SIEMENS

Edition 03/2023

CONFIGURATION MANUAL

SINAMICS

SINAMICS converter from firmware V6.1

Industrial Security Guideline

www.siemens.com/drives

SIEMENS

SINAMICS

Converters
Industrial Security

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 V6.1 or higher
Startdrive V18 SP1 or higher

03/2023, FW V6.1
A5E52484547B AA

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 AA
Ⓟ 04/2023 Subject to change

Table of contents

1 Introduction 9

1.1 About SINAMICS 9

1.2 About this manual 9
1.2.1 Content 9
1.2.2 Sales law 9
1.2.3 Target group 10
1.2.4 Standard scope 10
1.2.5 Websites of third-party companies 10

1.3 SINAMICS documentation 11

1.4 Service and Support 12
1.4.1 Siemens Industry Online Support on the Web 12
1.4.2 Siemens Industry Online Support on the road 12
1.4.3 Getting information about the product 13
1.4.4 Feedback on the technical documentation 14
1.4.5 mySupport documentation 14
1.4.6 Technical support 15
1.4.7 Training 16
1.4.8 Spare parts services 16

1.5 Important product information 16
1.5.1 Open-source software (OSS) 16
1.5.2 Compliance with the General Data Protection Regulation 17

2 Fundamental safety instructions 19

2.1 General safety instructions 19

2.2 Warranty and liability for application examples 19

2.3 Security information 19

3 Basic information 21

3.1 Data security in the industrial environment 21

3.2 Industrial security 22

3.3 Functional safety and industrial security 22

4 Security measures in automation and drive technology 25

4.1 Security measures 25

5 Security management 27

6 Operating environment and general security measures 29

6.1 Defense in depth concept 29

6.2 Security requirements for the intended operating environment 30

6.3 Plant security 30

6.3.1 Physical protection of critical production areas ... 31

6.4 Network security ... 32
6.4.1 Network segmentation ... 32
6.4.1.1 Separation between production and office networks ... 32
6.4.1.2 Network segmentation with SCALANCE S ... 33
6.4.2 Cloud Security ... 36

6.5 System integrity ... 36
6.5.1 IT infrastructure hardening measures ... 37
6.5.1.1 Services and ports ... 37
6.5.1.2 User accounts ... 37
6.5.1.3 Operating units used in the industrial context ... 37
6.5.1.4 Store sensitive data securely ... 38
6.5.1.5 Transport sensitive data securely ... 39
6.5.1.6 Secure passwords ... 39
6.5.1.7 Virus scanner ... 40
6.5.1.8 Allow lists ... 40
6.5.1.9 Product security notifications ... 40
6.5.2 Patch management ... 41
6.5.2.1 Windows patch management ... 41
6.5.2.2 Program updates in the TIA Portal ... 42
6.5.3 Data integrity ... 42

7 System overview ... 45

7.1 Communications interfaces ... 45
7.1.1 Service interface X127 ... 45
7.1.2 PROFINET interface X150 ... 46

7.2 Communication links ... 47

8 Security functions ... 49

8.1 Secure network ... 49

8.2 Identity and access management ... 49
8.2.1 Authentication mechanisms for users ... 49
8.2.2 Managing login data and user IDs ... 50
8.2.2.1 Restoring UMAC settings ... 52
8.2.2.2 Resetting the UMAC settings ... 52
8.2.2.3 Transferring and saving UMAC settings ... 53
8.2.3 Roles and function rights ... 54
8.2.3.1 Engineering roles with engineering function rights (only for Startdrive) ... 54
8.2.3.2 Roles for converters with runtime and engineering function rights ... 55
8.2.3.3 Roles for converters with runtime function rights ... 56
8.2.4 User Management and Access Control in the web server ... 58
8.2.4.1 User management in the web server ... 58
8.2.4.2 Characteristics of access control in the web server ... 59
8.2.4.3 Users with the "Drive Administrator" role ... 60
8.2.4.4 "Anonymous" user ... 61
8.2.5 User Management and Access Control in Startdrive ... 63
8.2.5.1 User management in Startdrive ... 63
8.2.5.2 Characteristics of access control in Startdrive ... 64
8.2.5.3 Users with the function right "Manage users and roles" ... 66
8.2.5.4 "Anonymous" user ... 67

8.3 Reduction of the attack surface ... 68
8.3.1 Least functionality of ports and protocols ... 69
8.3.2 Least functionality of hardware reports ... 71
8.3.3 Additional protective measures for hardware reports ... 72
8.3.4 Least functionality of software applications and functions ... 72

8.4 Secure communication channels and protected data storage ... 73
8.4.1 Protecting sensible data when being transferred (data in transit) ... 73
8.4.2 Protection of sensitive data when stored (data at rest) ... 73
8.4.3 Protection of UMAC data ... 74
8.4.4 Certificates for protected data transmission in web server ... 74
8.4.4.1 Digital certificate ... 74
8.4.4.2 Using an automatically generated certificate ... 74
8.4.4.3 Validating automatically generated certificates ... 75
8.4.4.4 Certificate management ... 75

8.5 System integrity ... 76
8.5.1 Software and information integrity ... 76
8.5.2 Verification of security functions ... 78
8.5.3 Input validation ... 78
8.5.4 Identify and address fault conditions ... 79
8.5.5 Timed distribution and synchronization ... 79
8.5.6 Firmware update ... 79
8.5.7 Backup and restore ... 80

8.6 Logging and monitoring ... 81
8.6.1 Monitoring access from untrusted zones ... 81
8.6.2 Logging of events ... 81
8.6.3 Monitoring and accessing logs ... 82

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

9.1 Secure operation ... 83

9.2 Secure disposal ... 83
9.2.1 Deletion of customer data on the converter ... 83
9.2.2 Dispose of memory cards securely ... 84

10 Security programs ... 87

11 Security settings in Startdrive ... 89

11.1 Default security settings ... 89
11.1.1 Default security settings in Startdrive ... 89
11.1.1.1 Configure access to Startdrive projects ... 89
11.1.1.2 Configure the settings to open the Security Wizard ... 90
11.1.2 Security settings for the drive ... 91
11.1.2.1 Manually starting the Security Wizard ... 91
11.1.2.2 User Management & Access Control ... 92
11.1.2.3 Ports and protocols ... 93
11.1.2.4 Activating/deactivating ports and protocols ... 95

11.2 User management and access control (UMAC) ... 96
11.2.1 Fundamentals ... 96
11.2.2 Project protection ... 96
11.2.2.1 Overview ... 96
11.2.2.2 Activating project protection ... 97

11.2.2.3 "Anonymous" user ... 98
11.2.2.4 Setting password policies ... 99
11.2.3 User management ... 100
11.2.3.1 Overview ... 100
11.2.3.2 System limits ... 101
11.2.3.3 Creating user accounts ... 102
11.2.3.4 "Anonymous" user ... 103
11.2.3.5 Activate/deactivate user accounts ... 103
11.2.3.6 Changing user accounts ... 104
11.2.3.7 Delete user accounts ... 104
11.2.3.8 Assigning/removing roles ... 105
11.2.3.9 Displaying rights of project users ... 105
11.2.3.10 Change password ... 106
11.2.3.11 Changing the password when a protected project is opened ... 106
11.2.3.12 Changing a password when working in a protected project ... 107
11.2.4 Access control ... 108
11.2.4.1 Overview ... 108
11.2.4.2 Adding and configuring roles ... 108
11.2.4.3 Example: Necessary rights for specific activities ... 109
11.2.4.4 Assign/remove rights ... 112
11.2.4.5 Changing roles ... 112
11.2.4.6 Deleting roles ... 113
11.2.5 User login ... 113
11.2.5.1 Overview ... 113
11.2.5.2 User login ... 114
11.2.5.3 Error messages and remedies ... 115
11.2.5.4 Changing a user ... 116
11.2.5.5 Logging off a user ... 117
11.2.6 Project lock ... 118
11.2.6.1 Overview ... 118
11.2.6.2 Lock project manually ... 119
11.2.6.3 Lock project automatically on inactivity ... 119
11.2.6.4 Remove project lock for local users ... 119
11.2.6.5 Remove project lock for single sign-on users ... 120
11.2.7 Downloading the UMAC to the device ... 120

11.3 Settings with the Security Wizard ... 121
11.3.1 Overview ... 121
11.3.2 Configuring security settings ... 124
11.3.2.1 Security settings for full protection ... 124
11.3.2.2 Security settings with low protection ... 129
11.3.3 Changing or subsequently adjusting security settings ... 131

11.4 Backup and restore ... 132

11.5 Certificates for secure communication ... 132
11.5.1 Fundamentals ... 132
11.5.2 Certificate types ... 133

12 Security settings in the web server ... 135

12.1 Fundamentals ... 135
12.1.1 Factory settings ... 135
12.1.2 Activating UMAC from the status bar ... 136
12.1.3 User login (read access activated) ... 137

12.1.4 User login (read access deactivated) ... 138
12.1.5 Changing a user ... 138
12.1.6 Logging off a user ... 139
12.1.7 User login after session timeout on inactivity (read access activated) ... 140
12.1.8 User login after session timeout on inactivity (read access deactivated) ... 141

12.2 Settings in the Security Wizard ... 142
12.2.1 Structure of the Security Wizard ... 142
12.2.2 Reloading pages of the web server ... 143
12.2.3 Configuring settings in the Security Wizard ... 143
12.2.3.1 Make basic settings when the web server is called for the first time ... 143
12.2.3.2 Start Security Wizard ... 144
12.2.3.3 Activating UMAC ... 144
12.2.3.4 Setting up a user with the "Drive Administrator" role ... 145
12.2.3.5 Configure the read access ... 146
12.2.3.6 Web server activation ... 147
12.2.3.7 Summary ... 148
12.2.3.8 Changing security settings ... 150
12.2.4 Working with low security settings ... 151
12.2.4.1 Modifying security settings ... 152

12.3 User management and access control (UMAC) ... 153
12.3.1 Overview ... 153
12.3.2 System limits ... 156
12.3.3 User management ... 156
12.3.3.1 Creating a new user account ... 156
12.3.3.2 Editing users ... 157
12.3.3.3 Editing the "Anonymous" user ... 157
12.3.3.4 Password policy ... 158
12.3.3.5 Change password policy ... 159
12.3.3.6 Changing your own user password ... 159
12.3.4 Access control ... 160
12.3.4.1 User roles and access rights ... 160
12.3.5 Checking UMAC settings ... 161
12.3.6 Reset UMAC settings ... 161

12.4 Ports and protocols ... 162
12.4.1 Activating/deactivating ports and protocols ... 163

12.5 Firmware update ... 164
12.5.1 Firmware update ... 164

12.6 Backup and restore ... 164

12.7 Certificates for secure communication ... 165
12.7.1 Fundamentals ... 165
12.7.2 Establish a protected HTTPS connection to the web server ... 166
12.7.3 Display information about the certificates ... 170

A Appendix ... 173

A.1 Additional information ... 173

Glossary ... 175

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 V6.1 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

See also

Security settings in Startdrive (Page 89)

Security settings in the web server (Page 135)

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).

Figure 1-1 The SINAMICS converter family

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 Security 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)
- Information about field services, repairs, spare parts, and much more (→ Services)
- 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

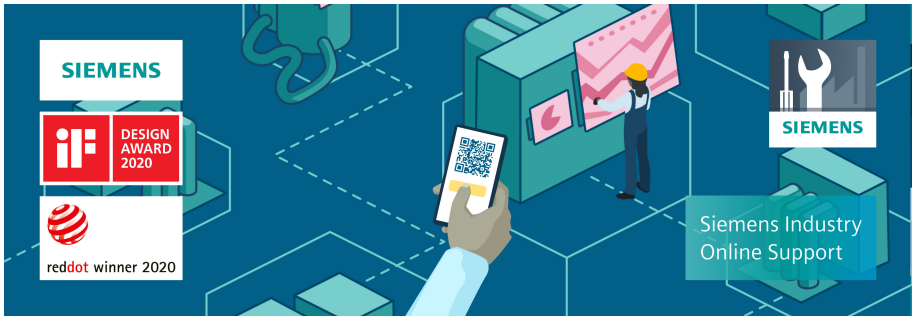


Figure 1-2 "Siemens Industry Online Support" app

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 1-3 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.

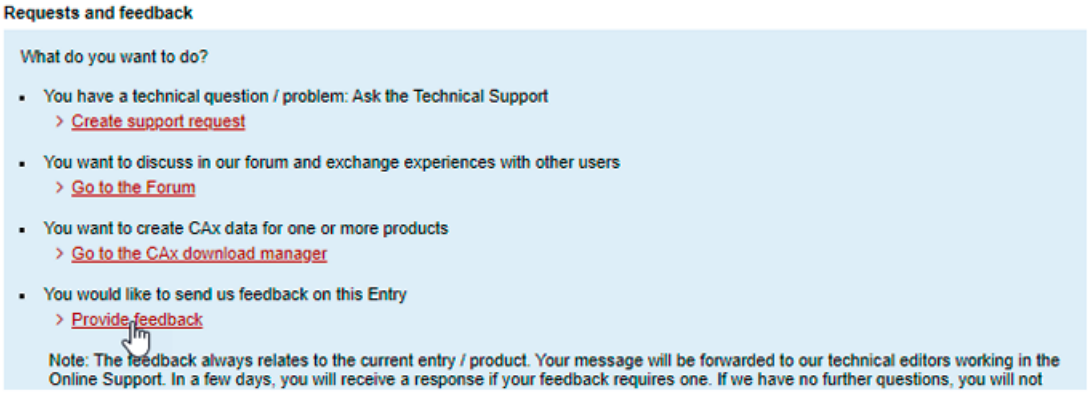


Figure 1-4 Requests and feedback

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):

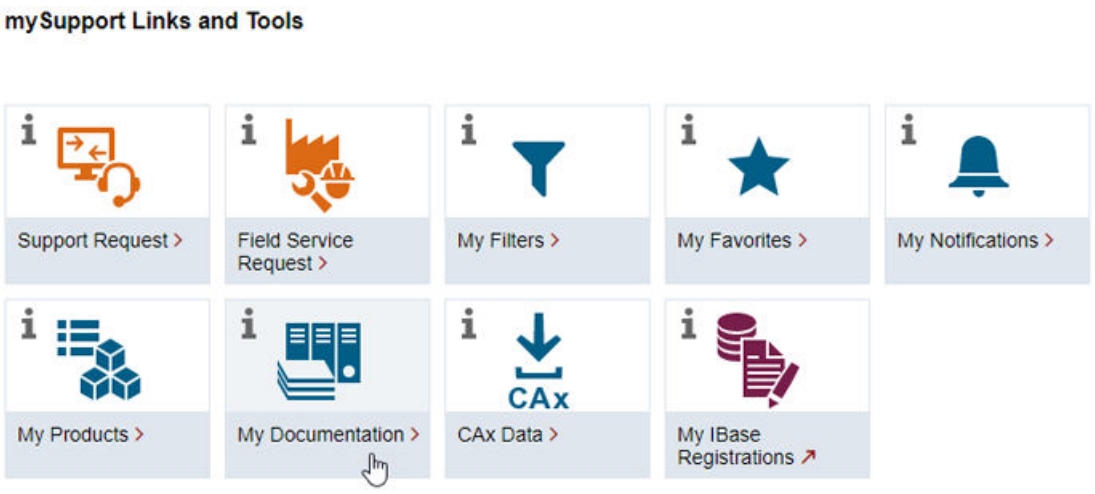


Figure 1-5 mySupport

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 are 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 these data are created, the author must give thought to data protection consent for these optional data. Siemens takes no responsibility for these data.
  These support contact data can be read and are freely accessible in, for example, the user interface as well as in the diagnostics report. These data are not encrypted.

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

The personal data are 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 they serve 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 security

Overview

Industrial security 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 security

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 and correct possible errors.
- 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 (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.
- Industrial security 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 can be found on the Internet (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 security 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 security field can be found on this website (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 security.

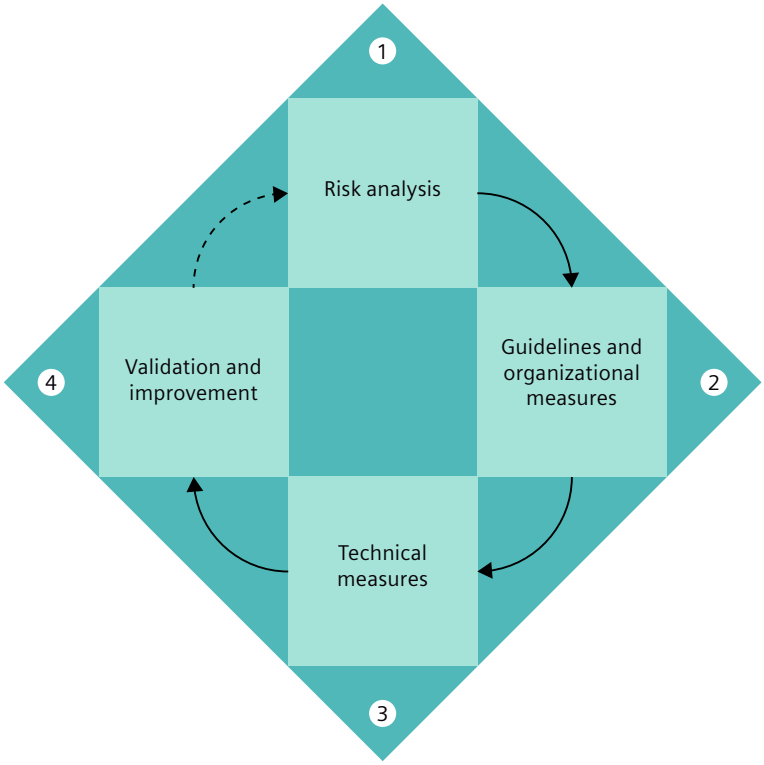


Figure 5-1 Security management process

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 security 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.

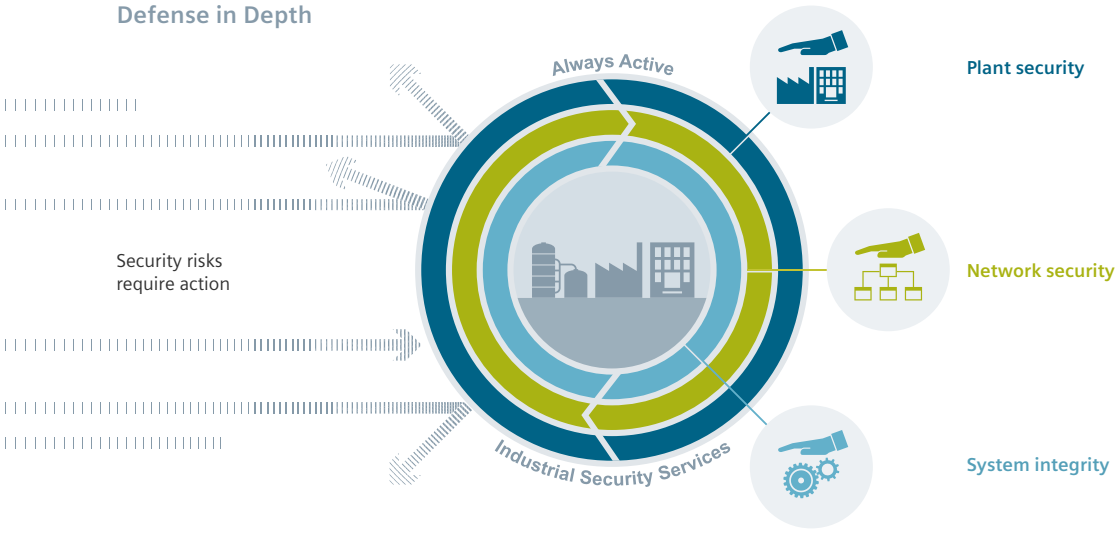
Operating environment and general security measures

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).

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 Security Appliances.

Requirement

Upstream SCALANCE S Industrial Security 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 Security 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.
- Protection of different network topologies
  Components such as the SCALANCE S615 have five 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.

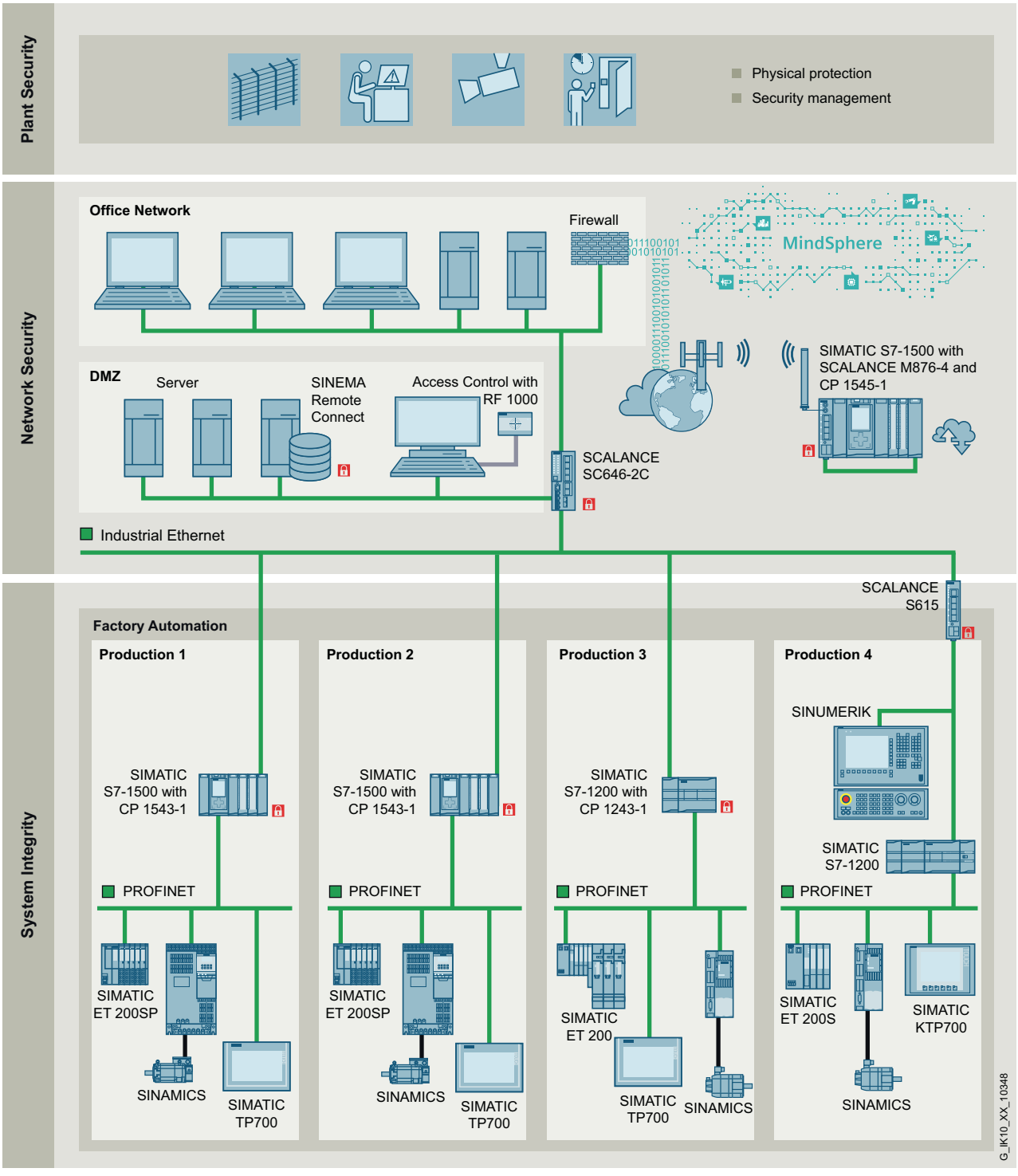


Figure 6-1 SCALANCE S application example

More information

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

- Network security with SCALANCE S Industrial Security 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)
- Siemens 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 69)".

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 41)".
  - A virus scanner is installed on the operating unit and regularly updated. In addition, "Allow lists (Page 40)" and "Network segmentation with SCALANCE S (Page 33)" methods can be used.
  - 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 32)".
- 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.

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) 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.

For this reason, always use "Industry Online Support (https://support.industry.siemens.com/cs/ww/en/sc/4868)" to keep yourself up to date about new

and relevant product security notifications for your products. 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 32)".

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 32)".

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 (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 (Page 31)" must be implemented.

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 Startdrive and/or web server commissioning tools is activated by default. Access is configured in the Security Wizard 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 PROFINET interface X150 must be in a secure protection area (see section "Network security (Page 32)"). 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.

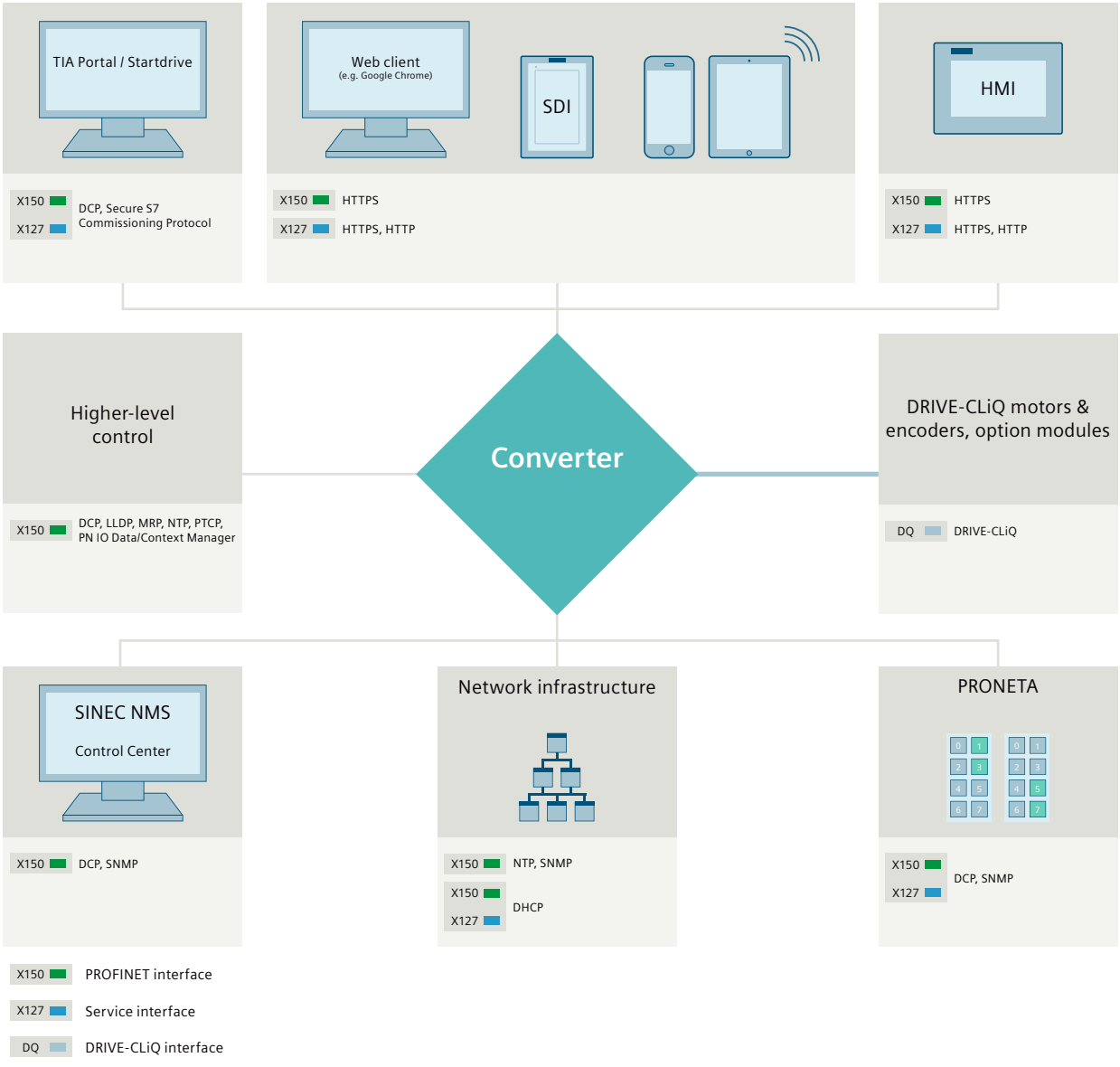


Figure 7-1 Communication links

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 69)".

Security functions

8

8.1 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 section "Network security (Page 32)" are implemented.

8.2 Identity and access management

8.2.1 Authentication mechanisms for users

Overview

The identification and authentication mechanisms for users are implemented in the following engineering tools:

- Startdrive in the TIA Portal
- Web server

Description

The identification and authentication mechanisms provided in the engineering tools make it possible to identify and authenticate human users definitively. The ability to configure user roles and rights implements the principle of least privilege for the activities that need to be completed.

Principle of least privilege

Basic principle in which users are assigned only the access rights the correspond to their duties and functions.

User Management and Access Control (UMAC)

In the specified engineering tools you can manage access to the converter by means of User Management and Access Control. You are able to create and manage user accounts. You

can allocate roles to user accounts allowing read or write access to the specific data. The following applies:

- Startdrive:
  The user roles and rights defined in UMAC are valid in the Startdrive project (if it is a protected project) and also for the relevant converter.
- Web server:
  The user roles and rights defined in UMAC are valid only for the relevant converter.

Maximum number of configurable user accounts

You can configure a maximum of 64 user accounts. This refers to one converter.

8.2.2 Managing login data and user IDs

Description

At least one user who is formally assigned the Administrator role must be designated in order to create, configure and manage user accounts. In the context of user management, this user is authorized to create, configure and manage other user accounts. Evaluate the assignment of the Administrator role carefully.

Who defines the Administrator role?

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

Predefined user accounts and access data

At the time of delivery, the runtime settings of the firmware do not contain predefined passwords.

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
  - Restore 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 roles (only in Startdrive)
- Configure user-defined roles
- Load UMAC configuration to the converter (download)

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 runtime role "Drive Administrator" or the runtime function right "Manage users and roles".
- Web server engineering tool:
  Users can each change their own password. Users with the runtime role "Drive Administrator" or the function right "Manage users and roles" are able to change all users' passwords.

When are passwords overwritten?

Passwords are overwritten in the following cases:

- Users change their own password
- Administrators change the password of a user
- Download the UMAC configuration to the drive
- Reset the drive fully to factory settings (with SD card)
- Restore drive settings and configuration from a backup file containing a UMAC configuration

More information

You can find more information about user roles and rights and their assignment in section "Roles and function rights (Page 54)".

8.2.2.1 Restoring UMAC settings

Restoring UMAC settings

The following functions for restoring UMAC settings are implemented in the engineering tools.

- Startdrive
  - Data storage of UMAC settings is part of the project in Startdrive/TIA Portal, and UMAC settings cannot be transferred between projects. This means that restoration is only possible through archiving of the project, together with all project data. It is not possible to separately restore UMAC settings alone.
- Web server
  - The UMAC settings are part of the converter backup. The UMAC data can be restored with the restore function. It is not possible to separately restore UMAC settings alone.

8.2.2.2 Resetting the UMAC settings

Resetting the UMAC settings

The following functions for restoring UMAC settings are implemented in the engineering tools.

- Startdrive
  - Activation of UMAC settings cannot be reset in the Startdrive project. As with other activities, changes to UMAC settings can be reset within the same project session using the undo function.
- Web server
  - Activation of UMAC settings also cannot be reset in the web server. The UMAC settings can be changed at any time by a user with the necessary rights. There is no undo function in the web server.

8.2.2.3 Transferring and saving UMAC settings

Transferring and saving UMAC settings

User accounts are created and managed in user management (UMAC).

User database

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

The login data in the user database is given the user names as unique identifiers.

UMAC settings

The UMAC settings including login data are transferred to the converter and saved as follows.

- **Startdrive**
  - Data storage in the TIA Portal:
    The TIA Portal has its own data storage as an **offline** tool. Login data created offline in a Startdrive project is saved in the project in encrypted form. To save the UMAC data in the converter, a download must take place.
  - Data storage in the converter:
    When the UMAC data is downloaded to the converter, the login data is saved in the user database in the internal memory of the converter.
    Firmware version V6.1 does not support uploading of UMAC data from the converter to the Startdrive project.
  - Transfer of UMAC data:
    The UMAC data is transferred in protected form using the S7 Protocol for Startdrive.
- **Web server**
  - Data storage in the web server/converter:
    The web server is an **online** tool so it does not have its own data storage. Login data is written directly to the user database in the internal memory of the converter and can be saved permanently with "RAM2ROM".
  - Transfer of UMAC data:
    For data transfer between the converter and the web server, communication via HTTPS is activated by default. In this case, the login data is transferred over the protected HTTPS connection.

8.2.3 Roles and function rights

8.2.3.1 Engineering roles with engineering function rights (only for Startdrive)

Overview

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

However, for online access to the drive, the engineering function rights undergo additional checks in many work areas.

The "Engineering-Administrator" role

All users with the "Engineering-Administrator" role can create other users and assign other roles to them in any combination.

The principle of least function rights must always be observed. For access to the engineering and converter data, users can only be assigned roles which are necessary in order to perform defined functions.

Assignment of roles to function rights

The following engineering 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 engineering roles can be created at any time.

The roles are assigned to the following engineering function rights 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

Engineering function rights	[1]	[2]
Edit Safety Integrated application of the drive	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

8.2.3.2 Roles for converters with runtime and engineering function rights

Assignment of roles to function rights

To simplify data transmission between online and offline configuration, assign the necessary engineering function rights not only to engineering roles but also to certain runtime roles. You assign the necessary function rights according to the tasks specified for the particular user.

The following system-defined roles are available by default:

No.	Runtime role
[1]	Drive Administrator[1)]
[2]	Drive Safety Engineer
[3]	Drive Engineer and Service
[4]	Drive Operator
[5]	Drive Guest

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 can be assigned to the system-defined roles.

Engineering function rights	[1]	[2]	[3]	[4]	[5]
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 Safety Integrated application of the drive	X	X	–	–	–
Manage users and roles	X	–	–	–	–

8.2.3.3 Roles for converters with runtime function rights

Assigning roles to rights

The following runtime roles are available.

No.	Runtime role
[1]	Drive Administrator[1)]
[2]	Drive Safety Engineer
[3]	Drive Ext. Role Fieldbus, Drive Ext. Role SDI Standard/Adv[2)]
[4]	Drive Engineer and Service
[5]	Drive Operator
[6]	Drive Guest

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

2) This role is not used with S210 converters. S210 does not use an SDI standard panel.

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 roles for access via fieldbus interface or SDI standard panel

The extended roles Drive Ext. Role Fieldbus and Drive Ext. Role SDI Standard/Adv are only available for access via a fieldbus protocol (see section Ports and protocols (Page 162)) or an SDI standard panel.

The roles include read as well as write rights to access the converter online and can be assigned to all user accounts. If the roles are assigned to the "Anonymous" user, access is possible **without authentication** via the fieldbus protocol or the SDI standard panel.

Note

Access via the SDI standard panel

Not all converters have an SDI standard panel. For example, S210 converters do not have an SDI standard panel.

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

Extended role	Explanations
Drive Ext. Role Fieldbus	**Which settings can be edited?** If this role is assigned to the "Anonymous" user, any user can use the fieldbus interface to read and edit the settings in the converter. Access does not require authentication. The following fieldbus protocols are supported: PROFINET, DCP, SNMP or the S7 Protocol for PCS7. **Which settings cannot be edited?** • Safety Integrated settings • UMAC settings **In what situations are the assigned function rights not checked?** • Cyclic communication • Reading data via DCP
Drive Ext. Role SDI Standard/Adv	**Which settings can be edited?** If this role is assigned to the "Anonymous" user, any user can use the integrated SDI standard panel to read and edit the settings in the converter. Access does not require authentication. The function rights contained in the role only affect access via the SDI standard panel. If the converter is housed in a lockable cabinet or cabinet room, this role can be used to grant trusted users extended access to the converter without an additional login. **Which settings cannot be edited?** Safety Integrated and UMAC settings cannot be edited with this role.

Restrict authorizations

Certain functions such as 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.

You are recommended to verify the assigned runtime roles and rights for the "Anonymous" user. Identify the potential risks arising from the assigned roles and rights and take appropriate security precautions.

8.2.4 User Management and Access Control in the web server

8.2.4.1 User management in the web server

Overview

Users of the converter can also be managed in the web server.

Description

You can use UMAC to allocate system-defined or user-defined roles to user accounts which allow read or write access to specific functions.

User accounts

The user accounts are assigned roles with different authorizations.

- Users with the "Drive Administrator" role:
  The names of these users can be freely assigned. A user assigned the "Drive Administrator" role is created by the user in the Security Wizard when the user activates UMAC.
  A password in accordance with the "password policy" must be assigned when these users are created. After login, the users have full access to the converter data displayed in the web server.
- Anonymous (predefined):
  This user account does not require authentication when accessing the converter.

Create and manage users

User accounts can only be created, edited and managed by users with the function right "Manage users and roles". Any user obtains this authorization when assigned the "Drive Administrator" role or a user-defined role with the "Manage users and roles" right.

Roles and function rights

Users are defined, configured and managed in user management (UMAC). Assigned roles and function rights are valid only for the relevant converter.

Runtime roles and function rights are available for accessing the converter. The assignment of function rights to the roles is protected and cannot be changed.

You can find more information on the assignment of function rights to the system-defined roles in section "Roles for converters with runtime function rights (Page 56)".

Clearing the UMAC settings

In a full reset of all device settings, all UMAC settings (such as created user accounts) are deleted. The full reset is only possible with a specially configured SD card.

The product documentation of the converter contains a description of the reset to factory settings, in section "Reset converter to factory settings".

8.2.4.2 Characteristics of access control in the web server

Overview

Except for the "Anonymous" user, all users must authenticate themselves with the specified login data when they access the web server.

Authentication mechanisms and characteristics

The authentication mechanisms in the web server have the following characteristics:

Function	Description	
Password policy	Default configuration	• Activated • Configurable
	Default settings	• Minimum password length: 8 characters • Minimum number of numeric characters (0-9): 1 • Minimum number of special characters: 1 • At least one uppercase 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 numeric characters (0-9): 0 to 32 • Minimum number of special characters: 0 to 32 • At least one uppercase 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 deactivated
	Default settings	• Password valid: – • Advance warning time for expiring password: – • Number of recently used passwords blocked for reuse: 1
	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: 0 to 365 days • Advance warning time for expiring password: 0 to 365 days • Number of recently used passwords blocked for reuse: 1 to 10
Limitation of failed login attempts	Configurability	The number of failed login attempts during user authentication is **not limited and not configurable**.
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 input or parts of the input are valid or invalid. This conceals the reason why the login failed.	

Function	Description	
Transfer of login data	For data transfer between the converter and the web server, communication via HTTPS is activated by default. In this case, the login data is transferred over 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.	
	More information about the transfer and storage of login data can be found in section "Managing login data and user IDs (Page 50)".	
Storage of login data	The login data for all configurable users is saved in the user database in the internal memory of the converter.	
	More information about the transfer and storage of login data can be found in section "Managing login data and user IDs (Page 50)".	
Session timeout on inactivity	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
	If the user's inactivity exceeds the specified time, that user is automatically logged out. The user is given 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 If users are logged out due to inactivity they can log back again in at any time with their login data. After login, the configured time for the session timeout is restarted. 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.	

More information about the configurability of user roles and access rights in the web server can be found in section "Authentication mechanisms for users (Page 49)".

8.2.4.3 Users with the "Drive Administrator" role

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. The last user with the "Manage users and roles" right cannot be deleted. Exception: In a full reset with a specially configured SD card (see section "Deletion of customer data on the converter (Page 83)") all users are deleted.

Creating, editing and managing user accounts

Users with the "Drive Administrator" role are authorized to perform the following actions for themselves, for the "Anonymous" user and for 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

8.2.4.4 "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 69)".

Configurability

The user does **not require authentication**. The account is activated by default and has the "Drive Ext. Role Fieldbus" role.

Note

When you activate the user account for the "Anonymous" user, the security of the converter is reduced according to the extent of the function rights that you assign to this user.

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 by any user. The user account cannot be deleted.[1)]
User name	The user name cannot be changed by any user. The user name cannot be configured.

Property	Description
Password	The user does not need a password and does not need to be authenticated. When the user is activated there is no need to log in.
Roles and function rights	The user account is assigned the "Drive Ext. Role Fieldbus" role by default.

1) However, the "Anonymous" user can be deactivated in user management.

More information

You can find more information on the assignment of roles and function rights in section Roles and function rights (Page 54).

Security information

The combination of the inability to perform authentication ("Anonymous" user) and the assignment of a role with extended authorizations poses a security risk. You should therefore give careful thought to assigning roles allowing write access to the converter data.

Extended roles for remote access

For remote access via external devices, the "Anonymous" user account has the following extended roles and function rights:

Function rights	Extended roles	
	Drive Ext. Role Fieldbus	Drive Ext. Role SDI Standard/Adv
Read drive data or acknowledge messages	X	X
Control drive in manual mode	X	X
Perform drive diagnostics	X	X
Perform firmware update	X	X
Create backup or load drive data to Startdrive	X	X
Edit web server settings	X	X
Edit device settings or drive application	X	X
Edit Safety Integrated application	–	–
Manage users and roles	–	–

The function rights only apply together with the activated interfaces for external access via a fieldbus or SINAMICS SDI standard panel. If these interfaces are not activated, the extended roles remain without function.

You can find more information about the communication interfaces in section "Communications interfaces (Page 45)".

8.2.5 User Management and Access Control in Startdrive

8.2.5.1 User management in Startdrive

Overview

Startdrive has its own user management system.

Description

You can use UMAC to allocate system-defined or user-defined roles to user accounts which allow read or write access to specific functions and data.

Activating UMAC

UMAC can be activated for converters either in the security settings with "Protect project" or with the Security Wizard. The method using the Security Wizard is described below:

Administrator

When user management is activated, the user is requested to create an administrator. Any user name can be chosen.

The user is automatically assigned the following roles:

- Engineering-Administrator
- Drive Administrator

This means that the administrator has all engineering and runtime function rights and has full access to the converter settings.

This also authorizes the user to create, edit and manage other user accounts.

"Anonymous" user

When user management is activated, the predefined user "Anonymous" is created automatically.

You can find more information about this user in section ""Anonymous" user (Page 67)".

Create and manage users

User accounts can only be created, edited and managed by users with the function right "Manage users and roles". Any user obtains this authorization when assigned one of the following roles:

- Engineering-Administrator
- Drive Administrator

The user "Administrator" is assigned both roles by default.

Roles and function rights

Users are defined, configured and managed in user management (UMAC). Assigned roles and function rights are valid only in the relevant project and also for the relevant inserted converter.

The configurable roles and function rights are divided into two groups.

- Engineering roles and function rights:
  Engineering function rights relate to the configuration of a converter in **online and offline mode**.
- Runtime roles and function rights:
  Runtime function rights relate to a device (e.g. converter, controller) which is accessed in **online mode**.
  The same runtime function rights are valid for Startdrive and web server.

Activities in Startdrive requiring access to the converter in online and/or offline mode must have a mixture of engineering and runtime roles.

Project protection/converter protection

When UMAC is activated in the Security Wizard, project protection and converter protection can be activated automatically. These two protection settings can be selected independently of each other, but they can also be combined.

Once activated, project protection can no longer be deactivated. Converter protection can be deactivated again by means of a full reset to factory settings (with SD card).

More information

You can find more information about user management in Startdrive under the heading "User management and security" in the Startdrive information system. You will also find notes on the dependencies between the individual roles and rights.

8.2.5.2 Characteristics of access control in Startdrive

Overview

In the TIA Portal, access control is configured with User Management and Access Control (UMAC) for the Startdrive project and individual drives.

Authentication mechanisms and characteristics

When user management (UMAC) is activated for the Startdrive project and the drive, the user also activates project protection for the Startdrive project at the same time. To open and edit the project, authorized users must authenticate themselves with the specified login data.

The authentication mechanisms in the TIA Portal have the following characteristics:

Function	Description	
Password policy	Default settings	• Minimum password length: 8 characters • Minimum number of numeric characters: 1 • Minimum number of special characters: 0 • At least one uppercase letter and one lowercase letter: Activated • Number of recently used passwords blocked for reuse: 5 • Activate password aging: Deactivated • Password validity (days): 60 • Advance warning time (days): 7
	Configurability	Settings are **globally** configurable for all project users except the "Anonymous" user.
	Authorization	Users with the function right "Manage users and roles"
	Valid values	• Minimum password length: 8 to 32 characters • Minimum number of numeric characters: 0 • Minimum number of special characters: 0 • At least one uppercase letter and one lowercase letter: Activated/deactivated • Number of recently used passwords blocked for reuse: 1 to 10 • Activate password aging: Activated/deactivated • Password validity (days): 1 to 365 • Advance warning time (days): 1 to 365
	Recommendations	We recommend assigning complex passwords with at least 12 characters and limiting the number of user accounts to the necessary minimum.
	You can find more information about the password policy and how it can be configured under the heading "Define password policy" in the Startdrive information system.	
Limitation of failed log-in attempts	Configurability	The number of failed login attempts during user authentication is **not limited and not configurable**.
Concealment of passwords	Passwords are concealed when login data is defined or requested. The input cannot be displayed in plain text.	
Concealment of error messages	Error messages about incorrect input contain no information indicating which input or parts of the input are valid or invalid. This conceals the reason why the login failed.	
Transfer of login data to the converter	The login data is transferred in protected form using the "Secure S7 Protocol for Startdrive".	
	You can find more information about the transfer of login data in section "Managing login data and user IDs (Page 50)".	
Storage of login data	The TIA Portal has its own data storage. Login data created **offline** in a Startdrive project is saved in the project in encrypted form. When the UMAC data is downloaded to the converter, the login data is saved in the user database in the internal memory of the converter.	
	More information about the storage of login data can be found in section "Managing login data and user IDs (Page 50)".	

Function	Description	
Project lock/ session timeout for local project users (refers to the Startdrive project in the TIA Portal)	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 function right "Manage users and roles"
	Valid values	1 to 60 min
	System behavior	If project protection is activated, a session timeout for local project users can be activated and configured.
	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.
	You can find more information under the heading "Lock project" in the Startdrive information system.	
Session timeout on inactivity (refers to the converter)	Default configuration	Configurable when individual users are edited
	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
	If the user's inactivity exceeds the specified time, that user is automatically logged out. The user is given 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 If users are logged out due to inactivity they can log back again in at any time with their login data. After login, the configured time for the session timeout is restarted. 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.	

8.2.5.3 Users with the function right "Manage users and roles"

Overview

Users with the function right "Manage users and roles" can create, edit and manage other users.

Configurability

The login data is configured by a user with the "Manage users and roles" right. Users can change their own password themselves.

Creating, editing and managing user accounts

Users with the function right "Manage users and roles" are authorized to perform the following actions for themselves, for the "Anonymous" user and for other users:

Category	Action	Own user account	Anonymous	Other users
General	Create user account	–	–	X
	Activate/deactivate user account	–	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 account	–	–	X
Session timeout	Configure session timeout	X	–	X
Roles and rights	Create user-defined roles and assign them in any combination[1)]	X	X	X
	Assign roles in any combination	X	X	X

1) Engineering and runtime function rights can be assigned flexibly to user-defined roles. Certain engineering function rights require the activation of other function rights. In this case, the necessary additional engineering function rights are activated automatically.

8.2.5.4 "Anonymous" user

Overview

The "Anonymous" user is created when a project is created.

Configurability

The user does **not require authentication**. The account is activated by default and has the "Drive Ext. Role Fieldbus" role.

Note

When you activate the user account for the "Anonymous" user, the project security is reduced according to the extent of the function rights that you assign to this user.

We recommend using the "Anonymous" user only for fieldbus access.

Property	Description
User account	Users with the function right "Manage users and roles" can activate/deactivate this user.
	The user account cannot be deleted by any user.
User name	The user name cannot be changed by any user.

Property	Description
Password	The user does not need a password and does not need to be authenticated.
Roles and function rights	No system-defined roles are assigned to the user account by default.

Creating, editing and managing user accounts

If the "Anonymous" user is assigned the role "Engineering-Administrator" or "Drive Administrator", the user is authorized to perform the same actions as the administrator.

NOTICE

Data manipulation due to access by anonymous users

Users who are not logged in are able to read the data of your project or converter and, with the relevant access rights, can manipulate data and thereby destroy the machine. When activating the "Anonymous" user, you will receive security information about the potential risk.

- You should therefore prevent regular access to the project and converter with this user account. Do not assign roles with engineering access rights to the "Anonymous" user.
- Carry out a risk analysis. Only assign roles to the "Anonymous" user if they do not present a risk according to the risk analysis.

8.3 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.

8.3.1 Least functionality of ports and protocols

Factory settings

Security measures related to network security are exclusively focused on Ethernet or PROFINET networks. You require the following information to match the security measures to the protocols used (e.g. firewall).

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).
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.

Interface	Protocol	Port number	Default settings			Description
			Runtime	Startdrive	Web server	
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
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.

8.3.2 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

Interface	Format	Delivery state	Best practice
SINAMICS SDI Standard[1)]	1.4"	Not protected	Protection from locked control cabinet
SD card slot	SD 6.1	Not protected	Protection from locked control cabinet

1) Not for SINAMICS S210.

More information

You can find more information about activating/deactivating ports and protocols in section "Least functionality of ports and protocols (Page 69)".

8.3.3 Additional protective measures for hardware reports

Description

Additional protective measures must be considered in an information security risk assessment (Page 27).

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.

8.3.4 Least functionality of software applications and functions

Description

Firmware version V6.1 does not support any Technology Extensions or other supplementary functions.

8.4 Secure communication channels and protected data storage

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

Overview

In protected communication, 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 commissioning tools is guaranteed with a combination of the following mechanisms.

Secure communication channels and protocols

Communication between the converter and the Startdrive and web server commissioning tools is protected with 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 47)".

Identification of communication devices

A certificate is required in order establish a protected connection between the converter and the Startdrive and web server commissioning tools. 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.

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

Implementation

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.

If project protection is activated in Startdrive, the user database is stored in the project in encrypted form.

8.4.3 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 (see section "Compliance with the General Data Protection Regulation (Page 17)").

8.4.4 Certificates for protected data transmission in web server

8.4.4.1 Digital certificate

Description

When you establish a protected HTTPS connection to the web server, you need a valid digital certificate for server authentication. This certificate is generated automatically in the SINAMICS converter.

8.4.4.2 Using an automatically generated certificate

Description

Common Internet browsers do not validate automatically generated certificates. The browsers classify these certificates as invalid, and they issue a security warning when an HTTPS connection is called.

For the browser to trust an automatically generated certificate, the root certificate that was generated automatically in the SINAMICS converter must be exported to the Protection & Security page of the web server, and then imported into the certificate store of the browser or the "Trusted Root Certification Authorities" folder in the Windows system. A trusted and secure HTTPS connection cannot be established until the certificate has been successfully imported.

Notes

Only use the automatically generated certificate in protected networks (e.g. PROFINET below a PLC) or for direct point-to-point connections. Commissioning must take place in a protected environment in order to guarantee that the trusted certificate is compatible with the device used.

8.4.4.3 Validating automatically generated certificates

Description

When an HTTPS connection to the web server is called, the validity of an automatically generated certificate is validated **by the browser being used and the web server**.

8.4.4.4 Certificate management

Overview

Depending on the browser used, automatically generated certificates can be imported into the certificate store of the Window system or of the browser.

Access to the Windows certificate store

The following table shows the similarities and differences between common browsers regarding access to the certificate store of the Windows system or of the browser in question:

Browser	Version	Engine	Certificate management
Google Chrome	80.0.3987.122 [64-bit]	Chromium	The browser only validates certificates that are saved in the certificate store of the Windows system. Certificates must be exported from the browser and cannot be directly imported into the certificate store.
Microsoft Edge	81.0.416.72 [64-bit]		
Mozilla Firefox	68.8.0 ESR [32-bit]	Gecko	The information about Google Chrome and Microsoft Edge is also applicable here. Mozilla Firefox also has its own certificate management integrated in the browser.

The descriptions in this section refer exclusively to the browser versions listed above. Browser response can deviate depending on the browser version being used.

8.5 System integrity

8.5.1 Software and information integrity

Implementation

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)
- 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.

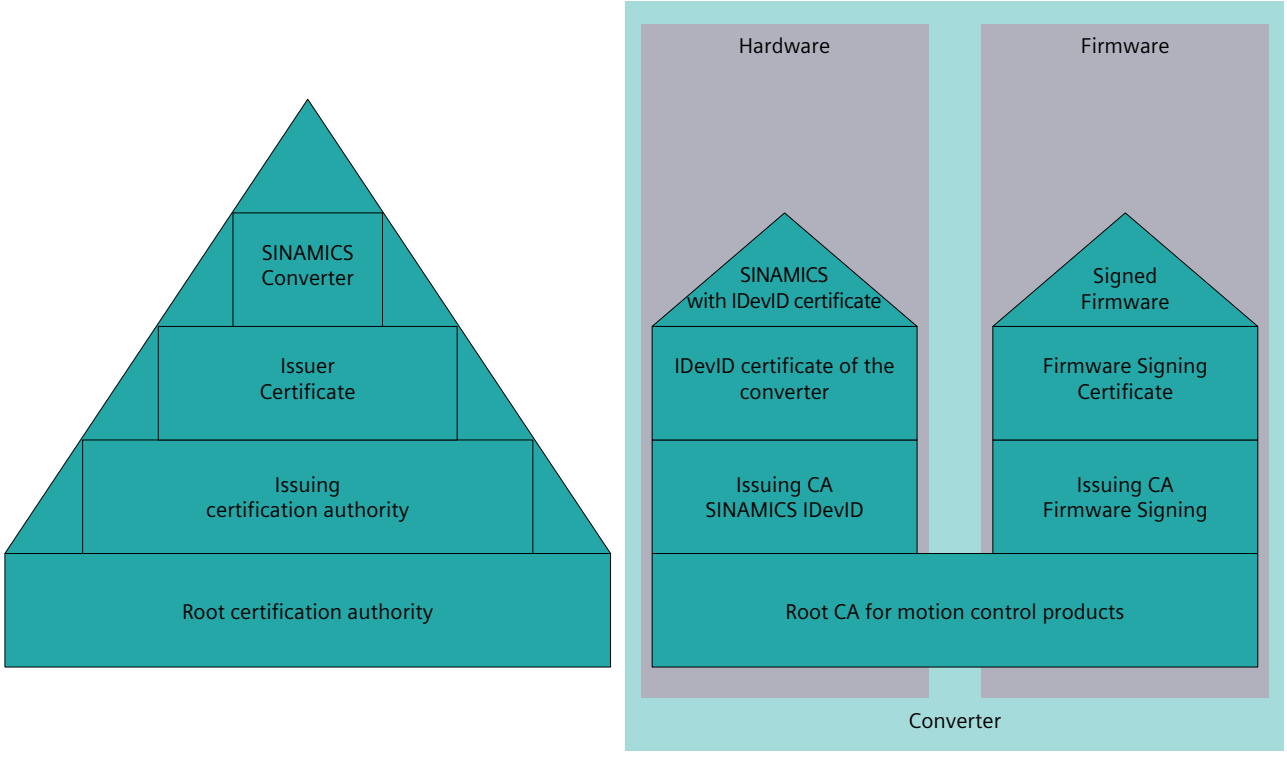


Figure 8-1 PKI architecture

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 being installed have not been changed unknowingly.

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 V6.1 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.

8.5.2 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.

8.5.3 Input validation

Implementation

The components validate the syntax, length and content of each input used as input data, or of input over external interfaces with direct impact on the actions of the components. The input validation is dependent on the context in which the values are entered.

8.5.4 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 (HMI interface with pushbuttons)

8.5.5 Timed distribution and synchronization

Implementation

You can find more information about creating time stamps for logging security-relevant events in section "Logging of events (Page 81)".

8.5.6 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 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

Additional information about available firmware versions can be found on this website: (https://support.industry.siemens.com/cs/ww/en/view/109812303)

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.

8.5.7 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 Startdrive and web server commissioning tools:

- 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 after replacing a device or during series commissioning.
- Restore settings to the factory setting:
  This function resets all converter settings to the factory values.
  Depending on the commissioning tool used, the following data is retained in the reset to factory settings:
  - Communication interface settings
  - UMAC and security settings
  - Language setting
  - Date and time

  This data is reset with a manual reset to factory settings with memory card. You can find more information in section "Deletion of customer data on the converter (Page 83)".
- Restore Safety Integrated settings to the factory setting:
  This function only resets the settings of the Safety Integrated Functions to 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 for protection against power failure. Using the memory card, for example, the backed-up settings can be transferred to other converters.
- Store the backup file in the operating unit:
  If you only wish to use the backup file at a later point in time, then place the backup file in a protected location in the operating unit or on a suitably protected network drive.

More information

See the relevant Product Information for more information about the "Backup and restore" function in Startdrive or web server.

8.6 Logging and monitoring

8.6.1 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.

Note that for products this is generally the responsibility of the system integrator.

8.6.2 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 interrupts
- 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 commissioning tools in the following documentation:

- Operating instructions "SINAMICS S210 servo drive system with S-1FK2 and S-1FT2"

8.6.3 Monitoring and accessing logs

Description

Not part of the product scope.

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 30)" must be complied with.

In addition, a suitable security management process (see section "Security management (Page 27)") must be applied. 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

Manual reset to factory settings with memory card

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. • For this reason, ensure secure deletion of data from all storage media **before disposing of the product**.

The subsequently listed data storage media used in SINAMICS S210 can potentially include customer data and, depending on the protection requirement, must be securely deleted or physically destroyed when disposing of the media:

- eMMC
- NVRAM

The manual reset to factory settings causes the customer data in the converter to be deleted.

You can find more information in section "Manual reset to factory settings with memory card" in the product documentation.

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 officially 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 data media 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 scanners
- 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

Development stages of security functionality

Multi-level security functionality is available for SINAMICS drives in the TIA Portal application "Startdrive".

- General security settings (Page 89)
  With the TIA Portal you centrally make overarching security settings across the drive and project. In the Inspector window, you also make specific security settings for the drive.
- User Management and Access Control (UMAC) (Page 96)
  The user management system enables you to manage access to the converter and the project. This involves creating user accounts and managing them. You allocate roles to the user accounts allowing read or write access to specific functions and data. To access the Startdrive project, users must authenticate themselves.
  Individual drives can also be protected. If a drive is protected, users must authenticate themselves for online access to the drive. This protection can only be deactivated with a manual reset to factory settings with memory card.
- Security Wizard (Page 121)
  With the help of the wizard, you make the fundamental safety settings for the drive as soon as it is created in the Startdrive project. The wizard uses important settings from the user management system (e.g. roles and rights) for this purpose.
- Certificates for secure communication (Page 132)
  The communication between an operating unit and a drive must be secure. By accepting certificates in secure connections, you categorize drives as "Trusted Devices".

11.1 Default security settings

11.1.1 Default security settings in Startdrive

11.1.1.1 Configure access to Startdrive projects

Overview

The security settings for access to Startdrive projects are configured centrally in the TIA Portal. The settings take effect immediately and apply globally to all Startdrive projects. The project does not have to be saved in order to do this.

Default settings for accessing protected projects

Group	Setting	Description
User authentication	Standard authentication procedure	This function specifies which authentication procedure is used by default. • "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.
Project lock	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. Constraints: • The project lock cannot be activated while the control panel is active. • 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 project user (minutes)	This function sets the time for a session timeout on inactivity of local project users. Constraints: • 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.

Procedure

1. Select the "Options > Settings" menu in Startdrive.
   The "Settings" screen is displayed in the work area.
2. In the secondary navigation, select menu "Security > Access protection".
3. Select the default process for user authentication or the project lock settings.

Result

The settings are stored automatically.

11.1.1.2 Configure the settings to open the Security Wizard

Overview

In the "Default settings" function view, you specify whether the Security Wizard opens automatically when a drive is created.

You use the Security Wizard to configure the security settings for the drive.

Procedure

1. Select the "Options > Settings" menu in Startdrive.
2. In the secondary navigation for settings, select the "Security > Default settings" menu.
3. Activate or deactivate the option "Do not display the wizard for the security settings for the drive after adding a drive".

Result

The settings are stored automatically.

11.1.2 Security settings for the drive

Overview

You configure the security settings for each drive individually 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 and Access Control
- Ports and protocols

11.1.2.1 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 "Settings with the Security Wizard (Page 121)".

11.1.2.2 User Management & Access Control

Overview

The "User Management & Access Control" section contains the following security settings for the drive.

Table 11-1 User Management & Access Control

Security 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

The displayed settings are the current settings of the selected converter in "User Management & Access Control", see section "User management and access control (UMAC) (Page 96)".

The option "Activate UMAC for the drive" is configurable.

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, provided the security 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

You can activate the option "Activate UMAC for the drive".

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 independently of the project protection, because the project protection is only valid for 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

You can also deactivate the option "Activate UMAC for the drive" in the project. However, if these security settings have already been loaded to the drive, the deactivation is rejected. When the drive data is loaded, a corresponding message appears.

11.1.2.3 Ports and protocols

Overview

In the "Ports and protocols" section, you configure the interfaces to access the drive.

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.

Description

The ports and protocols are listed below with their respective factory settings after the Security Wizard has run.

Table 11-2 Ports and protocols

Security setting for interfaces	Parameter	Factory setting	Details
X127: Web server access via HTTP (port 80)	c8995[3]	Deactivated	Unprotected communication. Man-in-the-Middle and Replay attacks can be used to intercept and manipulate data.
X150: Web server access via HTTPS (port 443)	c8997[1]	Deactivated	Protected communication via TLS 1.2 and TLS 1.3.
X127: Web server access via HTTPS (port 443)	c8995[1]	Activated	Protected communication via TLS 1.2 and TLS 1.3.

Table 11-3 Fieldbus and related protocols configuration

Security setting for interfaces	Parameter	Factory setting	Details
X150: Fieldbus protocol	–	PROFINET (cannot be changed)	The PROFINET Context Manager provides an endpoint mapper in order to establish an application relationship (PROFINET AR).
X127 and X150: DCP (always activated)	–	Activated (cannot be changed)	Discovery and Configuration Protocol (DCP) Identifies PROFINET devices and allows basic settings to be made.
X127 and X150: SNMP (port 161)	–	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.

Table 11-4 S7 protocol configuration

Security setting for interfaces	Parameter	Factory setting	Details
X150: Access via the S7 Protocol for PCS7 (port 102)	c8997[2]	Deactivated	Unprotected communication. Man-in-the-Middle and Replay attacks can be used to intercept and manipulate data. The S7 Protocol for PCS7 can be used in secure PCS7 environments.
X127: Access via the S7 Protocol for PCS7 (port 102)	c8995[2]	Deactivated	
X150: Access via the Secure S7 Protocol for Startdrive (port 102)	c8997[0]	Activated	Protected communication via TLS 1.2 and TLS 1.3. The Secure S7 Protocol for Startdrive is used for communication between Startdrive and the converter.
X127: Access via the Secure S7 Protocol for Startdrive (port 102)	c8995[0]	Activated	

Table 11-5 DHCP configuration

Security setting for interfaces	Parameter	Factory setting	Details
X127: DHCP (port 68)	–	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 (port 68)	–	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.

11.1.2.4 Activating/deactivating ports and protocols

Overview

Apply the principle of least functionality by deactivating the protocols that are not needed for access to the converter.

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.

Deactivated protocols cannot be used.

11.2 User management and access control (UMAC)

11.2.1 Fundamentals

Overview

The 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 group together various access rights to the project. In this way, different users can be given different access rights to functions. If UMAC has been activated, the project can only be opened and edited by authorized users.

Note

An activated project protection cannot be canceled.

More information

Detailed information on project protection can be found under the heading "Manage users and roles" in the information system of the TIA Portal.

11.2.2 Project protection

11.2.2.1 Overview

Overview

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

Description

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

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.

Project protection cannot be deactivated

Activated project protection cannot be deactivated.

Transferring protection settings to the drive

The "Download to device" function is used to transfer the protection 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 120)".

11.2.2.2 Activating project protection

Requirement

A project has been created.

Procedure

1. Open the "Security settings" folder in the project tree.
2. Double-click on the "Settings" navigation item.
   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 defined for the password when the user administration is activated for the first time:

   - 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

   As project administrator, you can adapt these the password policy to address your requirements.

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.

11.2.2.3 "Anonymous" user

Overview

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 must be activated either in user management or via the Security Wizard. If used carelessly, this user account is a security risk.

Restrict authorizations

Certain functions such as 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 if the "Anonymous" user has the relevant rights.

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.

You are recommended to verify the assigned runtime roles and rights for the "Anonymous" user. Identify the potential risks arising from the assigned authorizations and take appropriate security precautions.

Display authorizations

Assigned authorizations are displayed in the Inspector window, under "Protection & Security > User Management & Access Control", if a user with the "Manage users and roles" right has logged in.

11.2.2.4 Setting password policies

Overview

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.
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.

Requirements

- 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

To set the password policies, follow these steps:

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" command.
   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 policies apply to the entire project and also in the drive if protection is activated.

Note

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

11.2.3 User management

11.2.3.1 Overview

Description

The following functions are available for user account management:

- Create new local user (user account)
- Change local user data:
  - User names
  - Password
  - Authentication procedure
  - Runtime timeout
  - Comment
- Activate or deactivate user
  Only activated user accounts can log into a protected project.
  The following user accounts are imported when the UMAC settings are downloaded to the drive:
  - All activated user accounts
  - The "Anonymous" user account
    The "Anonymous" user account is imported to the drive regardless of whether it is activated or deactivated.
- Delete local user
- Global users or user groups can also be used for the project.

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

Feature	Description
Role	Cannot be deleted
Role name	Cannot be set
Assignment of rights through roles	Predefined assignment; cannot be changed
Availability	Always available; can be assigned to user accounts

- User-defined roles

Feature	Description
Role	Can be deleted
Role name	Can be set
Runtime timeout	Can be set[1)]
Assignment of rights through roles	Assignment possible
Availability	Can be assigned to user accounts

[1)] Not yet supported in firmware version V6.1.

You can define a comment and display the assigned rights for each role.

11.2.3.2 System limits

Description

The configuration of users with runtime function rights is checked when the offline settings are downloaded to the converter. The configuration must follow these rules:

Setting	Quantity
Maximum number of users	64
Maximum number of user-defined roles with runtime function rights	In addition to the system-defined roles with runtime function rights, a maximum of 20 user-defined roles with runtime function rights can be created and configured.
Maximum number of roles per user	One user can be assigned a maximum of 10 roles. **Note** System-defined and user-defined roles can be used in any combination. The maximum number of roles per user must not be exceeded.

If the configuration of one or more users does not follow the rules, a corresponding message appears.

The following rules apply to the configuration of users with engineering function rights only, and also to users with runtime function rights.

Setting	Quantity
Names for user roles: maximum number of characters	32
Names for user accounts: maximum number of characters	100
Password length: maximum number of characters	120

Dependencies between Startdrive and web server

When the offline settings including the UMAC settings are downloaded to the converter, Startdrive accesses the same user database as the web server. The configuration of users in Startdrive must therefore follow the described rules and be coordinated with them.

This applies particularly to the maximum number of users that can be created and configured.

Example: If you configure 64 users in Startdrive with authorizations for the relevant drive, you will not be able to create any more users in the web server after the offline settings have been downloaded to the converter.

11.2.3.3 Creating user accounts

Requirements

- 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.

Note

You can also create a new local user by copying an existing user. The assigned roles are then also assigned to the copied user. However, you must assign a new password to the copied user.

11.2.3.4 "Anonymous" user

Overview

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

Description

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

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.

11.2.3.5 Activate/deactivate user accounts

Requirements

- 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.

11.2.3.6 Changing user accounts

Requirements

- 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.

11.2.3.7 Delete user accounts

Requirements

- 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. Make sure that the selected authentication procedure is "Password". Change this setting if necessary.
4. Select "Delete" from the shortcut menu or press the <Del> key.

11.2.3.8 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 108)".

11.2.3.9 Displaying rights of project users

Requirements

- 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.

11.2.3.10 Change password

Overview

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

Description

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 104)".

11.2.3.11 Changing the password when a protected project is opened

Requirements

- 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 "Change password".
   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 then changed in the drive.

11.2.3.12 Changing a password when working in a protected project

Requirements

- 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 then changed in the drive.

11.2.4 Access control

11.2.4.1 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.

Each user can be assigned multiple system-defined roles. User-specific roles can also be created and assigned. This is done by a user with the "Manage users and roles" right.

There are 2 different groups of rights:

- Engineering rights (Page 54)
  These always relate to a protected Startdrive project (UMAC is activated for the project). However, these rights are also checked when a protected drive is accessed.
- Runtime rights (Page 56)
  These always relate to a protected device which is accessed in online mode (UMAC is activated for the drive).
  Runtime rights are available for converters with firmware version V6.1 or higher.
  The Startdrive and web server commissioning tools use the same runtime rights.

11.2.4.2 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.

11.2.4.3 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
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

Activity	Engineering rights[1)]	Runtime rights[2)]
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
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

Activity	Engineering rights[1)]	Runtime rights[2)]
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
Online access with the search for accessible devices (Life List)	–	The necessary rights depend on which actions are performed.

Activity	Engineering rights[1)]	Runtime rights[2)]
"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

11.2.4.4 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.

11.2.4.5 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.

11.2.4.6 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.

11.2.5 User login

11.2.5.1 Overview

Overview

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

- Project protection for the Startdrive project
- User Management and Access Control (UMAC) for access to the converter

Description

User authentication

If a Startdrive project has project protection, user authentication takes place when the project is opened. A successful login to the project automatically enables access to the device data in online mode if the access rights of a user are configured accordingly in the drive.

The login requires a user name to which certain access rights are assigned via system-defined or user-defined roles. A valid password must also be entered. A user with the "Manage users and roles" right configures the login data of 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.

11.2.5.2 User login

Overview

Authentication is necessary when a protected project is opened or after a timeout. A user name to which certain access rights are assigned via predefined roles is required for logging in.

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 115)".

11.2.5.3 Error messages and remedies

Error messages and remedies

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 your password data (user name, password). Enter the data correctly when you log in.
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.

11.2.5.4 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 still 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.

The procedure described here can interact with other functions, settings or configurations.

11.2.5.5 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.

The procedure described here can interact with other functions, settings or configurations.

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.

11.2.6 Project lock

11.2.6.1 Overview

Description

With a project lock you prevent unauthorized persons from accessing the project in your absence. This allows you to leave the project open while you are briefly away from your work station. You have two options for 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 in the TIA Portal. 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.

Project lock with ongoing processes

If you have initiated a process in the TIA Portal that takes longer than this, the process is first completed and then the project is locked. If a dialog requiring user action is open, the project is only locked after the dialog is closed.

Project lock with active control panel

As long as the control panel is active and you have master control over a drive, you cannot activate the project lock and the automatic project lock is also suspended in case of inactivity.

"Anonymous" user

Feature	Description
Lock project manually	Not possible
Lock project automatically on inactivity	Not possible

Security measures

The project lock is a way of increasing security in the immediate surroundings where you work. Therefore please follow these recommendations:

- As a user, always lock the project when you leave your work station.
- 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.

11.2.6.2 Lock project manually

Requirements

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

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.

11.2.6.3 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.

11.2.6.4 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.

11.2.6.5 Remove project lock for single sign-on users

Requirement

The project lock is active.

Procedure

1. In the "Project locked" dialog, click "Unlock".
   If there is still an active single sign-on session for the user who caused the project to be locked, the project is unlocked. However, if there is no single sign-on session or if the single sign-on session is for another user, the login window for the single sign-on session is displayed. In this case, perform step 2.
   Alternatively, you can also close the project if you do not want to log in again. Changes that have not been saved are discarded.
2. Log in with the user data of the user who locked the project. A different user cannot remove the project lock.

11.2.7 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 that is assigned the "Drive Administrator" role (see section "Roles for converters with runtime function rights (Page 56)").
  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.

11.3 Settings with the Security Wizard

11.3.1 Overview

Description

As soon as a drive is created, a Security Wizard helps you configure the security settings for the drive. Depending on the default settings in the TIA Portal, 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.

The Security Wizard uses the user accounts managed in user management (UMAC).

Deactivate the automatic start of the Security Wizard

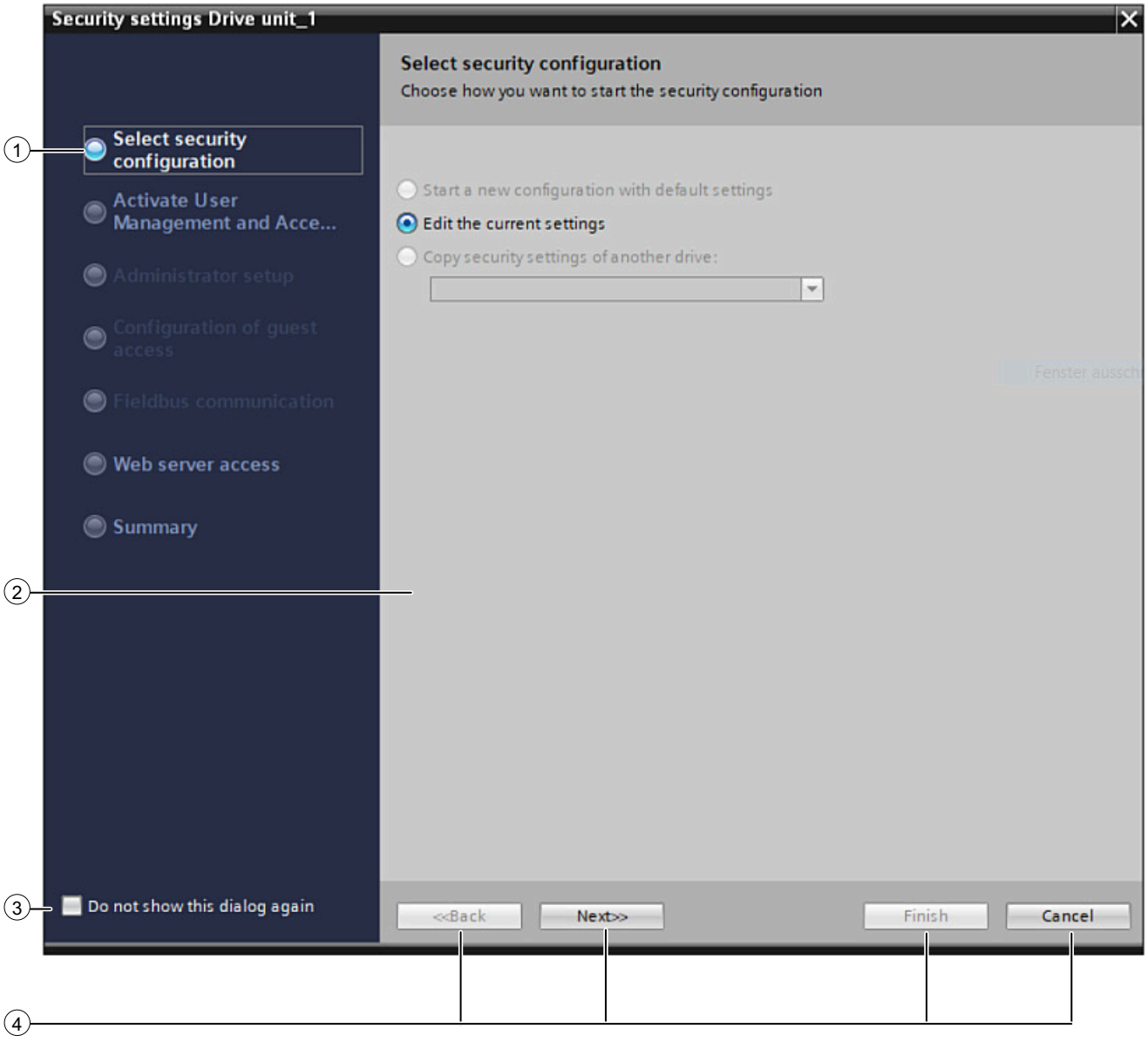
The automatic start of the wizard is deactivated in the following places in Startdrive:

- In the Security Wizard if the option "Do not show this dialog again" ③ option is activated.
- In the default security settings. You can find more information in section "Configure the settings to open the Security Wizard (Page 90)".

If the automatic start is deactivated, the default settings are automatically used in the wizard when another drive is created. Exception: activation of project protection.

Structure of the Security Wizard

In the Security Wizard, you configure the most important security settings for a drive.



① Navigation of the individual configuration screens in the Security Wizard
② Displayed configuration screen in the Security Wizard
③ Deactivate automatic opening of the Security Wizard
④ Toolbar for scrolling through the Security Wizard or for finishing or canceling the security settings

Figure 11-1 Example: Security Wizard

Setting ranges

The following basic settings are possible in the wizard:

- Making the basic selection
- Configuring access control
- Configuring the administrator
- Configuring guest access for users who are not logged in (anonymous)
- Configuring extended access rights for fieldbus communication
- Configuring extended access rights for access via a SINAMICS SDI standard panel (not with SINAMICS S210)
- Configuring the web server access

Each of these settings is explained in detail in the Security Wizard. At the end, all settings are once again summarized in an overview.

Start/end Security Wizard

You can manually start the Security Wizard again at any time using the "Start Security Wizard" button in the "Protection & Security" area of the device configuration.

Variant	Explanation
Close or cancel the Security Wizard	If you cancel the Security Wizard with "Close" or "X", the Security Wizard is closed. However, the wizard can be reopened later for the current drive. Result: When a new drive is created or a drive is uploaded with the factory settings, the default settings are taken from the wizard.
Exiting the Security Wizard **reliably**	Use the "Exit" button if you wish to reliably exit the Security Wizard. In this case, the security settings that have been made are applied. However, the settings can also be subsequently changed.

Loading the security settings into the converter

In order that the security settings are valid in the drive, this configuration data with the UMAC settings must be downloaded to the drive.

Note

Transferring UMAC data

Ensure that option "Refresh UMAC" is activated in dialog "Load preview". The activated option is the precondition that the UMAC data is also transferred to the drive.

You must be logged in as a user with the rights "Manage users and roles" and "Download to drives".

Details are contained in section "Downloading the UMAC to the device (Page 120)".

11.3.2 Configuring security settings

11.3.2.1 Security settings for full protection

Overview

SINAMICS drives can be protected using a Security Wizard as soon as they are created in the project. The Security Wizard guides you through the settings when you create them and informs you about the effects of the settings. This allows you to determine at an early stage which protection you want to assign to the newly created drive. You will normally configure the security settings according to the results of your risk analysis.

Requirement

Note

Dynamic default settings

Due to default settings elsewhere, security options may already be active in the Security Wizard settings areas. Not every individual default setting is described in the subsequent description.

Note

Complete settings

The sequence of steps in the security configuration described below includes UMAC activation. If you configure the individual steps other than as described, the wizard does not always present the next possible configuration step. In "Step 10 Overview", however, you can see an overview indicating whether your security settings are valid. If they are not, you will see information explaining which settings are outstanding or need to be configured differently.

Please observe the following requirements:

- Ideally, project protection is enabled for the active project.
  This allows the user accounts created in the user management settings also to be used in the Security Wizard.
- The option "Do not show this dialog again" was not activated when another drive was created in this project.
  OR
  The automatic start of the wizard was not deactivated in the drive defaults.

Step 1: Start Security Wizard

With the appropriate default setting, the Security Wizard opens automatically when a SINAMICS drive is added to the project (via the project tree or the hardware catalog). The start page of the wizard is displayed.

1. To create a new security configuration for the drive, click the "Change security settings" button.
   The "Select security configuration" settings area is displayed (step 2).
   If you want to perform the security configuration at a later time, click the option "Continue with low security settings" instead (see section "Security settings with low protection (Page 129)").

Step 2: Select security configuration

Proceed as follows if you wish to create a completely new configuration:

1. Activate option "Start new configuration with default settings".
2. Click "Next".
   The "Activate user administration and access control" settings area is displayed.

On the other hand, if you wish to apply the security configuration of another drive, then proceed as follows:

1. Activate the "Copy security settings of another drive" option.
   All security settings that should be applied in your drive are displayed below the option.
2. Then select the drive from which you want to copy the security settings.
3. Click "Next".
   The security settings of the selected drive are applied. In the next steps you can adapt the settings that have been applied.
   The "Activate User Management and Access Control" settings area is displayed.

Step 3: Activate User Management and Access Control

For high security, the setting "Activate UMAC for the drive" is a fundamental requirement. If UMAC is not activated for the drive, no more detailed settings (step 4 onward) can be made for it in the wizard. The protection "Activate UMAC for the project" is not mandatory. You are recommended to activate this protection.

1. If project protection is not activated for the project, activate the option "Activate UMAC for the project ...".
   If project protection was already active, this option is automatically active and cannot be changed. This option is automatically active with a new security configuration.

   Note

   Project protection can no longer be deactivated in the program.

2. Next, activate the option "Activate UMAC for the drive ...".
   This option is automatically active with a new security configuration.

3. Read the information in the settings area and confirm the option "I have read the information above and I understand the consequences of enabling UMAC".
4. Click "Next".
   The "Administrator setup" settings area is displayed.

Step 4: Administrator setup

In this step, a user with the "Manage users and roles" right is absolutely essential. Only these users will subsequently be allowed to change the user management of the drive. The next steps depend on whether in step 3 you activated UMAC for the drive only or also for the TIA project.

Scenario 1: UMAC is activated for the drive only:

If UMAC is activated for the drive only, it is only possible to create a user with the "Drive Administrator" role at this stage.

Note

The next time the Security Wizard is called, there will already be a user account. In this case, select the user with the "Drive Administrator" role.

1. In the "Create new user" area, enter the user name and password for the user.
2. To confirm all settings in this settings area, click "Next".
   The "Next" button becomes active only after all settings have been made in this area.
   The Security Wizard then displays the "Guest access configuration" area.

Scenario 2: UMAC is activated for the project and the drive:

If UMAC is activated for the project and the drive, you can also define an administrator user account at this stage.

Requirement	Settings
Project protection is deactivated	There is no project administrator yet. 1. Enter the user name of a new project and drive administrator. 2. Enter the user password twice.
Project protection is activated	When project protection is activated, a project administrator must be created. If there are other users with project administrator rights, you can choose from multiple users. 1. Select the desired user in the drop-down list "Use an existing user". The user will also be given the "Drive Administrator" role for the drive. Alternatively you can create a new user account for a user with the "Drive Administrator" role. 1. Activate the option "Create new user". 2. Assign a user name and a valid password.
Project protection is activated + the project administrator has the "Drive Administrator" right	No further action required. The project administrator is automatically also set up as a user with the "Drive Administrator" role.

1. To confirm all settings in this settings area, click "Next".
   The "Next" button becomes active only after all settings have been made in this area. The Security Wizard then displays the "Guest access configuration" area.

Step 5: Configuration of guest access

In this step, you specify whether users who are not logged in have guest access to the drive.

NOTICE
Data manipulation due to access by anonymous users Guest access by anonymous users represents a potential security risk. Guest access allows a potential attacker to 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.

If you activate guest access for users who are not logged in ("Anonymous"), such users have guest access to:

- The web server (on a selected drive)
- The "Startdrive" application in the TIA Portal
- All other permitted protocols

Note

If guest access is activated, the user ("Anonymous") is activated not only for the selected drive but for all drives in the project!

- The user ("Anonymous") is given the "Drive Guest" role for all drives in the project.

1. If you want to activate guest access for Anonymous, activate the option "Enable guest access to the drive".
   Guest access is associated with the runtime right "Read drive data or acknowledge messages".

   Note

   Guest access cannot be activated

   Guest access for the user account Anonymous cannot be activated in the following situation:

   The user account Anonymous has been assigned a role (except Drive Guest) which also contains the "Read drive data or acknowledge messages" right (e.g. Drive Operator)

2. To confirm all settings in this settings area, click "Next".
   The Security Wizard then displays the "Fieldbus communication" area.

Step 6: Fieldbus communication

In this step you specify whether users are allowed to change drive data without authentication using fieldbus protocols. This setting is activated in the Security Wizard by default.

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

Proceed as follows to permit access using the fieldbus protocols without authentication:

1. Activate the "Allow data to be changed with fieldbus communication" option.
2. Click "Next".
   The "Access to SINAMICS SDI standard panel" area is displayed.

Step 7: Access to SINAMICS SDI standard panel

In this step you specify whether users are allowed to change drive data without authentication using a panel. This setting is activated in the Security Wizard by default.

Note

SINAMICS S210 does not use a SINAMICS SDI standard panel. The "Access to SINAMICS SDI standard panel" area cannot be configured for S210 drives.

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

Proceed as follows to permit access using the panel without authentication:

1. Activate the "Allow drive data changes via the SDI standard panel" option.
2. Click "Next".
   The Security Wizard then displays the "Web server activation" area.

Step 8: Web server activation

For an unprotected drive, access via the PROFINET interface [X150] using an HTTPS protocol is active in the factory settings. This access option is automatically deactivated with the Security Wizard. If you still want to access the drive using the PROFINET interface [X150] and the web server anyway, you need to activate the access again manually.

NOTICE

Data manipulation due to an unprotected fieldbus cable

In accordance with the Defence in Depth concept, the PROFINET interface must be isolated from the remaining plant network (see Industrial Security (https://new.siemens.com/global/en/products/services/digital-enterprise-services/industrial-security-services.html)) in order to prevent unauthorized access and, in turn, data manipulation.

- Protect against access to cables and possibly open connections, for example, by installing in a control cabinet.

1. Activate the option "Activate SINAMICS web server access via PROFINET interface [X150] with HTTPS protocol".
2. To confirm these settings, click "Next".

Step 9: Summary (completing the security settings)

In the "Summary" area, the settings are summarized. You will also be informed whether read and write access to all drives is possible via a fieldbus protocol or the SINAMICS SDI standard panel.

Note

Security settings valid?

The wizard is checking your security settings. If your settings are incorrect or incomplete, the area will contain the relevant information. Unless you correct these settings you will be unable to finalize configuration in the Security Wizard. In this case the "Finish" button is disabled.

Click the "Finish" button to apply the valid security settings.

The security settings for the relevant drive will be applied in the project.

Result

The drive is created in the project with the selected security settings. You can change these security settings at a later point in time via the "Protection & Security" menu in the Inspector window, for example, in order to correct a security setting.

In order that the security settings are valid in the drive, the project data must be subsequently downloaded to the drive.

Details are provided in section "Downloading the UMAC to the device (Page 120)".

11.3.2.2 Security settings with low protection

Overview

SINAMICS drives can be protected using a Security Wizard as soon as they are created in the project.

If necessary, you can postpone the configuration of the security settings to a later time. However, the protection of the drive is then very low.

NOTICE
Data manipulation due to low protection Inadequately protected drive data makes it easier for potential attackers to have unauthorized access to the drive. Data manipulation can cause the drive to malfunction or damage it. • Only use low protection in absolutely exceptional cases and only when acceptable on the basis of a risk analysis, see section "Security management (Page 27)". • Make the settings that provide full protection at the earliest time possible (see section "Security settings for full protection (Page 124)").

Requirements

- Ideally, project protection is enabled for the active project.
- The option "Do not show this dialog again" was not activated when another drive was created in this project.

Step 1: Starting the Security Wizard

The Security Wizard usually opens automatically when a SINAMICS drive is created in the project (via the project tree or the hardware catalog). The start page of the wizard is displayed.

1. If you want to perform the security configuration at a later time, click the option "Continuing with low security settings".
   A security note indicates that you have selected a low degree of protection. This security setting is not recommended.
2. Click "OK" to confirm the alarm.
   The "Summary" area is displayed.

Step 2: Summary (completing the security settings)

In the "Summary" area, the resulting settings are summarized once again.

1. If you want to change the settings you can jump to the relevant settings area of the wizard and make changes there.
2. Click on "Finish" if you want to finalize and apply the settings.
   The security settings are applied to the newly created drive.

Result

The drive is created in the project with the selected security settings. You can change these security settings at a later point in time via the "Protection & Security" menu in the Inspector window, for example, in order to correct a security setting.

In order that the security settings are valid in the drive, you must then download them to the drive.

11.3.3 Changing or subsequently adjusting security settings

Overview

You can correct the existing security settings of a SINAMICS drive at any time via the drive properties in the Inspector window. There, you can also restart the Security Wizard (Security Wizard).

NOTICE
Data manipulation due to low protection Inadequately protected drive data makes it easier for potential attackers to have unauthorized access to the drive. Data manipulation can cause the drive and its environment to malfunction or damage them. • Apply the Defence in Depth concept (see Industrial Security (https://new.siemens.com/global/en/products/services/digital-enterprise-services/industrial-security-services.html)) and isolate all unnecessary interfaces from the remaining plant network in order to prevent unauthorized access and in turn data manipulation. • Make the settings that provide increased protection at the earliest time possible (see section "Security settings for full protection (Page 124)").

Requirements

- Ideally, project protection is activated.
  If project protection is activated, you need one user with the "Manage users and roles" right in order to start the Security Wizard.
- Ideally, the drive has already been configured with the Security Wizard.

Procedure

Note

The description below refers to UMAC changes using the Security Wizard. You can also make other changes in the Inspector window with the "Protection & Security" menu.

The security settings have been configured in Startdrive. You want to change the existing default security settings for the drive. Proceed as follows:

1. Select the required drive in the project tree.
2. In the inspector window, select the "Protection & Security > Security Wizard" menu.
3. Click the "Start Security Wizard" button on the right.
   The "Security settings..." dialog opens and the "Select security configuration" settings area is displayed.

4. Activate option "Edit current settings".
   If the security settings were previously configured with the wizard, you can correct the settings in each settings area (see section "Configuring security settings (Page 124)").
   If you want to change the security settings of another drive (if any) in the project, proceed as follows:
   – Activate the "Copy security settings of another drive" option.
   – Then select the drive from which you want to copy the security settings.
5. Correct the necessary security settings and click "Next" in each setting area.
6. Click "Finish" to finish and apply the settings.

Result

The security settings are accepted into the project.

11.4 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

11.5 Certificates for secure communication

11.5.1 Fundamentals

Overview

Connections between operating units and drives must be secure. Drives are classified as "Trusted Devices" and therefore as "secure" through the exchange of digital certificates. 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).

11.5.2 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 with a manual reset to factory settings with memory card.

Certificate attributes

Certificates contain information about the issuer.

Attribute	Meaning	Example
O	Organization	SIEMENS
C	Country/region	EN
CN	Common name	SINAMICS Embedded Root CA 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 142):
  With the help of the wizard, you make the fundamental safety settings for the converter the first time the web server is called. 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 153)
  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 162)".
  - "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 secure communication (Page 165)".

12.1 Fundamentals

12.1.1 Factory settings

Overview

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

Description

When the web server is called for the first time, the Security Wizard opens automatically. You can select one of the following options:

- "Configure security settings":
  The option "Activate UMAC for the drive" is selected by default. UMAC is activated after you confirm that you have read information about UMAC and understand the consequences of enabling it. This applies regardless of whether or not you complete the remaining steps in the Security Wizard.
- "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 "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 settings.

More information

More information about the Security Wizard can be found in section "Settings in the Security Wizard (Page 142)".

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 the following sections:
  - "Communications interfaces (Page 45)"
  - "Ports and protocols (Page 162)"

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" settings area.
3. Click on "Start Security Wizard".
4. Make the security settings in the wizard.

12.1.3 User login (read access activated)

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 has the "Read drive data or acknowledge events" right.

Procedure

1. Click the "Log in" 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.

See also

Configure the read access (Page 146)

12.1.4 User login (read 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 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 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.

See also

Configure the read access (Page 146)

12.1.5 Changing a user

Overview

A user cannot be changed 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 "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 on inactivity (read 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. You are given advance warning before being logged out.

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.

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 "Log in" 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 "Characteristics of access control in the web server (Page 59)".

See also

Configure the read access (Page 146)

12.1.8 User login after session timeout on inactivity (read 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. You are given advance warning before being logged out.

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.

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 "Characteristics of access control in the web server (Page 59)".

See also

Configure the read access (Page 146)

12.2 Settings in the Security Wizard

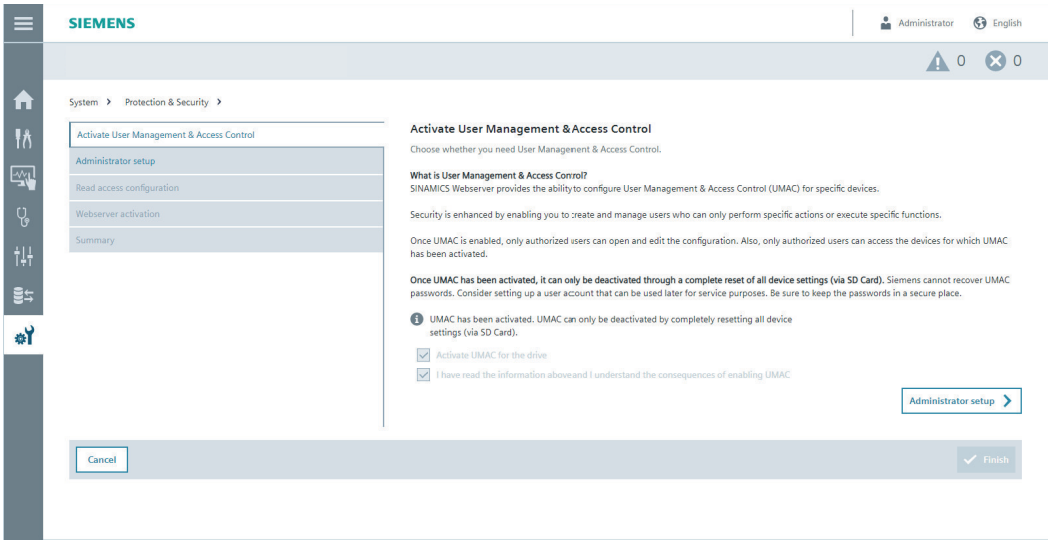
12.2.1 Structure of the Security Wizard

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 and take them into account while configuring the security settings.



Navigation within the wizard

You can navigate your way around settings that are already configured.

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 in the Security Wizard

12.2.3.1 Make 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 a manual reset to factory settings with memory card:

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

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.

More information

You can find more information about the manual reset to factory settings with memory card in section "Reset UMAC settings (Page 161)".

12.2.3.2 Start 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 150)".

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 with a manual reset to factory settings with memory card.
   You can find more information about the manual reset to factory settings with memory card in section "Reset UMAC settings (Page 161)".
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. To continue, click on "Read access configuration".

Result

The "Read access configuration" page appears.

12.2.3.5 Configure the read access

Overview

On the "Read access configuration" page, the option "Allow read access and acknowledgment of events even without logging in" is deactivated by default.

NOTICE
Data manipulation because users are not logged in Read access by users who are not logged in is 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 read access to the converter data and functions.

Settings in the "Anonymous" user account

Read access configuration in the Security Wizard for users who are not logged in has consequences for 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

Activate read access

To allow read access for users who are not logged in, proceed as follows:

1. Activate the option "Allow read access and acknowledgment of events even without logging in".
   If this option is activated, read access and acknowledgement of events are possible over all interfaces for users who are not logged in.
2. To continue, click on "Web server activation".

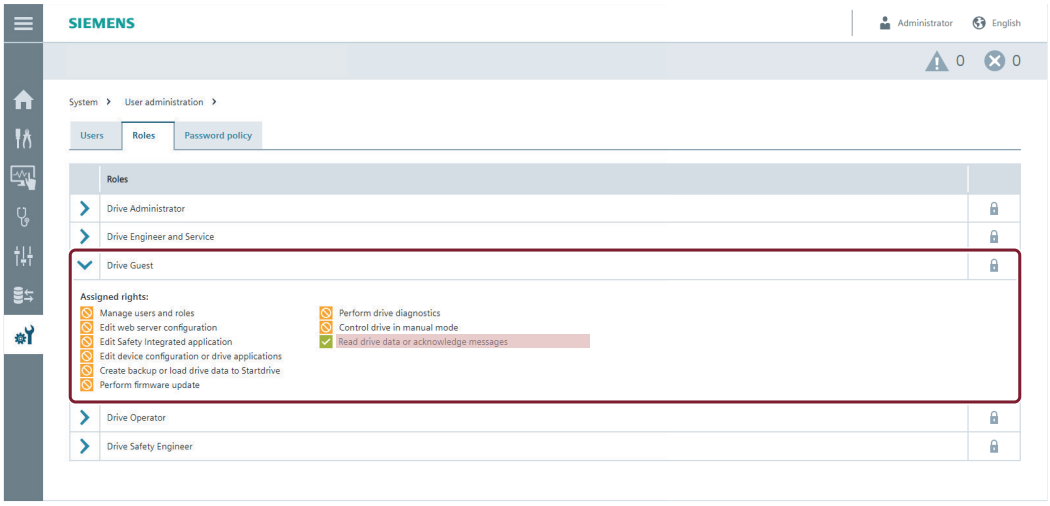
Result

The "Web server activation" page is displayed.

More information

Dependencies between activation/deactivation in the Security Wizard of read access for users who are not logged in and the settings in the "Anonymous" user account.

- When read access for users who are not logged in is activated in the Security Wizard, the "Anonymous" user is automatically assigned the "Drive Guest" role.
  The "Anonymous" user is allowed to read data and acknowledge errors via all interfaces.



- When read access for users who are not logged in is deactivated in the Security Wizard, the "Drive Guest" role is automatically removed from the "Anonymous" user.
  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 have consequences for read access. In the "Protection & Security" function view you can check the current settings for read access (Page 148) for users who are not logged in. You can find more information about the standard configuration of the user in section "User management and access control (UMAC) (Page 153)".

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 in section "Establish a protected HTTPS connection to the web server (Page 166)".

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 enables 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 any open connections must be implemented in a protected fashion, for example in a control cabinet.

2. To continue, click on "Summary".

Result

The "Summary" page is displayed.

12.2.3.7 Summary

Overview

The completed security settings are summarized on the "Summary" page.

Requirement

- The Security Wizard is started.
- UMAC is activated.
- An administrator/user is configured with the "Manage users and roles" right

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 commissioning
   - Advanced setup (not for SINAMICS S210)
   - 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.

More information

- Changing security settings:
  Users with the "Edit device configuration or drive applications" right can log in at a later time, start the Security Wizard in the "Protection & Security" function view and change the security settings.
  For this reason you should limit the number of users with the "Manage users and roles" right to the necessary minimum.
- Read access:
  In the "Protection & Security" function view you can check the current settings for read access for users who are not logged in.

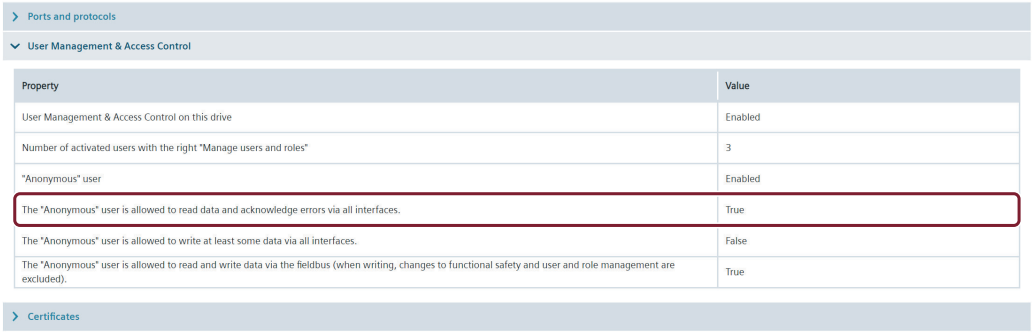


Figure 12-1 Example: Read access for users are not logged in

12.2.3.8 Changing security settings

Overview

Users with the "Edit device configuration or drive applications" right can change settings that have already been made in the Security Wizard.

Requirement

- Settings have already been made in the Security Wizard.
- 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. 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.

More information

- Reloading pages while the Security Wizard is running:
  If you start the Security Wizard to 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 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 (Page 143) in the Security Wizard.

If UMAC is activated, this option will only become available again after a manual reset to factory settings with memory card. You can find more information about the manual reset to factory settings with memory card in section "Reset UMAC settings (Page 161)".

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 "Make basic settings when the web server is called for the first time (Page 143)".

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 "Protection & Security" function view is displayed with the current security settings.
   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 166)".
- 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 162)".

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 144)
   - Setting up a user with the "Drive Administrator" role (Page 145)
   - Configure the read access (Page 146)
   - Web server activation (Page 147)
   - Summary (Page 148)
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 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.

12.3 User management and access control (UMAC)

12.3.1 Overview

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

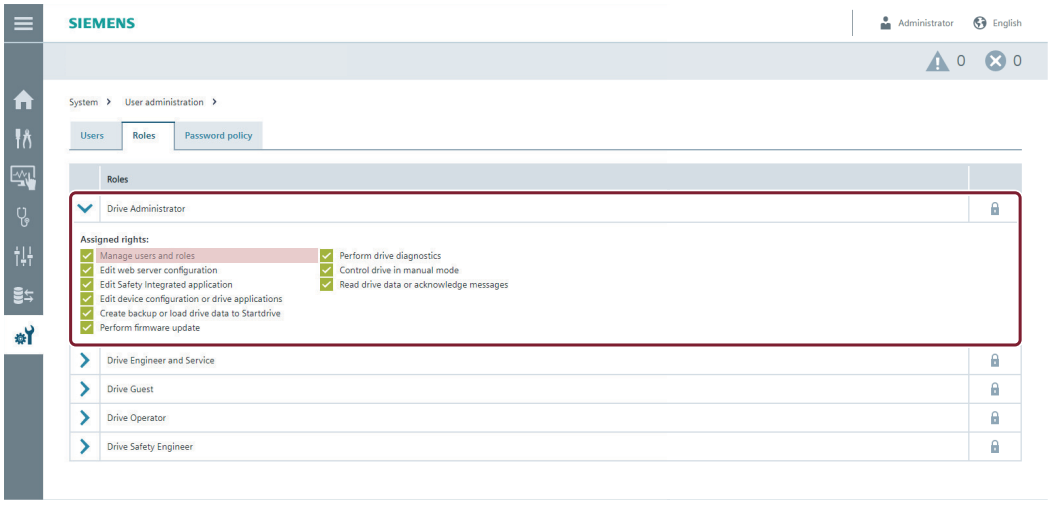
POWER ON with inserted memory card

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 72)".

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 "Users with the "Drive Administrator" role (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 (not for SINAMICS S210)

If the option "Allow read access and acknowledgment of events even without logging in" is activated in the Security Wizard, the "Anonymous" user is automatically assigned the role "Drive Guest".

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[1)] 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.

[1)] Not for SINAMICS S210.

More information about the roles and rights can be found in section "Roles for converters with runtime function rights (Page 56)".

Extend or restrict authorizations

Certain functions such as 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.

12.3.2 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

12.3.3 User management

12.3.3.1 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 converters with runtime function rights (Page 56)".

12.3.3.2 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.

12.3.3.3 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.

12.3.3.4 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.

12.3.3.5 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.

12.3.3.6 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.

12.3.4 Access control

12.3.4.1 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 converters with runtime function rights (Page 56)".

12.3.5 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.

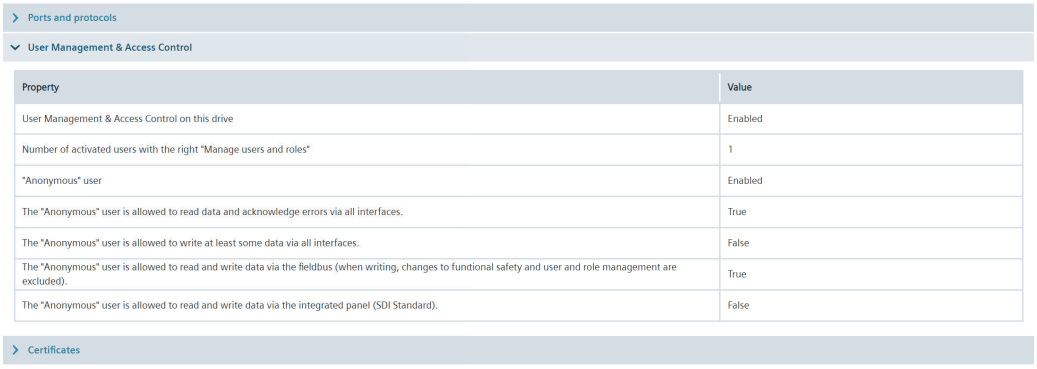


Figure 12-2 Overview of UMAC settings

UMAC settings that have already been made in the Security Wizard can be changed in the wizard. More information about this can be found in section "Changing security settings (Page 150)".

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.

12.3.6 Reset UMAC settings

More information

You can find more information in section "Manual reset to factory settings with memory card" in the product documentation.

12.4 Ports and protocols

Overview

In the "Ports and protocols" function view, you configure the interfaces to access the converter.

Factory settings

The ports and protocols are listed below with their respective factory settings.

- Ports and protocols

Security setting for interfaces	Parameter	Factory setting	Description
X127: Web server access via HTTP (port 80)	c8995[3]	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: Web server access via HTTPS (port 443)	c8995[1]	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: Web server access via HTTPS (port 443)	c8997[1]	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.

- Fieldbus and related protocols configuration

Security setting for interfaces	Parameter	Factory setting	Description
X150: Fieldbus protocol	–	PROFINET (cannot be changed)	The PROFINET Context Manager provides an endpoint mapper in order to establish an application relationship (PROFINET AR).
X127 and X150: DCP (always activated)	–	Activated (cannot be changed)	Discovery and Configuration Protocol (DCP) Identifies PROFINET devices and allows basic settings to be made.
X127 and X150: SNMP (port 161)	–	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.

- S7 protocol configuration

Security setting for interfaces	Parameter	Factory setting	Description
X127: Access via the S7 Protocol for PCS7 (port 102)	c8995[2]	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: Access via the S7 Protocol for PCS7 (port 102)	c8997[2]	Deactivated	
X127: Access via the Secure S7 Protocol for Startdrive (port 102)	c8995[0]	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: Access via the Secure S7 Protocol for Startdrive (port 102)	c8997[0]	Activated	

- DHCP configuration

Security setting for interfaces	Parameter	Factory setting	Description
X127: DHCP (port 68)	–	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 (port 68)	–	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.

12.4.1 Activating/deactivating ports and protocols

Overview

Apply the principle of least functionality by deactivating the protocols that are not needed for access to the converter.

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 in a non-volatile fashion.
   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 secure communication

12.7.1 Fundamentals

Overview

An HTTPS connection between the operating unit and the converter must be secure. The exchange of digital certificates places the converter in the "Trusted Devices" category.

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. The HTTPS certificate is classed as not trusted when the web server is called for the first time The browser establishes a non-secure HTTPS connection to the web server. The browser flags the non-secure connection with a security warning. The next time the web server is called, the HTTPS certificate is classed as trusted if it is signed by the root certificate. • 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. If the root certificate has been imported into the certificate store of the operating unit, the new HTTPS certificate is signed by the root certificate. The browser classes the HTTPS certificate as valid and establishes a secure HTTPS connection to the web server.
Root certificate	• Has a validity period of 2200 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. If the root certificate has been imported into the certificate store of the operating unit, the HTTPS certificate is signed when the web server is called. The browser classes the HTTPS certificate as valid and establishes a secure HTTPS connection to the web server.

Certificate attributes

Certificates contain information about the issuer.

Attribute	Meaning	Example
O	Organization	SIEMENS
C	Country/region	EN
CN	Common name	SINAMICS Embedded Root CA 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

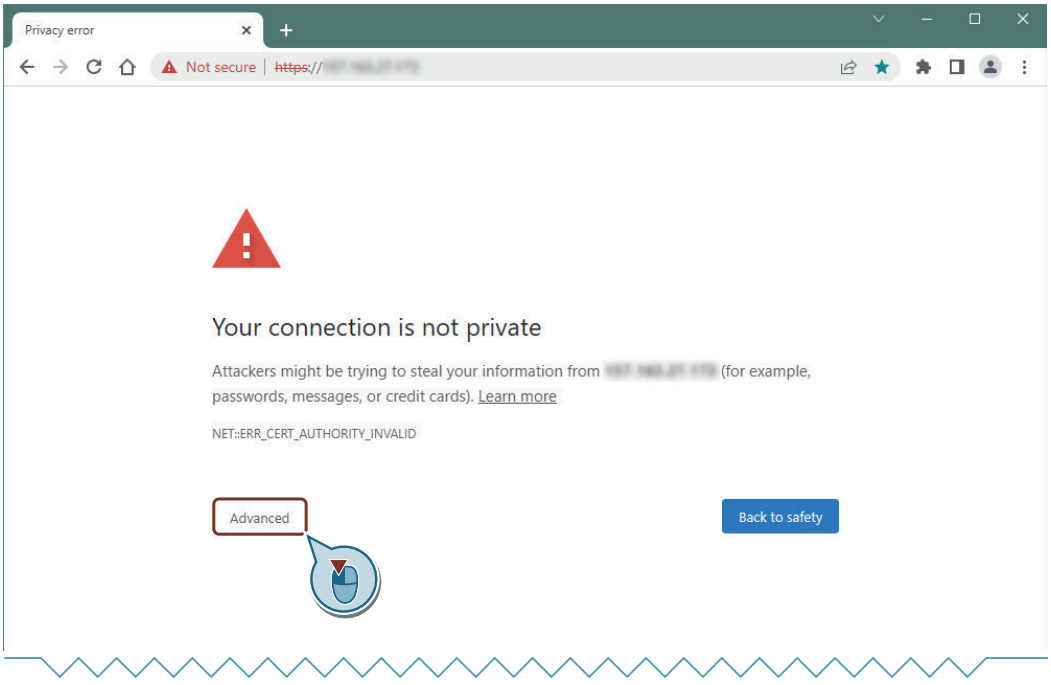
Requirements

- 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.

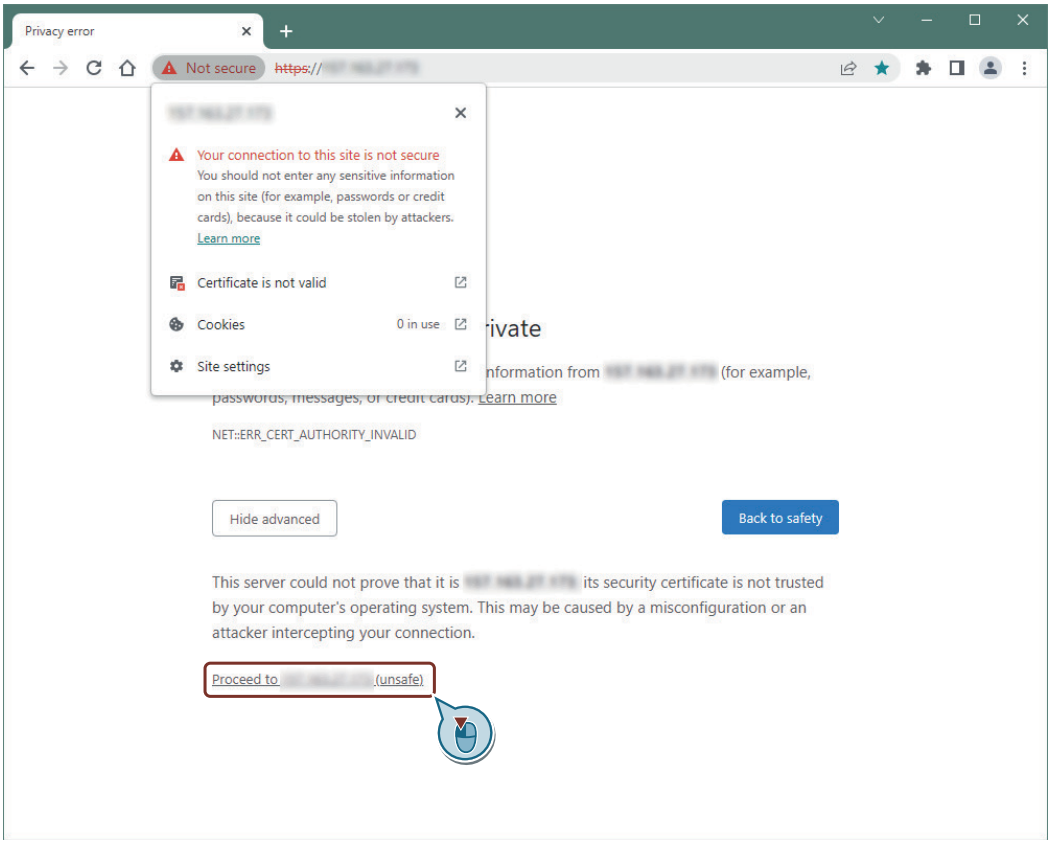
Procedure

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.

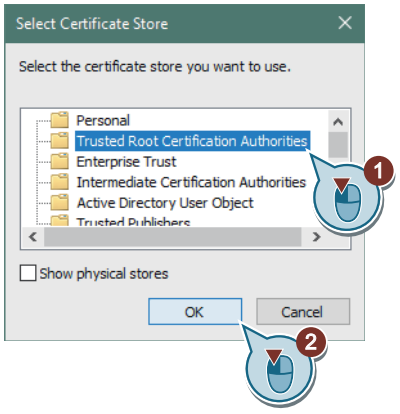


4. Click the "Continue to ... (non-secure)" button.
   The web server is called. The function view is displayed with the basic settings for the web server.



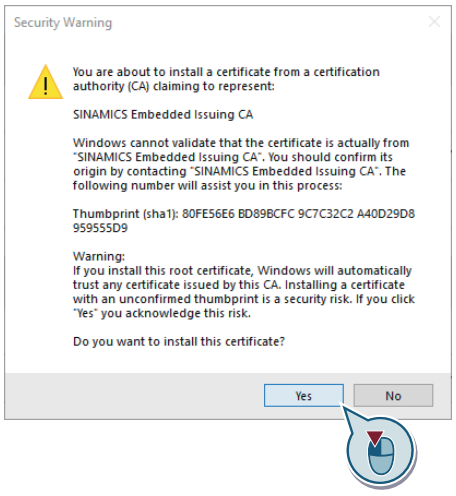
5. Make the basic settings for the web server.
   - Preferred language of the user interface
   - Converter date and time; either manually or via NTP
6. Click "Next".
   The "Welcome to the Security Wizard" page is displayed. One of the following options can be selected:
   - "Configure security settings":
     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 settings.
7. If you selected the option "Configure security settings", proceed as described in section "Configuring settings in the Security Wizard (Page 143)". 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

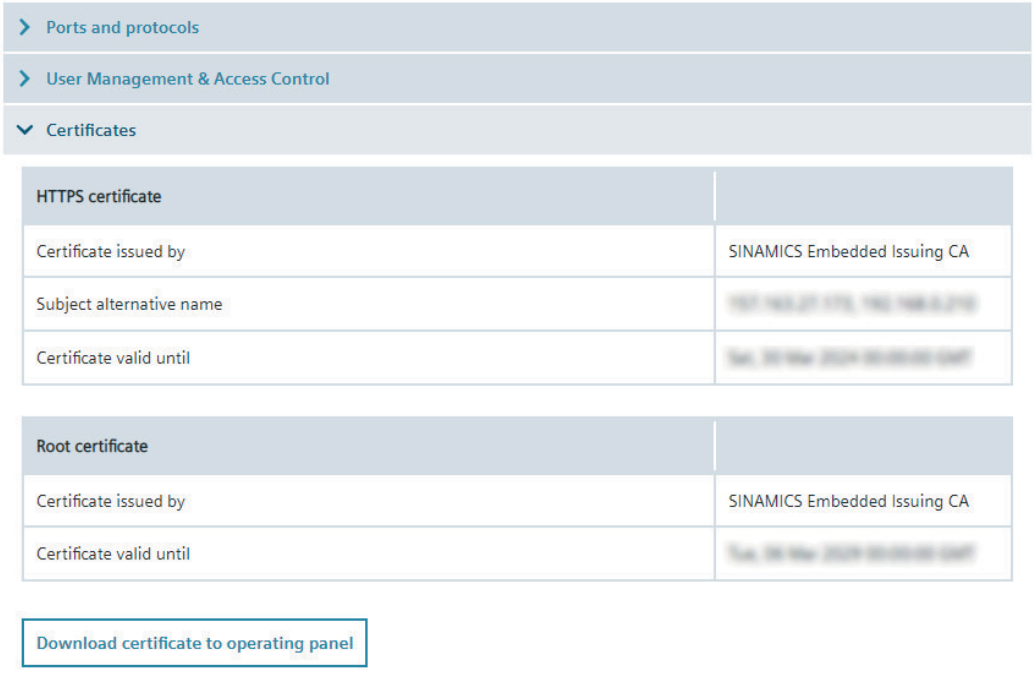
In the "Protection & Security" function view, the web server shows basic information about the certificates used. The information shown is generated automatically and cannot be edited.

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

Topics relating to Industrial Security

You can find more information about Industrial Security on the Internet:

- Industrial Security 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 security

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