.3.1.1 User management for the drive ... 58
8.3.1.2 User management for engineering in Startdrive ... 62
8.3.2 Access control ... 62
8.3.2.1 Roles for engineering in Startdrive with engineering function rights ... 62
8.3.2.2 Roles for engineering in Startdrive and access to the converter with engineering and runtime function rights ... 63
8.3.2.3 Roles for access to the converter with runtime function rights ... 64
8.3.3 Restoring UMAC settings ... 67
8.3.4 Deactivating UMAC ... 67

8.4 Reduction of the attack surface ... 68
8.4.1 Least functionality of ports and protocols ... 68
8.4.2 Least functionality of hardware reports ... 71
8.4.3 Additional protective measures for hardware reports ... 71
8.4.4 Least functionality of software applications and functions ... 72

8.5 Protected communication channels ... 73
8.5.1 Protecting sensible data when being transferred (data in transit) ... 73

8.5.2 Protection of UMAC data ... 74

8.6 Protected data storage ... 75
8.6.1 Protection of sensitive data when stored (data at rest) ... 75

8.7 System integrity ... 76
8.7.1 Software and information integrity ... 76
8.7.2 Verification of security functions ... 78
8.7.3 Input validation ... 79
8.7.4 Identify and address fault conditions ... 79
8.7.5 Firmware update ... 79
8.7.6 Backup and restore ... 80

8.8 Logging and monitoring ... 82
8.8.1 Monitoring access from untrusted zones ... 82
8.8.2 Logging of events ... 82

9 Recommendations for secure operation and secure disposal ... 83

9.1 Secure operation ... 84

9.2 Secure disposal ... 85
9.2.1 Deletion of customer data on the converter ... 85
9.2.2 Dispose of memory cards securely ... 85

10 Security programs ... 87

11 Security settings in Startdrive ... 89

11.1 Configure access to Startdrive projects in the TIA Portal ... 91
11.1.1 User authentication ... 91
11.1.2 Project lock ... 92
11.1.2.1 Session timeout for local project users ... 93
11.1.2.2 Project lock ... 94
11.1.2.3 Lock project manually ... 94
11.1.2.4 Lock project automatically on inactivity ... 94
11.1.2.5 Remove project lock for local users ... 95
11.1.2.6 Remove project lock for single sign-on users ... 95

11.2 Display settings of the Security Wizard for drives ... 96
11.2.1 Default settings ... 96

11.3 Settings for the drive ... 98
11.3.1 Manually starting the Security Wizard ... 98
11.3.2 User Management & Access Control ... 99
11.3.3 Activating/deactivating ports and protocols ... 100
11.3.4 Drive data encryption ... 101
11.3.4.1 Activate drive data encryption ... 102
11.3.4.2 Configure drive data encryption ... 103
11.3.4.3 Deactivate drive data encryption ... 104
11.3.4.4 Changing the drive password ... 105

11.4 User management and access control (UMAC) ... 106
11.4.1 Fundamentals ... 106
11.4.2 Project protection ... 106
11.4.2.1 Activating project protection ... 107
11.4.2.2 Access without authentication ... 108
11.4.3 Password policy ... 109

11.4.3.1 Configure password policy ... 110
11.4.4 User management ... 111
11.4.4.1 Overview ... 111
11.4.4.2 Creating user accounts ... 112
11.4.4.3 "Anonymous" user ... 113
11.4.4.4 Activate/deactivate user accounts ... 113
11.4.4.5 Changing user accounts ... 114
11.4.4.6 Delete user accounts ... 114
11.4.4.7 Assigning/removing roles ... 115
11.4.4.8 Displaying rights of project users ... 115
11.4.4.9 Change password ... 116
11.4.4.10 Changing the password when a protected project is opened ... 116
11.4.4.11 Changing a password when working in a protected project ... 117
11.4.5 Access control ... 118
11.4.5.1 Adding and configuring roles ... 118
11.4.5.2 Example: Necessary rights for specific activities ... 119
11.4.5.3 Assign/remove rights ... 122
11.4.5.4 Changing roles ... 123
11.4.5.5 Deleting roles ... 123
11.4.6 User login ... 124
11.4.6.1 User login ... 124
11.4.6.2 Error messages and remedies ... 126
11.4.6.3 Changing a user ... 126
11.4.6.4 Logging off a user ... 127
11.4.7 Downloading the UMAC to the device ... 128

11.5 Configuring settings for full protection ... 130
11.5.1 Basic information ... 131
11.5.2 Home page ... 133
11.5.3 Select security configuration ... 133
11.5.3.1 Transferring existing security settings to a new drive and editing them ... 134
11.5.3.2 Transferring existing security settings to a configured drive and editing them ... 134
11.5.3.3 Editing current settings ... 135
11.5.4 Activate User Management and Access Control ... 136
11.5.4.1 Configuring UMAC for project and drive (project protection not activated) ... 137
11.5.4.2 Configuring UMAC for project and drive (project protection already activated) ... 138
11.5.5 Administrator setup ... 139
11.5.5.1 Setting up a project and drive administrator ... 139
11.5.5.2 Creating a new user ... 140
11.5.5.3 Using an existing user ... 141
11.5.6 Configuration of guest access ... 142
11.5.7 Fieldbus communication ... 143
11.5.8 SINAMICS SDI Standard Panel access ... 144
11.5.9 Web server access ... 144
11.5.10 Drive data encryption ... 145
11.5.11 Overview (finishing the configuration) ... 146
11.5.12 Result of the configuration ... 146
11.5.13 Checking assigned roles and rights ... 147
11.5.14 Changing or subsequently adjusting security settings ... 147

11.6 Working with low security settings ... 149
11.6.1 Result of the configuration ... 150

11.7 Backup and restore ... 151

11.8 Certificates for protected communication 152
11.8.1 Fundamentals 152
11.8.2 Certificate types 152

12 Security settings in the web server 155

12.1 Fundamentals 156
12.1.1 Factory settings 156
12.1.2 Activating UMAC from the status bar 157
12.1.3 User login (guest access enabled) 157
12.1.4 User login (guest access deactivated) 158
12.1.5 Changing a user 159
12.1.6 Logging off a user 159
12.1.7 User login after session timeout due to inactivity (guest access activated) 160
12.1.8 User login after session timeout due to inactivity (guest access deactivated) 161

12.2 Settings in the Security Wizard 162
12.2.1 Structure of the Security Wizard 162
12.2.2 Reloading pages of the web server 162
12.2.3 Configuring settings for full protection 163
12.2.3.1 Making basic settings when the web server is called for the first time 163
12.2.3.2 Starting the Security Wizard 163
12.2.3.3 Activating UMAC 164
12.2.3.4 Setting up a user with the "Drive Administrator" role 164
12.2.3.5 Configure guest access 165
12.2.3.6 Web server activation 167
12.2.3.7 Drive data encryption 169
12.2.3.8 Summary 171
12.2.3.9 Changing security settings 172
12.2.4 Working with low security settings 173
12.2.4.1 Modifying security settings 174
12.2.4.2 Protecting the Safety configuration 175

12.3 User management and access control (UMAC) 176
12.3.1 System limits 178
12.3.2 User management 178
12.3.2.1 Creating a new user account 178
12.3.2.2 Editing users 179
12.3.2.3 Editing the "Anonymous" user 180
12.3.2.4 Password policy 180
12.3.2.5 Change password policy 181
12.3.2.6 Changing your own user password 181
12.3.3 Access control 182
12.3.3.1 User roles and access rights 182
12.3.4 Checking UMAC settings 183
12.3.5 Resetting the UMAC settings 183

12.4 Ports and protocols 184
12.4.1 Activating/deactivating ports and protocols 184

12.5 Firmware update 185
12.5.1 Firmware update 185

12.6 Backup and restore 186

12.7 Certificates for protected communication 187

12.7.1 Fundamentals 187
12.7.2 Establish a protected HTTPS connection to the web server 188
12.7.3 Display information about the certificates 192

A Appendix 195

A.1 Additional information 195

Glossary 197

Introduction

1

1.1 About SINAMICS

Description

With the SINAMICS converter series you can solve drive tasks in the low, medium and DC voltage range. All Siemens drive components, such as converters, motors, and controls, are matched to each other and can be integrated into your existing automation systems.

You can find more information via the SINAMICS YouTube playlist (https://www.youtube.com/playlist?list=PLw7lLwXw4H53rtHeTeifKtVMr2aXTYt0X).

1.2 About this manual

1.2.1 Content

Overview

This manual provides an overview of the product-specific security functions for converters with firmware version V6.2 or higher.

This documentation contains information about the secure operation of converters in the intended operating environments, about the configuration of security functions, and about measures to support system hardening.

1.2.2 Sales law

To illustrate possible application areas for our products, typical use cases are listed in this product documentation and in the online help. These are purely exemplary and do not constitute a statement on the suitability of the respective product for applications in specific individual cases. Unless explicitly contractually agreed, Siemens assumes no liability for such suitability. Suitability for a particular application in specific individual cases must be assessed by the user, taking into account all technical, legal, and other requirements on a case-by-case basis. Always observe the descriptions of the technical properties and the relevant constraints of the respective product contained in the product documentation.

1.2.3 Target group

Overview

This documentation is intended for the following target groups:

- Planners and project engineers
- System integrators
- IT department of machine manufacturers (OEM) or end users
- Commissioning engineers

1.2.4 Standard scope

Description

This documentation describes the functionality of the standard scope. This scope 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.

Further functions may be executable in the system, which are not explained in this documentation. However, there is no entitlement to these functions in the case of a new delivery or service.

This documentation does not contain all detailed information on all types of the product. Furthermore, 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.

1.2.5 Websites of third-party companies

Description

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 SINAMICS documentation

Description

Comprehensive documentation on the SINAMICS converter series can be found at Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/en/view/109807358).

You have the option of either displaying the documents or downloading them in the PDF and multimedia format.

The converter documentation essentially comprises the following manuals:

Table 1-1 SINAMICS documentation

Information	Documentation class	Content
Basic information	Operating Instructions	Compilation of all of the information required for secure converter operation
	Product Information	Information that only becomes known shortly before or even after start of delivery and is therefore not included in the associated user documentation
General information	Industrial Cybersecurity Configuration Manual	Information on the security functions and secure converter operation

1.4 Service and Support

1.4.1 Siemens Industry Online Support on the Web

Description

The following is available via Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/en/), among others:

- Product support
- Global forum for information and best practice sharing between users and specialists
- Local contact persons via the contact person database (→ Contact)
- Search for product info
- Important topics at a glance
- FAQs (frequently asked questions)
- Application examples
- Manuals
- Downloads
- Compatibility tool
- Newsletters with information about your products
- Catalogs/brochures

1.4.2 Siemens Industry Online Support on the road

Description



Figure 1-1 "Siemens Industry Online Support" app

The "Industry Online Support" app supports you in the following areas, for example:

- Resolving problems when executing 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 that our experts have drawn up:

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

There is a data matrix code or QR code on the nameplate of your product. Scan the code using the "Industry Online Support" app (https://support.industry.siemens.com/cs/ww/en/sc/2067) to obtain technical information about the device.

The app is available for Apple iOS and Android.

1.4.3 Getting information about the product

Overview

You can use the ID link to get information about your product.

The ID link is a globally unique identifier according to IEC 61406-1.

Requirement

There is a QR code on the product and on the product packaging.



Figure 1-2 QR code with ID link included

You can recognize the ID link by the frame with a black frame corner at the bottom right.

Procedure

Scan the QR code using either a standard code scanner or the "Industry Online Support" app.

When using a standard code scanner, you open the scanned ID link in an Internet browser that is provided on your device.

Result

You can use the ID link to get product data, manuals, declarations of conformity, certificates and other information about your product.

1.4.4 Feedback on the technical documentation

Description

We welcome your questions, suggestions, and corrections for this technical documentation. Please use the "Provide feedback" link at the end of the entries in Siemens Industry Online Support.

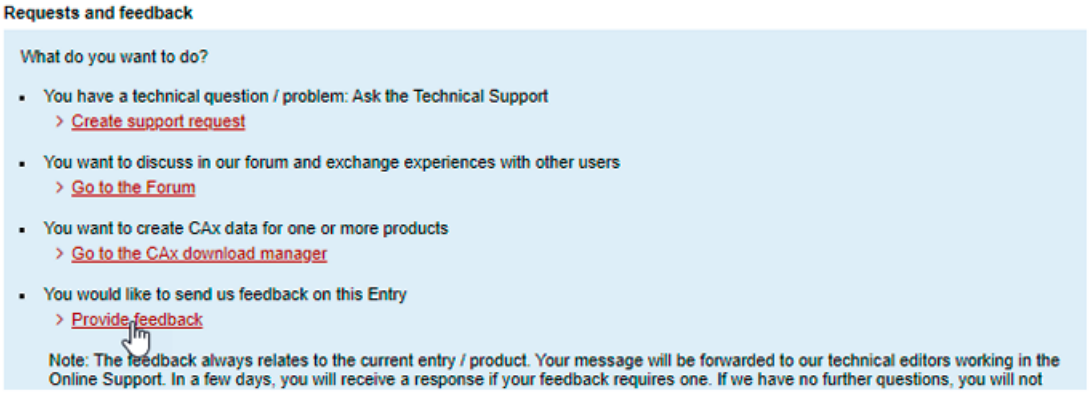


Figure 1-3 Requests and feedback

1.4.5 mySupport documentation

Description

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

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

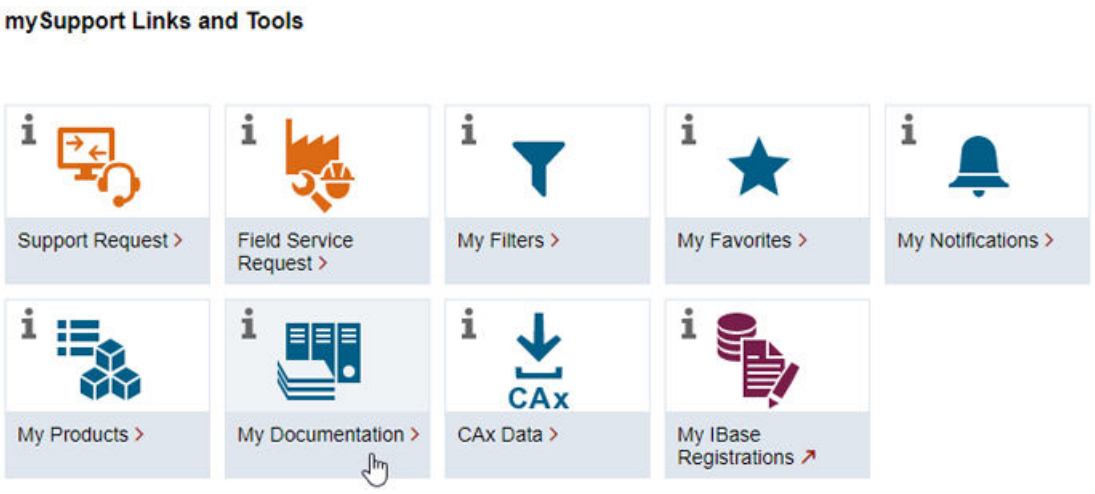


Figure 1-4 mySupport

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

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

1.4.6 Technical support

Description

Your routes to technical support (https://support.industry.siemens.com/cs/ww/en/sc/4868):

- Support Request (https://www.siemens.com/SupportRequest)
- Contact person database (https://www.automation.siemens.com/aspa_app)
- "Industry Online Support" mobile app

The Support Request is the most important input channel for questions relating to products from Siemens Industry. This will assign your request a unique ticket number for tracking purposes. The Support Request offers you:

- Direct access to technical experts
- Recommended solutions for various questions (e.g. FAQs)
- Status tracking of your requests

Technical support also assists you in some cases via remote support (https://support.industry.siemens.com/cs/de/en/view/106665159) to resolve your requests. A Support representative will assist you in diagnosing or resolving the problem through screen transfer.

More information on the Support service packages is available on the Internet via the following address (https://support.industry.siemens.com/cs/ww/en/sc/4869).

1.4.7 Training

Description

SITRAIN – Digital Industry Academy offers a comprehensive range of training courses on Siemens industrial products – directly from the manufacturer, for all industries and use cases, for all knowledge levels from beginner to expert.

More information can be found on the Internet via the following address (https://www.siemens.com/sitrain).

1.4.8 Spare parts services

Description

By using the online spare parts service "Spares on Web", you ensure the smooth operation of your product. The spare parts service is aimed at the following:

- Improved spare parts inventories by balancing stock and spare parts on call
- Minimized downtimes during a plant standstill
- Reduced costs

More information can be found on the Internet via the following address (https://www.sow.siemens.com).

1.5 Important product information

1.5.1 Open-source software (OSS)

Description

The license conditions and copyright information of the open-source software components used by the device are saved on the device itself. You can download license and copyright information onto your PC via the support page of the integrated web server.

1.5.2 Compliance with the General Data Protection Regulation

Description

Siemens complies with the principles of the **General Data Protection Regulation (EU),** in particular the principle of data minimization ("privacy by design"). For this SINAMICS product, this means:

- **User management and access control (UMAC)**
  The product processes or stores the following personal data:
  - Login data for user management and access control:
    User name, group, password, role, rights.

  The data for user management and access control is stored in the converter and optionally on a memory card.
- **Support data (optional)**
  For optimal support in service cases, the end user or machine manufacturer (OEM) can optionally store contact data (header, email address, telephone number, homepage) in the converter.
  If this data is created, the author must give thought to data protection consent for this optional data. Siemens takes no responsibility for this data.
  This support contact data can be read and is freely accessible in, for example, the user interface as well as in the diagnostics report. This data is not encrypted.

This data is used for user management and access control (UMAC) and for the support function. The storage of this data is appropriate and limited to what is necessary, as it is essential to identify the authorized operators and service contact.

The personal data is also available as part of the backup system to ensure fast recovery of use cases.

The above-mentioned personal data cannot be stored anonymously or pseudonymized, as it serves the purpose of identifying the operating personnel. The anonymization or pseudonymization, e.g. of the login data, must be performed using suitable login names and contact data by the plant/machine operator.

Our product does not provide any functions for automatically deleting personal data. Individual UMAC data can be deleted manually by authorized personnel as soon as this is deemed recommended/required.

Fundamental safety instructions 2

2.1 General safety instructions

⚠ WARNING

Danger to life if the safety instructions and residual risks are not observed

If the safety instructions and residual risks in the associated hardware documentation are not observed, accidents involving severe injuries or death can occur.

- Observe the safety instructions given in the hardware documentation.
- Consider the residual risks for the risk evaluation.

⚠ 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 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 specific customer solutions, but are only intended to provide support for 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.

2.3 Security information

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

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

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

For additional information on industrial security measures that may be implemented, please visit
https://www.siemens.com/industrialsecurity.

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

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

Further information is provided on the Internet:

Industrial Security Configuration Manual (https://support.industry.siemens.com/cs/ww/en/view/109810578)

⚠ 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 holistic, state-of-the-art industrial security concept for the installation or machine.
- Make sure that you include all installed products into the holistic industrial security concept.
- Protect files stored on exchangeable storage media from malicious software by with suitable protection measures, e.g. virus scanners.
- On completion of commissioning, check all security-related settings.

Basic information 3

3.1 Data security in the industrial environment

Overview

The topic of data security is becoming increasingly important in the industrial environment, especially due to the worldwide increase in legal requirements for data protection.

Possible threats:

Potential security threats include confidentiality, integrity, and availability. Examples of threats are:

- Espionage of data
- Manipulation of data or software
- Sabotage of production plants
- Plant downtime, for example due to malware

Possible corporate security vulnerabilities

Security vulnerabilities can occur in numerous places in an organization, such as:

- Employees
- Subcontractors
- Production plants and their components
- Network infrastructure
- Cellular and landline end devices
- The use of mobile data storage media (e.g. USB flash drives)

A holistic approach is needed to identify security problems and find solutions. Binding guidelines and regulations must address all relevant areas of a company.

Possible effects of a security incident

- Loss of intellectual property
- Loss of production or reduced product quality
- Negative company image and economic damage
- Catastrophic environmental influences
- Danger to people and machines

3.2 Industrial cybersecurity

Overview

Industrial cybersecurity groups together all measures to protect against:

- Loss of availability; e.g. due to destruction of data or Denial-of-Service (DoS)
- Loss of confidentiality; e.g. due to unauthorized access to data and networks
- Loss of integrity of data and applications due to changes or manipulation following unauthorized access

Protection objectives

- Guaranteed trouble-free operation and availability of production plants and processes
- Prevention of hazards to people and production due to cyber attacks
- Protection of industrial automation systems and components from unauthorized access, manipulation and loss of data
- Protection of industrial communication from espionage and manipulation
- Protection of confidential data from unauthorized accesses

When you implement security measures, make sure that the measures do not impair or endanger the operability of automation systems and components.

Networking and wireless technology

The developments below underscore the relevance of security functions and measures:

- Cloud computing, vertical integration and Internet of Things (IoT):
  Networking is becoming increasingly prevalent within and outside production plants, for example in applications for cloud computing, vertical integration and Internet of Things.
- Wireless technologies:
  The use of wireless technologies in production plants is more and more widespread, for example through the introduction of new WLAN and mobile communication standards.
- Worldwide remote access to plants and machines

To keep networked components and applications running smoothly, your plant needs a network infrastructure and applications that reliably protect against cyber attacks.

3.3 Functional safety and industrial cybersecurity

Safety functions

Safety functions handle the reliable functioning of safety-related components and functions, which must ensure that either the plant remains in a safe state or it is brought into a safe state if a fault occurs.

The highest priority is the prevention of systematic errors and the control of random errors or failures.

Functional safety guarantees the safety of persons and goods in the immediate vicinity of a component.

Security functions

Security functions and measures maintain the expected system behavior by protecting against cyber attacks or unintended manipulation.

Cyber attacks and threats potentially leading to the failure of a component occur throughout the life cycle. For this reason security functions and measures must be regularly evaluated and adapted.

Security measures in automation and drive technology

4

4.1 Security measures

Integration of security into the products

The following measures ensure the integration of security in current Siemens products for automation and drive technology:

- The "Secure product development lifecycle requirements" specified in IEC 62443-4-1 are implemented. The implementation was certified by TÜV.
- Code analyses are used to identify any errors. Code analyses run automatically.
- Siemens implements measures to safeguard integrity in its products and its manufacturing processes.
- Siemens constantly checks the measures relating to hardening:
  - Operating systems are configured in such a way that points of attack, e.g. via ports of unneeded services, are minimized.
  - Siemens tests its products to detect weak points at an early stage.
  - Siemens offers a focused hotfix/patch management service.

Protection of the development infrastructure and supply chain

As manufacturer of automation and drive products, Siemens supports secure operation of products by securing the development infrastructure and supply chains:

- Siemens ProductCERT (Cyber Emergency Readiness Team) is the central department for security-related incidents in the Siemens product and solution environment. Siemens ProductCERT supports development work with consulting and other services. Siemens ProductCERT makes information available on the Internet about current threats and vulnerabilities as well as the appropriate countermeasures:
  Siemens ProductCERT (https://www.siemens.com/cert)
- Industrial cybersecurity is a dynamic and complex subject that requires continuous monitoring, the adaptation of existing security measures and the introduction of new security measures. Information on how Siemens protects its products against cyber attacks can be found on the Internet.
  Securing Digitalization (https://securing-digitalization.dc.siemens.com)

Provision of patches, security components, and appropriate services

As manufacturer of automation and drive products, Siemens supports secure operation through direct support of system integrators and operating companies by providing patches, security components and the appropriate services:

- Siemens offers monitoring through a SIEM system to monitor residual risk. SIEM stands for Security Information and Event Management and has become an established term in IT security. Such systems are able to identify and evaluate security-relevant events and notify the system administrator.

Standards and regulations

Siemens takes the applicable industrial cybersecurity standards and regulations into consideration throughout the entire development process:

- ISO 2700X: Management of information security risks
- IEC 62443-4-1: Security for industrial automation and control systems: Secure product development lifecycle requirements

More information

More information on certifications and standards in the industrial cybersecurity field can be found on the Internet:

Certifications and standards (https://new.siemens.com/global/en/products/automation/topic-areas/industrial-security/certification-standards.html)

Security management

5

Overview

A security management process according to IEC 62443 and ISO 27001 forms the basis for implementation of industrial cybersecurity.

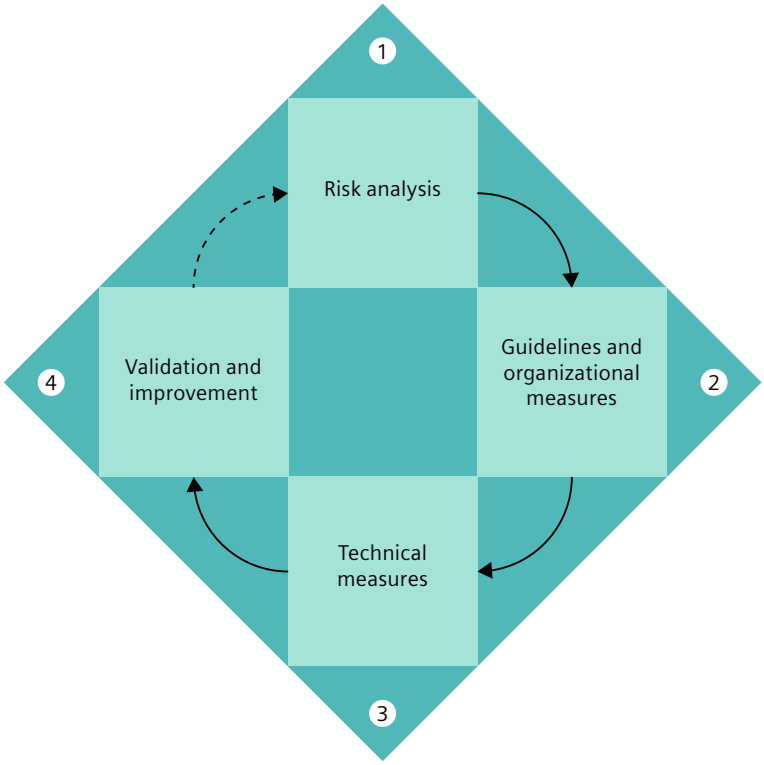


Figure 5-1 Security management process

Procedure

1. Carry out an information security risk analysis. Determine all potential risks and define countermeasures for reducing the risk to an acceptable level.
   An information security risk analysis includes the following steps:
   - Identification of threatened objects
   - Analysis of value and potential for damage
   - Threat and weak point analysis
   - Identification of existing security measures
   - Risk evaluation
   - Evaluation of effects with respect to protection goals: confidentiality, integrity, and availability
2. Define guidelines and introduce coordinated, organizational measures.
   Establish awareness of the high relevance of industrial cybersecurity at all levels in the company. Define guidelines and processes for a consistent approach to security compliance.
3. Introduce coordinated technical measures.
4. Conduct a security audit to ensure that all of the measures have been implemented and that they have also eliminated or reduced the identified risks.

Note

Continuous process

Due to ever-changing threat scenarios, this process must be constantly repeated. Implement the security management process as a continuous process.

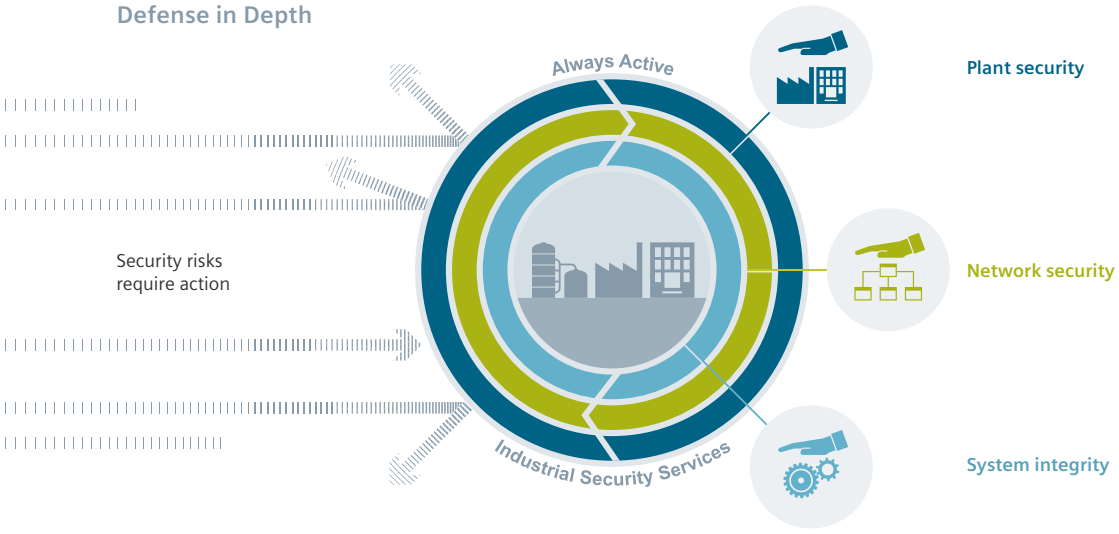
Operating environment and general security measures

6

6.1 Defense in depth concept

Overview

Defense in depth is the name of a general concept for deeply layered defense against cyber attacks and risks following the recommendations of IEC 62443.



Description

Digitalization and the increasing networking of machines and industrial plants are also increasing the risk of cyber attacks. To protect industrial plants and systems comprehensively against cyber attacks, measures must be applied simultaneously at all levels. From the operational up to the field level – from access control to copy protection.

Defense in depth addresses the following levels:

- **Plant security**
  Plant security uses various methods to secure the physical access of persons to critical components. This begins with the classical building entrance and extends to the safeguarding of sensitive areas using code cards.
- **Network security**
  Network security includes all measures taken to plan, implement and monitor security in networks. This includes the control of all interfaces, e.g. between the office network and automation network, or remote maintenance access.
- **System integrity**
  PC-based systems and the control and field level must be protected against cyber attacks. Steps include the following measures:
  - Integrated access protection to prevent unauthorized configuration changes using engineering tools or during maintenance.
  - Protection of communication against unauthorized manipulation to ensure high plant availability.
  - Use of antivirus software and allowlists to protect PC systems against malware.
  - Maintenance and update processes to keep the automation and drive systems up to date.

More information

More information on the defense in depth concept and the planning of a protection concept for industrial plants can be found on the Internet (https://new.siemens.com/global/en/products/automation/topic-areas/industrial-security.html).

We recommend that our customers make their employees aware of security risks (e.g. phishing attacks) through regular measures (e.g. training).

6.2 Security requirements for the intended operating environment

Converters are component parts of a machine, production plant or building infrastructure. They must only be operated in protection cells which are protected in accordance with the defense in depth concept.

6.3 Plant security

Unauthorized persons may be able to enter the production site/building and damage or alter production equipment as a result of gaps in a company's physical security. Confidential information can also be lost. Company locations and critical production units must therefore be protected using suitable measures.

6.3.1 Physical protection of critical production areas

Overview

The physical protection of critical production areas consists of two parts:

- Company security
- Production security

Company security

Company security must be ensured by taking the following measures:

- Closed off and monitored company premises
- Access controls with locks, code cards, security personnel
- Escorting of external personnel by company employees
- Security processes in the company are taught and followed by all employees

Production security

For the products described in this manual, production security must be ensured by taking the following measures, for example:

- Separate access controls for critical production areas
- Installation of critical components in lockable control cabinets/switching rooms
  Control cabinets/switching rooms must be secured with locks and must have monitoring and alarm signaling options. Do not use simple locks, such as universal, triangular/square or double-bit locks.
- Protection of power and data cables
  The flow of power and data between the converter and other drive components must be protected from manipulation, for example the cutting of cables.
- Configuration of the radio field to restrict the WLAN range so that it is not available outside the defined areas.
- Guidelines for the use of mobile data storage media, e.g. USB flash drives and memory cards
- Guidelines for the use of operating unit, e.g. PG/PC or mobile end devices

More information

More information on integrated Siemens security solutions can be found on this website (https://new.siemens.com/global/en/products/buildings/security/security-management.html).

6.4 Network security

Network security includes all measures taken to plan, implement and monitor security in networks. This includes the control of all interfaces, e.g. between the office network and automation network, or remote maintenance access.

6.4.1 Network segmentation

6.4.1.1 Separation between production and office networks

Overview

The strict separation of production networks from the other company networks allows you to create protection areas for your production networks.

Note

The products described in this manual must only be operated in defined protection areas.

Cell protection concept

The cell protection concept segments a production network into individual protection cells, between which all components communicate with each other in a protected way. This is a way of restricting threats and security incidents to individual cells. Cell protection reduces the vulnerability of the entire production plant and thereby increases its availability.

General security measures

Implement the general security measures within protection areas.

More information is provided in section "Reduction of the attack surface (Page 68)".

Firewall systems

In the simplest scenario, separation is achieved by means of an individual firewall system which controls and monitors communication between networks.

DMZ network

A separate DMZ network provides a more secure link between production and office networks. Here, firewalls prohibit direct communication between production and office networks. Communication only takes place indirectly over servers in the DMZ network.

Note

Production networks should also be divided into individual protection cells in order to protect critical communication mechanisms.

6.4.1.2 Network segmentation with SCALANCE S

Overview

To meet the security requirements for network protection and network segmentation, Siemens offers SCALANCE S Industrial Cybersecurity Appliances.

Requirement

Upstream SCALANCE S Industrial Cybersecurity Appliances are housed in a secured control cabinet/electrical room together with the converter components being protected. This ensures that data cannot be manipulated here unnoticed.

Description

SCALANCE S Industrial Cybersecurity Appliances have the following features and characteristics:

- Stateful inspection firewall
  For user-specific control and logging, firewall rules can be specified that only apply to certain users.
- Data encryption and authentication
  Using VPN via IPsec, a VPN tunnel can be established for secure data transfer between authenticated users.
- Address translation with NAT/NAPT
- Router functionality for broadband Internet access
- Connection to the demilitarized zone (DMZ)
  Components such as the SCALANCE S623 have an extra VPN port for secure connection to the DMZ for service and remote maintenance purposes.
- Protection of different network topologies
  Components such as the SCALANCE S615 have 5 Ethernet ports which can be used to protect different network topologies by firewall or VPN (IPsec and OpenVPN).

Application example

The following application example shows cell segmentation by several SCALANCE S modules, each of which is upstream of the automation cells. The data traffic to and from the devices within automation cells can be filtered and controlled with the SCALANCE S firewall. If required, the traffic between the cells can be encrypted and authenticated.

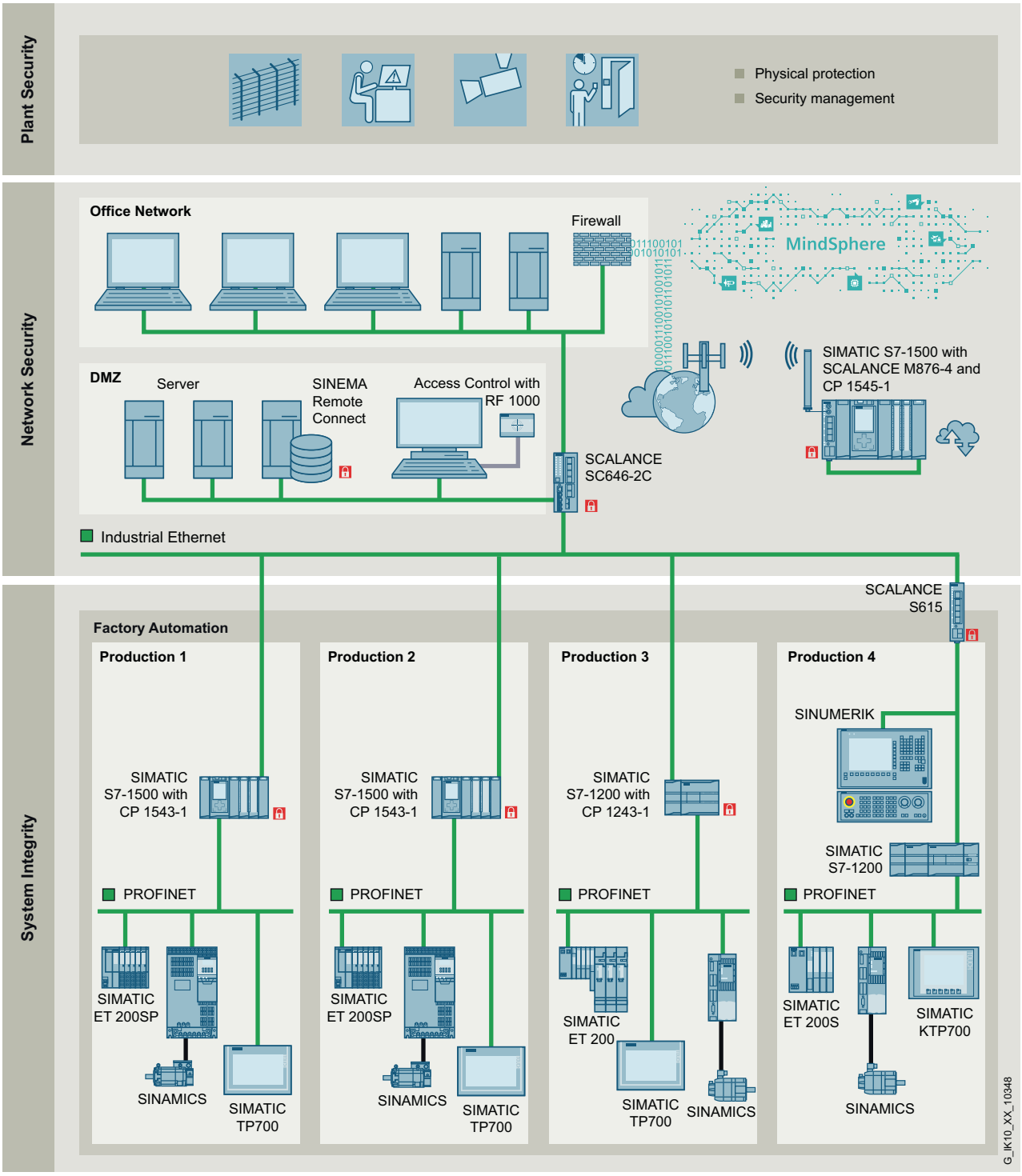


Figure 6-1 SCALANCE S application example

More information

You can find more information on SCALANCE S Industrial Security Appliances on the Internet:

Network security with SCALANCE S Industrial Cybersecurity Appliance (https://new.siemens.com/global/en/products/automation/industrial-communication/industrial-ethernet/network-security/scalance-s.html)

6.4.2 Cloud Security

Overview

The number of cloud applications is constantly increasing. That makes security measures in the cloud environment more important.

Initial orientation

The following addresses are designed to give you a general idea of how you can secure your system in the cloud environment. Inform yourself about the applicable requirements and tried and tested solutions and best practices.

- Center for Internet Security (CIS) (https://www.cisecurity.org)
  - CIS Controls Cloud Companion Guide
- Cloud Security Alliance (CSA) (https://cloudsecurityalliance.org)
  - Cloud Controls Matrix
  - Top Threats

Siemens cloud solutions

The following addresses provide information about Siemens cloud management solutions.

- Industrial Cloud Computing (https://www.plm.automation.siemens.com/global/en/our-story/glossary/industrial-cloud-computing/58773)
- MindSphere (https://www.plm.automation.siemens.com/global/en/products/mindsphere/)

6.5 System integrity

System integrity is understood to mean the "integrity" or "correctness" of the data or the correct response of the system. System integrity protection measures ensure that the data and functionality of the system cannot be manipulated by unauthorized persons and that manipulations can be detected.

6.5.1 IT infrastructure hardening measures

6.5.1.1 Services and ports

Recommendations

Activated services and ports represent a risk. To minimize the risk, only the necessary services for all of the automation components should be activated. More information about the configuration options for ports and protocols can be found in section "Least functionality of ports and protocols (Page 68)".

Ensure that all activated services are taken into account in the security concept. In particular: Web server, FTP, remote maintenance.

More information

You will find more information about the ports which are used in a converter in the following documentation for the product in question.

- Equipment manuals
- Operating Instructions

6.5.1.2 User accounts

Recommendations

Any active user account that allows access to the system is thus a potential risk. Therefore, take the following security measures:

- Use secure access data for user accounts. In particular, this includes assigning secure passwords.
- Reduce the number of user accounts to the necessary minimum. Deactivate or delete user accounts that are no longer being used.
- Only assign the necessary authorizations to user accounts.

6.5.1.3 Operating units used in the industrial context

Recommendations

Operating units (such as PG/PCs, tablet PCs and smartphones) used in the industrial context must meet the generally applicable security requirements.

To minimize risk, take the following security measures:

- The deployed operating unit is set up, administered, regularly checked and patched by the appropriate departments. In terms of the safe configuration of an operating unit, this means:
  - Programs and operating systems are installed on the operating unit only if they are supported and regularly serviced by the manufacturer.
  - Security updates and patches for the installed operating system are regularly installed on the operating unit.
    You can find more information on patch management in Windows operating systems in section "Windows patch management (Page 45)".
  - A virus scanner is installed on the operating unit and regularly updated. In addition, the following measures can be applied: "Allow lists (Page 44)" and methods of the "Network segmentation with SCALANCE S (Page 37)".
  - A firewall with appropriate settings is activated on the operating unit.
  - To protect sensitive data against unauthorized access, storage media (e.g. hard disks, SSD, eMMC) are encrypted.
  - To prevent unintended changes to the configuration, only system administrators should have administrator rights to the operating unit.
- Only use the deployed operating unit in protected cells. The operating unit must not be used in the office network or via the Internet.
  You can find more information about the separation of the office and automation networks in section"Network security (Page 36)".
- Secure PG/PCs against data theft using a lock or do not leave them unmonitored.
- Make sure that the screen of the operating unit is automatically locked if there is no activity.
- Disable interfaces that are not required, such as USB ports.

6.5.1.4 Store sensitive data securely

Recommendations

Examples of sensitive data stored on an operating unit include access data, project data and confidential data containing company secrets.

Ensure secure data storage when saving sensitive data on the operating unit.

To minimize risk, take the following security measures:

- Consistently mark your documents according to confidentiality levels by introducing a document classification.
- Store sensitive data on an operating unit or on network drives in encrypted form only.

- Protect your encrypted storage locations against unauthorized access and manipulation.
- Regularly back up the sensitive data. Protect the backups against unauthorized access, loss and manipulation.

6.5.1.5 Transport sensitive data securely

Recommendations

To minimize risk, take the following security measures:

- Only send sensitive data when absolutely necessary. Only use encrypted and signed emails or storage media with encryption. The storage media, such as USB flash drive or external hard disk, used to send the data must be regularly checked for viruses.
- Only transport sensitive data on a storage medium with encryption. The storage media, such as USB flash drive or external hard disk, used to transport the data must be regularly checked for viruses.

6.5.1.6 Secure passwords

Recommendations

NOTICE
Damage to components from data misuse Data can be easily misused by using passwords that are not secure enough. Attackers can use compromised access data to log into systems and manipulate the behavior of the drive. This can result in damage to components. • Develop guidelines for password renewal. Base the guidelines on the specifications of the national institutions for security and information technology. • Develop guidelines on handling access data. Make sure that the guidelines are implemented consistently in the deployed engineering tools. • Always keep the access data secret and make sure only an authorized group of people is given access to the data.

Observe the following guidelines when assigning new passwords:

- Do not assign passwords that can be easily guessed, e.g. words, simple key combinations on the keyboard.
- Passwords must always contain a combination of upper-case and lower-case letters as well as numbers and special characters. PINs must comprise an arbitrary sequence of digits.
- Assign passwords with the required minimum length.
- When assigning a password, always ensure you are adhering to the applicable company specifications, e.g. special password policy of the respective company.

Password management programs can be used to generate, save and manage passwords and PINs according to configurable rules.

More information

The German Federal Office for Information Security (BSI) (https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html) provides additional rules for creating secure passwords.

6.5.1.7 Virus scanner

Description

Antivirus programs and virus scanners are applications which detect, block and remove known computer viruses, computer worms, Trojan horses and other malware. Therefore, virus scanners do not protect against all malware and are only regarded as a supplement to general security measures.

Recommendations

Antivirus programs must not impair operation of the production plant.

Do not switch off an infected operating unit if that causes a loss of control of the production process.

To minimize risk, take the following security measures:

- Do not use online virus scanners:
  If you use an online virus scanner, confidential data can get into the wrong hands. Generally, therefore, do not use an online virus scanner.
- Up-to-date virus definitions:
  Make sure that the virus definitions in the database of your virus scanner are up to date at all times.
- Do not install multiple virus scanners:
  Avoid installing multiple virus scanners simultaneously on a single system.
- Connection to the production network:
  Only connect to the production network using an operating unit with virus protection.

6.5.1.8 Allow lists

Description

Allowlists are lists of applications that have been classed as trusted in a review.

These lists are used to decide which applications can be run on an operating unit. They provide protection against:

- Malware
- Unauthorized changes to installed applications and executable files (.exe, .dll)

6.5.1.9 Product security notifications

Recommendations

The threat scenarios for cyber attacks are diverse in nature and are continually changing.

Therefore, always keep yourself up to date about new and relevant product security announcements for your products: "Industry Online Support (https://support.industry.siemens.com/cs/ww/en/sc/4868)". Comply with the instructions provided in the product security notifications.

Siemens ProductCERT (https://www.siemens.com/cert) (Cyber Emergency Readiness Team) is the central department for security-related incidents in the Siemens product and solution environment. Siemens ProductCERT supports development work with consulting and other services. ProductCERT provides information about current threats and vulnerabilities as well as the appropriate countermeasures.

6.5.2 Patch management

6.5.2.1 Windows patch management

Description

NOTICE
Data manipulation through security vulnerabilities in the operating system Microsoft does not provide any automatic security updates, service packs or hotfixes for operating systems < Windows 10. This can leave the operating system with dangerous security vulnerabilities. • If you are using an operating system < Windows 10, take additional measures to protect the operating system. • If possible, always upgrade the operating system of your operating unit to the current version.

The **WSUS** (Windows Server Update Service) system functionality provided by Microsoft is available for Windows operating systems.

WSUS supports system administrators by rolling out Microsoft updates in large local networks. WSUS automatically downloads update packages and offers them to the Windows clients for installation. The automated update process ensures that the latest system and security updates are installed on the Windows clients.

Before installing system and security updates, please note the following points:

- Perform a system backup.
- System administrators must ensure that system and security updates do not impair the operability of production plants.
- Do not establish a direct Internet connection to the WSUS server! Ensure that the environment is secure and install an intermediate layer (e.g. DMZ network, firewall, SCALANCE S modules, etc.).

More information

You can find more information about network segmentation in section "Network segmentation (Page 36)".

6.5.2.2 Program updates in the TIA Portal

Description

If you have installed the TIA Portal on your operating unit (PG/PC, Notebook), you can start a search for program updates in the TIA Portal at any time. New versions of individual TIA Portal applications are displayed and can be installed. Installing a new version also fixes security vulnerabilities.

Also activate automatic notifications to receive information about available program updates.

Before installing program updates, please note the following points:

- Do not establish a direct Internet connection to the TIA Portal Update Server! Ensure that the environment is secure and install an intermediate layer (e.g. DMZ network, firewall, SCALANCE S modules, etc.).

More information

You can find more information about network segmentation in section "Network segmentation (Page 36)".

6.5.3 Data integrity

Description

NOTICE
Damage to data and the resulting malfunctioning of the system For automation and drive systems as well as controller components, data such as backups and programs can be imported from external sources. This data influences the behavior of these systems and should therefore be protected against unauthorized changes. Data such as backups, programs, and Technology Extensions can also be saved and archived. The systems currently do not provide the capability of ensuring the integrity of programs, backups, and Technology Extensions. Therefore take your own measures for ensuring integrity to guarantee the data integrity of your backups, Technology Extensions, or other saved data: • Apply the Siemens Industrial Holistic Security Concept: Siemens Industrial Holistic Security Concept (https://securing-digitalization.dc.siemens.com/). • Use digital signatures to protect data. • Ensure there is sufficient access protection: – Restrict access rights such as to data archives/Sharepoints accordingly. – Do not send any unencrypted/unsigned emails.

Data integrity is understood to mean the correctness (integrity) of data and the correct functioning of systems. Ensuring the integrity of the data is thus an essential goal of information security. Integrity protection should not be confused with protecting the confidentiality.

System overview

7

7.1 Communications interfaces

Overview

Communications interfaces are vulnerable mainly because they are necessarily highly visible, so it is extremely important to protect them and the data and services associated with them. Effective interface security must therefore ensure that only authorized identities are allowed access and that sensitive company data is protected from unauthorized accesses.

Description

Interface	Standard	Factory default settings	
		IP address	Subnet mask[1)]
Service interface X127	Ethernet	169.254.11.22	255.255.0.0
PROFINET interface X150	Industrial Ethernet	0.0.0.0	0.0.0.0

1) The IP addresses of the service and PROFINET interfaces must not be in the same subnet.

Regardless of the device to which a converter is connected over a network, the security measures relating to protection against physical access must be implemented: "Protection against physical access (Page 34)".

7.1.1 Service interface X127

Service interface X127

Converters can be connected to an operating unit via service interface X127. The following applies:

- The interface is intended for commissioning and diagnostics, which means that it must always be accessible.
- The SINAMICS Smart Adapter establishes a WLAN connection between service interface X127 of the converter and the operating unit.
- Only local networking in a closed and locked electrical cabinet is permissible

Security features

- Data transmission over HTTP is deactivated in the factory settings.

  ⚠ WARNING

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

  The HTTP protocol transmits data in unprotected form. This makes it easier to eavesdrop on sensitive data such as login data. This allows people to access the converter without authorization and manipulate data. As a result of incorrect or changed parameter assignment, the machine can malfunction, which in turn can lead to injury or death.

  - Only use connections with the HTTPS protocol for access so that all data is transferred in protected form.

  Data transmission over HTTPS is activated in the factory settings.

- Access via the engineering tools Startdrive and/or web server is activated by default. Access is configured in the wizard for security settings and on the Protection & Security page.

7.1.2 PROFINET interface X150

PROFINET interface X150

Converters are connected to several components, such as an operating unit or a higher-level control system, via PROFINET interface X150.

Security measures

The network at the PROFINET interface X150 must be in a secure protection area (see section "Network security (Page 36)"). Access to cables and open connections must be implemented in a protected fashion, such as in a control cabinet.

7.2 Communication links

Overview

Different communication protocols are used for data transfer between converters and components or operating units. The following graphic is a schematic representation of the possible connections and communication links.

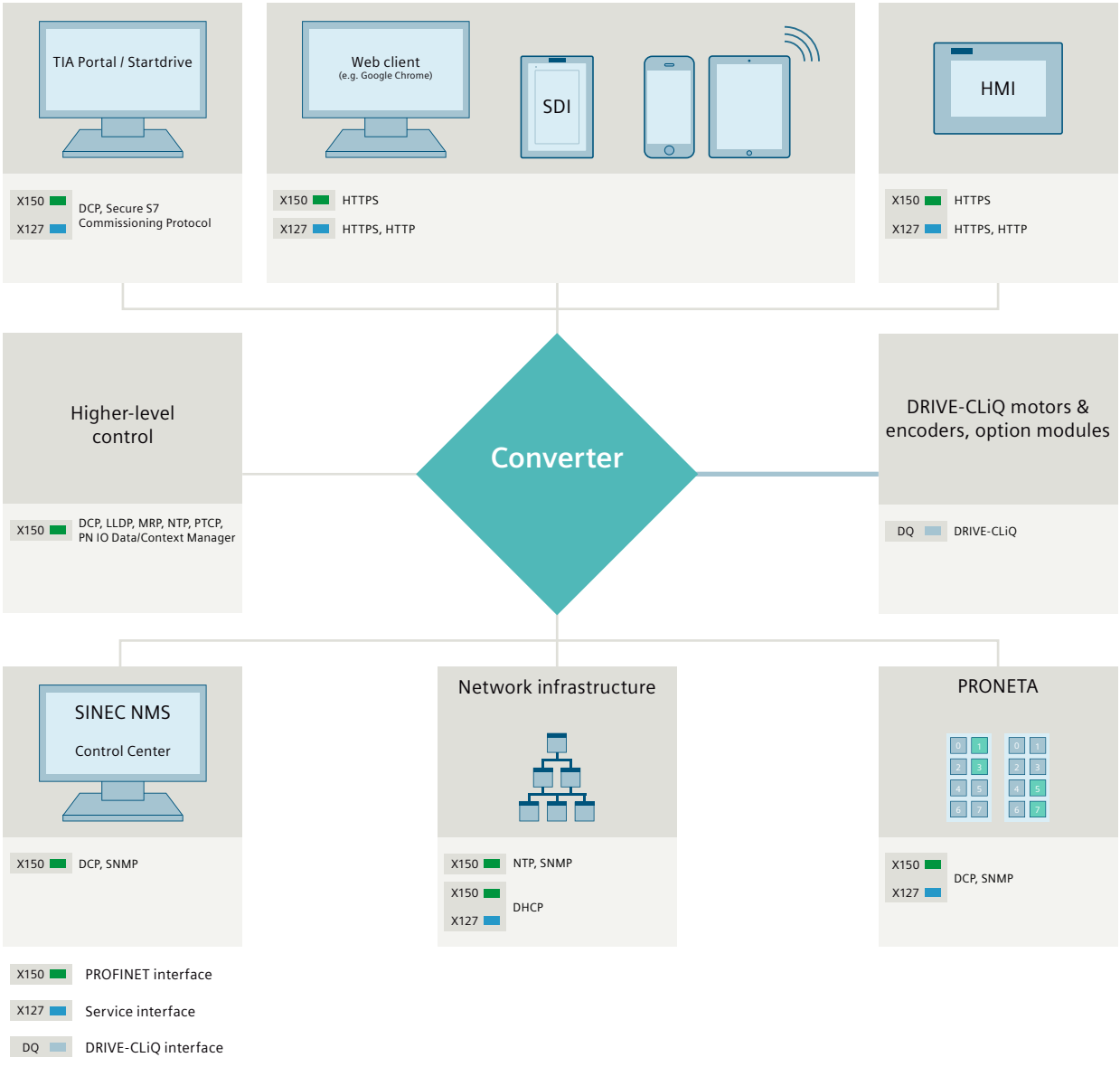


Figure 7-1 Communication links

More information

You can find more information about the protocols and interfaces used by a converter to communicate, and about the default firmware settings, in section "Least functionality of ports and protocols (Page 68)".

Security functions

8

8.1 Security settings

Description

This subchapter provides a general overview of the configuration of security settings for engineering in Startdrive itself and additionally for the configuration of security settings of the drive via Startdrive and via the web server.

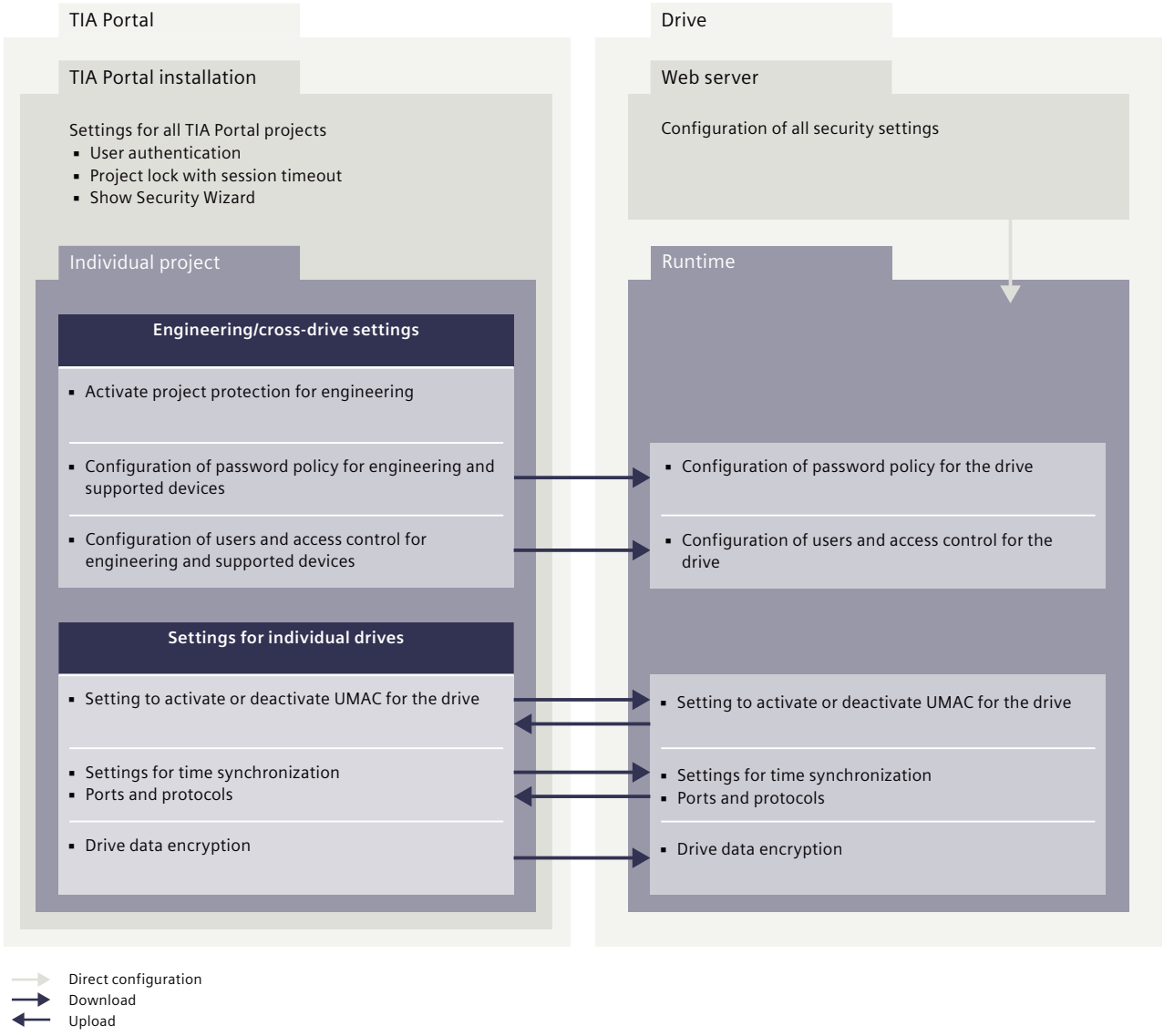


Figure 8-1 Security settings in the commissioning tools

To understand the security functions, it is important to distinguish between:

- the engineering process in Startdrive and its configuration of the security functions
- the behavior of the drive and the configuration of the security functions (e.g. via Startdrive or the web server)

The following security settings are available for the engineering process in Startdrive:

- Security settings that apply to all projects
  - User authentication: Standard procedure for user login when starting a project in Startdrive (see sections "User Management & Access Control (UMAC) (Page 56)" and "User authentication (Page 91)")
  - Project lock with session timeout (see sections "User Management & Access Control (UMAC) (Page 56)" and "Project lock (Page 92)")
  - Default settings for the Security Wizard (see section "Display settings of the Security Wizard for drives (Page 96)")
- Security settings that apply to individual projects
  - Project protection: Activating authentication and access control for the engineering process (see section "Project protection (Page 106)")
  - Configuration of users and access control for the engineering process and supported devices (see sections "User management (Page 111)" and "Access control (Page 118)")
  - Configuration of the password policy for engineering and supported devices (see sections "User Management & Access Control (UMAC) (Page 56)" and "Password policy (Page 109)")

The following security settings are available for the behavior of the drive:

- Configuration of user and access control (see sections "User management for the drive (Page 58)" and "User management and access control (UMAC) (Page 176)")
- Configuration of the password policy (see sections "User management for the drive (Page 58)" and "Password policy (Page 180)")
- Drive data encryption (see section "Drive data encryption (Page 169)")
- Settings for time synchronization (see section "Logging and monitoring (Page 82)")
- Ports and protocols (see section "Ports and protocols (Page 184)")
- Setting to activate/deactivate UMAC for the drive (see section "Activating UMAC (Page 164)")

These security settings can be configured both via Startdrive and via the web server.

When configuring these security settings via Startdrive, there is the great advantage that the configuration of user and access control and the configuration of password policies can be set across the board for all drives in the project.

8.2 Secure network

Network security includes all measures taken to plan, implement and monitor security in networks. This includes the control of all interfaces, e.g. between the office network and automation network, or remote maintenance accesses.

Concerning network security, it is assumed that the protective measures from the following section are implemented: "Network security (Page 36)".

8.3 User Management & Access Control (UMAC)

User Management and Access Control (UMAC) for the TIA Portal

TIA Portal allows you to use User Management and Access Control (UMAC) for projects. This means you can create and manage user accounts and roles in your project. The roles bundle different access rights for the project. In this way, different users can be given different access rights for functions. Once project protection has been activated, the project can only be opened and edited by authorized users.

User Management and Access Control (UMAC) for the drive

The drive offers the possibility to use User Management and Access Control (UMAC). This allows you to create and manage user accounts and roles in your project. The roles bundle different access rights for the drive. In this way, different users can be given different access rights for functions. After activating User Management and Access Control, the drive can be accessed via all communication protocols by authorized users only (e.g. via Startdrive or a web client).

The activated User Management and Access Control on the drive acts completely independently of an activated User Management and Access Control in a TIA Portal project.

8.3.1 User management

Description

User management includes the creation, use, grouping, modification and deletion of users/user data as a basis for access control. For the administration of user accounts, at least one user must be designated who is formally assigned the Administrator role. The Administrator role should only be assigned to persons who are trustworthy following an appropriate risk analysis.

Who defines the Administrator role?

The system integrator is responsible for the formal definition of users with Administrator role. The system integrator must also decide whether and to what extent the operating company is allowed to access user management.

Predefined user accounts and access data

With Startdrive, there are no predefined project users or passwords for new projects. There are no predefined users or passwords for the drive when it is delivered.

Administration functions

The following administration functions are available to Administrators in the Startdrive and web server engineering tools:

- Manage user accounts
  - Create user accounts

    Note

    Maximum number of configurable user accounts

    Up to 64 user accounts can be created and configured per converter.

  - Activate/deactivate user accounts
    Deactivated user accounts can be reactivated at any time. The assigned roles and rights as well as login information are retained.
  - Delete user accounts
  - Configure user accounts
  - Assigning roles to users
- Password management
  - Assign/change passwords
  - Configure password policy
    Administrators can define the structure and complexity of the passwords.
  - Configure password aging
- Session timeout on inactivity
  - Configure session timeout
- Configure user-defined roles (only in Startdrive)

Who-does-what matrix

To consistently apply the principle of least privilege, we recommend creating a who-does-what matrix before any user accounts are created. The necessary user accounts are then set up in user management (UMAC) according to the defined user profiles.

Changing passwords

- Startdrive engineering tool:
  Users can each change their own password. Users with the engineering role "Engineering-Administrator" or the function right "Manage users and roles" are able to change all users' passwords. Changed UMAC data can only be loaded to the converter with the "Drive Administrator" role or the runtime function right "Manage users and roles".
- Web server engineering tool:
  Users can each change their own password. Users with the "Drive Administrator" role or the runtime function right "Manage users and roles" can change the passwords of all users.

When are passwords overwritten?

Passwords are overwritten in the following cases:

- Users change their own password
- Administrators change the password of a user

When is the complete UMAC configuration in the drive changed/deleted?

- Download the UMAC configuration to the drive (download from Startdrive)
- Firmware downgrade
- Resetting all user-defined settings to factory settings
  You can find more information in section "Deletion of customer data on the converter (Page 85)".
- Restoring drive settings from a data backup (via web server or SD card)

User types in Startdrive

The following user types exist in Startdrive:

- Local users (project users) are created separately in each project.
- Global users are managed centrally in a user management server.

More information

More information about user types in Startdrive can be found in the TIA Portal information system (Help).

You can find more information about user roles and rights and their assignment in section "Access control (Page 62)".

8.3.1.1 User management for the drive

Overview

Users of the converter can be managed via Startdrive and the integrated web server (see section User management (Page 56)).

Description

The following configuration options are available for accessing the drive:

Function	Description	
Password complexity	Default configuration	• Activated • Configurable
	Default settings	• Minimum password length: 8 characters • Minimum number of digits (0-9): 1 • Minimum number of special characters: 0 • At least one uppercase letter and one lowercase letter: Yes
	Configurability	Settings are **globally** configurable for all user accounts except the "Anonymous" user.
	Authorization	• Any user with the function right "Manage users and roles"
	Valid values	• Minimum password length: 8 to 32 characters • Minimum number of digits (0-9): 0 to 32 • Minimum number of special characters: 0 to 32 • At least one uppercase letter and one lowercase letter: Yes / No
	Recommendations	We recommend assigning complex passwords with at least 12 characters and limiting the number of user accounts to the necessary minimum.
Renew password	Default configuration	• Not activated • Configurable if activated
	Default settings	• Password valid: – • Advance warning time for expiring password: – • Number of last used locked passwords: 5
	Configurability	Settings are **globally** configurable for all user accounts except the "Anonymous" user.
	Authorization	• Any user with the function right "Manage users and roles"
	Valid values	• Password valid: 1 to 365 days • Advance warning time for expiring password: 0 to 365 days • Number of last used locked passwords: 1 to 10
Concealment of passwords	Passwords are concealed when login data is defined or requested. To check the data entered, the user can see it in plain text by clicking on the eye icon.	
Concealment of error messages	Error messages about incorrect input contain no information indicating which inputs or parts of the inputs are valid or invalid. This conceals the reason why the login failed.	
Limitation of failed login attempts	Configurability: The number of failed login attempts during user authentication is **not limited and not configurable**.	

Function	Description	
Transfer of login data	For data transmission between the converter and the web server, communication via HTTPS is activated by default. In this case, the login data is transferred via the HTTPS connection in protected form. However, the login data is transferred in unprotected form with the HTTP transmission protocol, which can be activated as an option. This makes it easier to eavesdrop on the login data. The data between converter and Startdrive is transferred in protected form using the "Secure S7 protocol Startdrive".	
Session timeout on inactivity/ runtime timeout	Default settings	• Anonymous: Never • Any user except "Anonymous": 30 minutes
	Configurability	Settings are **individually** configurable for all user accounts except the "Anonymous" user.
	Authorization	Any user with the function right "Manage users and roles"
	Valid values	1 to 600 min
	The session timeout on inactivity applies only to connections via the web server and not to connections via Startdrive. If the user's inactivity exceeds the specified time, that user is automatically logged out. The user is given an advance warning before being logged out. The advance warning time before being logged out is not configurable. These are the default times: • 5 min if the timeout is set to ≥ 10 min • 1 min if the timeout is set to ≥ 3 min but < 10 min • No advance warning if the timeout is set to < 3 min The session timeout is suspended in the following cases: • During relatively long processes such as firmware updates until the process has completed. • If the control panel is active.	

Administrators

Configurability

Property	Description
User account	The relevant user accounts are created and activated during UMAC configuration.
User name	The user name is defined during UMAC configuration.
Password	The password is defined during UMAC configuration.
Roles and function rights	The user account is assigned the "Drive Administrator" role by default.

At least one user (except "Anonymous") with the "Manage users and roles" right must be activated at all times. If UMAC is enabled, the last user with the "Manage users and roles" right cannot be deleted.

Creating, editing and managing user accounts

Users with the "Manage users and roles" right are authorized to perform the following actions for themselves and for all other users:

Category	Action	Own user account	Anonymous	Other users
General	Create user	–	–	X
	Activate/deactivate user	–	X	X
	Assign user-defined names	X	–	X
	Change user-defined names	X	–	X
	Assign password (according to password policy)	X	–	X
	Change password	X	–	X
	Delete user	–	–	X
Session timeout	Configure session timeout	X	–	X
Roles and function rights	Assign roles in any combination	X	X	X

"Anonymous" user

Overview

The Anonymous user should only be used for access using the SINAMICS SDI Standard Panel and communication protocols which do not support authentication.

More information about the communication protocols which do not support authentication can be found in section "Least functionality of ports and protocols (Page 68)".

Configurability

Note

We recommend assessing the assigned authorizations for the "Anonymous" user in an information security risk assessment and implementing the resulting actions.

Property	Description
User account	Users with the function right "Manage users and roles" can activate/deactivate this user. The user account is activated by default.
	The user account cannot be deleted, but it can be deactivated in user management.
User name	The user name cannot be configured.
Password	The user does not need a password and does not need to be authenticated.
Roles and function rights	The roles "Drive Ext. Role Fieldbus" and "Drive Ext. Role SDI Standard/Adv" are assigned to the user account by default.

8.3.1.2 User management for engineering in Startdrive

Description

Startdrive projects provide user management and access control configuration, where users can be configured with corresponding roles and rights both for engineering in Startdrive and for the drives (see section "Security settings (Page 53)"). Details on user management for the drive via Startdrive and web server have already been described (see section "User management for the drive (Page 58)"). This section shows the details for engineering in Startdrive. Detailed information on engineering in Startdrive can be found in the TIA Portal information system (Help).

8.3.2 Access control

8.3.2.1 Roles for engineering in Startdrive with engineering function rights

Overview

Startdrive controls access to functions on the basis of rights, which by default are grouped into system-defined roles.

Before executing a user action, Startdrive checks the rights of a user, provided that project protection is enabled. Missing authorizations are displayed in a corresponding message/ banner.

The "Engineering-Administrator" role

Users with the "Engineering-Administrator" role have the "Manage users and roles" right. Users with the "Manage users and roles" right can create other users and assign any combination of roles to them as required.

Assignment of rights to roles

The following system-defined roles are available by default.

No.	Engineering role
[1]	Engineering-Administrator[1)]
[2]	Engineering-Standard

[1)] Possible role in order to use the UMAC settings from the project when the project data is loaded into the drive.

Other roles can be created at any time.

The following rights are assigned to the two engineering roles by default:

Engineering function rights	[1]	[2]
Open a project, read access only	X	X
Open and edit the project	X	X
Edit hardware configuration	X	X
Download to PLC	X	X
Download to drives	X	X
Download to other devices	X	X
Edit PLC program	X	X
Edit safety-related project data	X	–
Monitor PLC program	X	X
Control PLC program online	X	X
Create and edit traces	X	X
Edit drive applications	X	X
Edit drive Safety Integrated application	X	–
Control drive in manual mode	X	X
Show the configuration of security modules	X	–
Edit the configuration of security modules	X	–
Import project texts	X	X
Edit library types	X	X
Upgrade project	X	–
Manage users and roles	X	–
Change project via Openness API	X	X

8.3.2.2 Roles for engineering in Startdrive and access to the converter with engineering and runtime function rights

Assignment of rights to roles

To facilitate working with access-protected projects and access-protected converters, you can use roles that have both engineering and runtime rights. You assign the necessary roles to the respective user in accordance with the defined tasks.

The following roles with engineering and runtime function rights are available for drives by default:

No.	Roles with engineering and runtime function rights for drives
[1]	Drive Administrator[1)]
[2]	Drive Safety Engineer
[3]	Drive Engineer and Service

[1)] Possible role in order to use the UMAC settings from the project when the project data is loaded into the drive.

The following engineering function rights are assigned to the above roles:

Engineering function rights	[1]	[2]	[3]
Open and edit the project	X	X	X
Edit hardware configuration	X	X	X
Download to drives	X	X	X
Edit drive applications	X	X	X
Control drive in manual mode	X	X	X
Edit drive Safety Integrated application	X	X	–
Manage users and roles	X	–	–

8.3.2.3 Roles for access to the converter with runtime function rights

Assignment of rights to roles

The following roles are available by default for accessing the converter.

No.	Roles with runtime function rights for converters
[1]	Drive Administrator
[2]	Drive Safety Engineer
[3]	Drive Ext. Role Fieldbus, Drive Ext. Role SDI Standard/Adv
[4]	Drive Engineer and Service
[5]	Drive Operator
[6]	Drive Guest

The roles are assigned the following runtime function rights by default:

Runtime function rights	[1]	[2]	[3]	[4]	[5]	[6]
Read drive data or acknowledge messages	X	X	X	X	X	X
Control drive in manual mode	X	X	X	X	X	–
Perform drive diagnostics	X	X	X	X	–	–
Perform firmware update	X	X	X	X	–	–
Create backup or load drive data to Startdrive	X	X	X	X	–	–
Edit web server configuration	X	X	X	X	–	–
Edit device configuration or drive applications	X	X	X	X	–	–
Edit Safety Integrated application	X	X	–	–	–	–
Manage users and roles	X	–	–	–	–	–

Extended role for access via fieldbus protocols

The following fieldbus protocols do not have a login option for user authentication:

- PROFINET
  Only valid for acyclic communication with a controller.
- Siemens S7 Protocol for PCS7

- DCP
- SNMP

The extended role "Drive Ext. Role Fieldbus" offers the possibility to assign a user exclusively the necessary rights for access via fieldbus protocols.

For technical reasons, the "Anonymous" user is always used for access via the above fieldbus protocols. This user must be activated for access.

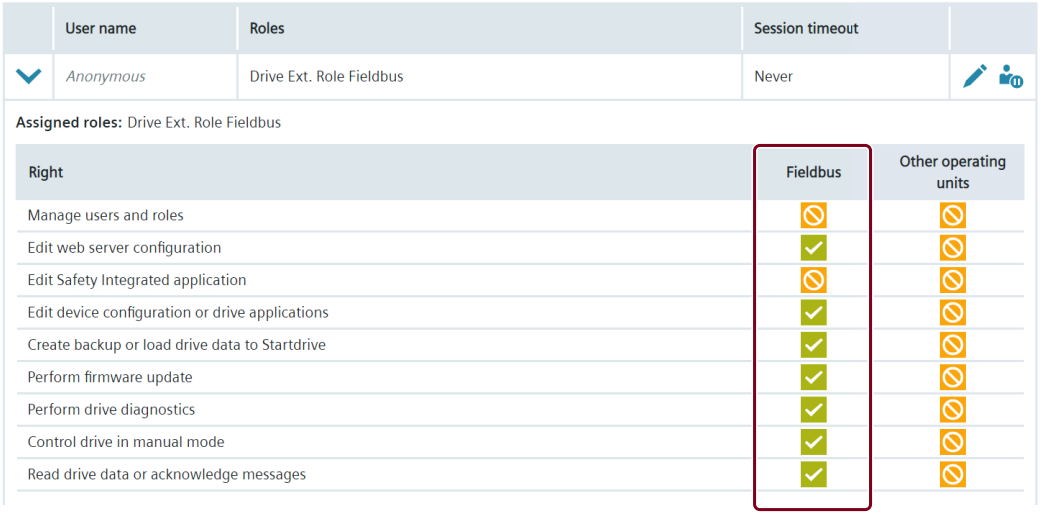


Figure 8-2 Rights for access via fieldbus protocols without authentication:

Edit settings

If the role is assigned to the "Anonymous" user, any user can use the fieldbus protocols to read and edit the settings in the converter.

The following settings cannot be edited:

- Safety Integrated settings
- UMAC settings

Check rights

The authorizations are not checked in the following cases:

- Cyclic communication
- Reading data via DCP

Extended role for access via the SDI Standard Panel

The extended role "Drive Ext. Role SDI Standard/Adv" makes it possible to assign to a user only the rights necessary for access via the integrated SDI Standard Panel.

For technical reasons, the "Anonymous" user is always used for access via the SDI Standard Panel. This user must be activated for access.

Note

Access via the SDI Standard Panel

In converters without an SDI Standard Panel, the extended role "Drive Ext. Role SDI Standard/ Adv" cannot be used.

Edit settings

If the role is assigned to the "Anonymous" user, any user can use the SDI Standard Panel to read and edit the settings in the converter. The following applies:

- Access does not require authentication.

  Note

  Physical protection against unauthorized access

  Carry out an information security risk assessment. Implement the measures for physical protection against unauthorized access as defined in the information security risk assessment.

- The function rights contained in the role only affect access via the SDI Standard Panel.

The following settings cannot be edited:

- Safety Integrated settings
- UMAC settings

Restrict authorizations

Certain functions such as acyclic fieldbus communication require the use of the "Anonymous" user account. Because this user is able to access the converter without authentication, the attack surface for unauthorized access is larger. Users who access the converter without authentication are able to read and change the drive data depending on the roles assigned to the "Anonymous" user.

When you activate the "Anonymous" user account, the security is reduced according to the extent of the rights that you give to this user. When activating the user account, you will receive security information about the potential risk.

We recommend assessing the assigned authorizations for the "Anonymous" user in an information security risk assessment and implementing the resulting actions.

8.3.3 Restoring UMAC settings

Overview

Restoring UMAC settings for a Startdrive project

UMAC settings are part of the project in Startdrive/TIA Portal and cannot be transferred between projects. This means that restoration is only possible through archiving of the project, together with all other project data. It is not possible to separately restore UMAC settings alone.

Restoring UMAC settings for the drive

The UMAC settings are part of the drive configuration and are backed up and restored along with all other project data. Restoring can be performed via the web server or an SD card. If the drive is configured via Startdrive, the UMAC data of the drive can be overwritten with a UMAC download.

8.3.4 Deactivating UMAC

Overview

- Startdrive project projection
  After successful activation, the protection of Startdrive projects can no longer be deactivated.
- Drive
  After successful activation, User Management and Access Control can no longer be deactivated.

8.4 Reduction of the attack surface

Description

The principle of least functionality provides that systems are only configured for necessary functions. This means that the systems only have the software required for the necessary tasks, only the necessary ports are open and only the necessary services are activated.

In Startdrive and web server, interfaces and implemented protocols can be configured using the Security Wizard and in the security summary page. All settings made by the user are displayed in a summary page in the relevant Security Wizard.

8.4.1 Least functionality of ports and protocols

Factory settings

Security measures concerning network security are intended for the communication over the existing Ethernet interfaces, e.g. X127 and X150.

You require the following information to match the security measures to the protocols used.

Interface	Protocol	Port number	Default settings			Description
			Runtime	Startdrive	Web server	
X127	HTTP	80	Deactivated	Deactivated	Deactivated	HTTP is used for communication with the web server. Data transport takes place in unprotected form. Man-in-the-Middle and Replay attacks can be used to intercept and manipulate data. You are therefore recommended to leave this protocol deactivated.
X127	HTTPS	443	Activated	Activated	Activated	HTTPS is used for communication with the web server. Data transport takes place in protected form via TLS V1.2 and TLS V1.3.
X150	HTTPS	443	Activated	Deactivated	Activated	HTTPS is used for communication with the web server. Data transport takes place in protected form via TLS V1.2 and TLS V1.3.
X150	PROFINET Context Manager	34964	Activated	Activated	Activated	The PROFINET Context Manager provides an endpoint mapper in order to establish an application relationship (PROFINET AR).

Interface	Protocol	Port number	Default settings			Description
			Runtime	Startdrive	Web server	
X127, X150	SNMP	161	Deactivated	Deactivated	Deactivated	The Simple Network Management Protocol (SNMP) enables the reading out and setting of network management data (SNMP managed Objects) by an SNMP manager. SNMP V1 is used.
X150	NTP	Dynamic	Deactivated	Deactivated	Deactivated	NTP is only supported for PROFINET (X150). An NTP client port (dynamic UDP port > 50,000) is only open at this interface.
X127	Siemens S7 Protocol for PCS7 (according to RFC 1006)	102	Deactivated	Deactivated	Deactivated	The Siemens S7 Protocol for PCS7 can only be used in PCS7 environments. Data transport takes place in unprotected form and must therefore be protected by other means.
X150	Siemens S7 Protocol for PCS7 (according to RFC 1006)	102	Deactivated	Deactivated	Deactivated	
X127	Secure S7 Protocol for Startdrive (according to RFC 1006)	102	Activated	Activated	Activated	The Secure S7 Protocol for Startdrive is used for communication between Startdrive and the converter. Data transport takes place in protected form via TLS V1.3. **Note** If this protocol is deactivated, commissioning will not be possible.
X150	Secure S7 Protocol for Startdrive (according to RFC 1006)	102	Activated	Activated	Activated	
X127, X150	DCP	Not relevant	Always activated	Always activated	Always activated	The Discovery and Configuration Protocol (DCP) is used by PROFINET to determine PROFINET devices and to make basic settings. DCP uses the special multicast MAC address: xx-xx-xx-01-0E-CF, xx-xx-xx = Organizationally Unique Identifier

Interface	Protocol	Port number	Default settings			Description
			Runtime	Startdrive	Web server	
X127	DHCP	68	Deactivated	Deactivated	Deactivated	One way to integrate converters into industrial networks is with automatic assignment of the IP address, subnet mask and gateway by a DHCP server.
X150	DHCP	68	Deactivated	Deactivated	Deactivated	One way to integrate converters into industrial networks is with automatic assignment of the IP address, subnet mask and gateway by a DHCP server. **Note** If PROFINET is used, IP addresses, subnet masks and gateways are assigned using DCP.

Configuration of ports and protocols

The access of applications to the converter can be restricted independently of the default settings. In addition, communication using individual interfaces and protocols can be activated or deactivated.

The system integrator decides on the configuration of access possibilities on the basis of the specific use case and the operating environment.

For more information about the settings see the product documentation:

Access with/without authentication

The configuration of ports and protocols cannot be viewed in isolation. The context including the following factors must always be taken into account:

- users defined in user management
- interfaces used
- operating units used
- data storage media used (e.g. memory cards)

The following table shows the various access options in the context of the factors above:

Options	Authentication	More information
Access with the following protocol: • HTTP	Yes	–
Access with the following protocols: • HTTPS • Secure S7 Protocol for Startdrive	Yes	–
Access with the following fieldbus protocols: • PROFINET • DCP • SNMP • S7 Protocol for PCS7	No	Access is with a controller, for example. The "Anonymous" user is used for access. This user must be activated for access. For access via the PROFINET protocol: • With cyclic communication, the UMAC settings are not considered. • With acyclic communication, the "Anonymous" user is used for access.

8.4.2 Least functionality of hardware reports

Description

Converters of protection class IP20 are intended for installation in a lockable control cabinet/ switching room. The locked control cabinet/switching room must provide sufficient protection against access by unauthorized persons.

Interface	Format	Delivery state	Best practice
X127	RJ45	Not protected	Protection from locked control cabinet
X150	RJ45	Not protected	Protection from locked control cabinet
SINAMICS SDI Standard	1.4"	Not protected	Protection from locked control cabinet
SD card slot	SD 6.1	Not protected	Protection from locked control cabinet

More information

You can find more information about activating/deactivating ports and protocols in section "Least functionality of ports and protocols (Page 68)".

8.4.3 Additional protective measures for hardware reports

Description

Additional protective measures must be considered in an information security risk assessment (Page 29).

Protective measures for communication interfaces

Communication interfaces such as the service interface X127 cannot be fully deactivated from the software. If the results of the information security risk assessment require additional protective measures for the communication interfaces, port locks (Siemens RJ45 port lock: Article No. 6GK1901-1BB50-0AA0) could be used for example.

Protective measures for memory card slots

The memory card slot on the converter cannot be deactivated from the software. If the results of the information security risk assessment require additional protective measures for the memory card slot, security seals could be used for example. Although they cannot prevent unauthorized access, they provide evidence afterwards that it has happened.

8.4.4 Least functionality of software applications and functions

Description

Firmware version V6.2 does not support any Technology Extensions or other supplementary functions.

8.5 Protected communication channels

8.5.1 Protecting sensible data when being transferred (data in transit)

Overview

In protected communication, confidential data is protected against access by unauthorized third parties during transmission by means of cryptographically secured communication channels and protocols. The integrity of the data is also verified.

Description

Protected communication between the converter and the engineering tools is ensured by a combination of the following mechanisms.

Secure communication channels and protocols

Communication between the converter and the Startdrive and web server engineering tools is protected using the following protocols:

- Secure S7 Protocol for Startdrive
- HTTPS

An overview of the communication links between the converter and other communication devices and the protocols used can be found in section "Communication links (Page 51)".

Identification of communication devices

A certificate is required to establish a protected connection between the converter and the engineering tools Startdrive and web server. This certificate is generated automatically in the SINAMICS converter.

For example, the first time a connection is established between the Startdrive engineering tool and the SINAMICS converter, the user is shown the certificate that was generated automatically in the SINAMICS converter. The user is asked whether to trust this certificate. If so, the connection is established and the converter is given the status "Trusted Device". The Startdrive engineering tool stores the certificate internally, meaning that the status "Trusted Device" is stored there permanently.

More information

You can find more information about establishing a protected HTTPS connection to the web server in section "Certificates for protected communication (Page 187)".

8.5.2 Protection of UMAC data

Description

If the customer wants to export personal data, for example in the form of a backup, it must be protected by the customer, e.g. by using the "Drive data encryption" feature.

8.6 Protected data storage

8.6.1 Protection of sensitive data when stored (data at rest)

Description

Authentication mechanisms and secure data deletion measures are central to the protection of sensitive data at rest.

UMAC settings

When user accounts are created, login data is grouped together in the UMAC settings for the relevant drive. This also applies to data required for validation and administration of the access data. When this data is saved/downloaded, it is transferred to the user database in the internal memory of the converter and saved.

Backup & restore

When user accounts are created, login data is grouped together in the UMAC settings for the relevant drive.

If UMAC is activated in the Security Wizard and a password is set for drive data encryption, the UMAC settings including the login data are protected. The UMAC data are then only encrypted in the backup files and also on the SD card if the SD card is inserted.

8.7 System integrity

8.7.1 Software and information integrity

Description

Cryptographic processes are essential in order to protect the integrity and authenticity of hardware and software products. The recommendations and requirements from IEC 62443 4-1 are observed in the development of security functions and the implementation of cryptographic processes.
The following Internet pages are for information only:

- German Federal Office for Information Security (BSI) (https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html)
- ENISA - European Union Agency for Cybersecurity (https://www.enisa.europa.eu/)
- ECRYPT - European Network of Excellence in Cryptology (https://www.ecrypt.eu.org/index.html)
- NIST Special Publication 800-88 Guidelines for Media Sanitization (https://nist.gov)

To guarantee the integrity and authenticity of hardware and firmware components, digital certificates are used. The certificates are linked to the Root CA certificate for converters/motion control products in a two-tier PKI architecture.

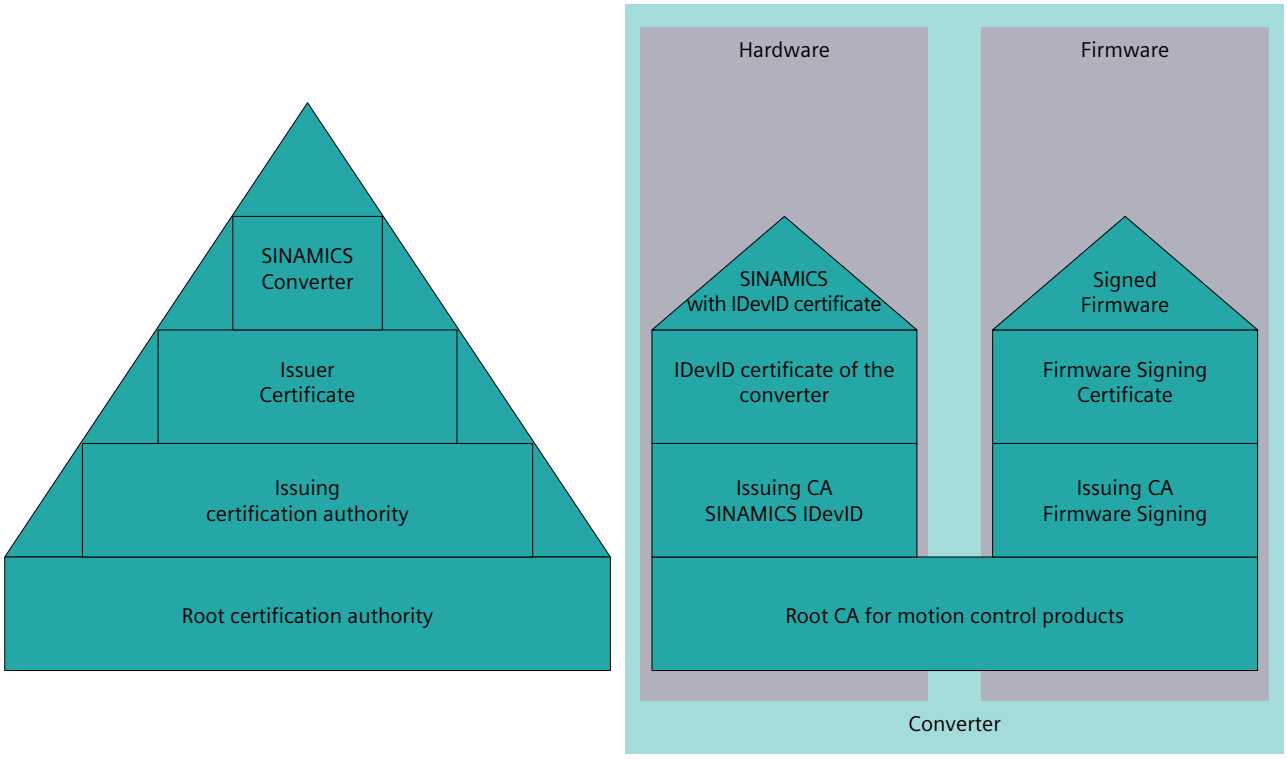


Figure 8-3 PKI architecture

Issuing CA SINAMICS IDevID

When delivered, converters have an Initial Device Identifier (IDevID) in the form of a digital certificate. The IDevID certificate is linked to the Root CA for motion control products via the Issuing CA certificate.

The IDevID certificate is generated in the production process and stored in the converter. The certificate is also an electronic representation of the nameplate with the identity of the converter.

Issuing CA Signing Certificate

The firmware in the converter and the software running during operation in runtime are checked on the basis of a code signing certificate during installation. The code signing certificate is linked to the Root CA certificate for motion control products via the certificate chain.

Integrity and authenticity check

The integrity and authenticity check takes place as part of the firmware update.

Integrity check

The integrity of the firmware is checked using cryptographic hash functions. The integrity check ensures that the software/data components to be installed have not been modified.

Authenticity check

The authenticity check during a firmware update is based on the cryptographic hash value from the integrity check. The hash value is also verified by the code signing certificate. The check of the signature chain ensures that there have been no changes in the software/data components used and that the software/data components used originate from a trusted source.

Application example

During a firmware update, the cryptographic hash value and the digital signature of the new firmware are checked against the cryptographic hash value calculated by the firmware update using the code signing certificate.

If the check is successful, the new firmware is moved to the internal memory of the Control Unit. If the check fails, and error message is displayed in the engineering tool.

Restore process

Firmware version V6.2 does not support an integrity and authenticity check for the restore process.

Boot process

Firmware version V6.1 does not support an integrity and authenticity check for the boot process.

Protection against malicious code

Converters are developed in accordance with the requirements of IEC 62443-4-1 (Secure product development lifecycle requirements). This applies to hardware as well as software products. There is further protection against malicious code because the integrity and authenticity of executable code is verified before installation.

8.7.2 Verification of security functions

Description

The product offers no automated mechanisms that are able to check correct operation of security functions in the context of acceptance tests or maintenance.

However, system integrators can check the following security functions manually:

- Authentication mechanisms
  Access attempts in which the login data (user name and password) of an authorized user are combined with invalid login data can be used to check the behavior of the available authentication mechanisms.
- Usage tracking
  The user roles and rights configured in user management (UMAC) authorize users to use specific functions and to perform actions. The scope of the functions and actions can be verified manually.
- Open ports
  The status of the communication interfaces is displayed on the Protection & Security page.

System integrators can describe the procedures in an instruction so that they can be used in acceptance tests.

8.7.3 Input validation

Implementation

The components validate syntax, length, and content of input data and of entries via external interfaces that have a direct impact on the component's actions. The input validation is dependent on the context in which the values are entered.

8.7.4 Identify and address fault conditions

Description

Error messages appearing in the applications and components listed below do not contain any information that would enable an attacker to identify and use fault conditions for an attack.

- Startdrive engineering tool
- Web server engineering tool
- SINAMICS SDI Standard

8.7.5 Firmware update

Overview

Updates mean that firmware versions with an extended scope of functions can be used. The extended scope of functions is also relevant for the security functions, which increase the availability of a converter throughout the entire product life cycle.

Description of function

Firmware updates change the settings in the converter according to the relative firmware version:

- For an update, the converter settings are retained.
- For a downgrade to a lower version, the converter is restored to factory settings. This also applies to hotfix versions.

The following options are normally available for a firmware update:

- Firmware update via memory card
- Firmware update via web server
- Firmware update via Startdrive

More information about the available firmware versions is provided in the product documentation of the converter.

Integrity and authenticity of the firmware files

The integrity of the firmware files is checked using cryptographic hash functions. Authenticity is verified with digital signatures.

The integrity and authenticity check ensures that the software/data components used have not been deliberately or accidentally manipulated.

More information

For more information about the firmware update, refer to the product information.

8.7.6 Backup and restore

Overview

With the "Backup and restore" function you can back up the converter data to a file and restore the configured settings again if necessary. Restoring the converter data restores the converter to a known state.

Description of function

The following functions are available in the engineering tools Startdrive and web server:

- Back up converter data:
  With this function, all converter data including the UMAC settings is backed up. Certificates are not part of the backed-up data.
- Restore converter data:
  You can use this function to load the backed-up converter data to the converter, e.g. after replacing a device or during series commissioning. If UMAC is activated in the Security Wizard and a password is set for drive data encryption, the UMAC settings including the login data are protected. If drive data encryption is enabled, this password will be requested when restoring.

- Restore settings to the factory setting:
  This function resets all converter settings to the factory values.
  Depending on the engineering tool used, the following data is retained when restoring the factory settings:
  - Communication interface settings
  - UMAC and security settings
  - Language setting
  - Date and time

  This data is reset to the factory settings by resetting all user-defined settings. You can find more information in section "Deletion of customer data on the converter (Page 85)".
- Restore Safety Integrated settings to the factory setting:
  This function only resets the settings of the Safety Integrated application to the factory settings. All other settings remain unchanged.

Recommendations

- Back up converter data:
  - After commissioning
  - After changes to the converter data
  - Before "Restore factory settings"
  - Before a firmware update or downgrade

  This makes it possible restore the converter to a known state.
- Operation with inserted memory card:
  If a converter is operated with an inserted memory card, the converter data is also written to the memory card so it is protected against power failure. Using the memory card, for example, the backed-up settings can be transferred to other converters.
- Storing the backup file in the operating unit/on a network drive:
  Place the backup file in a protected location in the operating unit or on a suitably protected network drive.

More information

For more information on the "Backup and restore" function in Startdrive or web server, refer to the product information for the converter used.

8.8 Logging and monitoring

8.8.1 Monitoring access from untrusted zones

Description

Monitoring of remote access from a non-trusted zone, e.g. for service, maintenance or monitoring purposes, is not part of the product scope.

8.8.2 Logging of events

Description

So that the correct time stamps are used for event logging, the time must be synchronized with the converter.

The synchronized time is used for the time stamp of the following events:

- Error messages and alarms
- Diagnostics buffer

The following options are available for time synchronization:

Time synchronization based on an NTP server

If a converter is connected to a controller via PROFINET interface X150, time synchronization in the converter and the controller can be set with an NTP server. In this case, the date and time are provided by the NTP server for all drive components.
If there is another device with an NTP server, time synchronization can also take place regardless of whether there is a controller or not.

Manual setting of the date and time

The date and time are set manually.

Using a real-time clock to advance the time in a power failure

Some converters have a real-time clock (RTC) built in. The real-time clock advances the time if the converter is de-energized for up to a few days.

Without a real-time clock, the time used when the converter restarts after a power failure is the latest time before the power failure.

More information

You can find more information about time synchronization with NTP in the Startdrive and web server engineering tools in the relevant product documentation.

Recommendations for secure operation and secure disposal

9

The procedure for secure operation and secure disposal is the responsibility of the operating company. The system integrator provides the operating company with a manual.

Recommendations for secure operation and securely disposing of the product are provided in this section. The system integrator can use this information when it creates the manual for secure operation.

9.1 Secure operation

Compliance with security requirements

To ensure secure operation for the intended operating environment, the assumptions listed in section "Security requirements for the intended operating environment (Page 33)" must be complied with.

In addition, a suitable security management process must be applied (see section "Security management (Page 29)"). The available security functions in the converter and in Startdrive must be configured and used on this basis, and operation of the converter and Startdrive must be secured by means of the necessary measures in the environment.

9.2 Secure disposal

9.2.1 Deletion of customer data on the converter

Resetting all user-defined settings to factory settings

NOTICE
Misuse of data resulting from insecure methods of deleting data Incomplete or non-secure deletion of data from storage media or the internal memory of a converter can result in data misuse by third parties. • Therefore, **before disposing of the product**, be sure to securely erase all data on all storage media used.

The data storage media installed and listed below can potentially include customer data and, depending on the protection requirement, must be securely deleted or physically destroyed when the media are disposed of:

- eMMC
- NVRAM

Resetting all user-defined settings to factory settings deletes the customer data in the converter. For more information on resetting all user-defined settings to factory settings, refer to the product information for the converter used.

If deletion with a memory card was unsuccessful, the relevant components on the PCB must be physically destroyed.

9.2.2 Dispose of memory cards securely

Description

The converter can be operated optionally with an SD card. The data on this SD card can be securely deleted with the relevant tools, on a PC for example.

Note

Physically destroying SD cards

SD cards are flash memories with defect management and if at all possible these should be physically destroyed.

More information

More information on securely deleting data is provided in the following sources:

- German Federal Office for Information Security (BSI) (https://www.bsi.bund.de/EN/Home/home_node.html):
  - "Completely deleting data on hard disks and smart phones" (only available in German)
  - IT Compendium of protection fundamentals - CON.6.A12 "Minimum requirements for techniques to destroy and delete"
- National Institute of Standards and Technology (NIST) (https://www.nist.gov/)
  - NIST Special Publication 800-88: Guidelines for Media Sanitization (only available in English)
- Secure destruction of data storage media is regulated in the DIN 66399 standard. The standard discusses the following topics:
  - Part 1 of the standard: Determination of the protection requirements and assignment of protection classes (1, 2 or 3).
  - Part 2 of the standard: Definition of the permissible material parts as a function of the storage medium type (semiconductor memory, here: flash memory) corresponding to the security level to be implemented (Table 6). For magnetic data storage media, see Table 5.

Security programs

10

Supported security programs in the TIA Portal

NOTICE
Data manipulation due to outdated virus scanner A virus scanner that is not updated regularly only provides insufficient protection for your data. Your system may be damaged by infiltrating malware. • Make sure that your virus scanner and its databases are always up-to-date. Perform updates regularly.

The following security programs help to verify the security of applications such as Startdrive:

- Virus scanner/allowlisting
- Encryption software
- Host-based intrusion detection systems

Use the compatibility tool for Automation and Drives (https://support.industry.siemens.com/cs/ww/en/view/64847781) to select suitable security programs.

Security settings in Startdrive

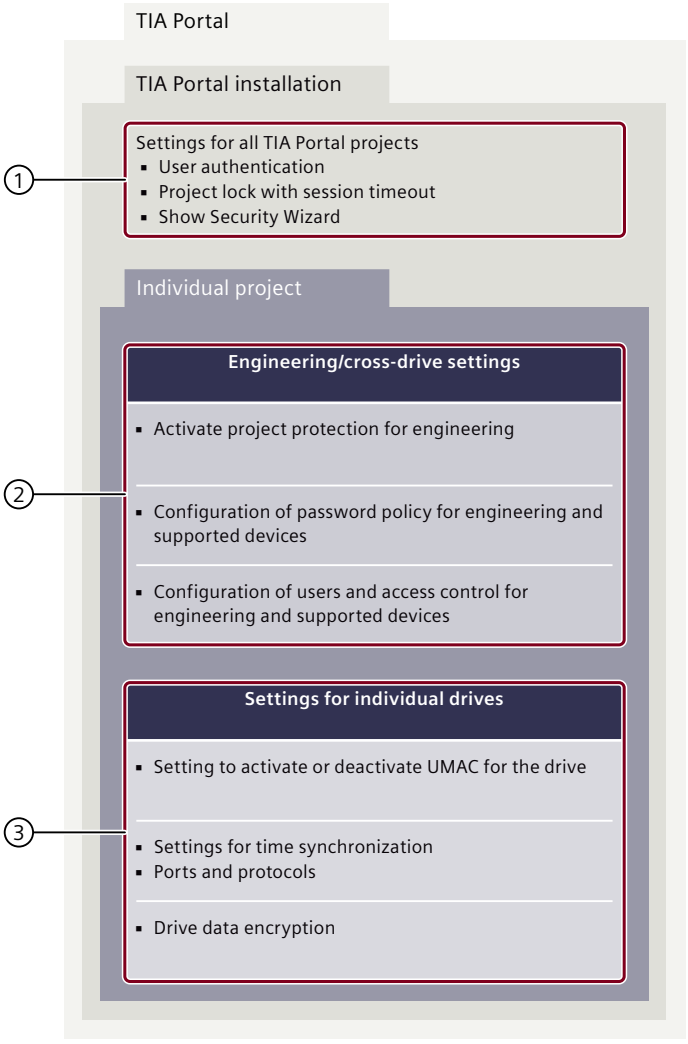
11

Overview

The TIA Portal and the TIA Portal application Startdrive provide various security functions covering multiple projects and multiple drives.

Description of function

The following figure illustrates the assignment of security functions to the respective configuration area in the TIA Portal.



① The settings apply globally to all TIA Portal projects.

② The settings apply to individual Startdrive projects in the TIA Portal and to all drives configured in a Startdrive project. The settings are transferred to the drive during the download to the drive.

③ The settings apply to individual drives configured in the Startdrive project. The settings are transferred to the drive during the download to the drive.

Figure 11-1 Overview: Security settings in the TIA Portal

11.1 Configure access to Startdrive projects in the TIA Portal.

Overview

The security settings for access to projects in the TIA Portal are configured globally for all projects. The configured settings are stored automatically and apply immediately.

Description of function

The function view with the settings for access to TIA Portal projects is opened from "Tools > Settings > Security > Access protection".

The following functions are available:

- User authentication
- Project lock with session timeout

11.1.1 User authentication

Overview

This function specifies which authentication procedure is used by default.

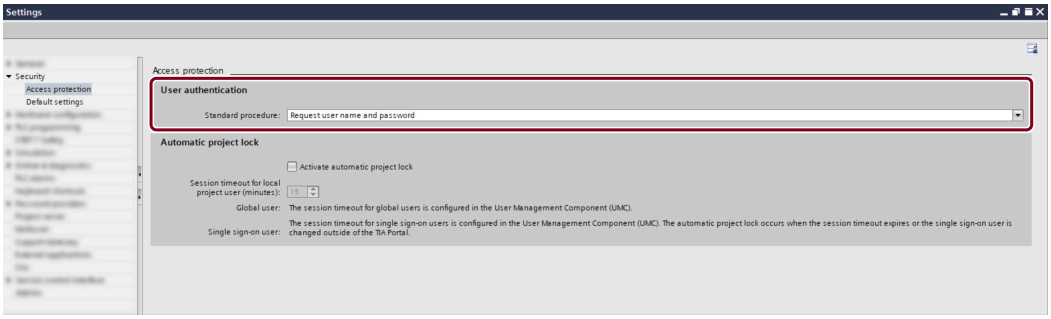


Figure 11-2 User authentication for projects in the TIA Portal

Description of function

The following options are available for user authentication:

Setting	Description
Standard authentication procedure	• "Request user name and password": When the project is opened a login dialog appears. Users with an active user account can log into the project. • "Use anonymous user": When the project is opened no login dialog appears. • "Use single sign-on session": When the project is opened the user is copied from the active single sign-on session in a UMC-S server. If there is no active single sign-on session, the single sign-on login dialog appears.

The configured settings are stored automatically and apply immediately.

11.1.2 Project lock

Overview

The project lock prevents unauthorized persons from accessing the project when a project user is absent.

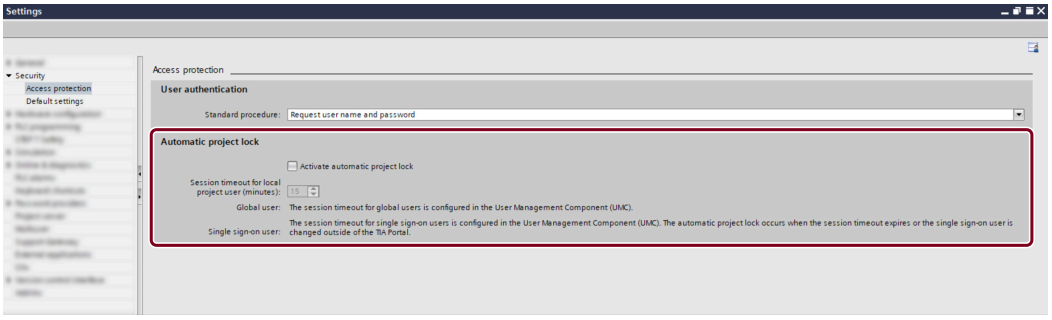


Figure 11-3 Automatic project lock for projects in the TIA Portal

Description of function

The function comprises the following subfunctions:

Function	Description
Activate the automatic project lock	This function specifies whether a project is automatically locked due to inactivity after the end of the configured session timeout. If the project lock is activated and no time is configured for the session timeout, the default setting of 15 minutes is used as the session timeout.
	In what circumstances can the project lock not be activated? • Control panel active: The project lock cannot be activated while the control panel is active.
	In what circumstances does the project lock provide no protection? • If the "Anonymous" user is the current user, the project lock provides no protection. Reason: The "Anonymous" user is logged into the project without authentication.
Session timeout for local project users (minutes)	This function sets the time for a session timeout on inactivity of local project users.
	In what circumstances is the automatic project lock suspended? • Control panel active: While the control panel is activated, the session timeout is suspended after the configured time. The project is locked after the control panel is deactivated if the session timeout expires again at this time. • Running processes: If processes are running, the project lock is suspended until the relevant processes have finished. • Open dialog with user action: If a dialog requiring user action is open, the project is not locked until after the dialog is closed.

The configured settings are stored automatically and apply immediately.

11.1.2.1 Session timeout for local project users

Description of function

The function has the following characteristics:

Default settings	• Not activated • 15 minutes if activated
Configurability	Settings are **globally** configurable in the TIA Portal for all project users except the "Anonymous" user.
Authorization	Users with the "Manage users and roles" right
Valid values	1 to 60 min
System behavior	If the project lock is activated, a session timeout for local project users can be activated and configured.

You can find more information under the heading "Lock project" in the Startdrive information system.

Recommendations

As an administrator, you should make the project lock mandatory for the entire company. For this purpose, you can define the automatic project lock on inactivity with a corresponding session timeout via an internal company settings file.

11.1.2.2 Project lock

Description of function

You have the following options when using the project lock:

- Lock project manually:
  For users logged on with single sign-on, the single sign-on session is closed first. Then the project is locked.
- Lock project automatically on inactivity:
  For local project users, you can define the duration of inactivity.
  For users logged on with single sign-on, the project is locked in the following cases:
  - The session timeout expires for the global user who is logged in. The single sign-on session is also closed.
  - The single sign-on session changes.
  - The single sign-on session is closed.

11.1.2.3 Lock project manually

Requirement

- A protected project is open.
- You are logged in to the project with a user account

Note

How to use the "Anonymous" user

If the "Anonymous" user is the current user, the project lock provides no protection.

Reason: The "Anonymous" user is logged into the project without authentication.

Procedure

1. Open the project view.
2. Click the down arrow in the toolbar next to the "User management" button.
   A drop-down list is opened in which the user management functions are listed.
3. Click "Lock the project".
   The "Project locked" dialog opens. In this dialog, you can remove the project lock again or close the project.

11.1.2.4 Lock project automatically on inactivity

Requirement

Startdrive is open.

Procedure

1. Select the "Settings" command in the "Options" menu.
   The "Settings" window is displayed in the work area.
2. Select the "Security" group in the area navigation.
3. Select the check box "Activate automatic project lock for all user types".
4. Only for project users: In the "Session timeout for local project users (minutes)" text box, enter the duration of inactivity after which the project should be locked automatically.

11.1.2.5 Remove project lock for local users

Requirement

The project is locked.

Procedure

1. In the "Project locked" dialog, enter the correct password for the logged-on user.
2. Confirm the entries with <Enter> or click "Unlock".
   Alternatively, you can also close the project if you do not want to log in again. Changes that have not been saved are discarded.

11.1.2.6 Remove project lock for single sign-on users

Requirement

The project is locked.

Procedure

1. In the "Project locked" dialog, click "Unlock".
   If the single sign-on session of the user whose project was locked is still active, the project is unlocked. If this is not the case, the login window for the single sign-on session is displayed. In this case, proceed as described in step 2.
   Alternative: If you do not want to log in again, close the project. Changes that have not been saved are discarded.
2. Log in with the user data of the user who locked the project.
   The project lock can only be removed by this user.

11.2 Display settings of the Security Wizard for drives

11.2.1 Default settings

Overview

The "Default settings" function view is used to change the automatic display settings of the Security Wizard when a PLC or a drive is added.



Figure 11-4 Configure the display of the Security Wizard

Description of function

The function view with the settings for the Security Wizard of the drive is opened from "Tools > Settings > Security > Default settings".

The configured settings are stored automatically and apply immediately.

Deactivating the automatic display of the Security Wizard

If the function is activated, the display of the Security Wizard when a drive is added is deactivated. When more drives are added, the Security Wizard is no longer displayed. This continues for as long as the function is deactivated in this function view.

The display of the Security Wizard when a drive is added can also be deactivated when a drive is added in the Security Wizard. Activating the option "Do not show this dialog again" also activates the function in the default settings.

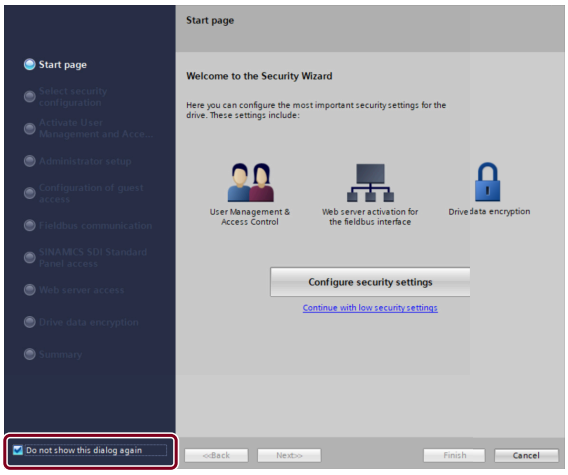


Figure 11-5 Alternative: Deactivate the display of the Security Wizard

Manually starting the Security Wizard

If the display of the Security Wizard when a drive is added is deactivated, the Security Wizard can be started manually for individual drives in the Inspector window with "General > Protection & Security > Wizard for security settings".

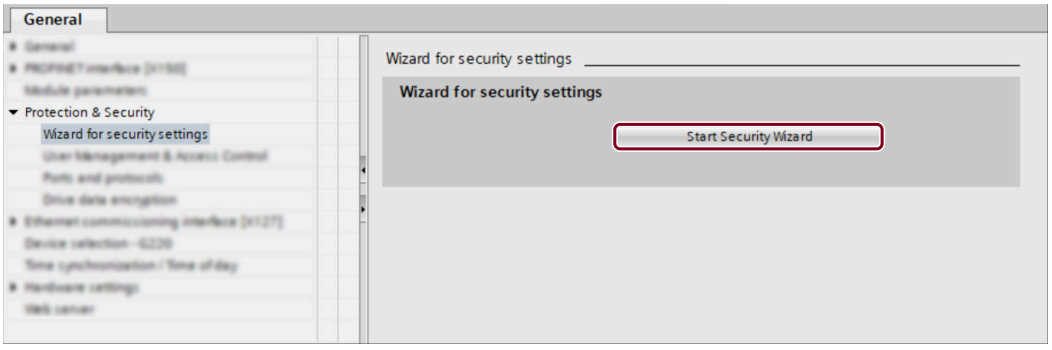


Figure 11-6 Starting the Security Wizard

You can find more information in section "Manually starting the Security Wizard (Page 98)".

11.3 Settings for the drive

Overview

You configure the security settings individually for each drive in the Inspector window.

Description of function

The "Device configuration" tab contains the following security settings in the entry "Protection & Security":

- Wizard for security settings
- User Management & Access Control
- Ports and protocols
- Drive data encryption

11.3.1 Manually starting the Security Wizard

Overview

The Security Wizard opens automatically when a drive is created in the project. To change security settings, you can open the wizard manually at any time.

Requirement

You are logged in as a user with the following rights:

- "Manage users and roles"
- "Edit hardware configuration"

Procedure

1. In the Inspector window, select the "Protection & Security > Wizard for security settings" menu.
2. Click the "Start Security Wizard" button.
   The "Security settings..." dialog opens.

Result

The Security Wizard opens.

More information

You will find detailed of the settings in section "Configuring settings for full protection (Page 130)".

11.3.2 User Management & Access Control

Overview

The "User Management & Access Control" section contains the current settings of the selected converter.

The following table shows the factory settings.

Table 11-1 User Management & Access Control

Setting	Factory setting in the Security Wizard
Activate UMAC for the drive.	Activated
The "Anonymous" user is activated.	Activated
The "Anonymous" user is allowed to read data and acknowledge errors via all interfaces.	Deactivated
The "Anonymous" user is allowed to write at least some data via all interfaces.	Deactivated
The "Anonymous" user is allowed to read and write data via the fieldbus (when writing, changes to functional safety and user and role management are excluded).	Activated

Unless configured otherwise, the Security Wizard opens with the above factory settings in the following situations:

- A new drive is created using the "Add new device" function.
- The functions "Upload from device" and "Upload device as new station" are run if the factory settings have not been changed in the drive.

Requirement

- You are logged in as a user with the "Manage users and roles" right.

Procedure

Proceed as follows to enable/disable the "Activate UMAC for the drive" option:

1. In the Inspector window, select the "Protection & Security > User Management & Access Control" menu.
2. Then select or clear the "Activate UMAC for the drive" option.

   Note

   This option can be activated at this point regardless of the project protection. Project protection applies only to engineering in Startdrive.

3. Make sure that the menu "Security settings > Users and roles" contains a UMAC configuration which is valid for the drive.
4. Load the project data into the drive.
5. Save the project file so it is protected against power failure.

Result

The settings are transferred to the drive.

Note

If UMAC is enabled and the UMAC settings are loaded into the drive, UMAC can no longer be disabled. When loading the UMAC settings into the drive, a corresponding message is displayed.

11.3.3 Activating/deactivating ports and protocols

Overview

In the "Ports and protocols" section, you configure the interfaces to access the drive. Apply the principle of least functionality by deactivating the protocols that are not needed for access to the converter.

You will find detailed information about the ports and protocols and the factory settings in section "Least functionality of ports and protocols (Page 68)".

Unless configured otherwise, the Security Wizard opens with the following factory settings in the following situations:

- A new drive is created using the "Add new device" function.
- The functions "Upload from device" and "Upload device as new station" are run, provided the security factory settings have not been changed in the drive.

Requirement

You are logged in as a user with the "Edit hardware configuration" right.

Procedure

1. In the Inspector window of a drive, select the "Protection & Security > Ports and protocols" menu.
2. Configure the interfaces to access the drive.
3. Load the project data into the drive.
4. Save the project file so it is protected against power failure.

Result

The settings are transferred to the drive.

11.3.4 Drive data encryption

Overview

The function encrypts sensitive data in the backup file and on the memory card of the converter. Sensitive data includes login data such as user names and passwords.

Description of function

The function has no impact on processes during commissioning, e.g. going online, reading and changing data, downloading or uploading data. The drive parameters are not included in the encrypted data.

Configuring the drive password

The password policy is configured in the security settings covering multiple drives. More information on configuration of the password policy can be found in section"Password policy (Page 109)".

The password aging settings will have no impact on the drive password for encryption of the drive data.

Note

Save the drive password in the project?

If the "Activate UMAC for the project" option is not activated, the drive password cannot be saved in the project. A corresponding message appears on screen.

Dependencies with activated/deactivated project protection

Requirements	Consequences and actions
• Project protection for the project is **activated**. • UMAC is activated for the drive. • Drive data encryption is activated.	If project protection is activated, the drive password is saved in the project.
• Project protection for the project is **not activated**. • UMAC is activated for the drive. • Drive data encryption is activated.	If project protection is not activated, the drive password is not saved in the project. The drive password is only saved in the drive.

More information about project protection can be found in section "Project protection (Page 106)".

Lost password

The following restrictions apply if the drive password is lost:

- The drive password cannot be changed.
- Drive data encryption cannot be deactivated.
- The drive data cannot be restored from a memory card.
  It is not possible to configure the UMAC data.
  All user-defined settings must be reset to factory settings. You can find more information in section "Deletion of customer data on the converter (Page 85)".

Recommendation:

- Keep the drive password somewhere safe such as a password manager. Make sure you can access the drive password if needed.

11.3.4.1 Activate drive data encryption

Requirement

You are logged in as a user with the "Manage users and roles" right.

Procedure

1. Select the required drive in the project tree.
2. Select the "Protection & Security > Drive data encryption" menu in the Inspector window.
3. Activate the "Encrypt sensitive drive data" option.
   The "Specify password" button becomes active.
4. Click the "Specify password" button to configure a drive password.
   A corresponding dialog opens.
5. Enter a drive password of your choice twice.
   The password must comply with the password policy. Only use ASCII characters.
6. Confirm with "OK".

7. Complete the drive configuration and then save the project.
8. Load the drive data to the device.

11.3.4.2 Configure drive data encryption

Overview

If there is an online connection to the drive, you can configure the drive data encryption directly in the drive. Change the settings via the "Online & Diagnostics" menu.

Requirement

- You are logged in as a user with the "Manage users and roles" right.
- There is an online connection between the drive and the operating unit.
  Direct functions can only be run in online mode.

Activate the function online

1. Select the required drive in the project tree.
2. In the drive project tree, select menu "Online & diagnostics".
3. In the secondary navigation open the "Functions > Password for encryption of the drive data" menu.
4. Activate the "Encrypt sensitive drive data" option.
   The "Specify password" button becomes active.
5. Click the "Specify password" button to assign a drive password.
   A corresponding dialog opens.
6. Enter a drive password of your choice twice.
   The password must comply with the password policy. Only use ASCII characters.
7. Confirm with "OK".
   The function is activated for the drive.
   You can make additional drive settings and subsequently save them.

Changing the password online

1. Select the required drive in the project tree.
2. In the drive project tree, select menu "Online & diagnostics".
3. In the secondary navigation open the "Functions > Password for encryption of the drive data" menu.
4. Click the "Change password" button to change an existing drive password.
   A corresponding dialog opens.
5. Enter the currently valid drive password.

6. Enter a drive password of your choice twice.
   The password must comply with the password policy. Only use ASCII characters.
7. Confirm with "OK".
   The function is activated for the drive.
   You can make additional drive settings and save them.

Deactivate the function

1. Select the required drive in the project tree.
2. In the drive project tree, select menu "Online & diagnostics".
3. In the secondary navigation open the "Functions > Password for encryption of the drive data" menu.
4. Deactivate the "Encrypt sensitive drive data" option.
   A corresponding dialog opens.
5. Enter the currently valid drive password.
6. Confirm with "OK".
   The function is deactivated.

11.3.4.3 Deactivate drive data encryption

Requirement

- You are logged in as a user with the "Manage users and roles" right.
- The drive password is known.

Procedure

1. Select the required drive in the project tree.
2. Select the "Protection & Security > Drive data encryption" menu in the Inspector window.
3. Deactivate the "Encrypt sensitive drive data" option.
   A corresponding dialog opens.
4. Enter the currently valid drive password.
5. Confirm with "OK".
   The function is deactivated.
6. Complete the drive configuration and save the project.
7. Load the drive data to the device.

11.3.4.4 Changing the drive password

Requirement

You are logged in as a user with the "Manage users and roles" right.

Procedure

1. Select the required drive in the project tree.
2. Select the "Protection & Security > Drive data encryption" menu in the Inspector window.
3. Click the "Change password" button to change an existing drive password.
   A corresponding dialog opens.
4. Enter the old drive password.
5. Enter a drive password of your choice twice.
   The password must comply with the password policy. Only use ASCII characters.
6. Confirm with "OK".
7. Load the drive data to the device.

11.4 User management and access control (UMAC)

11.4.1 Fundamentals

Overview

The TIA Portal allows you to use User Management and Access Control (UMAC) for projects.

Description of function

The following functions are configured using the security settings covering multiple drives:

- Project protection
- Password policy
- User Management & Access Control (UMAC)

More information

More information can be found in section "User Management & Access Control (UMAC) (Page 56)" or in the information system of the TIA Portal under the heading "Manage users and roles".

11.4.2 Project protection

Overview

Project protection is part of user management of the TIA Portal.

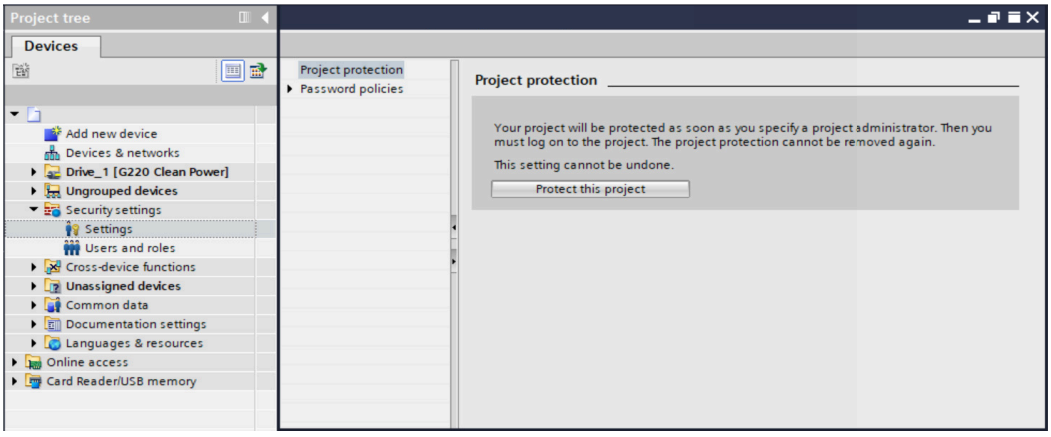


Figure 11-7 Project protection in the TIA Portal

Description of function

By activating the project protection, you automatically create a project administrator. With this user account, other users can be created.

Activated project protection cannot be deactivated.

User authentication

If the project is protected, you require the appropriate access rights for your user account and you must authenticate yourself at login. Authentication takes place when the protected project is opened or when there is a change of user.

Note

For users that were created before activation of project protection, the password needs to be entered again. It is not possible to log into the project without entering the password again.

The same applies to passwords in the protected drive after the UMAC data is reimported into the drive.

Transfer settings to the drive

The "Download to device" function is used to transfer the settings from the project to the drive.

The "Download UMAC to device" function transfers only the UMAC settings (user accounts, roles, password policies) to the drive. You can find more information in section "Downloading the UMAC to the device (Page 128)".

11.4.2.1 Activating project protection

Overview

The function is called in the project tree with "Settings > Project protection".

Requirement

A project has been created.

Procedure

1. Open the "Security settings" folder in the project tree.
2. Double-click the "Settings" entry.
   The editor for user management is opened. The area for project protection is displayed.
3. Click on "Protect this project".
   The "Protect project" dialog opens.
4. Enter a user name.

5. Enter a password.

Note

Password policy

The following policies are initially defined for the password:

- Minimum password length: 8 characters
- Minimum number of numeric characters: 1
- Minimum number of special characters: 0
- At least one uppercase and one lowercase letter: Activated
- Number of recently used passwords blocked for reuse: 5
- Activate password aging: Deactivated

When the project is open, the password policy can be customized.

6. Re-enter the password to confirm.
7. Optional: Enter a comment.
8. Confirm your entries with "OK".
   Project protection is activated.

Result

You are logged in as project administrator.

11.4.2.2 Access without authentication

Description of function

In a project, the system creates the "Anonymous" user by default. This user can log in without authentication.

This user account is deactivated as standard and is activated either in user management or in the Security Wizard. If used carelessly, this user account is a security risk.

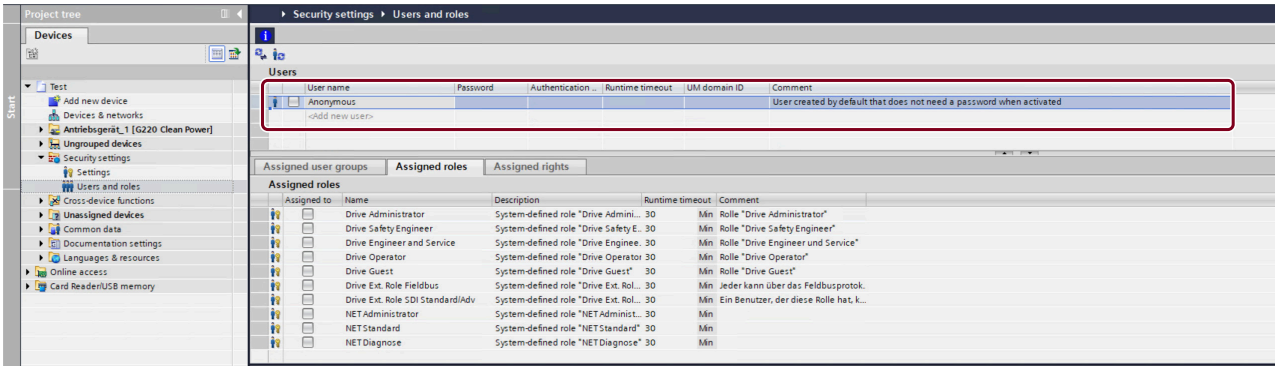


Figure 11-8 "Anonymous" user

Restrict authorizations

The "Anonymous" user can access the converter without authentication. Activating this user reduces security to the extent of the rights that you give to this user. When activating the user account, you will receive security information about the potential risk.

Carry out an information security risk analysis. Identify all potential risks related to the "Anonymous" user's authorizations and define countermeasures to reduce the risk to an acceptable level.

Display authorizations

Users with the "Manage users and roles" right access information about authorizations in the Inspector window, under "Protection & Security > User Management & Access Control".

11.4.3 Password policy

Overview

The password policy is configured for user accounts which may contain runtime rights as well as engineering rights.

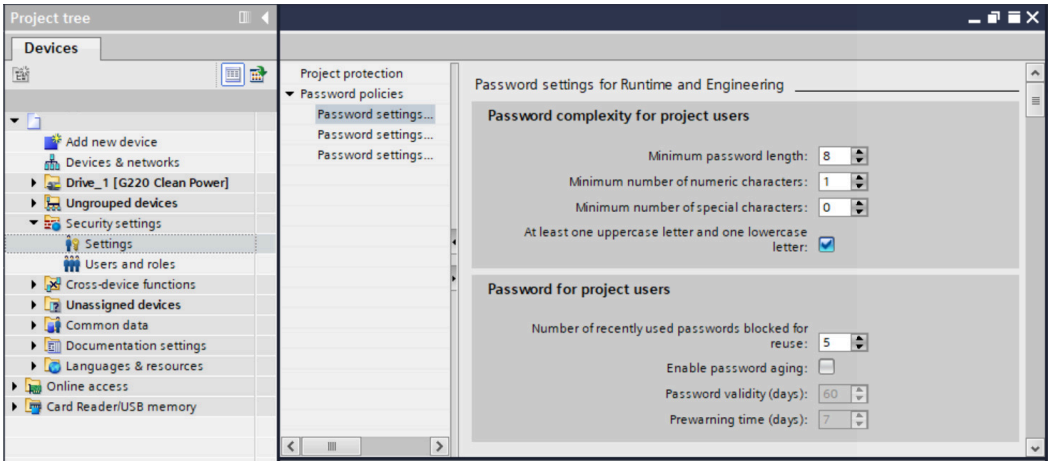


Figure 11-9 Password policy for user accounts

Description of function

You can define the structure and complexity of the user passwords. To do so, configure the following settings:

Setting	Meaning
Minimum password length	The minimum number of characters that the user password must have.
Minimum number of characters	The minimum number of numeric characters that the user password must contain.

Setting	Meaning
Minimum number of special characters	The minimum number of special characters that the user password must contain.
At least one uppercase letter and one lowercase letter	Specifies that the user password must contain at least one uppercase and one lowercase letter.
Number of last used locked passwords	Sets the number of recently used passwords that cannot be used as a new password.
Activate password aging	Specifies that the password only has a certain validity period after which it is invalid. If this option is selected, the password must be changed within the password validity. If the password is not changed in time, the corresponding user can no longer log into the protected project. A project administrator can still change the password for this user afterwards.
Password validity (days)	Sets the password validity in days, after which the password must be changed if password aging is activated.
Advance warning time (days)	Sets how many days before the user's password expires, a warning is provided to the user. The warning time must be less than that for the password validity.

11.4.3.1 Configure password policy

Requirement

- A project is open.
- If the project is protected, you must be logged in with a user account with the rights "Open and edit the project" and "Manage users and roles".

Procedure

Proceed as follows to define the password policy:

1. Open the project for which you want to set the password policies.
2. Open the "Security settings" folder in the project tree.
3. Double-click the "Settings" entry.
   The editor for the user management is opened and the area for project protection is displayed.
4. Select the navigation entry "Password settings for runtime and engineering".
5. Make all the desired settings.
6. Save the project.

Result

The password policy applies to the project and to all drives that have UMAC enabled.

Note

The password complexity policies are checked when a password is assigned or changed.

11.4.4 User management

11.4.4.1 Overview

Overview

The settings in User Management & Access Control (UMAC) determine users' access to:

- the project data and functions in Startdrive
- the functions and data in the drive
  The settings covering multiple drives apply to all drives configured in a project. For the settings to apply in a drive, UMAC must be activated in that particular drive. UMAC activation in the configured drives can be managed drive-by-drive in the project. We recommend activating UMAC for all drives configured in the project.

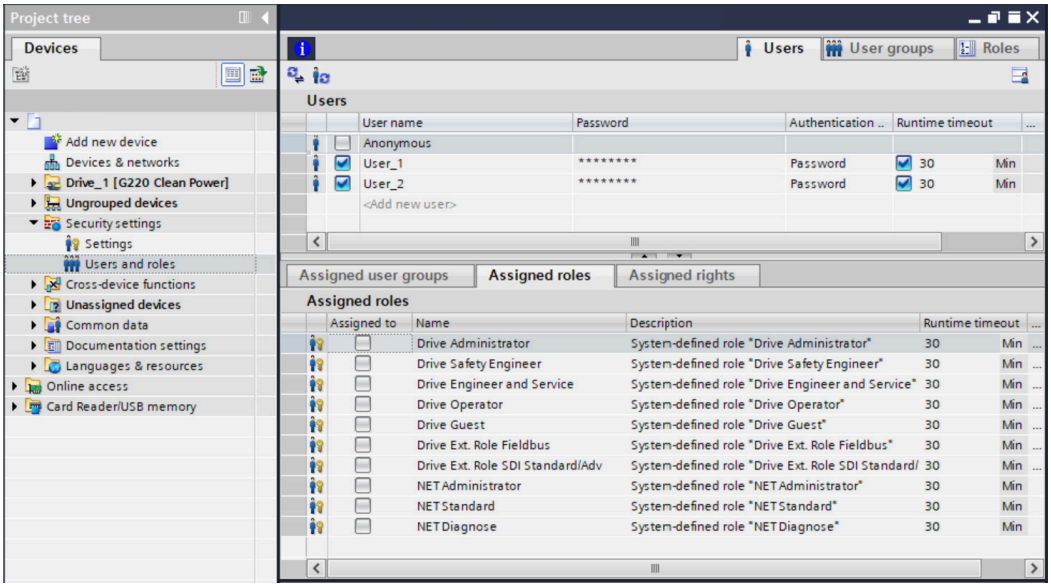


Figure 11-10 User Management and Access Control (UMAC)

Description of function

In user management, up to 64 user accounts can be created and managed. With roles, users are assigned access rights to the project and to configured drives. Users can be assigned different access rights to functions.

Assigning access rights through roles

Access rights are assigned to users through roles. The following role types are available:

- System-defined roles:
  The following roles are available in a protected project:
  - Engineering-Administrator
  - Engineering-Standard
- User-defined roles:
  For each role you can store a comment and display the assigned rights.

11.4.4.2 Creating user accounts

Requirement

- A protected project is open.
- You are logged in as a user with the "Manage users and roles" right.
- In "Security settings", the page opens in the "Users and roles" function view.

Procedure

1. Open the "Users" tab.
2. Click on "<Add new user>".
   A submenu opens, in which you can select the user type.
3. Click "Add new local user".
4. Enter a user name.
5. Click on the arrow in the field "Password".
6. Enter a password.
7. Re-enter the password to confirm.
8. Select the authentication procedure "Password".
9. Enter the desired runtime timeout.
   The runtime timeout is the time after which a user is logged out of a device. For drives, the logout happens on inactivity.
10. If necessary, enter a comment.
    The new local user is created and activated by default. To work with this user account in the project and on the drive, assign the necessary roles to it.

More information

- Copying an existing user account
  You can also create a new user account by copying an existing user account. The configured roles and rights are adopted.
  Login data
  When the new user account is created, the user name is renamed accordingly, e.g. "Username_1". The user name is freely configurable.
  A separate password must be assigned for the new user account.

11.4.4.3 "Anonymous" user

Overview

In a project, the system creates the "Anonymous" user by default. This user can log in without authentication.

Description of function

For security reasons, the anonymous user is deactivated and needs to be activated before use. When activating the "Anonymous" user account, you will receive a security note about the potential risks.

Feature	Description
User account	Cannot be deleted
User account data	Cannot be set
Availability	Can be activated/deactivated
Assignment of rights through roles	Assignment possible

You can set the default authentication procedure so that the anonymous user account is always used when opening the project.

11.4.4.4 Activate/deactivate user accounts

Requirement

- A protected project is open.
- You are logged in as a user with the "Manage users and roles" right.
- In "Security settings", the page opens in the "Users and roles" function view.

Procedure

Proceed as follows to activate or deactivate a user:

1. Open the "Users" tab.
2. Select the check box in the column before the user name to activate the respective user.
3. Clear the check box in the column before the user name to deactivate the respective user. For deactivated users, the role assignment is retained.

Note

Deactivated users are not imported when the UMAC settings are downloaded to the drive.

11.4.4.5 Changing user accounts

Requirement

- A protected project is open.
- You are logged in as a user with the "Manage users and roles" right.
- In "Security settings", the page opens in the "Users and roles" function view.

Procedure

1. Open the "Users" tab.
2. Click in the field whose data you want to change.
   You can only change the "Runtime timeout" time if the corresponding option is activated.
3. Change the user name, the password, the runtime timeout or the comment.

11.4.4.6 Delete user accounts

Requirement

- A protected project is open.
- You are logged in as a user with the "Manage users and roles" right.
- In "Security settings", the page opens in the "Users and roles" function view.

Procedure

1. Open the "Users" tab.
2. Select the local project user you want to delete.
3. Select "Delete" from the shortcut menu or press the <Del> key.

11.4.4.7 Assigning/removing roles

Overview

You can assign different roles, and therefore also rights, to the user accounts.

Requirement

- Engineering roles: A protected project is open.
- Runtime roles: No protected project required.
- You are logged in as a user with the "Manage users and roles" right.
- In "Security settings", the page opens in the "Users and roles" function view.

Procedure

1. Open the "Users" tab.
2. Select a user.
   Multiple selections are not possible.
3. In the "Assigned roles" section, activate the roles you want to assign to the user.
4. In the "Assigned roles" section, deactivate the roles you want to remove from the user.

More information

Detailed information about managing roles can be found in section "Adding and configuring roles (Page 118)".

11.4.4.8 Displaying rights of project users

Requirement

- Engineering roles: A protected project is open.
- Runtime roles: No protected project required.
- You are logged in as a user with the "Manage users and roles" right.
- In "Security settings", the page opens in the "Users and roles" function view.

Procedure

1. Open the "Users" tab.
2. Select the project user for which you want to display the assigned rights.
   Multiple selections are not possible.
3. In the bottom area of the "Users" tab open the "Assigned rights" tab.

11.4.4.9 Change password

Overview

If you change your password as a project user, only the password for this project will be changed.

Description of function

The following possibilities exist depending on the user type:

- When a protected project is opened:
  Local project users and global users that do not use the single sign-on procedure can change their password in the login dialog.
- When working in a protected project, using the toolbar:
  Local project users and global users that do not use the single sign-on procedure can change their password via the toolbar.
- When working in a protected or unprotected project, via the "Users and Roles" editor:
  Local project users can change their password via the "Users and Roles" editor. Project users must have the following rights:
  - Open and edit the project
  - Manage users and roles

  More information about changing the password via the "Users and Roles" editor can be found in section "Changing user accounts (Page 114)".

11.4.4.10 Changing the password when a protected project is opened

Requirement

- A protected project is open.
- You are logged in with a user account which has the "Open and edit the project" right.

Procedure

1. Select the "Open" command in the "Project" menu.
   The "Open Project" dialog opens. The list of recently used projects is displayed.
2. Select a protected project from the list.
3. Click "Open".
   The "Log in" dialog opens.
4. Click the "Change password" button.
   The "Change password" dialog opens.
5. Enter your user name.
6. Enter your current password.
7. Enter your new password.

8. Enter your new password again for confirmation.
9. Click the "OK" button to change your password.

Result

If you enter all the data correctly, your password will be changed. You can then use the new password when you log into this protected project.

After the UMAC data is downloaded to the drive, the password is also changed in the drive.

11.4.4.11 Changing a password when working in a protected project

Requirement

- A protected project is open.
- You are logged in with a user account which has the "Open and edit the project" right.

Procedure

1. Open the project view.
2. Click the down arrow () in the toolbar next to the "User management" button.
   A drop-down list is opened in which the user management functions are listed.
3. Click "Change password".
   The "Change password" dialog opens.
4. Enter your user name.
5. Enter your current password.
6. Enter your new password.
7. Enter your new password again for confirmation.
8. Click the "OK" button to change your password.

Result

If you enter all the data correctly, your password will be changed. You can then use the new password when you log into this protected project.

After the UMAC data is downloaded to the drive, the password is also changed in the drive.

11.4.5 Access control

Overview

To access protected drive data, every user requires the relevant authorizations. These rights are grouped together in roles and determine the data and functions each user is allowed to access.

Description

The following groups are distinguished in the roles and rights.

Roles

- System-defined roles:
  Each user can be assigned multiple system-defined roles.
- User-defined roles:
  Users with the "Manage users and roles" right can create user-defined roles and assign these roles to other users as needed.

Rights

- Engineering rights: (Page 62)
  These rights relate to a project that is protected by UMAC. These rights are also checked when accessing a protected drive online.
- Runtime rights: (Page 64)
  These rights relate to a drive that is protected by UMAC and that is accessed in online mode. Runtime rights are available for converters with firmware version V6.1 or higher.
  The same UMAC configuration is used to access the drive regardless of the access option, e.g. via Startdrive or the web server.

11.4.5.1 Adding and configuring roles

Requirement

- Engineering roles:
  A protected project is open.
- Runtime roles:
  No protected project required.
- You are logged in as a user with the "Manage users and roles" right.
- In "Security settings", the page opens in the "Users and roles" function view.

Procedure

1. Open the "Roles" tab.
2. Click "Add new role".
3. Enter a name for the role.

4. Optional: Set a time for the runtime timeout.
   The timeout is not used until a later program version.
5. Optional: Enter a comment.
   The new role has been created.

11.4.5.2 Example: Necessary rights for specific activities

The following is a list of necessary rights for standard activities.

- Access to the project:
  You only need engineering rights in your user account.
- Access to the drive:
  You need runtime rights in your user account. However, engineering rights are also necessary and are examined at the time of access.

Activity	Engineering rights[1)]	Runtime rights[2)]
Acknowledge alarms	• Open a project, read access only	• Read drive data or acknowledge messages
Create, delete or rename drive	• Open and edit the project • Edit hardware configuration	–
Device view, network view and topology view	• Open and edit the project • Edit hardware configuration	–
All settings in the "Properties" tab of the Inspector window[3)]	• Open and edit the project • Edit hardware configuration	–
Use control panel	• Open and edit the project • Control drive in manual mode	• Control drive in manual mode
Rotate & optimize	• Open and edit the project • Control drive in manual mode • Edit drive applications	• Edit device configuration or drive applications Requirement: – Read drive data or acknowledge messages – Control drive in manual mode – Perform drive diagnostics – Create backup or load drive data to Startdrive
Execute the measuring functions	• Open and edit the project • Control drive in manual mode • Edit drive applications	• Edit device configuration or drive applications Requirement: – Read drive data or acknowledge messages – Control drive in manual mode – Perform drive diagnostics – Create backup or load drive data to Startdrive
Evaluate traces	• Open and edit the project • Create and edit traces	• Perform drive diagnostics

Activity	Engineering rights[1)]	Runtime rights[2)]
Perform safety acceptance test	• Open and edit the project • Control drive in manual mode • Edit Safety Integrated application of the drive	• Control drive in manual mode • Perform drive diagnostics • Edit Safety Integrated application
Perform guided quick startup	• Open and edit the project • Control drive in manual mode • Edit hardware configuration • Edit drive applications • Download to drives	• Edit device configuration or drive applications Requirement: – Read drive data or acknowledge messages – Control drive in manual mode – Perform drive diagnostics – Create backup or load drive data to Startdrive
Load configuration from drive to project	• Open and edit the project • Edit hardware configuration • Edit drive applications • Edit Safety Integrated application of the drive If Safety Integrated settings have been changed.	• Create backup or load drive data to Startdrive
Load configuration from project to drive	• Open and edit the project • Download to drives • Manage users and roles If the configured users and roles are to be downloaded to the converter.	• Manage users and roles If UMAC is part of the download. • Edit device configuration or drive applications Requirement: – Read drive data or acknowledge messages – Control drive in manual mode – Perform drive diagnostics – Create backup or load drive data to Startdrive • Edit Safety Integrated application If Safety Integrated settings have been changed.
Make settings in the function view[4)]	• Open and edit the project • Edit drive applications	• Edit device configuration or drive applications Requirement: – Read drive data or acknowledge messages – Control drive in manual mode – Perform drive diagnostics – Create backup or load drive data to Startdrive

Activity	Engineering rights[1)]	Runtime rights[2)]
Make safety settings in the function view	• Open and edit the project • Edit Safety Integrated application of the drive If Safety Integrated settings have been changed.	• Edit Safety Integrated application
Manage user-defined parameter lists	Depending on the parameter settings that are changed via the user-defined lists. For safety parameters, the "Edit Safety Integrated application" right is explicitly required.	Depending on the parameter settings that are changed via the user-defined lists. For safety parameters, the "Edit Safety Integrated application" right is explicitly required.
Configure signal interconnections	• Edit hardware configuration The necessary rights depend on the settings and parameters used.	The necessary rights depend on the settings and parameters used.
Restore factory settings	• Open and edit the project • Edit drive applications • Edit Safety Integrated application of the drive If Safety Integrated settings have been changed.	• Edit device configuration or drive applications Requirement: – Read drive data or acknowledge messages – Control drive in manual mode – Perform drive diagnostics – Create backup or load drive data to Startdrive • Edit Safety Integrated application The necessary rights depend on which factory settings are restored.
Restore Safety Integrated factory settings	• Open and edit the project • Edit Safety Integrated application of the drive	• Edit Safety Integrated application
Retentively save	• Open and edit the project • Edit drive applications	• Edit device configuration or drive applications Requirement: – Read drive data or acknowledge messages – Control drive in manual mode – Perform drive diagnostics – Create backup or load drive data to Startdrive
Restart the drive	• Open and edit the project • Edit drive applications	• Edit device configuration or drive applications Requirement: – Read drive data or acknowledge messages – Control drive in manual mode – Perform drive diagnostics – Create backup or load drive data to Startdrive

Activity	Engineering rights[1)]	Runtime rights[2)]
Online access with the search for accessible devices (Life List)	–	The necessary rights depend on which actions are performed.
"Start Security Wizard" in the Inspector window	• Open and edit the project • Edit hardware configuration • Manage users and roles	–
All settings in the Inspector window under "Protection & Security"	• Open and edit the project • Edit hardware configuration	–
Use Openness	• Change project via Openness API	–

1) Engineering rights necessary in **online and offline mode**.

2) Runtime rights necessary in **online mode**.

3) Exception: safety telegram configuration

4) Exception: Safety Integrated settings

11.4.5.3 Assign/remove rights

Requirement

- Engineering roles:
  A protected project is open.
- Runtime roles:
  No protected project required.
- You are logged in as a user with the "Manage users and roles" right.
- In "Security settings", the page opens in the "Users and roles" function view.

Procedure

1. Open the "Roles" tab.
2. Select a user-defined role.
   Multiple selections are not possible.
3. In the lower area, open the tab with the category from which you want to assign or remove rights.
4. Activate the rights that you want to assign to the role.
5. Deactivate the rights that you want to remove from the role.

11.4.5.4 Changing roles

Requirement

- Engineering roles:
  A protected project is open.
- Runtime roles:
  No protected project required.
- You are logged in as a user with the "Manage users and roles" right.
- In "Security settings", the page opens in the "Users and roles" function view.

Procedure

1. Open the "Roles" tab.
2. Click in the field whose data you want to change.
3. Change the name, runtime timeout or comment.
   The timeout is not used until a later program version.

11.4.5.5 Deleting roles

Requirement

- Engineering roles:
  A protected project is open.
- Runtime roles:
  No protected project required.
- You are logged in as a user with the "Manage users and roles" right.
- In "Security settings", the page opens in the "Users and roles" function view.

Procedure

1. Open the "Roles" tab.
2. Select the user-defined role that you want to delete.
   System-defined roles cannot be deleted.
3. Select "Delete" from the shortcut menu or press the <Del> key.

11.4.6 User login

Overview

Converters running with firmware ≥ V6.1 have the following functions for access protection:

- User Management and Access Control (UMAC) for access to the converter

Description

User authentication

If project protection or the "UMAC for the project" function is enabled in the Security Wizard, users must authenticate themselves when opening the project. If the "UMAC for the drive" function is also enabled and the same login data applies for access to the drive as for access to the project, users can also access the drive data in online mode.

Valid login data must be entered to log in. A user with the "Manage users and roles" right configures the login data of your user account and assigns the necessary access rights to your user account.

"Anonymous" user

Activate access without authentication based on the "Anonymous" user account only if access without authentication is acceptable.

Multiple access

Multiple users with the necessary rights can access a converter at the same time. No priority is given to any particular user.

11.4.6.1 User login

Overview

Authentication is necessary when a protected project is opened or after a timeout.

Requirement

The project is protected.

Procedure

1. Click "Open existing project" in the secondary navigation in the portal view.
   A selection of recently used projects is displayed to the right in the detailed view.
2. Continue with one of the following options.
   - Select a project. Then click the "Open" button.
   - Click "Browse", double-click the required project in your directory structure, select project file "*.ap18.x". Then click the "Open" button.

   The "Log in" dialog box opens.
3. Select the user type.
   If you selected "Anonymous user" or "Single Sign-on", continue with step 5. Otherwise continue with step 4.
4. Enter your user name and your password.
   You can change your password at this point. A password change is mandatory in the following cases:
   - If a project user logs in after the password validity has expired.
     In this case, perform the steps for changing the password.
5. Click "OK".

Result

- Login successful:
  The selected project opens after you have successfully logged in.
  If your user account has the necessary rights, you can change the drive settings in the project. You can then establish an online connection to the device or load the configuration data to the drive.
- Login failed:
  An appropriate error message is output if the login was not successful.
  More information about possible error messages and remedies can be found in section "Error messages and remedies (Page 126)".

11.4.6.2 Error messages and remedies

Description

Message	Cause	Remedy
The drive cannot be accessed with the current login information.	• Login took place with a user account which does not have the necessary access rights. • The user account used is deactivated. • The passwords entered during login were incorrect. • The user name is invalid.	As the user, check that your user account gives you access rights to the drive. Check you login data. Enter the login data correctly.
The user was not able to be automatically authenticated. It is probable that different login data is configured for the project user and the device user.	• For the user account, different login data exists for the project and drive.	As a user with the "Manage users and roles" right, apply the relevant user account data from the project to the drive. As the user, change the password of your user account in the drive.
The user password has expired.	• The user password has expired.	Change the password for your user account.
Password change failed	• When the password was changed, the existing password was not correctly entered. • The password rules were violated when the new password was entered.	When changing the password, enter the existing password and new password according to the valid password rules. The password rules are displayed when you enter the password.

11.4.6.3 Changing a user

Overview

In a protected project, you can change the logged-in user.

The project is automatically closed by the system and opened again if you switch from a user with no write permissions to a user with write permissions or vice versa. Editors for which the newly logged-in user has no rights are possibly also closed.

Note

Before changing the user, close all connections to the drives to which you are logged in as a user. Reason: The login data for existing online connections is not changed when the user changes.

Requirement

- A protected project is open.
- The user being newly logged in has at least the "Open project read-only" right.

Procedure

1. Open the project view.
2. Click the down arrow in the toolbar next to the "User management" button.
   A drop-down list is opened in which the user management functions are listed.
3. Click "Change user".
   If there are still unsaved changes, the "Save project" dialog opens. You can save your changes.
   The "Change user" dialog opens.
4. Select the user type.
5. Enter your user name.
   This step is not necessary if you have selected "Anonymous user" or "Single sign-on" as the user type.
6. Enter your password.
   This step is not necessary if you have selected "Anonymous user" or "Single sign-on" as the user type.
7. Click "OK".

Result

The selected user is logged in to the protected project.

No logout during active connections

When changing users, all existing connections to the drives remain active and the original login data continues to be used for these connections.

11.4.6.4 Logging off a user

Requirement

A protected project is open.

Procedure

1. Open the project view.
2. Click the down arrow in the toolbar next to the "User management" button.
   A drop-down list is opened in which the user management functions are listed.
3. Click "Log out and close the project".
   - If changes have been made to the project since it was last saved, a message is displayed. Then, specify whether the changes should be saved.
   - If no changes have been made to the project since it was last saved, the project is closed immediately.

Result

The active user is logged out and the project is closed.

Note

Login using single sign-on

If you are logged in via single sign-on, you are then also logged out of the single sign-on session when you log out of the project.

To prevent this, close the project without logging out. This will keep you logged in to the single sign-on session. You can open protected projects without repeating authentication if you have sufficient rights.

11.4.7 Downloading the UMAC to the device

Overview

The UMAC settings of the project are optionally downloaded with the project data to the drive ("Download project data to the device"). If necessary you can also download the UMAC settings directly to the drive independently of the project. The following UMAC data can be loaded:

- UMAC password policy
- UMAC assignment of rights to roles
- UMAC user accounts (including assigned roles)

Requirement

- An online connection exists between the operating unit and the drive.
- UMAC is activated for the drive in the project settings.
- There is an active user account in the project which is assigned the "Drive Administrator" role.
  OR
  There is an active user account in the project that is assigned the "Manage users and roles" rights for the drive.

Procedure

Follow these steps to download the UMAC settings to the device in online mode:

1. Select the required drive in the project tree.
2. Open the "Download UMAC to the device" shortcut menu.
   The prerequisites for downloading the UMAC settings are checked.
   If the check is successful, a notice appears stating that the UMAC settings will be overwritten in the drive.
3. Confirm this notice.

Result

The UMAC settings are downloaded into the drive, where they can be stored so they are protected against power failure.

11.5 Configuring settings for full protection

Overview

The settings for protecting a drive are configured using the Security Wizard already when adding it to the project.

The Security Wizard guides you through the settings when adding a drive and informs you about the effects of the settings.

Requirement

The following functions are set as follows:

- Project protection for the project is activated.
  This means that the user accounts created in the user administration of the TIA Portal can also be used in the Security Wizard.
  You can find more information about the project protection configuration in section "Project protection (Page 106)".
- The automatic display of the Security Wizard when adding a drive is not deactivated.
  You can find more information in section "Default settings (Page 96)".

Configuring full protection

To define the settings for full protection, perform an information security risk analysis. You can find more information in section "Security management (Page 29)".

Dynamic default settings

Due to default settings and the configuration of settings elsewhere in TIA Portal, certain options in the Security Wizard may already be enabled or disabled.

The descriptions in the following sections are based on standard scenarios and do not cover all use cases. The sequence of configuration steps and the state of the displayed functions may differ from the described standard scenarios depending on the use case.

The settings made in the Security Wizard are summarized and checked in the last step of the configuration. The wizard displays information about functions whose configuration is missing or needs to be changed.

11.5.1 Basic information

Overview

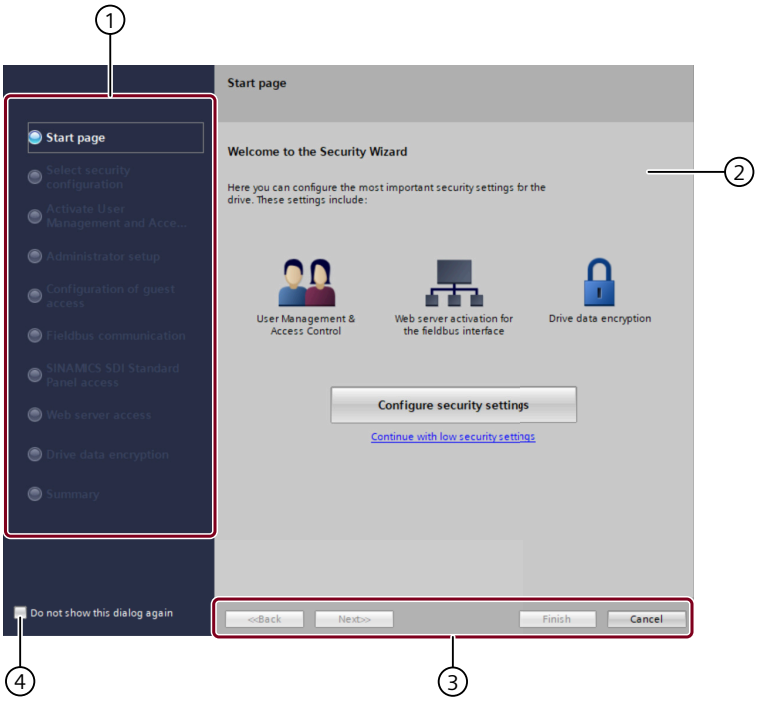
The Security Wizard starts automatically when you perform one of the following actions:

- You add a new drive to the project tree.
- You add a new drive via hardware selection.
- You load project data from a drive to the project. The project data of the drive must be in the factory settings.
  This is the case the first time the project data is loaded or when it is loaded after a reset to factory settings.

Description of function

The Security Wizard is used to configure the security settings for a drive.

Structure of the Security Wizard



① Navigation of the individual setting areas in the Security Wizard
② To display a selected setting area in the Security Wizard
③ Deactivate the automatic start of the Security Wizard
④ Toolbar for scrolling through the Security Wizard and for finishing or canceling the configuration

Figure 11-11 Example: Security Wizard

Setting areas

The Security Wizard allows you to navigate between the following setting areas:

- Home page
- Select security configuration
- Activate User Management and Access Control
- Administrator setup
- Configuration of guest access
- Fieldbus communication
- SINAMICS SDI Standard Panel access
- Web server access
- Drive data encryption
- Overview

Each setting area contains information and notes on the respective functions. Notes on individual functions are only displayed when the function is selected.

In the last step, all settings are summarized in an overview.

Exiting the Security Wizard

Variant	Explanation
Exiting the Security Wizard with "Cancel"	The settings are not applied. The configuration of the settings can be completed at a later time.
Exiting the Security Wizard with "Finish"	The settings are applied. The configuration of the settings can be changed at a later time.

Manually starting the Security Wizard

You can find more information in section "Manually starting the Security Wizard (Page 98)".

Loading the security settings into the converter

For the security settings to take effect in the drive, the configuration data and the UMAC settings must be loaded into the drive.

Note

Transferring UMAC data

When loading the settings into the drive, make sure that the "Update UMAC" option is enabled in the "Load preview" dialog.

When working with a protected project, you must be logged in with the following rights:

- "Manage users and roles"
- "Download to drives"

You can find more information in section "Downloading the UMAC to the device (Page 128)".

More information

- Deactivating the automatic display of the Security Wizard:
  If the automatic display of the wizard is deactivated, the default settings in the wizard are adopted when another drive is created. Exception: activation of project protection.
  You can find more information on this in section "Default settings (Page 96)".

11.5.2 Home page

Overview

By default, the Security Wizard is automatically displayed when a drive is added to the project.

Configuring security settings

Click the "Security settings" button to start configuring the security settings.

Skipping configuration

If you want to skip the configuration and perform it at a later time, click "Continuing with low security settings".

You can find more information on this in section "Working with low security settings (Page 149)".

Result

The next setting area is displayed.

11.5.3 Select security configuration

Overview

Use the "Start a new configuration with default settings" function to configure the security settings for a drive newly added to the project.

Requirement

- A new drive has been added and the Security Wizard has been started.
- Further drives with configured security settings:
  If there are already protected drives in the project, the option "Copy security settings of another drive" is available. Otherwise the function is grayed out.

Procedure

1. Read the displayed information and notes.
2. Select the option "Start a new configuration with default settings".
3. Click "Next" to apply the settings.

Result

The next setting area is displayed.

11.5.3.1 Transferring existing security settings to a new drive and editing them

Overview

Use the "Copy security settings of another drive" function to copy the security settings of a configured drive to a new or different drive.

Requirement

- A new drive has been added and the Security Wizard has been started.
- Further drives with configured security settings:
  If there are already protected drives in the project, the option "Copy security settings of another drive" is available. Otherwise the function is grayed out.

Procedure

If the option "Copy security settings of another drive" is available, it is automatically selected.

1. Read the displayed information and notes.
2. In the drop-down list, select the drive whose security settings you want to apply.
3. Click "Next" to check or edit the security settings.

Result

The next setting area is displayed.

11.5.3.2 Transferring existing security settings to a configured drive and editing them

Overview

Use the "Copy security settings of another drive" function to copy the security settings of a configured drive to another drive and edit the settings.

In this use case, the option "Start a new configuration with default settings" is not available.

Requirement

- The Security Wizard is called manually.
  You can find more information in section "Manually starting the Security Wizard (Page 98)".
- Further drives with configured security settings:
  If there are already protected drives in the project, the option "Copy security settings of another drive" is available. Otherwise the function is grayed out.

Procedure

If the option "Copy security settings of another drive" is available, it is automatically selected.

1. Read the displayed information and notes.
2. In the drop-down list, select the drive whose security settings you want to apply.
3. Click "Next" to edit the security settings.

Result

The next setting area is displayed.

11.5.3.3 Editing current settings

Overview

Use the "Edit the current settings" function to change the security settings of a configured drive.

In this use case, the option "Start a new configuration with default settings" is not available.

Requirement

- The Security Wizard is called manually.
  You can find more information in section "Manually starting the Security Wizard (Page 98)".
- Further drives with configured security settings:
  If there are already protected drives in the project, the option "Copy security settings of another drive" is available. Otherwise the function is grayed out.

Procedure

If the option "Copy security settings of another drive" is available, it is automatically selected.

1. Read the displayed information and notes.
2. Select the option "Edit the current settings".
3. Click "Next".

Result

The next setting area is displayed.

11.5.4 Activate User Management and Access Control

Overview

The following options are available in this step:

- "Activate UMAC for the project ..." (hereafter: UMAC for the project)
  With this function, a user with the "Engineering-Administrator" role is created. To access the project, the user must authenticate himself.
- "Activate UMAC for the drive ..." (hereafter: UMAC for the drive)
  With this function, a user with the "Drive Administrator" role is created. To access the drive, the user must authenticate himself.
  The "Drive Administrator" role includes the "Manage users and roles" right. Users with this right can subsequently create and manage additional users to access the drive.

Recommendation

For protected access to the project and the drive, make sure that both options are enabled.

Applications

The following applications are possible:

- The "Engineering-Administrator" and "Drive Administrator" users are created separately. The following applies:
  - The "Engineering-Administrator" role is assigned to the "Engineering-Administrator" user.
  - The "Drive Administrator" role is assigned to the "Drive Administrator" user.
  - The users have their own login data.
- The "engineering administrator" user has already been created. The following applies:
  - The existing user account for accessing the project is also used for accessing the drive. In this case, there is no need to create another user as "Drive Administrator".
  - The existing user account has the "Engineering-Administrator" role. The existing user account is additionally assigned the "Drive Administrator" role.
- The "UMAC for the project" function is disabled. The following applies:
  - In this case, only the "Drive Administrator" user is created. The "Drive Administrator" role is assigned to the user.
  - Access to the project is not protected.

11.5.4.1 Configuring UMAC for project and drive (project protection not activated)

Overview

In this use case, the following options are displayed in the "Activate User Management and Access Control" setting area:

- UMAC for the project
  This option is already selected.
- UMAC for the drive
  This option is already selected.

Requirement

- Project protection is not activated.
  You can find more information about the project protection configuration in the security settings of the project in section "Project protection (Page 106)".
- In the previous step, the option "Start a new configuration with default settings" was selected.

Procedure

1. Read the displayed information and notes.
2. Check the option "I have read the information above and ...".
   The following setting areas are activated:
   - Administrator setup
   - Configuration of guest access
   - Fieldbus communication
   - Access to SINAMICS SDI Standard Panel
3. Click "Next" to apply the settings.

   Note

   Activated project protection cannot be deactivated.

4. Proceed as follows, see section "Setting up a project and drive administrator (Page 139)".

Result

The next setting area is displayed.

11.5.4.2 Configuring UMAC for project and drive (project protection already activated)

Overview

In this use case, the following options are displayed in the "Activate User Management and Access Control" setting area:

- UMAC for the project
  The option is grayed out and cannot be edited.
- UMAC for the drive
  This option is already selected.

Requirement

- Project protection is activated.

  Note

  Activated project protection cannot be deactivated.

  You can find more information about the project protection configuration in the security settings of the project in section "Project protection (Page 106)".
- In the previous step, the option "Start a new configuration with default settings" was selected.

Procedure

1. Read the displayed information and notes.
2. Check the option "I have read the information above and ...".
   The following setting areas are activated:
   - Administrator setup
   - Configuration of guest access
   - Fieldbus communication
   - Access to SINAMICS SDI Standard Panel
3. Click "Next" to apply the settings.
4. Proceed as follows, see section "Using an existing user (Page 141)".

Result

The next setting area is displayed.

11.5.5 Administrator setup

Overview

The further procedure depends on the following conditions:

- Security settings of the project for project protection
  AND / OR
  Settings in the "Activate User Management and Access Control" setting area

11.5.5.1 Setting up a project and drive administrator

Overview

In this use case, the following option is displayed in the "Administrator setup" setting area:

- "Set up a project and drive administrator"

Requirement

- Project protection is not activated in the security settings of the project.
  You can find more information about the project protection configuration in the security settings of the project in section "Project protection (Page 106)".
- The following options in the "Activate User Management and Access Control" setting area are activated and selected:
  - UMAC for the project
  - UMAC for the drive

Procedure

1. Read the displayed information and notes.
2. Define a user name and a password for the user account in the "Set up a project and drive administrator" area.
   The password must comply with the password policy. Only use ASCII characters.

   Note

   If the Security Wizard is called when adding another drive, the user created here can be used. You can find more information in section "Using an existing user (Page 141)".

3. Click "Next" to apply the settings.
   The "Next" button is activated only when the settings have been fully configured.

Result

The next setting area is displayed.

More information

- Checking assigned roles and rights:
  You can find more information on this in section "Checking assigned roles and rights (Page 147)".

11.5.5.2 Creating a new user

Overview

In this use case, the following options are displayed in the "Administrator setup" setting area:

- "Use an existing user"
  This option is grayed out and cannot be edited.
- "Create a new user"
  This option is activated and selected.

Requirement

- Project protection is not activated in the security settings of the project.
  You can find more information about the project protection configuration in the security settings of the project in section "Project protection (Page 106)".
- The following options in the "Activate User Management and Access Control" setting area are activated and selected:
  - UMAC for the drive

  The "Activate UMAC for the project ..." option in the "Activate User Management and Access Control" setting area has been deselected.

Procedure

1. Read the displayed information and notes.
2. Define a user name and a password for the user account in the "Create new user" area.
   The password must comply with the password policy. Only use ASCII characters.
   The user account of the new user is created in the user administration with the "Drive Administrator" role.

   Note

   If the Security Wizard is called when adding another drive, the user created here can be used.
   You can find more information in section "Using an existing user (Page 141)".
3. Click "Next" to apply the settings.
   The "Next" button is activated only when the settings have been fully configured.

Result

The next setting area is displayed.

More information

- Checking assigned roles and rights:
  You can find more information on this in section "Checking assigned roles and rights (Page 147)".

11.5.5.3 Using an existing user

Overview

In this use case, the following options are displayed in the "Administrator setup" setting area:

- "Use an existing user"
- "Create a new user"

Requirement

- Project protection is activated in the security settings of the project.

  Note

  Activated project protection cannot be deactivated.

  You can find more information about the project protection configuration in the security settings of the project in section "Project protection (Page 106)".
- The following options in the "Activate User Management and Access Control" setting area are activated and selected:
  - UMAC for the project
  - UMAC for the drive

Using an existing user

This option is already selected. In the drop-down list below the option, the user already configured for access to the project is displayed.

To use the login data of the already configured user to access the drive, proceed as follows:

1. Read the information in the setting area.
2. Click "Next" to confirm the settings.

Creating a new user

Proceed as follows to configure a new user for access to the drive data:

1. Read the displayed information and notes.
2. Select the "Create a new user" option.

3. Define a user name and a password for the user account.
   The password must comply with the password policy. Only use ASCII characters.
   The user account of the new user is created in the user administration with the "Drive Administrator" role.

   Note

   If the Security Wizard is called when adding another drive, the user created here can be used.

4. Click "Next" to apply the settings.
   The "Next" button is activated only when the settings have been fully configured.

Result

The next setting area is displayed.

More information

- Checking assigned roles and rights:
  You can find more information on this in section "Checking assigned roles and rights (Page 147)".

11.5.6 Configuration of guest access

Overview

The following option is displayed in this setting area:

- "Enable guest access to the drive"
  The function is deactivated by default.

When the function is activated, users are given read access to the drive data. Access does not require authentication.

NOTICE
Data manipulation due to access without authentication Access without authentication represents a potential security risk. Potential attackers can identify security vulnerabilities in the system and use this to gain unauthorized access. Data manipulation can alter the settings, causing the converter to malfunction or damaging it. • Apply suitable measures to ensure that only persons classified as trusted are assigned guest access to the drive data.

How to use the "Anonymous" user

Activating guest access activates the "Anonymous" user for all drives in the project.

The "Drive Guest" role is automatically assigned to the "Anonymous" user.

Access options

The following options are available:

- Web server of the relevant drive
- Startdrive in the TIA Portal
- SINAMICS SDI Standard Panel
- All activated ports and protocols
  More information about the factory settings for ports and protocols can be found in section "Least functionality of ports and protocols (Page 68)".

Procedure

1. Read the displayed information and notes.
2. Activate the "Enable guest access to the drive" function.
   Guest access is associated with the right "Read drive data or acknowledge messages".

   Note

   Guest access cannot be activated

   Guest access for the "Anonymous" user cannot be activated in the following situation:
   - The "Anonymous" user is already assigned a role that includes the right "Read drive data or acknowledge messages".
3. Click "Next" to apply the settings.

Result

The next setting area is displayed.

11.5.7 Fieldbus communication

Overview

In this setting area you specify whether users are allowed to change drive data without authentication via the fieldbus communication. The function is activated by default.

When the access is activated, the "Anonymous" user is automatically assigned the "Drive Ext. Role Fieldbus" role. The access applies to all drives in the project.

Procedure

1. Read the displayed information and notes.
2. Activate the "Allow data to be changed via fieldbus communication" function.
3. Click "Next" to apply the settings.

Result

The next setting area is displayed.

11.5.8 SINAMICS SDI Standard Panel access

Overview

In this setting area you specify whether users are allowed to change drive data without authentication via a panel. The function is activated by default.

When the access is activated, the "Anonymous" user is automatically assigned the "Drive Ext. Role SDI Standard/Adv" role. The access applies to all drives in the project.

Description

1. Read the displayed information and notes.
2. Activate the "Allow drive data to be changed via the SDI Standard Panel" function.
3. Click "Next" to apply the settings.

Result

The next setting area is displayed.

11.5.9 Web server access

Overview

In this setting areas you activate/deactivate web server access via the PROFINET interface X150.

Access via the PROFINET interface X150 with HTTPS protocol is activated in the factory setting for an unprotected drive. This access option is disabled ab default in the Security Wizard.

NOTICE
Data manipulation due to an unprotected fieldbus cable To prevent unauthorized access and data manipulation, the PROFINET interface must be separated from the rest of the plant network according to the Defence in Depth concept. • Protect against access to cables and open connections, for example, by installing in a control cabinet. • More information is provided on the Internet: Industrial Cybersecurity Services (https://new.siemens.com/global/en/products/services/digital-enterprise-services/industrial-security-services.html)

Procedure

1. Read the displayed information and notes.
2. Activate the function "Activate SINAMICS Webserver access via PROFINET interface [X150] with HTTPS protocol".
3. Click "Next" to apply the settings.

Result

The next setting area is displayed.

11.5.10 Drive data encryption

Description

The function encrypts sensitive data in the backup file and on the SD card of the drive. Sensitive data includes login data such as user names and passwords.

The function has no impact on processes during commissioning, for example: go online, read and change data, download or upload data. The drive parameters are not included in the encrypted data.

Activating encryption

The function is activated by default. A drive password must be set for the encryption of the drive data.

When a password is set, the following actions are possible:

- Change password
- Deactivate encryption

The drive password must be known to be able to perform these actions.

Lost password

The following restrictions apply if the drive password is lost:

- The drive password cannot be changed.
- Drive data encryption cannot be deactivated.
- The drive data cannot be restored from a memory card.
  It is not possible to configure the UMAC data.
  All user-defined settings must be reset to factory settings. You can find more information in section "Deletion of customer data on the converter (Page 85)".

Recommendation:

- Keep the password somewhere safe such as a password manager. Make sure you can access the password if needed.

Dependencies with activated/deactivated project protection

Depending on whether project protection is enabled or disabled, certain dependencies occur. You can find more information on this in section "Drive data encryption (Page 101)".

11.5.11 Overview (finishing the configuration)

Description

The configured settings are summarized in the overview. In addition, information on access via fieldbus communication and panel is displayed.

Validity check

The Security Wizard checks the configured settings.

If all settings are valid, the configuration can be completed by clicking "Finish". The settings are saved in the project.

If settings are incorrect or incomplete, corresponding information about them is displayed. The "Finish" button is disabled. To complete the configuration, the displayed errors and inconsistencies must be corrected.

11.5.12 Result of the configuration

Description

The drive is created in the project with the configured settings.

Changing settings

To change the settings, the Security Wizard can be called manually. You can find more information on this in section "Manually starting the Security Wizard (Page 98)".

The settings can also be changed directly via the "Protection & Security" menu in the inspector window.

Loading the settings into the drive

For the settings to take effect in the drive, the project data must be loaded into the drive.

You can find more information on this in section "Downloading the UMAC to the device (Page 128)".

11.5.13 Checking assigned roles and rights

Description

When you have finished configuring the settings in the Security Wizard, you can call up the user administration and check the assigned roles and rights of the configured users.

You can call up the user administration in the project navigation via "Security settings > Users and roles". When you select the corresponding user in the list, the assigned roles and rights are displayed to you. Roles and rights are displayed in different tabs.

11.5.14 Changing or subsequently adjusting security settings

Overview

To change or make the settings subsequently, the Security Wizard can be called up manually. You can find more information in section "Manually starting the Security Wizard (Page 98)".

The settings can also be changed directly via the "Protection & Security" menu in the inspector window.

Requirement

The following functions are set as follows:

- Project protection for the project is activated.
  This means that the user accounts created in the user administration of the TIA Portal can also be used in the Security Wizard.
  You can find more information about the project protection configuration in section "Project protection (Page 106)".

Procedure

1. Select the required drive in the project tree.
2. In the inspector window, select the "Protection & Security > Security Wizard" menu.
3. Click on "Start Security Wizard".
   The "Security settings..." dialog opens and the "Select security configuration" setting area is displayed.
4. Activate the function "Edit the current settings".
   If the existing settings for the drive were configured earlier using the Security Wizard, you can change the settings in each setting area.
   If you want to use the existing settings of another drive, proceed as follows:
   – Activate the "Copy security settings of another drive" function.
   – In the drop-down list, select the drive whose security settings you want to apply.
5. Click "Finish" to apply the settings.

Result

The settings are saved in the project.

11.6 Working with low security settings

Overview

Working with low security settings is not recommended.

NOTICE
Data manipulation due to low protection An inadequately protected drive makes it easier for potential attackers to access the drive data. Data manipulation can cause the drive to malfunction or damage it. • Use the low security settings only in exceptional cases and if this is justifiable after conducting an information security risk analysis, see section "Security management (Page 29)". • Configure the settings for full protection right after adding a drive/several drives in the project. You can find more information on this in section "Configuring settings for full protection (Page 130)".

Requirement

Ideally, the following functions are set as follows:

- Project protection for the project is activated.
  This means that the user accounts created in the user administration of the TIA Portal can also be used in the Security Wizard.
  You can find more information about the project protection configuration in section "Project protection (Page 106)".
- The automatic display of the Security Wizard when adding a drive is not deactivated.
  You can find more information in section "Default settings (Page 96)".

Procedure

To skip the configuration of settings in the Security Wizard and perform it at a later time, proceed as follows:

1. Click on "Continuing with low security settings".
   A security note indicates that you have selected the low degree of protection.
2. Click "OK" to confirm the message.
   The "Summary" area is displayed. In the summary the settings are summarized.
3. Click "Finish" to apply the settings.

Result

The settings are saved in the project.

11.6.1 Result of the configuration

Description

The drive is created in the project with the configured settings.

Changing settings

To change the settings, the Security Wizard can be called manually. You can find more information on this in section "Manually starting the Security Wizard (Page 98)".

The settings can also be changed directly via the "Protection & Security" menu in the inspector window.

Loading the settings into the drive

For the settings to take effect in the drive, the project data must be loaded into the drive.

You can find more information on this in section "Downloading the UMAC to the device (Page 128)".

11.7 Backup and restore

More information

There is basic information about the function in section "Backup and restore (Page 80)".

You will find more detailed information about the function in Startdrive in the following documentation for the product in question.

- Operating Instructions
- Commissioning Manual

11.8 Certificates for protected communication

11.8.1 Fundamentals

Overview

Connections between operating units and drives must be secure. By exchanging digital certificates and validation by the user, drives are classified as so-called "Trusted Devices" and therefore as "secure". Protected communication is possible with these Trusted Devices.

The necessary certificates are created the first time the SINAMICS drive is accessed. Examples:

- When calling the "Online & diagnostics" screen
- When calling the dialogs "Download to device" or "Extended download to device"
- When accessing the drive online via the search for "Accessible devices"
  For this access, it is not necessary that a drive has been created in the project.

The previously generated certificate then applies to subsequent accesses. New certificates are only generated if necessary (IP address changed or certificate expired).

11.8.2 Certificate types

Overview

A certificate is required to establish a protected connection to a SINAMICS drive. The necessary certificates are generated automatically the first time the drive is accessed. Here, the drive acts as a certification instance, issuing the necessary certificates for communication.

Note

Restoring factory settings

When the "Restore factory settings" function is run, stored certificates are not overwritten or deleted.

Certificates are only deleted by resetting all user-defined settings to the factory settings. You can find more information in section "Deletion of customer data on the converter (Page 85)".

Certificate attributes

Certificates contain information about the issuer.

Attribute	Meaning	Example
O	Organization	SIEMENS
C	Country/region	EN

Attrib-ute	Meaning	Example
CN	Common name	SINAMICS Embedded Issuing CA, *serial number*=<SN>
OU	Organizational unit	Copyright (C) SIEMENS AG 20XX All rights reserved

Note

Display certificates

When you establish a connection to the drive, you can display the details of the certificates.

- To view the details, click on the "Display certificates" button in the "Connection to drive" message dialog.

Security settings in the web server 12

Development stages of security functionality

Multi-level security functionality is available in the web server for SINAMICS drives.

- Security Wizard (Page 162):
  Using the wizard, you already make basic security settings for the converter when you call up the web server for the first time. The wizard uses important settings from the user management system (e.g. roles and rights) for this purpose.
- User Management and Access Control (UMAC): (Page 176)
  User Management and Access Control (UMAC) enables you to manage access to the converter. This involves creating user accounts and managing them. You allocate roles to user accounts allowing read or write access to specific functions. Access to the converter data and functions is defined using predefined roles.
- Security settings at a glance:
  In the "Protection & Security" function view, you can use the following drop-down lists to view the security settings that have been made, and sometimes configure them directly:
  - "Ports and protocols":
    In this display area you can check the current settings for the communication interfaces.
    You also have option to configure the interfaces for access to the converter.
    You can find more information in section "Ports and protocols (Page 184)".
  - "User Management & Access Control"
    In this display area you can check the current UMAC settings.
    You can change the displayed UMAC settings in the "User management" function view.
  - "Certificates"
    This display area contains basic information about the certificates used.
    You also have the option of downloading a root certificate allowing you to establish a secure HTTPS connection to the web server.
    You can find more information about using certificates in section "Certificates for protected communication (Page 187)".

12.1 Fundamentals

12.1.1 Factory settings

Overview

User Management and Access Control (UMAC) is deactivated in the converter factory setting.

Description

When calling the web server for the first time or after resetting all user-defined settings to factory settings, the first thing you do is make the basic settings for the web server. For more information on resetting all user-defined settings to factory settings, see section "Deletion of customer data on the converter (Page 85)".

When the basic settings are completed, the Security Wizard starts automatically. The following options are displayed:

- "Configure security settings":
  The option "Activate UMAC for the drive" is selected by default. UMAC is activated when the following steps are performed:
  - You confirm on the "Activating User Management & Access Control" page that you have read the information about UMAC and understand the consequences of activation.
  - On the "Administrator setup" page, you configure the login data for a user who has all available rights for the drive.

  You can find more information in section "Configuring settings for full protection (Page 163)".
- "Continue with low security settings":

NOTICE
Data manipulation due to low security settings Inadequately protected converter data and functions make it easier for potential attackers to gain unauthorized access to the converter. Data manipulation can change the Safety Integrated settings or generally disrupt or damage the converter. • Use the low security settings only in exceptional cases and only for a very limited period. Make sure that no unauthorized persons can access the converter, e.g. when the converter is not yet connected to a network. • Carry out an information security risk assessment. Use the low security settings only if this option poses no risk according to the result of the risk assessment.

  If you select the option "Continuing with low security settings", the converter is operated, for example, without UMAC settings. Users are able to access the converter data and functions without authentication.
  You can start the Security Wizard at a later time in the "Protection & Security" function view and make the necessary changes to the security settings.

More information

More information about the Security Wizard can be found in section "Settings in the Security Wizard (Page 162)".

12.1.2 Activating UMAC from the status bar

Overview

If UMAC is not activated, "No user management" appears in the status bar.

The converter is being operated without UMAC settings. Users are able to access the converter data and functions without authentication.

Requirement

The converter and operating unit are connected to each other.

You can find more information in section "Communications interfaces (Page 49)".

Procedure

1. Click on "No user management" in the status bar.
   A drop-down list is opened.
2. Click on "Activate user management".
   The web server displays the "System > Protection & Security" function view.
3. Click on "Start Security Wizard".
4. Make the security settings in the wizard.

12.1.3 User login (guest access enabled)

Overview

Users can only access data and functions they are authorized to use.

Requirement

- UMAC is activated.
- You can use an active user account to access the web server.
- The "Anonymous" user is activated and has the "Read drive data or acknowledge events" right.

Procedure

1. Click the "Login" button in the status bar of the web server.
   A corresponding dialog opens.
2. Enter your user name and your password.
3. Click "Login".

Result

If you have entered the login data correctly, you are logged in.

Converter data and functions are displayed according to the access rights assigned to your user account.

12.1.4 User login (guest access deactivated)

Overview

Users can only access data and functions they are authorized to use.

Requirement

- UMAC is activated.
- You can use an active user account to access the web server.
- The "Anonymous" user is deactivated and does not have the "Read drive data or acknowledge events" right.

Procedure

1. Enter your user name and your password on the "Login required" page.
2. Click "Login".

Result

If you entered the login data correctly, you are logged in and the home page of the web server appears.

Converter data and functions are displayed according to the access rights assigned to your user account.

12.1.5 Changing a user

Overview

A user cannot be changed if one of the following functions is active.

- Quick setup
- Safety Integrated commissioning
- Control panel
- Firmware update
- Backup or restore

Requirements

- UMAC is activated.
- You are logged into the web server.

Procedure

1. Click on the name of the logged-in user in the status bar.
   A drop-down list is opened.
2. Select the "Change user" option .
   A login dialog appears.
3. Enter your user name and your password.
4. Click "Login".

Result

If your user account is not authorized to access the most recent function view, the home page of the web server appears.

12.1.6 Logging off a user

Overview

A user cannot be logged out if one of the following functions is active.

- Quick commissioning
- Safety commissioning
- Control panel
- Firmware update
- Backup or restore

Requirements

- UMAC is activated.
- You are logged into the web server.

Procedure

1. Click on the name of the logged-in user in the status bar.
   A drop-down list is opened.
2. Select the "Log out" option .
   If you made changes to the configuration, the "Save changes" prompt will appear.
3. Confirm with "Save" or log out without saving.

12.1.7 User login after session timeout due to inactivity (guest access activated)

Overview

If a session timeout on inactivity is configured for your user account, you are automatically logged out after the specified period of inactivity. If the set time is ≥ 3 min, you will be informed about the upcoming logout.

The session timeout is suspended in the following cases:

- During relatively long processes such as firmware updates until the process has completed.
- If the control panel is active.

Requirements

- UMAC is activated.
- You are logged into the web server.
- A session timeout is configured for your user account.
- The "Anonymous" user has the "Read drive data or acknowledge events" right.

Procedure

1. Click the "Login" button in the status bar of the web server.
2. Enter your user name and your password.
3. Click "Login".

Result

If you have entered the login data correctly, you are logged in.

Converter data and functions are displayed according to the access rights assigned to your user account.

More information

You can find more information about the ability to configure the session timeout on inactivity in section "User management for the drive (Page 58)".

12.1.8 User login after session timeout due to inactivity (guest access deactivated)

Overview

If a session timeout on inactivity is configured for your user account, you are automatically logged out after the specified period of inactivity. If the set time is ≥ 3 min, you will be informed about the upcoming logout.

The session timeout is suspended in the following cases:

- During relatively long processes such as firmware updates until the process has completed.
- If the control panel is active.

Requirements

- UMAC is activated.
- You are logged into the web server.
- A session timeout is configured for your user account.
- The "Anonymous" user does not have the "Read drive data or acknowledging events" right.

Procedure

1. Enter your user name and your password on the "Login required" page.
2. Click "Login".

Result

If you have entered the login data correctly, you are logged in.

Converter data and functions are displayed according to the access rights assigned to your user account.

More information

You can find more information about the ability to configure the session timeout on inactivity in section "User management for the drive (Page 58)".

12.2 Settings in the Security Wizard

12.2.1 Structure of the Security Wizard

Overview

In the Security Wizard, you configure the security settings for the converter.

Description

The Security Wizard guides you through all the settings and provides important information and notes about each of them.

Read the information and notes carefully. Take the information and notes into account while configuring the security settings.

Navigation within the wizard

Individual steps might be grayed out. They will be activated once the previous settings are configured.

Finish security settings

The "Finish" button is activated once all the steps in the wizard have been completed.

Cancel security settings

You can cancel configuration of the security settings at any time. The Security Wizard is closed and the "Welcome to the Security Wizard" page is displayed. The settings made are not saved.

12.2.2 Reloading pages of the web server

Requirement

- The web server is being called for the first time.

Description

If you are configuring the settings in the Security Wizard and use <F5> or to reload the pages of the web server, the Security Wizard will close. The web server then displays the function view with the basic settings. The basic settings and the settings in the Security Wizard are not saved.

12.2.3 Configuring settings for full protection

12.2.3.1 Making basic settings when the web server is called for the first time

Overview

Make the following settings when the web server is called for the first time or after resetting all user-defined settings to factory settings:

- Preferred language of the user interface
- Converter date and time; either manually or via NTP

For more information on resetting all user-defined settings to factory settings, see section "Deletion of customer data on the converter (Page 85)".

Requirement

- The web server is being called for the first time.

Procedure

1. Set the desired language.
2. Set the date and time of the converter.
3. Click "Next".

Result

The "Welcome to the Security Wizard" page is displayed.

12.2.3.2 Starting the Security Wizard

Overview

When the basic settings are completed, the Security Wizard starts automatically. You can configure the security settings immediately.

After configuring the settings you can start the Security Wizard at a later time and change the settings. More information about this can be found in section "Changing security settings (Page 172)".

Requirement

- The basic settings have been made.

Procedure

Click the "Configure security settings" button.

Result

The "Activate User Management & Access Control" page appears.

12.2.3.3 Activating UMAC

Overview

Once User Management and Access Control (UMAC) is activated, converter settings can only be read and changed by authorized users. The individual access rights are defined in the user account of the relevant user.

Requirement

- The Security Wizard is started.

Procedure

On the "Activate User Management & Access Control" page, the "Activate UMAC for the drive" option is selected by default. To activate UMAC, proceed as follows:

1. Carefully read all the information about UMAC.
2. Select the option "I have read the information above and I understand the consequences of enabling UMAC".
   UMAC is activated and can only be deactivated by resetting all user-defined settings to factory settings.
   You can find more information in section "Deletion of customer data on the converter (Page 85)".
3. To continue, click on "Administrator setup".

Result

The "Administrator setup" page is displayed.

12.2.3.4 Setting up a user with the "Drive Administrator" role

Overview

On the "Administrator setup" page, you can configure a user with all authorizations to access the converter data and functions.

The user is assigned the "Drive Administrator" role with the "Manage users and roles" right. This authorizes the user to create and configure other users in user management, and to change the user account settings.

Other users with the "Manage users and roles" right can be created, changed or deleted in user management. If UMAC has been activated, at least one user with the "Manage users and roles" right must exist if UMAC is enabled. This user can be neither deactivated nor deleted in user management.

Requirement

- The Security Wizard is started.
- UMAC is activated.

Procedure

1. Enter the user name of the administrator.
2. Enter the password for the administrator.
   Follow the applicable password policy .
3. Enter the password again in the "Confirm password" field.
   A message is displayed if the entries do not match.
4. Click on "Guest access configuration" to continue.

Result

The "Guest access configuration" page is displayed.

12.2.3.5 Configure guest access

Overview

On the "Guest access configuration" page, the "Enable guest access to the drive" option is deactivated by default.

NOTICE
Data manipulation because users are not logged in Guest access represents a potential security risk. Potential attackers can identify security vulnerabilities and use them to gain unauthorized access. Manipulation of the converter settings can cause the converter to malfunction or damage it. • Apply suitable measures to ensure that only persons classified as trusted are assigned guest access to the converter data and functions.

Settings in the "Anonymous" user account

The configuration of guest access in the Security Wizard affects the settings in the "Anonymous" user account. Therefore pay attention to the notes in the "Technical information" field in the user interface. More information is provided below.

Requirement

- The Security Wizard is started.
- UMAC is activated.
- An administrator/user is configured with the "Manage users and roles" right

Activating guest access

Proceed as follows if you want to permit guest access to the drive:

1. Activate the "Enable guest access to the drive" option.
   If this option is enabled, acknowledging events is possible for non-logged-in users via all interfaces.
2. To continue, click on "Web server activation".

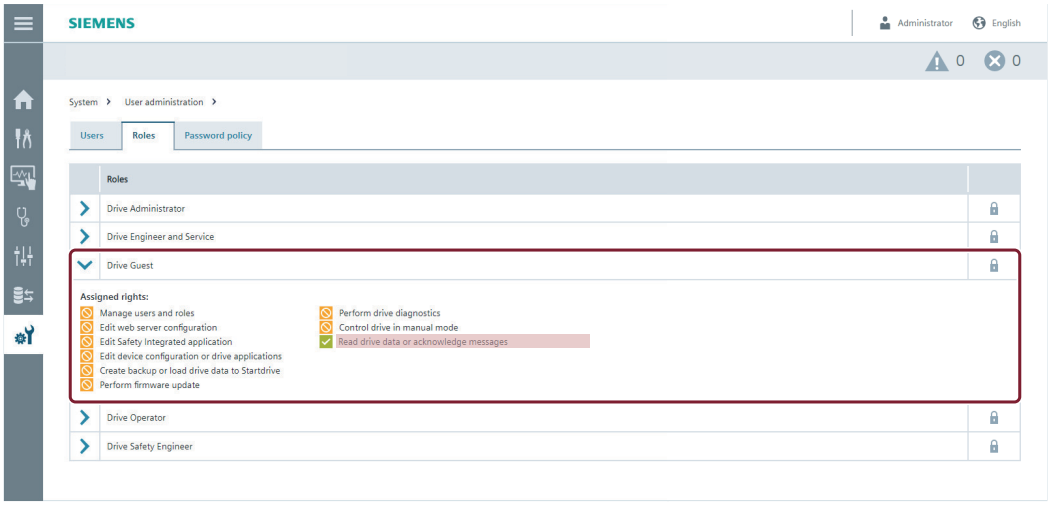
Result

The "Web server activation" page is displayed.

More information

Dependencies between enabling/disabling guest access in the Security Wizard and settings in the "Anonymous" user account.

- If guest access is enabled in the Security Wizard, the "Anonymous" user is assigned the "Drive Guest" role.
  The "Anonymous" user is allowed to read data and acknowledge errors via all interfaces.



- If guest access is deactivated in the Security Wizard, the "Anonymous" user's "Drive Guest" role is revoked.
  The "Anonymous" user is configured outside of the Security Wizard in the "User management" function view. Depending on the configuration, the settings in the "Anonymous" user account affect guest access. You can check the current settings for guest access in the "Protection & Security" function view.
  You can find more information about the standard configuration of the user in section "User management and access control (UMAC) (Page 176)".

12.2.3.6 Web server activation

Overview

On the "Web server activation" page, you configure the interfaces and protocols for access via the web server.

The following options are selected by default:

- "Enable SINAMICS web server access via service interface [X127] with HTTPS protocol"
- "Enable SINAMICS web server access via PROFINET interface [X150] with HTTPS protocol"

To establish a protected HTTPS connection to the converter, proceed as described, see section "Establish a protected HTTPS connection to the web server (Page 188)".

Requirement

- The Security Wizard is started.

Procedure

1. Configure access via the desired interfaces and protocols.
   The following options are available:
   – "Enable SINAMICS web server access via service interface [X127] with HTTP protocol"
     This option is deactivated by default.

     Note
     Security measures for communication via service interface X127

     In accordance with the defense in depth concept, the service interface must be housed in a control cabinet. The factory settings of the service interface [X127] allow a protected HTTPS connection to the converter.

     Note
     Software manipulation if unencrypted HTTP connections are used

     The HTTP protocol transfers unprotected data. This permits password theft, for example, and can lead to data manipulation by unauthorized persons and consequent loss or damage. Therefore only allow connections over HTTPS so that all data is transferred in protected form.

   – "Enable SINAMICS web server access via service interface [X127] with HTTPS protocol"

     Note
     Security measures for communication via service interface X127

     In accordance with the defense in depth concept, the service interface must be housed in a control cabinet. The factory settings of the service interface [X127] allow a protected HTTPS connection to the converter.

   – "Enable SINAMICS web server access via PROFINET interface [X150] with HTTPS protocol"

     Note
     Security measures for communication via PROFINET interface X150

     In accordance with the defense in depth concept, the PROFINET interface must be isolated from the remaining plant network. Access to cables and open connections must be implemented in a protected fashion, for example in a control cabinet.

2. To continue, click on "Summary".

Result

The "Drive data encryption" page is displayed.

12.2.3.7 Drive data encryption

Configuring a password

Overview

The function encrypts sensitive data in the backup file and on the memory card of the converter. Sensitive data includes login data such as user names and passwords.

The function is activated by default.

Lost password

The following restrictions apply if the drive password is lost:

- The drive password cannot be changed.
- Drive data encryption cannot be deactivated.
- "Backup and restore" function:
  Application: The drive data is restored from an encrypted backup file.
  - If the drive password used to encrypt the drive data in the backup file is changed, the drive password will be prompted when restoring. Restoring the drive data without knowing the drive password is not possible in this case.
    For more information on the "Backup and restore" function in the web server, refer to the product information for the converter used.
- The drive data cannot be restored from a memory card.
  It is not possible to configure the UMAC data.
  All user-defined settings must be reset to factory settings. You can find more information in section "Deletion of customer data on the converter (Page 85)".

Recommendation:

- Keep the password somewhere secure, e.g. in a password manager. Make sure you can access the password if needed.

Requirement

- The Security Wizard is started.
- UMAC is activated.
- An administrator/user is configured with the "Manage users and roles" right

Procedure

1. Enter a password of your choice twice.
   The password must comply with the password policy. The applicable password policy appears in the tooltip.
2. To continue, click on "Summary".

Result

The "Summary" page is displayed.

Change password

Requirement

- The "Drive data encryption" function is activated.
- The drive password used to encrypt the drive data in the backup file is known.
- You are logged in as a user with the "Edit device configuration or drive applications" right.

Procedure

1. Open the "Protection & Security" function view.
2. Click the "Start Security Wizard" button.
   The "Welcome to the Security Wizard" page is displayed.
3. Click the "Change security settings" button.
4. In the Security Wizard, navigate to the "Drive data encryption" page.
5. Click the "Change password" button.
   A corresponding dialog opens.
6. Enter the currently valid password.
7. Enter a password of your choice twice.
   The password must comply with the password policy. The applicable password policy appears in the tooltip.
8. Click the "Change password" button.
9. Click "Finish" to apply the changed settings.
   The "Finish" button is only activated if the current page contains settings that can be changed and have been changed.

Result

The changed settings are saved in the converter so they are protected against power failure.

Deactivate drive data encryption

Requirement

- The "Drive data encryption" function is activated.
- The drive password used to encrypt the drive data in the backup file is known.
- You are logged in as a user with the "Edit device configuration or drive applications" right.

Procedure

1. Open the "Protection & Security" function view.
2. Click the "Start Security Wizard" button.
   The "Welcome to the Security Wizard" page is displayed.
3. Click the "Change security settings" button.
4. In the Security Wizard, navigate to the "Drive data encryption" page.
5. Click the "Deactivate encryption" button.
   A corresponding dialog opens.
6. Enter the currently valid password.
7. Click the "Deactivate encryption" button.

   Note

   Restoring drive data from an encrypted backup file

   If you deactivate the "Drive data encryption" function after creating a backup file, you will still need the drive password to restore the encrypted drive data. Restoring the drive data without knowing the drive password is not possible in this case.

   For more information on the "Backup and restore" function in the web server, refer to the product information for the converter used.

8. Click "Finish" to apply the changed settings.
   The "Finish" button is only activated if the current page contains settings that can be changed and have been changed.

Result

The changed settings are saved in the converter so they are protected against power failure.

12.2.3.8 Summary

Overview

The completed security settings are summarized on the "Summary" page.

Requirement

- The Security Wizard is started.

Procedure

1. Click "Finish" to finish and apply the settings in the Security Wizard.
   The web server checks the security settings. You will receive a message indicating whether the settings were completed successfully.
2. Select the option you want to continue with.
   The following options are available:
   - Quick setup
   - Advanced setup
   - Free navigation through the web server menus
3. To confirm the selection, click "Next".

Result

The Security Wizard is ended and the settings are applied to the converter.

12.2.3.9 Changing security settings

Requirement

- Depending on which settings you want to change, you are logged in as a user with the "Manage users and roles" and/or "Edit device configuration and drive applications" right.

Procedure

1. Open the "Protection & Security" function view.
2. Click the "Start Security Wizard" button.
   The "Welcome to the Security Wizard" page is displayed.
3. Click the "Change security settings" button.
4. Please pay attention to the information on the individual pages.
5. Change the security settings as required.
6. Click "Finish" to apply the changed settings.
   The "Finish" button is only activated if the current page contains settings that can be changed and have been changed.

Result

The web server checks the security settings. If the process can be completed, the settings are stored so they are protected against power failure.

The "Protection & Security" function view is displayed.

12.2.4 Working with low security settings

Overview

On the "Welcome to the Security Wizard" page, you can select the option "Continue with low security settings". This means you will skip the configuration of the security settings in the Security Wizard, see section "Configuring settings for full protection (Page 163)".

If UMAC is enabled, this option is only available again after resetting all user-defined settings to factory settings. You can find more information in section "Deletion of customer data on the converter (Page 85)".

Requirement

NOTICE
Data manipulation due to low security settings Inadequately protected converter data and functions make it easier for potential attackers to gain unauthorized access to the converter. Data manipulation can change the Safety Integrated settings or generally disrupt or damage the converter. • Use the low security settings only in exceptional cases and only for a very limited period. Make sure that no unauthorized persons can access the converter, e.g. when the converter is not yet connected to a network. • Carry out an information security risk assessment. Use the low security settings only if this option poses no risk according to the result of the risk assessment.

- The web server is being called for the first time.
- The basic settings have been made.
  You can find more information in section "Making basic settings when the web server is called for the first time (Page 163)".

Procedure

1. On the Security Wizard welcome page, select the option "Continue with low security settings".
   A security note is displayed.
2. To confirm the message, click "Next".
   The Security Wizard is closed.
   You can start the Security Wizard at a later time and configure the settings.

Result

The settings to access the web server are the same as the factory settings. In the factory settings, access to the web server is predefined as follows:

- Access via the service interface X127 and PROFINET interface X150 over HTTPS is activated
  To establish a secure HTTPS connection to the converter, proceed as described in section "Establish a protected HTTPS connection to the web server (Page 188)".
- Access via the service interface X127 over HTTP is deactivated.

More information

More information about the factory settings for ports and protocols can be found in section "Ports and protocols (Page 184)".

12.2.4.1 Modifying security settings

Requirement

- The first time the web server was called, you selected the option "Continue with low security settings".

Procedure

1. Open the "Protection & Security" function view.
2. Click the "Start Security Wizard" button.
   The "Welcome to the Security Wizard" page is displayed.
3. Click the "Configure security settings" button.
4. Change the settings as required. Please pay attention to the information on the individual pages of the Security Wizard.
   You can find more information on the individual steps in the following sections:
   - Activating UMAC (Page 164)
   - Setting up a user with the "Drive Administrator" role (Page 164)
   - Configure guest access (Page 165)
   - Web server activation (Page 167)
   - Drive data encryption (Page 169)
   - Summary (Page 171)
5. Click "Finish" to apply the settings.
   The "Finish" button is activated once all the steps in the wizard have been completed.

Result

The web server checks the security settings. If the process can be completed, the settings are stored so they are protected against power failure.

The "Protection & Security" function view is displayed.

More information

- Reloading pages while the Security Wizard is running:
  If you start the Security Wizard to subsequently modify the security settings and use <F5> or ↻ to reload the pages of the web server, the Security Wizard will close. The web server displays the "Protection & Security" function view. The changed settings are not saved.

12.2.4.2 Protecting the Safety configuration

Overview

If UMAC is not activated, the configuration of the Safety Integrated settings is not protected. Users can access the drive data and change the Safety configuration without authentication.

The message A01637 "Safety configuration not protected" is displayed.

For more information on the message A01637 "Safety configuration not protected", refer to the SINAMICS List Manual for G220.

Requirement

- The first time the web server was called, you selected the option "Continue with low security settings".
- Safety Integrated settings are configured.

Procedure

Proceed as follows to activate UMAC and acknowledge the message A01637 "Safety configuration not protected":

1. Proceed as follows to activate UMAC and configure the security settings, see section "Modifying security settings (Page 174)".
2. Switch the converter off and on again.

Result

After the start-up, the alarm is no longer displayed.

12.3 User management and access control (UMAC)

Overview

User Management and Access Control (UMAC) enables you to manage access to the converter. This involves creating user accounts and managing them. You allocate roles to user accounts allowing read or write access to specific functions. Access to the converter data and functions is defined using predefined roles.

UMAC must be activated to be able to create and edit user accounts for access to the converter.

Note

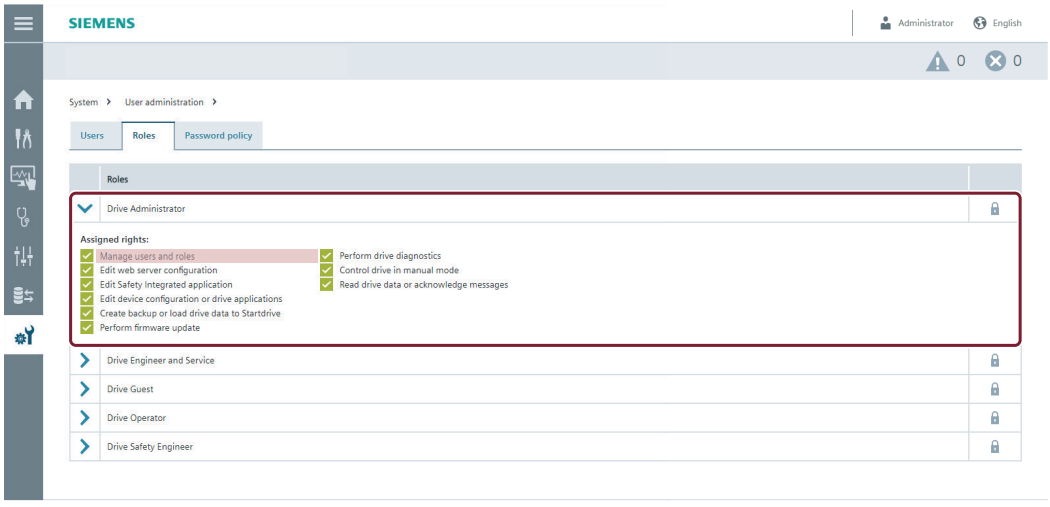
POWER ON with inserted memory card

Files on a memory card are transferred to the converter irrespective of the configured UMAC settings. The operation requires no authentication.

For information about additional protective measures for memory card slots, see section "Additional protective measures for hardware reports (Page 71)".

Users with the "Manage users and roles" right

When UMAC is activated in the Security Wizard, the user is prompted to create a user with the "Drive Administrator" role. This role is associated with the "Manage users and roles" right.



The assigned rights give this user full access to the converter data and functions. The "Manage users and roles" right authorizes this user to create, edit and manage other user accounts.

In user management, other users can be configured with the "Drive Administrator" role

For more information about the characteristics of users with the "Drive Administrator" role, see section "Administrators (Page 60)".

"Anonymous" user

The predefined "Anonymous" user account is available in user management. This user does not require authentication when accessing the converter.

The following roles are assigned to the user by default:

- Drive Ext. Role Fieldbus
- Drive Ext. Role SDI Standard/Adv

When the "Enable guest access to the drive" option is activated in the Security Wizard, the "Anonymous" user is automatically assigned the "Drive Guest" role.

For more information about the characteristics of the "Anonymous" users, see ""Anonymous" user (Page 61)".

Standard configuration of roles and rights

After the Security Wizard is completed with default settings, the "Anonymous" user has the following authorizations:

Options	Roles	Authorizations
Access with the following fieldbus protocols: • PROFINET • DCP • SNMP • S7 Protocol for PCS7	Drive Ext. Role Fieldbus	For access via fieldbus protocols, the "Anonymous" user in the standard configuration has read and write access to the converter data and functions. The role does not contain write rights for the following functions: • User Management and Access Control (UMAC) • Safety Integrated Functions The user does not need to be authenticated. **Note** For access via the PROFINET protocol: • With cyclic communication, the UMAC settings are not considered. • With acyclic communication, the "Anonymous" user is used for access. **Note** For access via the DCP protocol: • For read access via DCP, the UMAC settings are not considered.
Access via the SINAMICS SDI Standard Panel	Drive Ext. Role SDI Standard/Adv	For access via the panel, the "Anonymous" user in the standard configuration has read and write access to the converter data and functions. The role does not contain write rights for the following functions: • User Management and Access Control (UMAC) • Safety Integrated Functions The user does not need to be authenticated.

More information about the roles and rights can be found in section "Roles for access to the converter with runtime function rights (Page 64)".

Extend or restrict authorizations

Certain functions such as acyclic fieldbus communication require the use of the "Anonymous" user. Because this user is able to access the converter without authentication, the attack surface for unauthorized access is larger. When the "Anonymous" user is activated, the security is reduced according to the extent of the rights that you give to this user. When activating the user, you will receive security information about the potential risk.

You are recommended to verify the assigned roles and rights for the "Anonymous" user. Identify the potential risks arising from the assigned authorizations and take appropriate protective measures.

12.3.1 System limits

Description

If UMAC is activated the following system limits apply:

Setting	Quantity
Maximum number of users	64
Names for user accounts: maximum number of characters	100
Password length: maximum number of characters	120

12.3.2 User management

12.3.2.1 Creating a new user account

Requirement

- You are logged in as a user with the "Manage users and roles" right.

Procedure

1. Call the "Users" function view with "System > User management > Users".
   The list of existing users is displayed.
2. Click on "Add user".
   The dialog box for this opens.
3. Enter a user name.
4. Assign a password.
   The applicable password policy appears in the tooltip .
   Only use ASCII characters.
5. Enter the password in the "Confirm password" field.
   A message is displayed if the entries do not match.

6. Select one or more roles from the drop-down list "Assigned roles".
   The rights for each role appear in the tooltip .
7. Optionally, specify a session timeout.
   Valid values: 1 to 600 min.
   The session timeout is suspended in the following cases:
   - During relatively long operations such as firmware updates until the operation has completed.
   - If the control panel is active.
8. Confirm your entries with "OK".
   The dialog closes.
9. Click to save the settings in a non-volatile fashion.
   The Save icon is not shown if the "Save automatically" function is activated.

Result

The new user account is activated and appears in the list of users.

More information

There is detailed information about assigning rights to the available roles in section "Roles for access to the converter with runtime function rights (Page 64)".

12.3.2.2 Editing users

Requirement

- You are logged in as a user with the "Manage users and roles" right.

Procedure

Icon	Explanation
	Clicking on this icon opens the "Edit user" dialog. This dialog enables you to change the settings for a user account.
	Clicking on this icon deactivates the user account. Users to whom this user account is allocated will not be able to access the converter.
	Clicking on this icon activates the user account. Users to whom this user account is allocated are able to access all or only certain converter data and functions. **Note** Converter data and functions are displayed according to the access rights assigned to the user account.
	Clicking on this icon deletes the user account. The user account is deleted only once the action has been confirmed via the confirmation prompt in the corresponding dialog.

12.3.2.3 Editing the "Anonymous" user

Requirement

- You are logged in as a user with the "Manage users and roles" right.

Procedure

Icon	Explanation
	Clicking on this icon opens the "Edit user" dialog. This dialog enables you to change the role assignment for the user.
	Clicking on this icon deactivates the user. Access to the converter data and functions is only possible with authentication.
	Clicking on this icon activates the user. Access to the converter data and functions is possible without authentication. **Note** For access without authentication, converter data and functions are displayed according to the access rights assigned to the "Anonymous" user.

12.3.2.4 Password policy

Overview

In the "Password policy" tab of the "User management" function view, the following are specified:

- Password complexity
- Password renewal

The policy applies globally to all users who need to authenticate themselves.

You can change the policy and specify whether and according to which rules the assigned passwords must regularly be renewed.

Only use ASCII characters.

Password complexity

The password complexity is specified with the following settings:

Policy	Factory setting	Adjustable values
Minimum password length	8 characters	Valid values: 8 - 32 characters
Minimum number of characters	1	Valid values: 0 - minimum password length
Minimum number of special characters	0	Valid values: 0 - minimum password length
At least one uppercase letter and one lowercase letter	Yes	Yes/no

Password renewal

The time and rules for password renewal are specified with the following settings:

Policy	Factory setting	Adjustable values
Number of last used locked passwords	5	Valid values: 1 - 10
Activate password aging	Deactivated	Activated/deactivated
Password validity	60 days	Valid values: 0 - 365 days
Advance warning time for expiring password	5 days	Valid values: 0 - 365 days Must not be longer than the password validity.

12.3.2.5 Change password policy

Requirement

- You are logged in as a user with the "Manage users and roles" right.

Procedure

1. Call the "Password policy" function view with "System > User management > Password policy".
2. Configure the password complexity settings.
3. Activate password renewal and make the required settings.
4. Confirm the entries with "Apply settings".
5. Click to save the settings in a non-volatile fashion.
   The Save icon is not shown if the "Save automatically" function is activated.

12.3.2.6 Changing your own user password

Overview

Users with an active user account can change their own password themselves at any time. However, the name of the user can only be changed by a user with the "Manage users and roles" right

If password renewal is activated, users must change their password at a specified interval. If the password expires, the user is prompted to renew the password at the next login.

Requirement

You have an active user account to access the web server and converter.

Procedure

1. On the home page of the web server, click on the name of your user account in the upper right corner.
   A drop-down list is opened.
   If your password has already expired, the password dialog "Password has expired" appears. Then proceed as described from step 3.
2. Select the "Change password" option .
   The "Change password" dialog opens.
3. Enter the old password.
4. Enter a new password.
5. Enter the new password again.
6. Confirm your entries with "OK".
7. Click to save the settings in a non-volatile fashion.
   The Save icon is not shown if the "Save automatically" function is activated.

Result

Your password has been changed.

12.3.3 Access control

12.3.3.1 User roles and access rights

Overview

User accounts can be assigned roles to which certain function rights are attached. The access concept provides for the assignment of different roles.

Requirement

- You are logged in as a user with the "Manage users and roles" right.

Procedure

Call the "Roles" function view with "System > User management > Roles".

More information

There is detailed information about assigning function rights to the available user roles in section "Roles for access to the converter with runtime function rights (Page 64)".

12.3.4 Checking UMAC settings

Overview

In the "User Management & Access Control" area of the "Protection & Security" function view there is a general overview of the current UMAC settings.

UMAC settings that have already been made in the Security Wizard can be changed in the wizard. You can find more information on this in section "Changing security settings (Page 172)".

All UMAC settings can also be changed in the "User management" function view.

Requirement

- You are logged in as a user with the "Manage users and roles" right.

Procedure

1. Open the "Protection & Security" function view.
2. Open the "User Management & Access Control" drop-down list.
3. Check the displayed UMAC settings.

12.3.5 Resetting the UMAC settings

For more information on resetting all user-defined settings to factory settings, see section "Deletion of customer data on the converter (Page 85)".

12.4 Ports and protocols

12.4.1 Activating/deactivating ports and protocols

Overview

In the "Ports and protocols" function view, you configure the interfaces to access the converter. Apply the principle of least functionality by deactivating the protocols that are not needed for access to the converter.

You will find detailed information about the ports and protocols and the factory settings in section "Least functionality of ports and protocols (Page 68)".

Requirement

You are logged in as a user with the "Edit device configuration or drive applications" right.

Procedure

1. Open the "Protection & Security" function view.
   The "Ports and protocols" drop-down list is open by default.
2. Configure the interfaces to access the converter.
3. Click to save the settings so they are protected against power failure.
   The Save icon is not shown if the "Save automatically" function is activated.

Result

The settings are saved in the converter.

If you have disabled the interface that you are using to access the web server, you will be logged out of the converter. Log into the web server using an active interface.

12.5 Firmware update

12.5.1 Firmware update

More information

There is basic information about the function in section "Firmware update (Page 79)".

You will find more detailed information about the function in the web server in the following documentation for the product in question.

- Operating Instructions
- Commissioning Manual

12.6 Backup and restore

More information

There is basic information about the function in section "Backup and restore (Page 80)".

You will find more detailed information about the function in the web server in the following documentation for the product in question.

- Operating Instructions
- Commissioning Manual

12.7 Certificates for protected communication

12.7.1 Fundamentals

Overview

The HTTPS connection between the operating unit and the converter must be protected.

To establish a protected HTTPS connection to the web server, a valid certificate is required. This certificate is generated automatically in the converter.

Certificate types

The following table provides an overview of the certificates used and their characteristics:

Certificate type	Description
HTTPS certificate	• Generated automatically when the web server is called for the first time. The necessary certificate files are included in the firmware files of the converter. • Contains the IP address of the interface used for the communication. – Behavior when the IP address is changed: If the IP address of the interface is changed during commissioning or later, the HTTPS certificate loses its validity. The HTTPS certificate is automatically replaced with a new HTTPS certificate the next time the web server is called.
Root certificate	• Has a validity period of 2199 days. • The certificate is included in the firmware files of the converter. • Needed in order for the HTTPS certificate to be signed by a trusted root certification authority.

Certificate attributes

Certificates contain information about the issuer.

Attribute	Meaning	Example
O	Organization	SIEMENS
C	Country/region	EN
CN	Common name	SINAMICS Embedded Issuing CA, *serial number*=<SN>
OU	Organizational unit	Copyright (C) SIEMENS AG 2022 All rights reserved

Security warning with non-secure HTTPS connection

Browsers classify automatically generated certificates as not trusted, and they issue a security warning when an HTTPS connection is called. In these situations, the browser can establish a non-secure HTTPS connection to the web server.

Certificate management

The following table shows essential features of the listed browsers concerning certificate management in the Microsoft Windows system:

Browser[1)]	Version	Engine	Certificate management
Google Chrome[2)]	≥ Version 83	Chromium	Chromium-based browsers only access certificates that are saved in the certificate store of the Microsoft Windows system.
Microsoft Edge	≥ Version 88		
Mozilla Firefox	≥ Version 91	Geko	Mozilla Firefox has its own certificate management integrated in the browser.

1) Whichever browser you use, we recommend using the most up-to-date version.

2) For Windows 10 > Version 1803, we recommend Google Chrome.

12.7.2 Establish a protected HTTPS connection to the web server

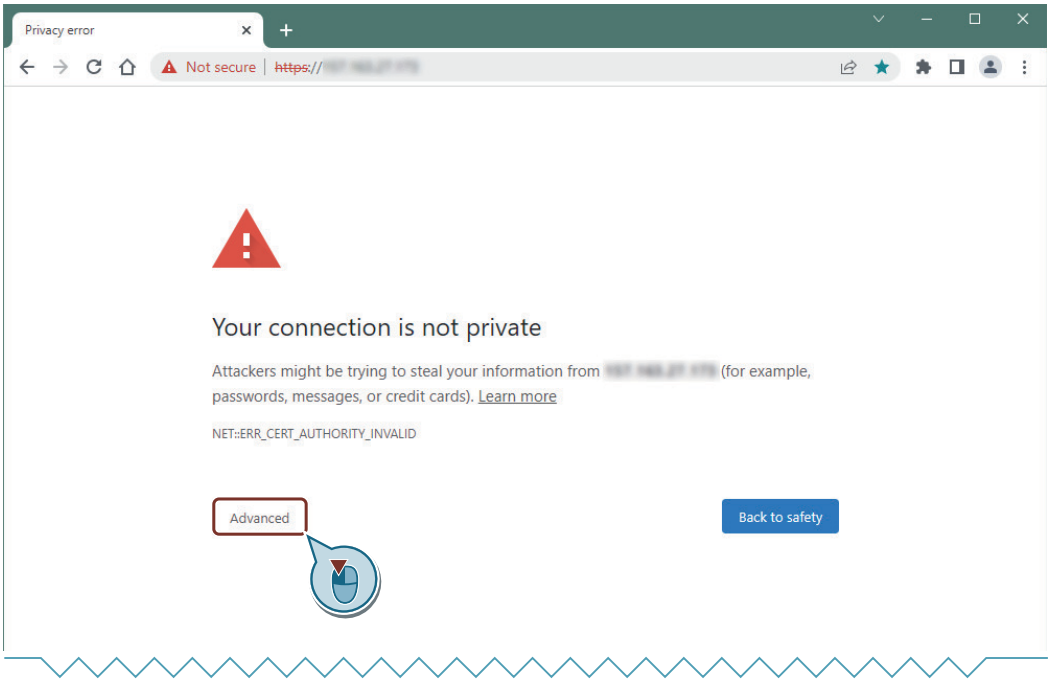
Requirement

- The converter and operating unit are connected to each other.
  The settings for interfaces X127 and X150 are contained in the "Protection & Security" function view.
- The web server is being called for the first time over an HTTPS connection.
- You have administrator rights on the operating unit.
  The administrator rights are needed in order to make changes in the certificate store of the Microsoft Windows system.

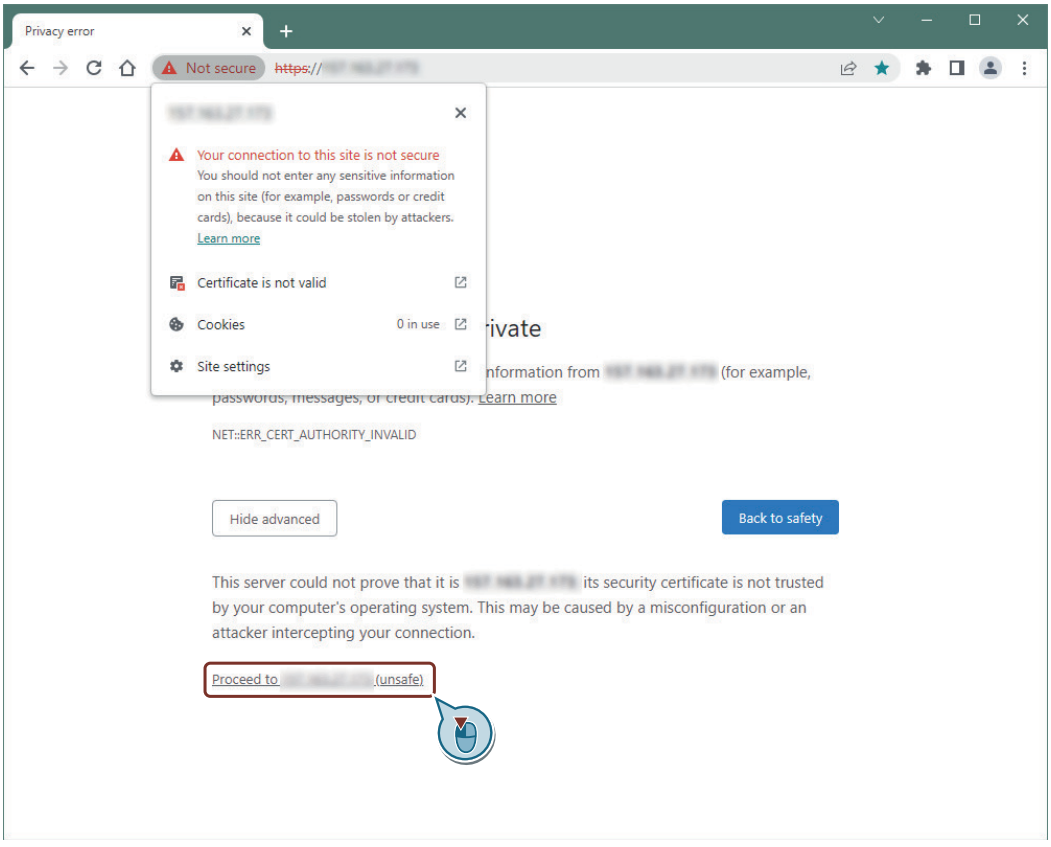
Procedure

1. Open the browser in your operating unit.
2. Call the web server using the IP address of your converter, e.g. https://169.254.11.22.
   The web browser classes the HTTPS connection as non-secure.

3. Click the "Extended" button.

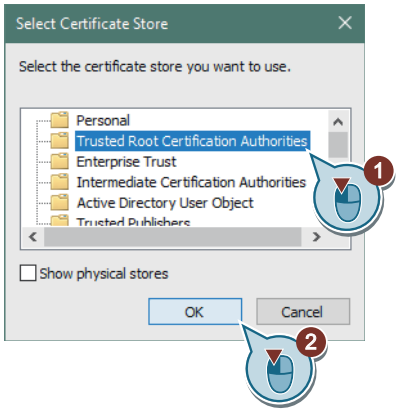


4. Click the "Continue to ... (non-secure)" button.
   The web server is called. The function view is displayed with the basic settings for the web server.



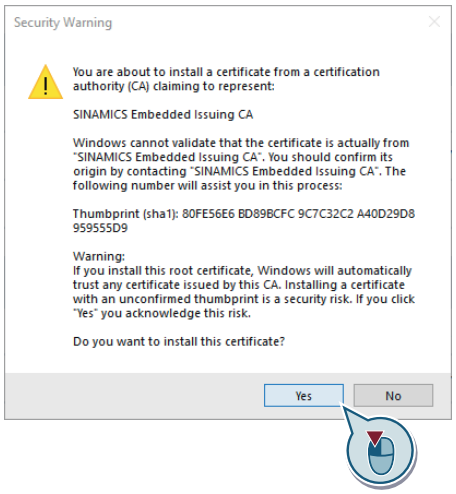
5. Make the basic settings for the web server.
   You can find more information in section "Making basic settings when the web server is called for the first time (Page 163)".
6. Click "Next".
   The "Welcome to the Security Wizard" page is displayed. One of the following options can be selected:
   - "Configure security settings":
     We recommend this setting for comprehensive protection.
   - "Continue with low security settings":
     If you select the option "Continue with low security settings", the converter is operated without UMAC settings. Users are able to access the converter data and functions without authentication.
     You can start the Security Wizard at a later time in the "Protection & Security" function view and make the necessary changes to the security settings.
7. If you selected the option "Configure security settings", proceed as follows, see section "Configuring settings for full protection (Page 163)". Now open the "Protection & Security" function view.
8. If you selected the option "Continue with low security settings", after confirming the message with "Next" you will see the "Protection & Security" function view.

9. Open the "Certificates" drop-down list.
   The information shown cannot be edited.
10. Click "Download certificate to operating panel".
    The "ROOT_CERT.DER" file is downloaded to the downloads folder of the operating unit. The file appears in the browser's download bar.
11. Optional: Move the file to the preferred folder on your operating unit.
    Choose a folder that all local users are able to access.
12. Open the file directly from the browser's download bar.
    The certificate information is displayed.
13. Optional: Open the folder containing the file "ROOT_CERT.DER" and double-click on the file.
    The certificate information is displayed.
14. Click "Install certificate".
    The "Certificate Import Wizard" appears.
    The option "Current Users" is selected.
15. Click "Next".
16. Select the option "Place all certificates in the following store".
17. Click "Browse...".
18. From the list of certificate stores, select the "Trusted Root Certification Authorities" store and then click "OK".
    The selection appears in the "Certificate store" field.



19. Click "Next".
    The selected settings are displayed.

20. Click "Finish".
    A security warning is displayed.



21. To install the certificate, click "Yes".
    A message appears indicating that the import operation was successful.

Result

The root certificate has been imported into the certificate store of the operating unit.

If you call the web server again, the browser classes the HTTPS certificate as trusted and establishes a protected HTTPS connection to the web server.

12.7.3 Display information about the certificates

Overview

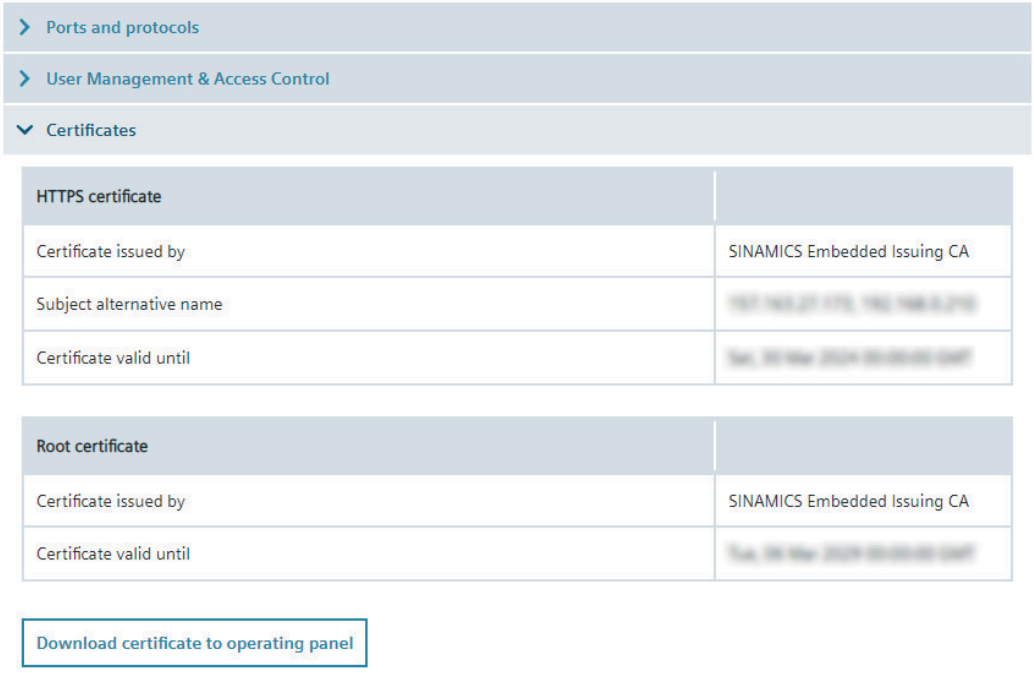
In the "Protection & Security" function view, the web server shows basic information about the certificates used. The information shown is generated automatically and cannot be edited.

Requirements

- The converter and operating unit are connected to each other.
  The settings of interfaces X127 and X150 are contained in the "Protection & Security" function view.
- You are logged in as a user with the "Manage users and roles" right.

Procedure

1. Open the "Protection & Security" function view.
2. Open the "Certificates" drop-down list.



Appendix

A

A.1 Additional information

Description

You can find more information about industrial cybersecurity on the Internet:

- Industrial Cybersecurity Services (https://support.industry.siemens.com/cs/ww/en/sc/4973)
- Cyber security (https://new.siemens.com/global/en/company/topic-areas/cybersecurity.html)
- Always active (https://new.siemens.com/global/en/products/automation/topic-areas/industrial-security/certification-standards.html#Alwaysactive)
- Certifications and standards (https://new.siemens.com/global/en/products/automation/topic-areas/industrial-security/certification-standards.html)

Glossary

Allowlist

An allowlist is a positive list that can be used to protect IT systems. The allowlist is based on the approach that basically everything that is not explicitly entered in the list is prohibited. As a consequence, only requested and trustworthy entries are in the allowlist. This means that the entries in the list represent exceptions to the general block rule.

Attack

An attempt to destroy a resource, to deprive it of its protection, to change it, to deactivate it, to steal it, to gain unauthorized access to it or to use it in an illegal way.

Attack surface

The scope to which a system can be deprived of its protection so that it can be attacked.

Authentication

Verification of the identity of a user, process or device, frequently as prerequisite for the permission to access resources.

Authenticity

Proof of authenticity of electronic data means proof that the data is genuine (see "Integrity") and is uniquely assigned to the author, creator and/or sender. Protecting the authenticity of electronic data is only possible in combination with measures to protect its integrity (see "Integrity").

Examples of protective measures include the use of digital signatures and certificates.

Authorization

The right granted by a system entity to access a system resource.

Availability

Property to be accessible and usable when requested by an authorized entity.

Brute force

There are no efficient algorithms for solving many of the problems in computer science. The most natural and simplest approach to an algorithmic solution for a problem is to simply try out all possible solutions until the correct one is found. This method is called brute-force searching. One typical application is given again and again when it comes to

listing an example of brute-force searching - the "cracking" of passwords. Passwords are often encrypted using cryptographic hash functions. Directly calculating the password from the hash value is practically impossible. However, a password cracker can calculate the hash values of numerous passwords. If a value matches the value of the stored password, then the password (or another, randomly matching password) has been found. In this case, brute force refers to the simple trial and error approach of entering every possible password.

Cloud computing

Cloud computing is the storage of data in a remote data center, and can also involve the execution of programs that are not installed on local computers, but rather in the (metaphoric) cloud.

Confidentiality

Property which ensures that the information is not made available or disclosed to unauthorized individuals, entities or processes.

Cyber security

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It also includes the security of information technologies and electronic information. The term is broad and applies to everything from computer security to disaster recovery, i.e. the restoration after an incident, to the training of end users.

Defense in depth

Creation of multiple security mechanisms, especially in a layer structure, with the intention of making attacks more difficult.

Denial of service (DoS)

Denial of service (DoS) is the non-availability of an IT-based service that is normally available. Although there can be many reasons for such non-availability, the term "DoS" is generally used when infrastructure systems are overloaded. This can be the result of an unintentional overload or through a deliberate attack on a server, a computer or other components in a network.

DMZ

The demilitarized zone is an autonomous subnet that separates the local area network (LAN) from the Internet through firewall routers (A and B). The firewall routers are configured in such a way that they reject data packets for which there were no previous data packets. If a data packet is sent from the Internet to the server, it is therefore rejected by firewall router A. If, however, a hacker gains access to a server within the DMZ and sends data packets to the LAN in an attempt to analyze or hack it, these are rejected by firewall router B.

Firewall

Device to connect networks with one another, which restricts the exchange of data between two connected networks.

Hacker

Person involved in an intentional hacking activity. The reasons for these activities can be malicious or not malicious, or also remain within the limits of what is ethically and legally acceptable.

Hardening

Procedure in which the security of a system is increased by reducing the attack surface.

Incident

One or more unwanted or unexpected events that impair the company operation and endanger the information security. The cause can be security vulnerabilities, incorrect configurations or misconduct and their exploitation.

Industrial cybersecurity

Measures to increase the industrial security standards of a plant. They protect against unauthorized access to higher-level control systems, industrial controls and PC-based systems of the plant as well as against cyber attacks.

Information security

Safeguards the confidentiality, integrity and availability of information.

Information security risk assessment

In an information security risk assessment, important security measures for applications are identified, evaluated and implemented. Security vulnerabilities and weak points in the applications will also be prevented.

Integrity

Proof of integrity of electronic data means proof that the data is complete and unchanged. Protecting the integrity of electronic data is only possible in combination with measures to protect its authenticity (see "Authenticity").

Examples of protective measures include the use of cryptographic processes.

Internet of Things (IoT)

General term for technologies of a global infrastructure of information organizations which allow physical and virtual objects to be linked together and allows them to work together via information and communication techniques.

IPsec (Internet Protocol Security)

IPsec is an expansion of the Internet protocol (IP) to include encryption and authentication mechanisms. This way, the Internet protocol can transport cryptographically secured IP packets via insecure public networks.

Malware

Malware is a general term for programs that have been developed to damage users. There are numerous types of malware, e.g. viruses, trojans, rootkits or spyware.

Man-in-the-disk attack

The concept of a "man-in-the-disk" attack is similar to that of a "man-in-the-middle" attack as it includes intercepting and editing data, which is exchanged between an external memory and an application.

Man-in-the-middle attack

In cryptography and cyber security, a man-in-the-middle attack is a cyber attack where the attacker secretly interjects in the communication between two parties and possibly changes the associated data. The two parties involved think that they are directly communicating with one another as the attacker interjected himself between the two parties.

NAT (Network Address Translation)

NAT is a process used in IP routers that connect local networks to the Internet. Since, in general, Internet access is only via one IP address (IPv4), all other nodes in the local network require a private IP address. Private IP addresses can be used several times, but are not valid in public networks. For this reason, nodes with a private IP address cannot communicate with nodes outside the local network. In order for all computers with a private IP address to have access to the Internet, the Internet access router must replace the IP addresses of the local nodes with a separate, public IP address in all outgoing data packets. In order for the incoming data packets to be assigned to the correct station, the router saves the current TCP connections in a table. The NAT router "memorizes" which data packets belong to which TCP connection. This process is called NAT (Network Address Translation).

OpenVPN

OpenVPN is a program to establish a virtual private network (VPN) via a protected TLS connection. Libraries belonging to the OpenSSL program are used to encrypt the communication. OpenVPN uses either UDP or TCP for transferring data.

Operating unit

An operating unit is a programming device, a PC, a notebook, or a mobile end device such as a tablet or smartphone.

Patch management

Area of the system management whose tasks include the procurement, testing and installing of several patches (code changes) for an administered computer system or in such a system. At the same time, a subprocess of the Security Vulnerability Management whose tasks include the correction and containment of security vulnerabilities for Siemens products by means of software corrections.

Patterns of viruses

Designation for the database of virus scanners, which contains the schematic and code-specific structure of all known viruses. This is usually a file that is used and processed by the virus scanners. The schemata contained in the file are used when checking for viruses and with them the files to be checked are compared.

Phishing

The term "phishing" describes the threat of "using bait to fish for passwords" in emails, via counterfeit links or even text messages (e.g. SMS). What are known as "phishers" attempt to obtain data via serious or official-looking emails and websites. With the aid of malware, they exploit weak points, e.g. in the operating system or web browser.

Remote access

Use of systems which are within the perimeter of the security zone and that can be accessed from another geographical location with the same rights as if the systems were physically at the same location.

Security

Safeguards the confidentiality, integrity and availability of a product, a solution or a service.

Security vulnerability

Weak point in a computer system that allows an attacker to violate the integrity of the system. As a rule, this is the result of program errors or design defects in the system.

A weak point of a resource or operator element that can be exploited by one or more threats.

SIEM system

SIEM stands for Security Information and Event Management. Such systems are able to identify and evaluate security-relevant events and notify the administrator.

Switch

Network component for connecting several end devices or network segments in a local network (LAN).

Threat

Potential cause of an undesirable incident which may result in damage to a system or organization.

VPN (Virtual Private Network)

A protected connection of computers or networks via the Internet. It enables confidential data to be exchanged via public networks.

WSUS (Windows Server Update Services)

Windows Server Update Services (WSUS in short) is the software component of the Microsoft Windows Server since Version 2003 which is responsible for patches and updates. It is the successor version of the Software Update Services software component.

More information

Siemens:
www.siemens.com

Industrial Security:
www.siemens.com/industrialsecurity

Siemens AG
Digital Industries
Motion Control
Postfach 3180
91050 Erlangen
Germany

Scan the QR-Code for product information